***Parametry minimalne sprzętu i oprogramowania***

Spis treści

[Zestawienie ilościowe 3](#_Toc191970316)

[1 Stacja robocza 4](#_Toc191970317)

[2 Monitor 27” 11](#_Toc191970318)

[3 Laptop 12](#_Toc191970319)

[4 Stacja robocza All-in-one 18](#_Toc191970320)

[5 Klaster serwerów 25](#_Toc191970321)

[5.1 Serwery 25](#_Toc191970322)

[5.2 Macierz 29](#_Toc191970323)

[6 System do archiwizacji danych z deduplikacją 32](#_Toc191970324)

[7 Biblioteka taśmowa 43](#_Toc191970325)

[8 UPS Rack 45](#_Toc191970326)

[9 UTM klasy korporacyjnej 46](#_Toc191970327)

[10 Punkt dostępowy 52](#_Toc191970328)

# Zestawienie ilościowe

|  |  |  |
| --- | --- | --- |
| Wymagania | Nazwa | ilość |
| Rozdział 1 | Stacja robocza typ A | 4 |
| Rozdział 1 | Stacja robocza typ B | 4 |
| Rozdział 2 | Monitor 27” | 12 |
| Rozdział 5 | Laptop | 18 |
| Rozdział 6 | Stacja robocza All-in-one | 22 |
| Rozdział 7 | Klaster serwerów (komplet) | 1 |
| Rozdział 8 | System do archiwizacji danych z deduplikacją | 1 |
| Rozdział 9 | Biblioteka taśmowa | 1 |
| Rozdział 10 | UPS rack | 1 |
| Rozdział 11 | UTM klasy korporacyjnej | 1 |
| Rozdział 12 | Punkt dostępowy (komplet) | 4 |

# Stacja robocza typ A/B

|  |  |
| --- | --- |
| Cecha | Wymagania minimalne |
| Typ | Komputer stacjonarny. W ofercie wymagane jest podanie modelu, symbolu oraz producenta. |
| Zastosowanie | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, graficznych, edukacyjnych, obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna i graficzna. |
| Procesor | Procesor dedykowany do pracy w komputerach stacjonarnych, osiągający w teście Passmark CPU Mark, w kategorii Average CPU Mark wynik minimum 43 000 pkt. według wyników opublikowanych na stronie <http://www.cpubenchmark.net/cpu_list.php> |
| Pamięć RAM | 64GB DDR5 w układzie 2x32GB , pamięć działająca w trybie Dual Channel.  Możliwość rozbudowy do min 128GB.  Min. 4 sloty pamięci na płycie głównej, w tym min. dwa słoty wolne. |
| Pamięć masowa | Min. 1TB M.2 SSD PCIe NVMe  Dodatkowy dysk SATA min. 1TB 7200 obr./min  Kontroler RAID 0/1 dla dysków M.2  Kontroler RAID 0/1/5/10 dla dysków SATA III  Obudowa musi umożliwiać montaż dodatkowo min. dwóch dysków M.2 |
| Karta graficzna | 1. Zintegrowana z procesorem,   **Uwaga! 4 stacje robocze typ B należy dodatkowo wyposażyć w dodatkową kartę graficzną o parametrach jak niżej:**   1. **8GB**  pamięci niewspółdzielonej graficzna osiągająca w teście Passmark G3D Mark, w kategorii Average G3D Mark wynik minimum 14 000 pkt. według wyników opublikowanych na stronie <https://www.videocardbenchmark.net/gpu_list.php> oraz posiadająca minimum 4x DisplayPort 2.1 |
| Wyposażenie multimedialne | 1. Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, wewnętrzny głośnik w obudowie komputera. Port słuchawek i mikrofonu na przednim panelu lub port combo. 2. Wbudowany czytnik kart multimedialnych SD 4.0 na przednim panelu obudowy, niezajmujący wnęki żadnej wnęki w obudowie. |
| Klawiatura i mysz | Bezprzewodowa klawiatura i mysz w kolorze czarnym |
| Obudowa | Typu Mini Tower z obsługą kart wyłącznie o pełnej wysokości. Umożliwiająca montaż 2 x dysków 3.5” wewnątrz obudowy. Napęd optyczny zamontowany w dedykowanej wnęce zewnętrznej 5.25” typu slim. Obudowa fabrycznie przystosowana do pracy w orientacji pionowej. Suma wymiarów obudowy nieprzekraczająca 1050mm.  Zasilacz o mocy min. 500W pracujący w sieci 230V 50/60Hz prądu wyposażony w złącze 6-pinowe i jedno złącze 2 + 6-pinowe dla karty graficznej, o efektywności min. 92% przy obciążeniu zasilacza na poziomie 50  Moduł konstrukcji obudowy w jednostce centralnej komputera powinien pozwalać na demontaż kart rozszerzeń, napędu optycznego, dysku 3,5” bez konieczności użycia narzędzi (wyklucza się użycia wkrętów, śrub motylkowych, śrub radełkowych). Obudowa posiadająca czujnik otwarcia współpracujący z oprogramowaniem zarządzająco – diagnostycznym. Obudowa z gniazdem dla linki metalowej, po zamontowaniu brak możliwości otwarcia. Wbudowany wizualny system diagnostyczny oparty o sygnalizację LED np. włącznik POWER, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, sygnalizacja oparta na zmianie statusów diody LED (zmiana barw oraz miganie). Oferowany system diagnostyczny nie może wykorzystywać slotów na płycie głównej, wnęk zewnętrznych obudowy oraz nie może być uzyskany przez konwertowanie, przerabianie innych złączy na płycie głównej nie wymienionych w specyfikacji a które nie są dedykowane dla systemu diagnostycznego. Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie oraz musi być wpisany na stałe w BIOS. |
| Bezpieczeństwo | Ukryty w laminacie płyty głównej układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Próba usunięcia dedykowanego układu doprowadzi do uszkodzenia całej płyty głównej.  Zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu BIOS lub szybkiego menu boot’owania, umożliwiający przetestowanie w celu wykrycia usterki zainstalowanych komponentów bez konieczności uruchamiania systemu operacyjnego. System musi posiadać wszystkie swoje funkcjonalności w przypadku: braku dysku, uszkodzenia dysku, sformatowania dysku, braku dostępu do sieci, internetu. Nie dopuszcza się stosowania wewnętrznych i zewnętrznych urządzeń w celu uzyskania funkcjonalności systemu diagnostycznego. Pełna obsługa systemu diagnostycznego za pomocą klawiatury i myszy jak i samej myszy. Czujnik otwarcia obudowy, musi zbierać zdarzenia i zapisywać je w BIOS |
| BIOS | BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera lub nazwę modelu oferowanego komputera. Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy. BIOS wyposażony w automatyczną detekcję zmiany konfiguracji, automatycznie nanoszący zmiany w konfiguracji w szczególności: procesor, wielkość pamięci, pojemność dysku. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania (w tym również systemu diagnostycznego) i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: wersji BIOS, nr seryjnym komputera, ilości zainstalowanej pamięci RAM, prędkości zainstalowanych pamięci RAM, technologii wykonania pamięci, sposobie obsadzeniu slotów pamięci z rozbiciem na wielkości pamięci i banki, typie zainstalowanego procesora, ilości rdzeni zainstalowanego procesora, minimalnej i maksymalnej osiąganej prędkości zainstalowanego procesora, pojemności zainstalowanego lub zainstalowanych dysków twardych, MAC adresie zintegrowanej karty sieciowej, zintegrowanym układzie graficznym, kontrolerze audio. Funkcja umożliwiająca wł/wy kamery, mikrofonu, audio.  Do odczytu wskazanych informacji nie mogą być stosowane rozwiązania oparte o pamięć masową (wewnętrzną lub zewnętrzną), zaimplementowane poza systemem BIOS narzędzia, np. system diagnostyczny, dodatkowe oprogramowanie.  Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń, możliwość ustawienia hasła systemowego/użytkownika umożliwiającego uruchomienie komputera (zabezpieczenie przed nieautoryzowanym uruchomieniem) przy jednoczesnym zdefiniowanym haśle administratora. Użytkownik po wpisaniu hasła systemowego/użytkownika w BIOS jest wstanie zidentyfikować ustawienia oraz dokonać zmiany hasła systemowego/użytkownika. Możliwość ustawienia haseł użytkownika i administratora składających się z cyfr, małych liter, dużych liter oraz znaków specjalnych. Możliwość ustawienia portów USB w trybie „no BOOT” (podczas startu komputer nie wykrywa urządzeń bootujących typu USB). Możliwość wyłączania portów USB pojedynczo.  Dedykowane pole inwentarzowe umożliwiająca wpisanie oznaczenia sprzętu bez potrzeby wykorzystania dodatkowego oprogramowania, jak i konieczności aktualizacji BIOS. Pole po nadaniu numeru nie może być edytowalne oraz nie może ulec czyszczeniu przy aktualizacji BIOS. |
| Wirtualizacja | Sprzętowe wsparcie technologi wirtualizacji realizowane łącznie w procesorze, chipsecie płyty główej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu). |
| Zgodność z systemami operacyjnymi i standardami | Oferowane modele komputerów muszą poprawnie współpracować z oferowanym systemem operacyjnym (do oferty załączyć wydruk ze strony producenta oferowanego oprogramowania potwierdzający certyfikację dla oferowanego urządzenia). |
| System operacyjny | Zainstalowany system operacyjny Windows 11 Professional, klucz licencyjny musi być zapisany trwale w BIOS i umożliwiać instalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego. |
| Certyfikaty i standardy | 1. Certyfikat ISO9001 dla producenta sprzętu (załączyć dokument potwierdzający spełnianie wymogu) 2. Certyfikat ISO14001 dla producenta sprzętu (załączyć dokument potwierdzający spełnianie wymogu) 3. Certyfikat ISO50001 dla producenta sprzętu (załączyć dokument potwierdzający spełnianie wymogu) 4. Deklaracja zgodności CE (załączyć do oferty) 5. Certyfikat TCO, wymagana certyfikacja na stronie: <http://tcocertified.com/product-finder/> – załączyć do oferty wydruk z strony 6. Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych”, pkt. 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gram. |
| Ergonomia | Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji obserwatora w trybie pracy dysku twardego (IDLE) wynosząca maksymalnie 30 dB (załączyć wymagany dokument). |
| Wymagania dodatkowe | Złącza i porty wlutowane w płytę główną i wyprowadzone bezpośrednio na zewnątrz obudowy bez stosowania rozgałęziaczy, hubów czy poprzez wyprowadzenie z portów znajdujących się wewnętrznie na płycie:   1. panel przedni: 2. min. 2x USB 3.2 Gen 1 w tym jeden dosilony 3. min. 2x USB 3.2 typ C gen 2, w tym min jeden port 20 Gbps 4. 1 x port audio Combo typu Jack 5. 1 x czytnik kart SD 4.0 6. panel tylny: 7. 2 x DisplayPort 1.4 port 8. 2 x USB 3.2 Type-C Gen 2 (10 Gbps) 9. Min. 4 porty USB typ A w tym min. 2 x USB 3.2 Gen 2 (10 Gbps) 10. 1 x RJ45 port 10/100/1000 Mbps 11. Port szeregowy   Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona na etapie produkcji logiem producenta oferowanej jednostki, dedykowana dla danego urządzenia, wyposażona w: 1 x PCIe x16 gen 5.0 , 1 x PCIe x4 gen 4.0, 1 x PCIe x1 gen 3.0, 4 x DIMM z obsługą do 128 GB DDR5 RAM, 4 x SATA III, trzy złącza M.2 dla dysków (bez stosowania kart rozszerzeń PCIe), jedno złącze M.2 dla karty sieci bezprzewodowej (bez stosowania kart rozszerzeń PCIe). Zintegrowany z płytą główną kontroler RAID 0/1/5 dla dysków SATA oraz RAID 0/1 dla dysków M.2.  Karta sieci bezprzewodowej Wi-Fi 6E z modułem Bluetooth 5.3  Bezprzewodowy zestaw mysz optyczna i klawiatura w układzie polski programisty  Wbudowana nagrywarka DVD +/-RW o prędkości min. 8x  Opakowanie musi być wykonane z materiałów podlegających powtórnemu przetworzeniu. |
| Wsparcie techniczne producenta | 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 gwarancji | Gwarancja producenta świadczona na miejscu u klienta.  Okres gwarancji: zgodnie z ofertą Wykonawcy lecz nie mniej niż 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 – dokumenty potwierdzające załączyć do oferty.  Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta – wymagane dołączenie do oferty oświadczenia Producenta potwierdzonego, że serwis będzie realizowany przez Autoryzowanego Partnera Serwisowego Producenta lub bezpośrednio przez Producenta  W przypadku awarii dysk twardy zostaje u Zamawiającego – do oferty załączyć oświadczenie podmiotu realizującego serwis lub producenta o spełnieniu tego warunku  Zamawiający wymaga narzędzia do zarządzania zgłoszeniami serwisowymi samodzielnie przez portal internetowy lub inne narzędzie nie wymagające działań po stronie dostawcy. Narzędzie powinno umożliwiać:   1. samodzielne wystawianie zgłoszeń serwisowych, śledzenie stanu zgłoszenia, komunikację z serwisem producenta przez edycję zlecenia i stanu zlecenia 2. dostęp do materiałów serwisowych - co najmniej podręczników serwisowych i not serwisowych 3. dostęp do materiałów szkoleniowych 4. możliwości dodawania plików do otwieranego lub otwartego zlecenia (zdjęcia uszkodzeń, opisy etc.) 5. śledzenie historii zleceń - raporty ze zleceń, historia - dla poszczególnych zleceń lub dla poszczególnych komputerów 6. możliwość samodzielnego zarządzania wysyłką części (decyzja o zamówieniu części zamiennych i diagnostyka po stronie zamawiającego) 7. możliwość rejestrowania i zarządzania zdarzeniami serwisowymi - agregowania zdarzeń z oprogramowania zarządzającego dostarczonego przez producenta, możliwość konwertowania zdarzeń na zgłoszenia serwisowe do producenta - z poziomu narzędzia. 8. możliwość spięcia systemu serwisowego producenta z systemem helpdesk zamawiającego (dostępność API co najmniej dla opcji wystawienie zlecenia, sprawdzenie stanu zlecenia, raport zleceń) 9. tworzenia kont dla inżynierów serwisu z możliwością sprawdzenia statystyk wydajności / jakości ich pracy. |
| Dodatkowe oprogramowanie | Oprogramowanie zarządzające producenta komputera instalowane na etapie produkcji urządzenia, umożliwiające:   1. monitorowanie komputera i generowanie zgłoszeń o błędach / nieprawidłowym działaniu w zakresie pracy komponentów i wydajności systemów 2. powiadamiania o nowych wersjach sterowników i umożliwienie użytkownikowi wykonania upgrade systemu 3. powiadamianie o problemach wydajnościowych i diagnozowanie / rozwiązywanie takich problemów 4. śledzenia kluczowych komponentów i przewidywanie awarii przed ich wystąpieniem.   Oprogramowanie poducenta komputera z nieograniczoną licencją czasowo na użytkowanie umożliwiające:   1. upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS’u z certyfikatem zgodności producenta do najnowszej dostępnej wersji, 2. 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 o: 3. poprawkach i usprawnieniach dotyczących aktualizacji 4. dacie wydania ostatniej aktualizacji 5. priorytecie aktualizacji 6. zgodności z systemami operacyjnymi 7. jakiego komponentu sprzętu dotyczy aktualizacja 8. wszystkich poprzednich aktualizacjach z informacjami jak powyżej. 9. wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne 10. możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika, aplikacji która tego wymaga. 11. rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty ( dd-mm-rrrr ) 12. sprawdzenia historii upgrade’u z informacją jakie sterowniki były instalowane z dokładną datą ( dd-mm-rrrr) i wersją (rewizja wydania) 13. 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. |
| Dodatkowe oprogramowanie biurowe | Pakiet biurowy o minimalnych wymaganiach: edytor tekstu, arkusz kalkulacyjny, tworzenie prezentacji, obsługa poczty elektronicznej.  Wykonawca dla każdego z dostarczanych komputerów dostarczy licencję oprogramowania, który musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:   1. Pełna polska wersja językowa graficznego interfejsu użytkownika. 2. Do aplikacji musi być dostępna dokumentacja w języku polskim. 3. Zachowanie zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Word, Excel i PowerPoint: 2013, 2016, 2019 z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń. 4. Pakiet zintegrowanych aplikacji biurowych musi zawierać: 5. Edytor tekstów 6. Arkusz kalkulacyjny 7. Narzędzie do tworzenia prezentacji 8. Obsługa poczty elektronicznej (w tym kalendarz, kontakty i zadania) 9. Oprogramowanie biurowe w najnowszej dostępnej na rynku wersji. 10. Zamawiający nie dopuszcza zaoferowania pakietów biurowych, programów i planów licencyjnych opartych o rozwiązania chmury oraz rozwiązań wymagających stałych opłat w okresie używania zakupionego produktu. 11. Dla oprogramowania musi być publicznie znany cykl życia dotyczący rozwoju wsparcia technicznego – w szczególności w zakresie bezpieczeństwa. Wymagane jest prawo do instalacji aktualizacji i poprawek do danej wersji oprogramowania, udostępnianych bezpłatnie na stronie internetowej w okresie co najmniej 2 lat. 12. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych 13. Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki: 14. posiada kompletny i publicznie dostępny opis formatu, 15. umożliwia wykorzystanie schematów XML 16. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy) 17. Arkusz kalkulacyjny musi umożliwiać: 18. Tworzenie raportów tabelarycznych 19. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych 20. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu. 21. Formatowanie czasu, daty i wartości finansowych z polskim formatem 22. Zapis wielu arkuszy kalkulacyjnych w jednym pliku. 23. Tworzenie raportów tabelarycznych 24. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML) 25. Obsługę kostek OLAP 26. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych 27. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych 28. Wyszukiwanie i zamianę danych 29. Wykonywanie analiz danych przy użyciu formatowania warunkowego 30. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie 31. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności 32. Edytor tekstów musi umożliwiać: 33. Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty 34. Wstawianie oraz formatowanie tabel 35. Wstawianie oraz formatowanie obiektów graficznych 36. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne) 37. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków 38. Automatyczne tworzenie spisów treści 39. Formatowanie nagłówków i stopek stron 40. Śledzenie zmian wprowadzonych przez użytkowników 41. Określenie układu strony (pionowa/pozioma) 42. Wydruk dokumentów 43. Wykonywanie korespondencji seryjnej, bazując na danych adresowych pochodzących z arkusza kalkulacyjnego 44. Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2003, 2007, 2010, 2013, 2016 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu 45. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji 46. Możliwość wczytywania pików pdf wraz z automatyczną konwersją tekstu i tabel. 47. Możliwość zapisywania plików w formacie pdf. 48. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać: Przygotowywanie prezentacji multimedialnych, które będą: 49. Prezentowanie przy użyciu projektora multimedialnego 50. Drukowanie w formacie umożliwiającym robienie notatek 51. Zapisanie jako prezentacja tylko do odczytu. 52. Nagrywanie narracji i dołączanie jej do prezentacji 53. Opatrywanie slajdów notatkami dla prezentera 54. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo 55. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego 56. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym 57. Możliwość tworzenia animacji obiektów i całych slajdów 58. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera 59. Aplikacja do tworzenia prezentacji powinna umożliwiać zapis prezentacji w formie klipu video i pliku pdf. 60. Narzędzie do zarządzania pocztą elektroniczną, kalendarzem, kontaktami i zadaniami musi umożliwiać: 61. Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego 62. Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców 63. Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną 64. Automatyczne grupowanie poczty o tym samym tytule 65. Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy 66. Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia 67. Zarządzanie kalendarzem 68. Udostępnianie kalendarza innym użytkownikom 69. Przeglądanie kalendarza innych użytkowników 70. Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach 71. Zarządzanie listą zadań 72. Zlecanie zadań innym użytkownikom 73. Zarządzanie listą kontaktów 74. Udostępnianie listy kontaktów innym użytkownikom 75. Przeglądanie listy kontaktów innych użytkowników 76. Możliwość przesyłania kontaktów z innym użytkownikami. |

# Monitor 27”

|  |  |
| --- | --- |
| Cecha | Wymagania minimalne |
| Obraz/wyświetlacz | 1. Rozmiar panelu: 68,6 cm / 27 cali 2. Współczynnik proporcji: 16:9 3. Typ panelu LCD: Technologia IPS 4. Typ wyświetlacza: System W-LED 5. Rozstaw pikseli: 0,2331 x 0,2331 mm 6. Jasność: 300 cd/m² 7. Kolory wyświetlacza: 16,7 Mln 8. Współczynnik kontrastu (typowy): 1000:1 9. Czas reakcji (standardowy): 4 ms (szarości)\* 10. Kąt patrzenia: 178º (poz.) / 178º (pion.), 11. Min. rozdzielczość: 2560 x 1440 przy 75 Hz |
| Porty | 1. Wejście sygnału: 2. HDMI 1.4 x 1, 3. DisplayPort 1.2 x 1, 4. Wyjście audio 5. USB 3.2 x 4 (typu downstream, min 1 z funkcją szybkiego ładowania BC 1.2) |
| Głośniki | Wbudowane głośniki 2x 5W |
| Regulacja wysokości/ pochylenia/ obrót | 1. Regulacja wysokości: 130 mm 2. Obracanie w pionie: +/- 90 stopni 3. Pochylanie wzdłużne: -5/20 stopni |
| Zasilanie i pobór prądu | 1. Wewnętrzny zasilacz, 100–240 V AC, 50–60 Hz 2. Tryb wyłączenia/czuwania: max 0,5 W 3. Tryb włączenia: max 30 W |
| Wyposażenie dodatkowe | 1. Blokada Kensington, 2. Mocowanie VESA (100 x 100 mm) 3. Wbudowana kamera internetowa o rozdzielczości 5,0 megapiksela, mikrofon i wskaźnik LED (dla Windows Hello) 4. Mikrofon z redukcją szumów |
| Gwarancja | Okres gwarancji: zgodnie z ofertą Wykonawcy, lecz nie mniej niż 24 miesiące.  Gwarancji realizowanej przez autoryzowany serwis producenta |

# Laptop

|  |  |
| --- | --- |
| Cecha | Wymagania minimalne |
| Zastosowanie | Komputer mobilny będzie wykorzystywany dla potrzeb aplikacji biurowych, edukacyjnych, obliczeniowych, dostępu do Internetu oraz poczty elektronicznej. |
| Przekątna ekranu | 15,6” FHD (1920 x 1080), powłoką przeciwodblaskową, jasność 250 nits, kontrast min. 600:1, gama koloru min. NTSC 45% (typowo) |
| Procesor | Procesor dedykowany do pracy w notebookach osiągający w teście PassMark Performance Test wynik minimum **14 500** punktów Passmark CPU Mark wg wyników ze strony : <http://www.passmark.com/products/pt.htm> |
| Pamięć RAM | Min16GB z możliwością rekonfiguracji lub rozbudowy do min 64GB.  Płyta główna wyposażona w dwa sloty na pamięć, w tym jeden slot wolny, nie dopuszcza się pamięci wlutowanych |
| Pamięć masowa | Min. 512GB SSD M.2 NVMe |
| Karta graficzna | Zintegrowana z procesorem |
| Klawiatura | 1. Klawiatura w układzie US – QWERTY z wydzieloną po prawej stronie klawiaturą numeryczną i wbudowanym w klawiaturze podświetleniem, min. 98 klawiszy. Wszystkie klawisze funkcyjne typu: regulacja głośności, print screen dostępne w ciągu klawiszy F1-F12. Nie dopuszcza się innego układu a w szczególności między klawiszami ALT i CTRL (oprócz klawisza FN i Windows z lewej strony) 2. Dedykowane klawisze funkcyjne do: wyciszenia głośników, wyciszenia mikrofonów, regulacji głośności, regulacji podświetlenia klawiatury, regulacji jasności ekranu. |
| Mysz i torba do laptopa | 1. Mysz bezprzewodowa wyposażona w 3 przyciski (1 programowalny), rozdzielczość DPI min 4000, wskaźnik naładowania baterii, kolor czarny 2. Torba do przenoszenia laptopa dostosowana do wymiarów laptopa koloru czarnego. |
| Multimedia | 1. Karta dźwiękowa zintegrowana z płytą główną, wbudowane dwa głośniki stereo o mocy 2 x 2W. 2. Cyfrowe mikrofony z funkcją redukcji szumów i poprawy mowy wbudowany w obudowę matrycy. 3. Kamera internetowa FHD RGB 2 MPIX, trwale zainstalowana w obudowie matrycy z wbudowaną mechaniczną przysłoną. 4. 1 port audio typu combo (słuchawki i mikrofon) |
| Łączność bezprzewodowa | Wbudowana karta Wi-Fi 6E z Bluetooth |
| Bateria i zasilanie | 1. Bateria Lithium-ion min. 54Wh z obsługą technologii szybkiego ładowania, umożliwiającą szybkie naładowanie baterii do poziomu 80% w czasie 1 godziny. 2. Zasilacz o mocy min. 65W adapter 4.5mm |
| Waga | Waga maks. 2 kg z oferowaną baterią |
| Obudowa | Szkielet obudowy i zawiasy notebooka wzmacniane, dookoła matrycy uszczelnienie chroniące klawiaturę notebooka po zamknięciu przed kurzem i wilgocią.  Komputer spełniający normy MIL-STD-810H w zakresie min. 7 method (do oferty załączyć certyfikat lub oświadczenie producenta) |
| 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. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji, oraz posiadać: datę produkcji komputera (data produkcji nieusuwalna), o kontrolerze audio, procesorze, a w szczególności min. i max. osiągana prędkość, pamięci RAM z informacją o taktowaniu i obsadzeniu w slotach. Niezmazywalne (nieedytowalne) pole asset tag. Możliwość ustawienia hasła dla administratora, możliwość ustawienia hasła systemowego/użytkownika które jednocześnie będzie blokować uruchamianie systemu z jakichkolwiek urządzeń oraz umożliwia zalogowanie się do BIOS w celu zmiany swojego hasła, możliwość ustawienia hasła dla dysku NVMe, możliwość konfiguracji zależności między tymi hasłami, hasła muszą umożliwiać zawarcia w sobie znaków specjalnych, liczb i liter, Możliwość odczytania informacji o stanie naładowania baterii (stanu użycia), podpiętego zasilacza, zarządzanie trybem ładowania baterii (np. określenie docelowego poziomu naładowania). Możliwość nadania numeru inwentarzowego z poziomu BIOS bez wykorzystania dodatkowego oprogramowania, jak i konieczności aktualizacji BIOS , po nadaniu numeru pole nie może być edytowalne. |
| Certyfikaty | 1. Certyfikat ISO 9001 dla producenta sprzętu (należy załączyć do oferty) 2. Certyfikat ISO 14001 dla producenta sprzętu (należy załączyć do oferty) 3. Deklaracja zgodności CE (załączyć do oferty) 4. Certyfikat ISO 50001(należy załączyć do oferty) 5. Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki 6. Potwierdzenie kompatybilności komputera z oferowanym systemem operacyjnym (wydruk ze strony producenta oprogramowania) 7. EnergyStar – załączyć do oferty certyfikat lub wydruk z strony <https://www.energystar.gov/> 8. Certyfikat TCO dla oferowanego modelu, wymagana certyfikacja na stronie: <https://tcocertified.com/product-finder/> – załączyć do oferty wydruk z strony. |
| Ergonomia | Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji obserwatora w trybie IDLE wynosząca maksymalnie 22dB (załączyć do oferty oświadczenie producenta) |
| 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:   1. procesor 2. pamięć RAM 3. dysk twardy 4. zasilanie/ładowanie 5. klawiatury 6. test wyświetlacza/matrycy 7. audio/głośników 8. zintegrowanej karty sieciowej LAN 9. układ graficzny/video 10. kamera internetowa 11. bateria 12. wentylator 13. porty USB   Testy możliwe do wykonania w formie szybkiej i zaawansowanej lub dedykowanej formie dla danego komponentu, Pełna obsługa systemu diagnostycznego za pomocą samej klawiatury, urządzenia wskazującego, myszy i jednocześnie za pomocą klawiatury i myszy. System zapewniający zachowujący pełną funkcjonalność nawet w przypadku braku dysku twardego oraz jego uszkodzenia, nie wymagający stosowania zewnętrznych nośników pamięci masowej oraz dostępu do internetu i sieci lokalnej. Procedura POST traktowana jest jako oddzielna funkcjonalność. |
| 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.  Czytnik linii papilarnych |
| System operacyjny | Zainstalowany system operacyjny Windows 11 Professional, klucz licencyjny zapisany trwale w BIOS, umożliwiać instalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego. |
| Oprogramowanie dodatkowe | Dołączone do oferowanego komputera oprogramowanie producenta z nieograniczoną licencją czasowo na użytkowanie umożliwiające:   1. upgrade i instalacje wszystkich sterowników dostarczonych w obrazie systemu operacyjnego producenta, BIOS’u z certyfikatem zgodności producenta do najnowszej dostępnej wersji, 2. możliwość przed instalacją sprawdzenia każdego sterownika, BIOS’u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji: 3. o poprawkach i usprawnieniach dotyczących aktualizacji 4. dacie wydania ostatniej aktualizacji 5. priorytecie aktualizacji 6. zgodność z systemami operacyjnymi 7. jakiego komponentu sprzętu dotyczy aktualizacja 8. wszystkie poprzednie aktualizacje z informacjami jak powyżej od punktu a do punktu e. 9. wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne 10. możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika, aplikacji która tego wymaga. 11. rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty (dd-mm-rrrr) 12. sprawdzenia historii upgrade’u z informacją jakie sterowniki były instalowane z dokładną datą (dd-mm-rrrr) i wersją (rewizja wydania) 13. dokładny wykaz wymaganych sterowników, aplikacji, BIOS’u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu \*.xml 14. -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. 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: 1x HDMI 1.4, 1x RJ-45, 2x USB 3.2 gen 1 typu A (w tym jeden zasilaniem), 1x USB4 Typu C z przepustowością 20Gbps i z obsługą DP 1.2, port zasilania (nie zajmujący portów USB typ C), złącze linki zabezpieczającej. |
| Warunki gwarancyjne, wsparcie techniczne | 1. Gwarancja producenta świadczona na miejscu u klienta. 2. Okres gwarancji: zgodnie z ofertą Wykonawcy, lecz nie mniej niż 24 miesiące. 3. Czas reakcji serwisu - do końca następnego dnia roboczego 4. Firma serwisująca musi posiadać ISO 9001: 2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty. 5. Oświadczenie producenta komputera, że w przypadku niewywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem 6. W przypadku awarii dysk twardy zostaje u Zamawiającego – do oferty załączyć oświadczenie podmiotu realizującego serwis lub producenta o spełnieniu tego warunku 7. Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. 8. 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) |
| Dodatkowe oprogramowanie biurowe | Pakiet biurowy o minimalnych wymaganiach: edytor tekstu, arkusz kalkulacyjny, tworzenie prezentacji, obsługa poczty elektronicznej.  Wykonawca dla każdego z dostarczanych komputerów dostarczy licencję oprogramowania, który musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:   1. Pełna polska wersja językowa graficznego interfejsu użytkownika. 2. Do aplikacji musi być dostępna dokumentacja w języku polskim. 3. Zachowanie zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Word, Excel i PowerPoint: 2013, 2016, 2019 z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń. 4. Pakiet zintegrowanych aplikacji biurowych musi zawierać: 5. Edytor tekstów 6. Arkusz kalkulacyjny 7. Narzędzie do tworzenia prezentacji 8. Obsługa poczty elektronicznej (w tym kalendarz, kontakty i zadania) 9. Oprogramowanie biurowe w najnowszej dostępnej na rynku wersji. 10. Zamawiający nie dopuszcza zaoferowania pakietów biurowych, programów i planów licencyjnych opartych o rozwiązania chmury oraz rozwiązań wymagających stałych opłat w okresie używania zakupionego produktu. 11. Dla oprogramowania musi być publicznie znany cykl życia dotyczący rozwoju wsparcia technicznego – w szczególności w zakresie bezpieczeństwa. Wymagane jest prawo do instalacji aktualizacji i poprawek do danej wersji oprogramowania, udostępnianych bezpłatnie na stronie internetowej w okresie co najmniej 2 lat. 12. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych 13. Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki: 14. posiada kompletny i publicznie dostępny opis formatu, 15. umożliwia wykorzystanie schematów XML 16. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy) 17. Arkusz kalkulacyjny musi umożliwiać: 18. Tworzenie raportów tabelarycznych 19. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych 20. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu. 21. Formatowanie czasu, daty i wartości finansowych z polskim formatem 22. Zapis wielu arkuszy kalkulacyjnych w jednym pliku. 23. Tworzenie raportów tabelarycznych 24. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML) 25. Obsługę kostek OLAP 26. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych 27. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych 28. Wyszukiwanie i zamianę danych 29. Wykonywanie analiz danych przy użyciu formatowania warunkowego 30. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie 31. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności 32. Edytor tekstów musi umożliwiać: 33. Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty 34. Wstawianie oraz formatowanie tabel 35. Wstawianie oraz formatowanie obiektów graficznych 36. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne) 37. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków 38. Automatyczne tworzenie spisów treści 39. Formatowanie nagłówków i stopek stron 40. Śledzenie zmian wprowadzonych przez użytkowników 41. Określenie układu strony (pionowa/pozioma) 42. Wydruk dokumentów 43. Wykonywanie korespondencji seryjnej, bazując na danych adresowych pochodzących z arkusza kalkulacyjnego 44. Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2003, 2007, 2010, 2013, 2016 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu 45. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji 46. Możliwość wczytywania pików pdf wraz z automatyczną konwersją tekstu i tabel. 47. Możliwość zapisywania plików w formacie pdf. 48. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać przygotowywanie prezentacji multimedialnych, które będą: 49. Prezentowanie przy użyciu projektora multimedialnego 50. Drukowanie w formacie umożliwiającym robienie notatek 51. Zapisanie jako prezentacja tylko do odczytu. 52. Nagrywanie narracji i dołączanie jej do prezentacji 53. Opatrywanie slajdów notatkami dla prezentera 54. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo 55. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego 56. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym 57. Możliwość tworzenia animacji obiektów i całych slajdów 58. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera 59. Aplikacja do tworzenia prezentacji powinna umożliwiać zapis prezentacji w formie klipu video i pliku pdf. 60. Narzędzie do zarządzania pocztą elektroniczną, kalendarzem, kontaktami i zadaniami musi umożliwiać: 61. Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego 62. Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców 63. Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną 64. Automatyczne grupowanie poczty o tym samym tytule 65. Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy 66. Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia 67. Zarządzanie kalendarzem 68. Udostępnianie kalendarza innym użytkownikom 69. Przeglądanie kalendarza innych użytkowników 70. Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach 71. Zarządzanie listą zadań 72. Zlecanie zadań innym użytkownikom 73. Zarządzanie listą kontaktów 74. Udostępnianie listy kontaktów innym użytkownikom 75. Przeglądanie listy kontaktów innych użytkowników 76. Możliwość przesyłania kontaktów z innym użytkownikami. |

# Stacja robocza All-in-one

|  |  |  |
| --- | --- | --- |
| Cecha | Wymagania minimalne | |
| Typ | Komputer stacjonarny. Typu All in One, komputer fabrycznie wbudowany w obudowę monitora. W ofercie wymagane jest podanie modelu producenta komputera. | |
| Zastosowanie | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna | |
| Procesor | Procesor dedykowany do pracy w komputerach stacjonarnych, osiągający w teście Passmark CPU Mark, w kategorii Average CPU Mark wynik nie niższy niż **34 500** pkt. według wyników opublikowanych na stronie <https://www.cpubenchmark.net/cpu_list.php> | |
| Pamięć RAM | 32GB w układzie 1x 32GB, jeden slot wolny, możliwość rozbudowy do min 64GB. | |
| Pamięć masowa | 1TB SSD M.2 NVMe  Możliwość montażu drugiego dysku M.2  Możliwość skonfigurowania RAID 0/1 pomiędzy dyskami | |
| Karta graficzna | Karta graficzna zintegrowana z procesorem | |
| Matryca | Rozmiar matrycy / plamki | Min. 23,8” IPS / max. 0,270mm |
|  | Rozdzielczość | FHD (1920x1080) |
|  | Jasność typowa | 250 cd/m² |
|  | Kontrast typowy | 1000:1 |
|  | Barwa koloru (typowa) | 99% sRGB |
|  | Kąty typowe | 178(+/- 89) / 178 (+/-89) |
|  | Rodzaj matrycy | Matowa IPS |
| Wyposażenie multimedialne | Karta dźwiękowa zintegrowana z płytą główną, wbudowane dwa głośniki min. 5W na kanał.  Wbudowana w obudowę matrycy cyfrowa kamera RBG 5,0 MP. Mechanicznie chowana w obudowie (nie dopuszcza się kamer przekręcanych i wystających poza obrys obudowy)  Wbudowane w obudowę dwa mikrofony | |
| Obudowa | 1. Typu All-in-One zintegrowana z monitorem min. 23.8”. Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej, demontaż tylnej pokrywy musi odbywać się bez użycia narzędzi. Systemu montażowy VESA 100. Suma wymiarów obudowy bez zainstalowanego standu max. 96cm. 2. Zasilacz wewnętrzny o mocy max. 240W, 80 plus Platinum 3. Zasilacz w oferowanym komputerze musi się znajdować na stronie <http://www.plugloadsolutions.com/80pluspowersupplies.aspx> do oferty należy dołączyć wydruk potwierdzający spełnienie wymogu 80plus 4. Wbudowany w obudowie wizualny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, w szczególności: uszkodzenia lub braku pamięci RAM, uszkodzenia płyty głównej, awarii procesora. System musi zapisywać logi zdarzeń w BIOS. System diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów wymaganych w specyfikacji. 5. Każdy komputer musi być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, oraz wpisanym na stałe w BIOS. 6. Podstawa jednostki typu All – in – One musi umożliwiać: 7. Regulację pochyłu pionowego w zakresie od -5 do 30 stopni. 8. Regulację wysokości w zakresie minimum 10 cm. 9. Ustawienie jednostki w trybie Pivot. 10. Obrót podstawy w lewą oraz prawą stronę. | |
| Zgodność z systemami operacyjnymi i standardami | Oferowane modele komputerów muszą poprawnie współpracować z oferowanym systemem operacyjnym (do oferty należy załączyć certyfikat ze strony producenta oprogramowania ). | |
| Bezpieczeństwo / diagnostyka | 1. Płyta główna zawierająca układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego 2. Zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu BIOS lub szybkiego menu boot’owania, umożliwiający przetestowanie w celu wykrycia usterki zainstalowanych komponentów bez konieczności uruchamiania systemu operacyjnego. System musi posiadać wszystkie swoje funkcjonalności w przypadku: braku dysku, uszkodzenia dysku, sformatowania dysku, braku dostępu do sieci, internetu. Nie dopuszcza się stosowania wewnętrznych i zewnętrznych urządzeń w celu uzyskania funkcjonalności systemu diagnostycznego. Pełna obsługa systemu diagnostycznego za pomocą klawiatury i myszy jak i samej myszy. 3. Czujnik otwarcia obudowy, musi zbierać zdarzenia i zapisywać je w BIOS | |
| BIOS | 1. BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera lub nazwę modelu oferowanego komputera. Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy. BIOS wyposażony w automatyczną detekcję zmiany konfiguracji, automatycznie nanoszący zmiany w konfiguracji w szczególności: procesor, wielkość pamięci, pojemność dysku. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania (w tym również systemu diagnostycznego) i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: wersji BIOS, nr seryjnym komputera, ilości zainstalowanej pamięci RAM, prędkości zainstalowanych pamięci RAM, technologii wykonania pamięci, sposobie obsadzeniu slotów pamięci z rozbiciem na wielkości pamięci i banki, typie zainstalowanego procesora, ilości rdzeni zainstalowanego procesora, minimalnej i maksymalnej osiąganej prędkości zainstalowanego procesora, pojemności zainstalowanego lub zainstalowanych dysków twardych, MAC adresie zintegrowanej karty sieciowej, zintegrowanym układzie graficznym, kontrolerze audio. Funkcja umożliwiająca wł/wy kamery, mikrofonu, audio. 2. Do odczytu wskazanych informacji nie mogą być stosowane rozwiązania oparte o pamięć masową (wewnętrzną lub zewnętrzną), zaimplementowane poza systemem BIOS narzędzia, np. system diagnostyczny, dodatkowe oprogramowanie. 3. Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń, możliwość ustawienia hasła systemowego/użytkownika umożliwiającego uruchomienie komputera (zabezpieczenie przed nieautoryzowanym uruchomieniem) przy jednoczesnym zdefiniowanym haśle administratora. Użytkownik po wpisaniu hasła systemowego/użytkownika w BIOS jest wstanie zidentyfikować ustawienia oraz dokonać zmiany hasła systemowego/użytkownika. Możliwość ustawienia haseł użytkownika i administratora składających się z cyfr, małych liter, dużych liter oraz znaków specjalnych. Możliwość ustawienia portów USB w trybie „no BOOT” (podczas startu komputer nie wykrywa urządzeń bootujących typu USB). Możliwość wyłączania portów USB pojedynczo. 4. Dedykowane pole inwentarzowe umożliwiająca wpisanie oznaczenia sprzętu. Pole po nadaniu numeru nie może być edytowalne. | |
| Certyfikaty i standardy | 1. System zarządzania jakością - certyfikat ISO9001 dla producenta sprzętu (załączyć dokument potwierdzający spełnianie wymogu) 2. System zarządzania środowiskowego - certyfikat ISO14001 dla producenta sprzętu (załączyć dokument potwierdzający spełnianie wymogu) 3. System zarządzania energią - certyfikat ISO50001 dla producenta sprzętu (załączyć dokument potwierdzający spełnianie wymogu) 4. Deklaracja zgodności CE (załączyć do oferty) 5. Urządzenia wyprodukowane są przez producenta, zgodnie z normą PN-EN ISO 50001 6. Certyfikat TCO, wymagana certyfikacja na stronie: <http://tcocertified.com/product-finder/>– załączyć do oferty wydruk z strony 7. Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych”, pkt. 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gram. | |
| Ergonomia | Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji operatora w trybie pracy jałowej dysku twardego (IDLE) wynosząca maksymalnie 24 dB (załączyć oświadczenie producenta) | |
| System Operacyjny | Zainstalowany system operacyjny Windows 11 Professional, klucz licencyjny zapisany trwale w BIOS, umożliwiać reinstalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego. | |
| Wymagania dodatkowe | Wbudowane porty:   1. 1x DP++ 1.4a 2. 1x HDMI In 1.4b 3. 1x HDMI 2.1 out 4. 1x USB 3.2 Gen 2 (10 Gbps) z PowerShare 5. 1x USB 3.2 Gen 2x2 (20 Gbps) Type-C 6. 3x USB 3.2 Gen 2 (10 Gbps) 7. 2x USB 3.2 Gen 1 (5 Gbps) z SmartPower On 8. Wymagane porty USB wbudowane w obudowie , nie dopuszcza się stosowania rozgałęziaczy, hub’ów itp. 9. 1x Universal audio jack 10. 1x RJ-45 port 10/100/1000 Mbps 11. Czytnik kart SD 4.0 12. Wbudowana karta WiFi 6E AX + bluetooth 5.3 13. Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona logo producenta oferowanej jednostki, dedykowana dla danego urządzenia; wyposażona w min. 2 złącza SO - DIMM z obsługą do 64GB DDR5 pamięci RAM, min. 2 złącza M.2 2280 dla dysku twardego oraz 1 złącze M.2 karty WiFi. 14. Bezprzewodowy zestaw mysz optyczna i klawiatura USB w układzie polski programisty 15. Napęd optyczny DVD +/-RW wbudowany w obudowę lub podstawę urządzenia | |
| Warunki gwarancji  Wsparcie techniczne | 1. Gwarancja producenta świadczona na miejscu u klienta. 2. Okres gwarancji: zgodnie z ofertą Wykonawcy, lecz nie mniej niż 24 miesiące. 3. Czas reakcji serwisu - do końca następnego dnia roboczego 4. Firma serwisująca musi posiadać ISO 9001: 2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty. 5. Oświadczenie producenta komputera, że w przypadku niewywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem 6. W przypadku awarii dysk twardy zostaje u Zamawiającego – do oferty załączyć oświadczenie podmiotu realizującego serwis lub producenta o spełnieniu tego warunku 7. 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). 8. Zamawiający wymaga narzędzia do zarządzania zgłoszeniami serwisowymi samodzielnie przez portal internetowy lub inne narzędzie nie wymagające działań po stronie dostawcy. Narzędzie powinno umożliwiać: 9. samodzielne wystawianie zgłoszeń serwisowych, śledzenie stanu zgłoszenia, komunikację z serwisem producenta przez edycję zlecenia i stanu zlecenia 10. dostęp do materiałów serwisowych - co najmniej podręczników serwisowych i not serwisowych 11. dostęp do materiałów szkoleniowych 12. możliwości dodawania plików do otwieranego lub otwartego zlecenia (zdjęcia uszkodzeń, opisy etc.) 13. śledzenie historii zleceń - raporty ze zleceń, historia - dla poszczególnych zleceń lub dla poszczególnych komputerów 14. możliwość samodzielnego zarządzania wysyłką części (decyzja o zamówieniu części zamiennych i diagnostyka po stronie zamawiającego) 15. możliwość rejestrowania i zarządzania zdarzeniami serwisowymi - agregowania zdarzeń z oprogramowania zarządzającego dostarczonego przez producenta, możliwość konwertowania zdarzeń na zgłoszenia serwisowe do producenta - z poziomu narzędzia. | |
| Dodatkowe oprogramowanie | Oprogramowanie producenta komputera z nieograniczoną czasowo licencją na użytkowanie umożliwiające:   1. upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS’u z certyfikatem zgodności producenta do najnowszej dostępnej wersji, 2. sprawdzenie przed zainstalowaniem wszystkich sterowników, aplikacji oraz BIOS bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem w celu uzyskania informacji o: poprawkach i usprawnieniach dotyczących aktualizacji, dacie wydania ostatniej aktualizacji, priorytecie aktualizacji, zgodności z systemami operacyjnymi 3. dostęp do wykazu najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne 4. włączenie/wyłączenie funkcji automatycznego restartu w przypadku, kiedy jest wymagany przy instalacji sterownika, aplikacji 5. sprawdzenie historii aktualizacji z informacją, jakie sterowniki były instalowane z dokładną datą i wersją (rewizja wydania) 6. dostęp do wykaz wymaganych sterowników, aplikacji, BIOS’u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu \*.xml 7. dostęp do raportu uwzględniającego informacje o znalezionych, pobranych i zainstalowanych aktualizacjach z informacją, jakich komponentów dotyczyły, możliwość exportu takiego raportu do pliku \*.xml 8. Raport musi zawierać datę i godzinę podjętych i wykonanych akcji/zadań w przedziale czasowym min. 1 roku. 9. W ofercie należy podać nazwę oprogramowania | |
| Dodatkowe oprogramowanie biurowe | Pakiet biurowy o minimalnych wymaganiach: edytor tekstu, arkusz kalkulacyjny, tworzenie prezentacji, obsługa poczty elektronicznej.  Wykonawca dla każdego z dostarczanych komputerów dostarczy licencję oprogramowania, który musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:   1. Pełna polska wersja językowa graficznego interfejsu użytkownika. 2. Do aplikacji musi być dostępna dokumentacja w języku polskim. 3. Zachowanie zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Word, Excel i PowerPoint: 2013, 2016, 2019 z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń. 4. Pakiet zintegrowanych aplikacji biurowych musi zawierać: 5. Edytor tekstów 6. Arkusz kalkulacyjny 7. Narzędzie do tworzenia prezentacji 8. Obsługa poczty elektronicznej (w tym kalendarz, kontakty i zadania) 9. Oprogramowanie biurowe w najnowszej dostępnej na rynku wersji. 10. Zamawiający nie dopuszcza zaoferowania pakietów biurowych, programów i planów licencyjnych opartych o rozwiązania chmury oraz rozwiązań wymagających stałych opłat w okresie używania zakupionego produktu. 11. Dla oprogramowania musi być publicznie znany cykl życia dotyczący rozwoju wsparcia technicznego – w szczególności w zakresie bezpieczeństwa. Wymagane jest prawo do instalacji aktualizacji i poprawek do danej wersji oprogramowania, udostępnianych bezpłatnie na stronie internetowej w okresie co najmniej 2 lat. 12. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych 13. Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki: 14. posiada kompletny i publicznie dostępny opis formatu, 15. umożliwia wykorzystanie schematów XML 16. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy) 17. Arkusz kalkulacyjny musi umożliwiać: 18. Tworzenie raportów tabelarycznych 19. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych 20. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu. 21. Formatowanie czasu, daty i wartości finansowych z polskim formatem 22. Zapis wielu arkuszy kalkulacyjnych w jednym pliku. 23. Tworzenie raportów tabelarycznych 24. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML) 25. Obsługę kostek OLAP 26. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych 27. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych 28. Wyszukiwanie i zamianę danych 29. Wykonywanie analiz danych przy użyciu formatowania warunkowego 30. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie 31. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności 32. Edytor tekstów musi umożliwiać: 33. Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty 34. Wstawianie oraz formatowanie tabel 35. Wstawianie oraz formatowanie obiektów graficznych 36. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne) 37. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków 38. Automatyczne tworzenie spisów treści 39. Formatowanie nagłówków i stopek stron 40. Śledzenie zmian wprowadzonych przez użytkowników 41. Określenie układu strony (pionowa/pozioma) 42. Wydruk dokumentów 43. Wykonywanie korespondencji seryjnej, bazując na danych adresowych pochodzących z arkusza kalkulacyjnego 44. Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2003, 2007, 2010, 2013, 2016 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu 45. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji 46. Możliwość wczytywania pików pdf wraz z automatyczną konwersją tekstu i tabel. 47. Możliwość zapisywania plików w formacie pdf. 48. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać przygotowywanie prezentacji multimedialnych, które będą: 49. Prezentowanie przy użyciu projektora multimedialnego 50. Drukowanie w formacie umożliwiającym robienie notatek 51. Zapisanie jako prezentacja tylko do odczytu. 52. Nagrywanie narracji i dołączanie jej do prezentacji 53. Opatrywanie slajdów notatkami dla prezentera 54. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo 55. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego 56. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym 57. Możliwość tworzenia animacji obiektów i całych slajdów 58. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera 59. Aplikacja do tworzenia prezentacji powinna umożliwiać zapis prezentacji w formie klipu video i pliku pdf. 60. Narzędzie do zarządzania pocztą elektroniczną, kalendarzem, kontaktami i zadaniami musi umożliwiać: 61. Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego 62. Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców 63. Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną 64. Automatyczne grupowanie poczty o tym samym tytule 65. Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy 66. Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia 67. Zarządzanie kalendarzem 68. Udostępnianie kalendarza innym użytkownikom 69. Przeglądanie kalendarza innych użytkowników 70. Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach 71. Zarządzanie listą zadań 72. Zlecanie zadań innym użytkownikom 73. Zarządzanie listą kontaktów 74. Udostępnianie listy kontaktów innym użytkownikom 75. Przeglądanie listy kontaktów innych użytkowników 76. Możliwość przesyłania kontaktów z innym użytkownikami. | |

# Klaster serwerów

Klaster serwerów zbudowany jest z 2 serwerów oraz wspólnej macierzy. Parametry składowych klastra opisują tabele poniżej.

## Serwery

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla sprzętu** |
| **Obudowa** | Obudowa Rack 19” o wysokości max 2U wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. |
| **Płyta główna** | Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera. |
| **Procesor** | Zainstalowane dwa procesory min. 16-rdzeniowe, min. 2.8GHz z częstotliwości nominalnej, klasy x86, osiągające minimalne wyniki testów w konfiguracji dwuprocesorowej:   1. SPECrate2017\_int\_base wynik min. 333pkt 2. SPECrate2017\_int\_peak wynik min. 344pkt 3. SPECrate2017\_fp\_base wynik min. 466pkt 4. SPECrate2017\_fp\_peak wynik min. 479pkt 5. Maksymalny TDP dla procesora 200W 6. Wynik testu musi być opublikowany na stronie <https://www.spec.org/cpu2017/results/> w dniu złożenia oferty. 7. Do oferty należy załączyć wyniki testów |
| **RAM** | 512GB (w układzie 8x64GB)o częstotliwości taktowania minimum 3200MHz, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać min. 1TB pamięci RAM. |
| **Funkcjonalność pamięci RAM** | 1. Demand Scrubbing, 2. Patrol Scrubbing, 3. Permanent Fault Detection (PFD) |
| **Gniazda PCI** | Minimum 8 slotów PCIe x8 generacji 4 |
| **Interfejsy sieciowe/** | Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 10/25Gb SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) obsadzone wkładkami |
| **Kontroler SAS HBA** | Zainstalowana 4 portowa karta SAS HBA umożliwiająca podłączenie oferowanej macierzy |
| **Dyski twarde** | 1. Zainstalowane 2 dyski M.2 NVMe SSDs o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1. |
| **Wbudowane porty** | 3 x USB z czego nie mniej niż 1x USB 3.0, 2xVGA z czego jeden na panelu przednim. |
| **Video** | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920 x 1200 |
| **Zasilacze** | Redundantne, Hot-Plug min. 1100W każdy. Klasy Titanium |
| **Bezpieczeństwo** | 1. Zatrzask górnej pokrywy oraz blokada na ramce panela frontowego zamykane na klucz w celu do ochrony nieautoryzowanego dostępu do dysków twardych i wewnętrznych elementów serwera. 2. Możliwość wyłączenia w BIOS funkcji przycisku zasilania. 3. BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła 4. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. 5. Moduł TPM 2.0 6. Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera. 7. Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem. 8. Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust). |
| **Diagnostyka** | Serwer musi być wyposażony w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze. |
| **Karta Zarządzania** | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:   1. zdalny dostęp do graficznego interfejsu Web karty zarządzającej; 2. zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); 3. szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; 4. wsparcie dla IPv6; 5. wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; 6. możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; 7. integracja z Active Directory; 8. wsparcie dla dynamic DNS; 9. wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. 10. możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera 11. możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera |
| **Certyfikaty** | Serwer musi być wyprodukowany zgodnie z normą ISO-9001, ISO-14001, ISO-50001 - **dołączyć do oferty jako przedmiotowy środek dowodowy**.  Serwer musi posiadać deklarację CE - **dołączyć do oferty jako przedmiotowy środek dowodowy**. |
| **System operacyjny** | Zamawiający wymaga dostarczenia oprogramowania systemowego w najnowszej aktualnej wersji, nieograniczonej czasowo. Licencja musi uprawniać do uruchamiania oprogramowania systemowego (dalej: SSO) w postaci **nielimitowanej** wirtualnych środowisk SSO za pomocą wbudowanych mechanizmów wirtualizacji.  Dostarczona licencja musi być kompatybilna z dostarczonym serwerem oraz musi być zgodna z prawami licencyjnymi producenta.  SSO musi posiadać następujące, wbudowane cechy:   1. możliwość wykorzystania, co najmniej 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 min. 64TB przez każdy wirtualny serwerowy system operacyjny, 3. możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania min. 8000 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: 10. pozwalają na zmianę rozmiaru w czasie pracy systemu, 11. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, 12. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, 13. umożliwiają zdefiniowanie list kontroli dostępu (ACL), 14. wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość, 15. wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających min. certyfikat FIPS 140-2 16. możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET, 17. możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów, 18. wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych, 19. graficzny interfejs użytkownika, 20. zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, 21. wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play), 22. możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu, 23. dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa, 24. możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: 25. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, 26. 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 SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,     * ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,     * odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza, 27. zdalna dystrybucja oprogramowania na stacje robocze, 28. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej, 29. 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, 30. szyfrowanie plików i folderów, 31. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec), 32. możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów, 33. serwis udostępniania stron WWW, 34. wsparcie dla protokołu IP w wersji 6 (IPv6), 35. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 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 model), 36. możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet, 37. wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath), 38. możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego, 39. mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty, 40. możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. |
| **Licencje dostępowe** | Na cały KLASTER należy dostarczyć 70 licencji dostępowych na użytkownika tzw. USER CAL |
| **System bazodanowy** | System bazodanowy (SBD) 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,  8. 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.  9. 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.  10. 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.  11. 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.  12. 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).  13. 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.  14. 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.  15. 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.  16. 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.).  17. 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.  18. 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.  19. 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.  20. Raportowanie zależności między obiektami - SBD musi udostępniać informacje o wzajemnych zależnościach między obiektami bazy danych.  21. 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.  22. 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.  23. 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.  24. 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).  25. 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).  26. Wbudowany system analityczny musi posiadać narzędzie do rejestracji i śledzenia zapytań wykonywanych do baz analitycznych.  27. Wbudowany system analityczny musi obsługiwać wielojęzyczność (tworzenie obiektów wielowymiarowych w wielu językach – w zależności od ustawień na komputerze klienta).  28. 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.  29. 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.  30. 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.  31. Środowisko raportowania powinno być osadzone i administrowane z wykorzystaniem mechanizmu Web Serwisów (Web Services).  32. 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.  33. 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.  34. SBD musi umożliwiać wysyłkę raportów drogą mailową w wybranym formacie (subskrypcja).  35. Wbudowany system raportowania musi posiadać rozszerzalną architekturę oraz otwarte interfejsy do osadzania raportów oraz do integrowania rozwiązania z różnorodnymi środowiskami IT.  36. 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.  37. 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.  38. W celu zwiększenia bezpieczeństwa i niezawodności system bazy danych musi udostępniać komendę pozwalającą użytkownikowi na utrwalenie na dysku wszystkich zatwierdzonych asynchronicznych transakcji (lazy commit).  Licencja ma umożliwiać pracę na oferowanym klastrze serwerów z możliwością przenoszenia maszyny VM z systemem bazodanowym (SBD) w dowolnym momencie pomiędzy fizycznymi hostami klastra  Wraz z systemem bazodanowym (SBD) należy dostarczyć 15 licencji dostępowych na użytkownika tzw. USER CAL |
| **Warunki gwarancji** | 1. Gwarancja producenta. 2. Okres gwarancji zgodny z ofertą Wykonawcy lecz nie krótszy niż 24 miesiące, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. 3. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. 4. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. 5. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. 6. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta. 7. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. 8. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. 9. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji urządzenia. 10. Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. 11. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. 12. Firma serwisująca musi posiadać ISO 9001 oraz ISO-27001 na świadczenie usług serwisowych – dokumenty potwierdzające należy załączyć do oferty. 13. Wskazana firma serwisująca musi posiadać autoryzacje producenta urządzeń – na potwierdzenie należy załączyć ogólnodostępny dokument np. certyfikat lub deklaracją producenta, potwierdzającą autoryzację dla wskazanej firmy serwisującej do świadczenia usług serwisowych w imieniu producenta urządzenia. W przypadku gdy dany producent nie posiada takiego ogólnodostępnego dokumentu, Zamawiający dopuszcza Oświadczenie Producenta ze wskazaniem firm(y) serwisującej świadczącej usługi serwisowe dla jej urządzeń na terenie Polski – dokumenty potwierdzające należy załączyć do oferty.   Wymagane dokumenty i oświadczenia dołączyć do oferty jako przedmiotowy środek dowodowy |

## Macierz

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla sprzętu** |
| Typ obudowy | Macierz musi być przystosowana do montażu w szafie rack 19”, w oferowanej konfiguracji o wysokość maksymalnie 2U. |
| Przestrzeń dyskowa | Zainstalowane:60TB przestrzeni RAW opartej o dyski pojemności nie mniejszej niż 3,84TB SSD oraz zapewnić 1 dysk dodatkowo działający jako tzw, HotSpare |
| Możliwość rozbudowy | Macierz musi obsługiwać (bez wymiany kontrolerów macierzy), co najmniej 264 dyski twarde. |
| Obsługa dysków | 1. Macierz musi mieć możliwość obsługiwania dysków SSD, SAS i Nearline SAS. 2. Macierz musi umożliwiać mieszanie napędów dyskowych SSD, SAS i NL SAS w obrębie pojedynczej półki dyskowej. Macierz musi obsługiwać dyski 2,5” jak również 3,5”. |
| Sposób zabezpieczenia danych | 1. Macierz musi obsługiwać mechanizmy RAID zgodne z RAID0, RAID1, RAID10, RAID5, RAID6 oraz RAID z tzw. rozproszoną wolną pojemnością, realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków (tzw. wide-striping). 2. Macierz musi umożliwiać definiowanie globalnych dysków spare oraz dedykowanie dysków spare do konkretnych grup RAID. 3. Macierz musi również oferować możliwość zdefiniowania grup dyskowych z tzw. rozproszoną wolną pojemnością, która nie wykorzystuje tradycyjnych dysków zapasowych (integracja dysków zapasowych i nieaktywnych do zwiększenia dostępności i wydajności macierzy, zwiększenie szybkości odbudowy macierzy na wypadek awarii dysku). 4. Macierz musi umożliwiać obsługę dysków różnej pojemności w ramach grupy dysków. |
| Tryb pracy kontrolerów macierzowych | 1. Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe. 2. Wszystkie kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów. |
| Pamięć cache | 1. Macierz musi posiadać minimum sumarycznie 32 GB pamięci cache. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM. 2. Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi. 3. Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania bateryjnego lub z zastosowaniem innej technologii przez okres minimum 5 lat. |
| Rozbudowa pamięci cache | 1. Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 8 TB z wykorzystaniem dysków SSD lub kart pamięci flash. 2. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z rozwiązaniem. |
| Interfejsy | Macierz musi posiadać, co najmniej 8 portów 12Gb SAS (4 porty na kontroler), |
| Zarządzanie | 1. Zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego. 2. Zarządzanie macierzą musi odbywać się bezpośrednio na kontrolerach macierzy z poziomu przeglądarki internetowej. |
| Zarządzanie grupami dyskowymi oraz dyskami logicznymi | 1. Macierz musi umożliwiać zdefiniowanie, co najmniej 500 wolumenów logicznych w ramach oferowanej macierzy dyskowej. 2. Musi istnieć możliwość rozłożenia pojedynczego wolumenu logicznego na wszystkie dyski fizyczne macierzy (tzw. wide-striping), bez konieczności łączenia wielu różnych dysków logicznych w jeden większy. 3. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. |
| Thin Provisioning | 1. Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning. 2. Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych (wymagana obsługa standardu T10 SCSI UNMAP). 3. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. |
| Tiering | 1. Macierz musi posiadać funkcjonalność Tiering między dyskami SSD i SAS i między dyskami SAS i NL SAS. 2. Tiering musi obejmować wszystkie woluminy w danej puli dyskowej. 3. Dyski SSD mogą być wykorzystane zarówno do uzyskania pojemności w warstwie wydajności lub na potrzeby zwiększenia pamięci podręcznej odczytu w celu przyspieszenia operacji losowego odczytu z jednej lub wielu warstw napędów mechanicznych. |
| Wewnętrzne kopie migawkowe | 1. Macierz musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. 2. Kopia migawkowa wykonuje się bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii. 3. Macierz musi wspierać minimum 1012 kopii migawkowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. |
| Wewnętrzne kopie pełne | 1. Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. 2. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. |
| Migracja danych w obrębie macierzy | 1. Macierz dyskowa musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych (ang. Sub-LUN). Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. 2. Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na min. 3 typach dysków obsługiwanych przez macierz, a jego części będą realokowane na podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności dostarczanego urządzenia. |
| Zdalna replikacja danych | 1. Macierz musi umożliwiać asynchroniczną replikację danych do innej macierzy z tej samej rodziny. Replikacja musi być wykonywana na poziomie kontrolerów, bez użycia dodatkowych serwerów lub innych urządzeń i bez obciążania serwerów podłączonych do macierzy. 2. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z urządzeniem. |
| Podłączanie zewnętrznych systemów operacyjnych | 1. Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami). 2. Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, RHEL, SLES, Vmware, Citrix. 3. Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Dopuszcza się rozwiązania bazujące na natywnych możliwościach systemów operacyjnych. 4. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów obsługiwanych przez oferowane urządzenie. |
| Redundancja | 1. Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów. 2. Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap”, a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory. 3. Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy. |
| Dodatkowe wymagania | 1. Oferowany system dyskowy musi się składać z pojedynczej macierzy dyskowej. Niedopuszczalna jest realizacja zamówienia poprzez dostarczenie wielu macierzy dyskowych. 2. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych (par kontrolerów macierzowych) połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN czy wirtualizatorem macierzy dyskowych. 3. Możliwość ograniczania poboru zasilania przez dyski, które nie obsługują operacji we/wy, poprzez ich zatrzymanie. |
| Warunki gwarancji | 1. Gwarancja producenta. 2. Okres gwarancji zgodny z ofertą Wykonawcy lecz nie krótszy niż 24 miesiące, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. 3. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. 4. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. 5. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. 6. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta. 7. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. 8. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. 9. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji urządzenia. 10. Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. 11. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. 12. Firma serwisująca musi posiadać ISO 9001 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. 13. Wskazana firma serwisująca musi posiadać autoryzacje producenta urządzeń – na potwierdzenie należy załączyć ogólnodostępny dokument np. certyfikat lub deklaracją producenta, potwierdzającą autoryzację dla wskazanej firmy serwisującej do świadczenia usług serwisowych w imieniu producenta urządzenia. W przypadku gdy dany producent nie posiada takiego ogólnodostępnego dokumentu, Zamawiający dopuszcza Oświadczenie Producenta ze wskazaniem firm(y) serwisującej świadczącej usługi serwisowe dla jej urządzeń na terenie Polski – dokumenty potwierdzające należy załączyć do oferty.   Wymagane dokumenty i oświadczenia dołączyć do oferty jako przedmiotowy środek dowodowy |

# System do archiwizacji danych z deduplikacją

|  |  |
| --- | --- |
| Wymagania minimalne | |
| Urządzenie musi być przeznaczone do deduplikacji i przechowywania kopii zapasowych. Urządzenie musi spełniać wymagania wyspecyfikowane w niniejszej tabeli. | |
| Dostarczone urządzenie musi oferować przestrzeń min. 24 TB netto (powierzchni użytkowej) bez uwzględniania mechanizmów protekcji. | |
| Dostarczone urządzenie powinno umożliwiać rozbudowę o warstwę typu CLOUD dedykowaną do długotrwałego przechowywania danych (tzw. Long Term Retention) – dane o określonej retencji (zgodnie z założoną polityka retencyjną), bez pośrednictwa dodatkowych urządzeń (typu GATEWAY) powinny zostać przemigrowane (w postaci zdeduplikowanej) na dodatkową warstwę, wymagane wsparcie dla AWS oraz Microsoft Azure. Wymagana enkrypcja danych przechowywanych na warstwie typu Cloud. Wymagane dostarczenie licencji na przestrzeń min. 64TB netto dla warstwy CLOUD. | |
| 1.      Oferowane urządzenie musi posiadać minimum 4 porty 10GB SFP+ obsadzone wkładkami 10Gb SR MM  2.      wymagana możliwość obsługi każdym z w/w portów protokołów CIFS, NFS, deduplikacja na źródle. | |
| Oferowane urządzenie musi umożliwiać jednoczesny dostęp wszystkimi poniższymi protokołami:  1.      CIFS, NFS  2.      zapewniającym deduplikację na źródle, wymagane wsparcie dla eksploatowanej przez Zamawiającego aplikacji Veeam Backup and Replication  3.      VTL (min. 10 jednocześnie) | |
| Wymagane jest dostarczenie licencji, pozwalającej na jednoczesną obsługę protokołów CIFS, NFS, dedupliakacja na źródle, VTL do oferowanej pojemności urządzenia | |
| Oferowane pojedyncze urządzenie musi osiągać zagregowaną wydajność (dla maksymalnej konfiguracji) protokołami: NFS   co najmniej 10 TB/h (dane podawane przez producenta) oraz co najmniej 20 TB/h z wykorzystaniem deduplikacji na źródle (dane podawane przez producenta). | |
| 1.      Urządzenie musi pozwalać na jednoczesną obsługę minimum 250 strumieni w tym jednocześnie:  a.      zapis danych minimum 150 strumieniami  b.      odczyt danych minimum 50 strumieniami  c.      replikacja minimum 50 strumieniami  pochodzących z różnych aplikacji oraz dowolnych protokołów (CIFS, NFS, VTL, deduplikacja na źródle) oraz dowolnych interfejsów (FC, LAN) w tym samym czasie.  2.      Wymienione wartości 250 jednoczesnych strumieni dla wszystkich protokołów (czyli jednocześnie 150 dla zapisu i jednocześnie 50 strumieni dla odczytu i jednocześnie 50 strumieni dla replikacji) musi mieścić w przedziale oficjalnie rekomendowanym i wspieranym przez producenta urządzenia.  3.      Wszystkie zapisywane strumienie muszą podlegać globalnej deduplikacji przed zapisem na dysk (in-line) jak opisano w niniejszej specyfikacji. | |
| Oferowane urządzenie musi mieć możliwość emulacji następujących bibliotek taśmowych:  1.      StorageTek L180  lub  2.      IBM TS 3500 | |
| Oferowane urządzenie musi mieć możliwość emulacji napędów taśmowych min. LTO5 oraz LTO7 | |
| Urządzenie musi umożliwiać (w przypadku VTL’a) emulację minimum 250 napędów, emulację min. 30 000 slotów w przypadku poj. biblioteki taśmowej oraz emulację sumarycznie min.  60 000 slotów. | |
| Oferowane urządzenie musi deduplikować dane in-line przed zapisem na nośnik dyskowy. Na wewnętrznych dyskach urządzenia nie mogą być zapisywane dane w oryginalnej postaci (niezdeduplikowanej) z jakiegokolwiek fragmentu strumienia danych przychodzącego do urządzenia. | |
| 1.      Technologia deduplikacji musi wykorzystywać algorytm bazujący na zmiennym, dynamicznym bloku jednak o wielkości nie większej niż 12 kB.  2.      Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych co oznacza, że urządzenie musi dzielić otrzymany pojedynczy strumień danych na bloki o różnej długości, bez konieczności podejmowania czynności mających na celu ustalenie predefiniowanej długości bloków używanych do deduplikacji danych określonego typu.  3.      Deduplikacja zmiennym, dynamicznym blokiem oznacza, że wielkość każdego bloku (na jaki są dzielone dane pojedynczego strumienia backupowego) może być inna niż poprzedniego oraz jest indywidualnie ustalana przez algorytm deduplikacji zastosowany w urządzeniu, oferowane urządzenie nie może dzielić jakiegokolwiek pojedynczego strumienia danych backupowych na bloki o ustalonej, tej samej długości. | |
| 1.      Oferowany produkt musi posiadać obsługę mechanizmów globalnej deduplikacji dla danych otrzymywanych jednocześnie wszystkimi protokołami (CIFS, NFS, VTL, deduplikacja na źródle) przechowywanych w obrębie całego urządzenia co oznacza, że przechowywany na urządzeniu fragment danych nie może być ponownie zapisany bez względu na to, jakim protokołem zostanie ponownie otrzymany.  2.      Wszystkie emulowane jednocześnie w obrębie urządzenia biblioteki wirtualne (VTL) oraz udziały NFS/CIFS również powinny podlegać globalnej deduplikacji – blok danych otrzymany i zapisany w wirtualnej bibliotece „A”, nie może zostać ponownie zapisany, jeśli trafi do innej wirtualnej biblioteki „B” w obrębie tego samego urządzenia (to samo dotyczy udziałów NFS/CIFS). Przestrzeń składowania zdeduplikowanych danych musi być jedna dla wszystkich protokołów dostępowych, co oznacza zastosowanie pojedynczej bazy deduplikatów bez względu na ilość/rodzaj używanych jednocześnie protokołów dostępowych. | |
| 1.      Proces deduplikacji musi odbywać się in-line – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy.  2.      Zapisowi na system dyskowy muszą podlegać tylko unikalne bloki danych nie zapisane jeszcze na system dyskowy urządzenia. Dotyczy to każdego fragmentu przychodzących do urządzenia danych.  3.      Wymaganie nie będzie spełnione, jeżeli deduplikacja in-line realizowana będzie przez zewnętrzną aplikację backup’ową. Wymaganie deduplikacji in-line dotyczy zapisu danych przez każdy z wymaganych intefejsów, w przypadku interfejsów: NFS, CIFS oraz VTL realizacja deduplikacji in-line nie może w żadnym stopniu zależeć od konkretnej aplikacji backu’owej, dane zapisywane poprzez interfejsy NFS CIFS bez użycia jakiejkolwiek aplikacji backup’owej również muszą być deduplikowane w sposób in-line | |
| Proponowane rozwiązanie nie może w żadnej fazie korzystać (w całości lub częściowo) z bufora na składowanie danych w postaci oryginalnej (niezdeduplikowanej) w celu ich późniejszej deduplikacji (wymagana deduplikacja in-line) | |
| Wszystkie unikalne bloki przed zapisaniem na dysk muszą być dodatkowo kompresowane. | |
| Tryb zapisu zabezpieczanych danych nie może umożliwiać nadpisywania danych, dane mogą być zapisywane jedynie w trybie append-only, dane, dla których wygasła retencja powinny zostać usunięte podczas procesu czyszczenia tzw. Cleaning, wymaganie dotyczy wszystkich danych zapisanych na urządzeniu a nie wybranych grup danych objętych działaniem blokad zabezpieczających przed usunięciem/modyfikacją danych. | |
| 1.      Oferowane urządzenie musi wspierać (wymagane formalne wsparcie producenta urządzenia), co najmniej następujące aplikacje: Veeam Backup and Replication, RMAN, Microsoft SQL Server Management Studio.  2.      W przypadku współpracy z każdą z poniższych aplikacji:  a.      Veeam Backup and Replication  b.      RMAN (dla ORACLE)  c.      Microsoft SQL Server Management Studio (dla Microsoft SQL)  3.      Urządzenie musi umożliwiać deduplikację na źródle i przesłanie nowych, nie znajdujących się jeszcze na urządzeniu bloków poprzez sieć LAN.  4.      Deduplikacja w wyżej wymienionych przypadkach musi zapewniać, aby z zabezpieczanych serwerów do urządzenia były transmitowane poprzez sieć LAN jedynie fragmenty danych nie znajdujące się dotychczas na urządzeniu. | |
| 1.      W przypadku przyjmowania backupów z Veeam Backup and Replication, Oracle RMAN oraz Microsoft MSSQL (przy wykorzystaniu Microsoft SQL Server Management Studio), urządzenie musi umożliwiać deduplikację na źródle i przesłanie nowych, nieznajdujących się jeszcze na urządzeniu bloków poprzez sieć FC.  2.      Deduplikacja w wyżej wymienionych przypadkach musi zapewniać, aby z serwerów do urządzenia były transmitowane poprzez sieć FC tylko fragmenty danych nie znajdujące się dotychczas na urządzeniu. | |
| Oferowane urządzenie powinno umożliwiać uruchamianie maszyn wirtualnych VMware bezpośrednio z danych backupowych bez konieczności odtwarzania danych. | |
| Wymagana funkcjonalność Load Balancing oraz Link Failover w obrębie portów wykorzystywanych przez aplikację backupową. | |
| Wymagane wsparcie dla backupów typu Virtual Synthetics. | |
| W przypadku deduplikacji na źródle poprzez sieć IP (LAN oraz WAN), wymagana możliwość szyfrowania komunikacji kluczem minimum 256 bitów. | |
| Urządzenie powinno umożliwiać zaszyfrowanie przechowywanych danych, wymagane licencje umożliwiające zaszyfrowanie i przechowywanie zaszyfrowanych danych w obrębie maksymalnej pojemności oferowanego urządzenia. | |
| Urządzenie musi wspierać deduplikację na źródle poprzez sieć FC (SAN) minimum dla następujących systemów operacyjnych:  1.      Windows  2.      Linux (RedHat, SuSE) | |
| 1.      Oferowane urządzenie musi umożliwiać bezpośrednią replikację danych do drugiego urządzenia takiego samego typu. Konfiguracja replikacji musi być możliwa w każdym z trybów:  a.      jeden do jednego  b.      wiele do jednego  c.      jeden do wielu  d.      kaskadowej (urządzenie A replikuje dane do urządznia B, które te same dane replikuje do urządzenia C).  2.      Replikacja musi się odbywać w trybie asynchronicznym. Transmitowane mogą być tylko te fragmenty danych (bloki) które nie znajdują się na docelowym urządzeniu. Ewentualna licencja na replikację nie jest przedmiotem postępowania. | |
| Urządzenie musi umożliwiać wydzielenie określonych portów Ethernet dedykowanych do replikacji. | |
| W przypadku wykorzystania portów Ethernet do replikacji urządzenie musi umożliwiać przyjmowanie backupów, odtwarzanie danych, przyjmowanie strumienia replikacji, wysyłanie strumienia replikacji tymi samymi portami. | |
| W przypadku replikacji danych między dwoma urządzeniami oferowanego typu, wymagana możliwość kontroli przez: Microsoft SQL Server Management Studio, muszą być możliwe do uzyskania jednocześnie wszystkie następujące funkcjonalności:  1.      replikacja odbywa się bezpośrednio między dwoma urządzeniami bez udziału serwerów pośredniczących  2.      replikacji podlegają tylko te fragmenty danych (na poziomie bloków używanych do deduplikacji), które nie znajdują się na docelowym urządzeniu  3.      replikacja zarządzana jest z poziomu wymaganej aplikacji  4.      aplikacja posiada informację o obydwu kopiach zapasowych znajdujących się w obydwu urządzeniach bez konieczności przeprowadzania procesu inwentaryzacji | |
| Oferowane urządzenie musi działać poprawnie przy zapełnieniu danymi na poziomie co najmniej 90%. Dokumentacja urządzenia nie może wskazywać na ew. problemy, obostrzenia, które są efektem zapełnieniu urządzenia zabezpieczanymi danymi, na poziomie mniejszym niż 90%. | |
| Wymagana możliwość ograniczenia pasma używanego do replikacji między dwoma urządzeniami – oferowane urządzenie powinno być wyposażone w mechanizm umożliwiający zarządzaniem stopnia wykorzystania pasma na potrzeby replikacji. | |
| Zdeduplikowane i skompresowane dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID 6 bądź równoważnej. | |
| 1.      Oferowane urządzenie musi pozwalać na realizację oraz przechowywanie SnapShot’ów, czyli umożliwiać zamrożenie obrazu danych (stanu backupów) w urządzeniu na określoną chwilę. Oferowane urządzenie musi również umożliwiać odtworzenie danych ze Snapshot’u.  2.      Odtworzenie danych ze Snapshot’u nie może wymagać konieczności nadpisania danych produkcyjnych jak również nie może oznaczać przerwy w normalnej pracy urządzenia (przyjmowania/odtwarzania backupów). | |
| Urządzenie musi pozwalać na przechowywanie minimum 500 Snapshotów jednocześnie w obrębie oferowanej przestrzeni, przy zachowaniu globalnej deduplikacji oraz standardowego trybu pracy urządzenia – umożliwiającego wykorzystanie wszystkich dostępnych funkcjonalności. | |
| Urządzenie musi umożliwiać podział na logiczne części. Dane znajdujące się w każdej logicznej części muszą być między sobą deduplikowane (globalna deduplikacja między logicznymi częściami urządzenia). | |
| Urządzenie musi mieć możliwość podziału na minimum 10 logicznych części pracujących równolegle. Producent musi oficjalnie wspierać pracę minimum 10 logicznych części pracujących równolegle z pełną wydajnością urządzenia. | |
| Dla każdej z w/w logicznych części oferowanego urządzenia musi być możliwość zdefiniowania oddzielnego użytkownika zarządzającego daną logiczną częścią deduplikatora. Użytkownicy zarządzający logiczną częścią A muszą widzieć tylko i wyłącznie zasoby logicznej części A i nie mogą widzieć żadnych innych zasobów oferowanego urządzenia. | |
| Wymagana możliwość zaprezentowania każdej z logicznych części oferowanego urządzenia jako niezależnego urządzenia dostępnego za pośrednictwem:  1.      CIFS  2.      NFS  3.      VTL  4.      deduplikacja na źródle | |
| 1.      Urządzenie musi umożliwiać zdefiniowanie blokady skasowania danych (funkcjonalność WORM). Blokada skasowania danych musi chronić plik w zdefiniowanym czasie przed usunięciem pliku, modyfikacją pliku.  2.      Blokada skasowania danych musi działać w dwóch trybach (do wyboru przez administratora):  a.      Możliwość zdjęcia blokady przed upływem ważności danych  b.      Brak możliwości zdjęcia blokady przed upływem ważności danych (COMPLIANCE), w tym wypadku wymagane wsparcie norm SEC 17a-4(f) lub ISO Standard 15489-1 w zakresie ochrony danych  3.      Licencje na blokadę usunięcia/zmiany przechowywanych plików muszą być dostarczone wraz z urządzeniem.  4.      Wymagana możliwość automatycznego uruchamiania blokady (podczas zapisu) WORM dla danych zapisywanych na obszar objęty działaniem wspomnianej blokady. W każdym przypadku wymagana również możliwość używania blokady WORM dla obrazu danych uzyskanych poprzez użycie wymaganej funkcjonalności SnapShot. Zamawiający zastrzega możliwość prośby o dostarczenie ogólnodostępnej dokumentacji oferowanego produktu potwierdzającego spełnienie wymaganej funkcjonalności). | |
| Urządzenie musi mieć możliwość przechowywania danych niezmienialnych:  1.      video  2.      grafika  3.      nagrania dźwiękowe  4.      pliki pdf  na udziałach CIFS/NFS. | |
| 1.      Urządzenie musi weryfikować dane po zapisie (nie chodzi o ew. weryfikację danych indeksowych generowanych przez urządzenie, ale o weryfikację wszystkich zabezpieczanych danych backup’owych). Każda zapisana na dyskach porcja danych musi być odczytana i porównana z danymi otrzymanymi przez urządzenie. Powyższa weryfikacja powinna być realizowana w locie, czyli przed usunięciem z pamięci oryginalnych danych (otrzymanych z aplikacji backupowej), musi być realizowana w trybie ciągłym (a nie ad-hoc), wymagane parametry wydajnościowe urzadzenia muszą uwzględniać tę funkcjonalność.  2.      Wymagane potwierdzenie opisanej funkcjonalności w oficjalnej dokumentacji producenta oferowanego urządzenia.  Zamawiający zastrzega możliwość prośby o dostarczenie ogólnodostępnej dokumentacji oferowanego produktu potwierdzającego spełnienie wymaganej funkcjonalności). | |
| Urządzenie musi automatycznie usuwać przeterminowane dane (bloki danych nie należące do backupów o aktualnej retencji) w procesie czyszczenia. | |
| Proces usuwania przeterminowanych danych (czyszczenia) nie może uniemożliwiać pracy procesów backupu / odtwarzania danych (zapisu / odczytu danych z zewnątrz do systemu). | |
| Wymagana możliwość zdefiniowania maksymalnego obciążenia urządzenia procesem usuwania przeterminowanych danych (poziomu obciążenia procesora), wymagane potwierdzenie w ogólno dostępnej dokumentacji. Zamawiający zastrzega możliwość prośby o dostarczenie ogólnodostępnej dokumentacji oferowanego produktu potwierdzającego spełnienie wymaganej funkcjonalności) | |
| Wymagana możliwość zdefiniowania harmonogramu wg. którego wykonywany jest proces usuwania przeterminowanych danych (czyszczenia), realizowany równolegle z procesami backup/restore/replication. | |
| Standardowa częstotliwość usuwania przeterminowanych danych (czyszczenie) nie powinna być większa niż 1 raz na tydzień - minimalizując czas w którym backupy/odtworzenia narażone są na spowolnienie (weryfikacja wymagania na podstawie dokumentacji typu DOBRE PRAKTYKI publikowanej przez producenta). | |
| Urządzenie musi umożliwiać systemowo (wbudowana funkcjonalność) - realizację procesu pierwszego czyszczenia dopiero po przekroczeniu 75% zajętości oferowanej przestrzeni. | |
| Urządzenie musi mieć możliwość zarządzania poprzez  1.      Interfejs graficzny dostępny z przeglądarki internetowej  2.      Poprzez linię komend (CLI) dostępną z poziomu ssh (secure shell) | |
| Oprogramowanie do zarządzania musi rezydować na oferowanym na urządzeniu deduplikacyjnym. | |
| Oferowane urządzenie musi mieć możliwość sprawdzenia pakietu upgrade’ującego firmware urządzenia (GUI lub CLI), to znaczy sprawdzenia czy nowa wersja systemu nie spowoduje problemów z urządzeniem. | |
| Urządzenie musi być rozwiązaniem kompletnym, appliancem sprzętowym pochodzącym od jednego producenta. Zamawiający nie dopuszcza stosowania rozwiązań typu gateway. Oferowany typ urządzenia musi być oficjalnie dostępne w ofercie producenta przed ukazaniem się niniejszego postępowania. | |
| 1. Gwarancja producenta. 2. Okres gwarancji zgodny z ofertą Wykonawcy lecz nie krótszy niż 24 miesiące, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. 3. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. 4. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. 5. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. 6. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy. 7. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta. 8. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. 9. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. 10. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji urządzenia. 11. Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. 12. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. 13. Firma serwisująca musi posiadać ISO 9001 oraz ISO-27001 na świadczenie usług serwisowych – dokumenty potwierdzające należy załączyć do oferty. 14. Wskazana firma serwisująca musi posiadać autoryzacje producenta urządzeń – na potwierdzenie należy załączyć ogólnodostępny dokument np. certyfikat lub deklaracją producenta, potwierdzającą autoryzację dla wskazanej firmy serwisującej do świadczenia usług serwisowych w imieniu producenta urządzenia. W przypadku gdy dany producent nie posiada takiego ogólnodostępnego dokumentu, Zamawiający dopuszcza Oświadczenie Producenta ze wskazaniem firm(y) serwisującej świadczącej usługi serwisowe dla jej urządzeń na terenie Polski – dokumenty potwierdzające należy załączyć do oferty.   Wymagane dokumenty i oświadczenia dołączyć do oferty jako przedmiotowy środek dowodowy | |
| Wymagania minimalne Oprogramowania do backupu | |
| **Nazwa** | **Minimalne wymagania dla oprogramowania backupowego** |
| Wymagania ogólne | 1. Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 6.x, 7.x i 8.0 oraz Microsoft Hyper-V 2016, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej 2. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS, obiektowych pamięci masowych kompatybilnych z Microsoft Azure, AWS S3 i urządzeń kompatybilnych z protokołem S3 oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux. |
| Funkcjonalności | 1. Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej 2. Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków 3. 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 4. 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. 5. Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli. 6. Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier. 7. Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu. 8. Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania 9. Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time) 10. Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu 11. Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API 12. Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji 13. 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 14. Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania 15. Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych. 16. Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej 17. Oprogramowanie musi wymagać autoryzacji dwuch administratorów backupu do wykonania krytycznych operacji (np skasowanie backupu, dodanie kolejnego administratora) 18. Oprogramowanie musi posiadać integracje z systemami zarządania kluczami szyfrującymi (KMS) 19. Oprogramowanie musi posiadać integracje z systemami typu SIEM 20. Oprogramowanie musi posiadać asystenta produktu opartego o AI, pozwalającego na przeszukiwanie dokumentacji technicznej. Powinna istnieć możliwość wyłączenia tej opcji. |
| Wymagania RPO | 1. Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej 2. Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych. 3. 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 z dokładnością do pojedynczego datastoru 4. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware. 5. Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware. 6. Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy (LTO oraz IBM 3592). 7. Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son) 8. Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard. 9. 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. 10. Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN. 11. 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. 12. Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO. 13. Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik 14. Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding) 15. Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN) |
| Wymagania RTO | 1. 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, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage’u użytego do przechowywania kopii zapasowych. 2. Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna) 3. 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 4. Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre 5. Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL, Oracle i PostgreSQL bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne. 6. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków 7. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform. 8. Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień 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 9. Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V. 10. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell 11. Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM 12. Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej. 13. Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA, elementów AD Sites oraz pozwalać na odtworzenie haseł. 14. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2013SP1 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego. 15. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur. 16. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2013 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji. 17. 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. 18. Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux. 19. Oprogramowanie musi wspierać granularne odtwarzanie baz danych SAP HANA do oryginalnej lub innej lokalizacji 20. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN 21. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle 22. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI 23. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez IBM Db2 24. Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN |
| Ograniczenie ryzyka | 1. Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna) 2. Dla VMware’a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach. 3. 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 4. Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. 5. Oprogramowanie musi analizować indeksy systemów plików zabezpieczanych maszyn w poszukiwaniu rozszerzeń, notatek żądania okupu oraz innych oznak obecności ransomware/malware 6. Oprogramowanie musi mieć możliwość skanowania plików backupu przy pomocy znanych sygnatur złośliwego oprogramowania 7. Oprogramowanie, bazując na wyuczonynym modelu maszynowym (machine learning) musi w locie wykrywać oznaki złośliwego oprogramowania (malware, ransomware) oraz cyberataków 8. Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego. |
| Środowiska fizyczne | 1. Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego 2. Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych 3. Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE 4. Rozwiązanie musi wspierać system operacyjny macOS 5. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix 6. Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą) 7. Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster 8. Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów 9. Rozwiązanie musi wspierać backup podłączonych dysków USB 10. Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym 11. Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury) 12. Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone 13. Rozwiązanie musi wspierać kontrolę pasma sieciowego 14. Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych 15. Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN 16. Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft 17. Rozwiązanie musi wspierać technologię BitLocker 18. Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania 19. Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla Microsoft Exchange 2013SP1 i nowszych, Microsoft Active Directory 2008 i nowszych, Microsoft Sharepoint 2013 i nowszych, Microsoft SQL 2008 i nowszych, Oracle 11g i nowszych oraz PostgreSQL 12 i nowszych 20. Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych 21. Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL, Oracle I PostgreSQL poprzez bezpośrednie uruchomienie ich z pliku backupu. 22. Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere, Hyper-V, Nutanix AHV, Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform 23. Rozwiązanie musi wspierać szyfrowanie 24. Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne 25. Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego 26. Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej 27. Rozwiązanie musi wspierać tworzenie wielu zadań backupowych |
| Monitoring | 1. System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich 2. System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie 3. System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 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. 4. System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter 5. System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn 6. System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel 7. System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk 8. System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora 9. System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów 10. System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard) 11. System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna 12. System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego 13. System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta 14. System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych. 15. 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. 16. System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware |
| Raportowanie | 1. System musi umożliwiać raportowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie 2. System musi umożliwiać raportowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 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. 3. System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów. 4. System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V 5. System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF 6. System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc 7. System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach 8. System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów 9. System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych 10. System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych 11. System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury 12. System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta 13. System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych. 14. System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach ‘what-if’. 15. System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware 16. System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots) 17. System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie |
| Wsparcie techniczne i aktualizacyjne | Powyższe funkcjonalność mają działać w środowisku wirtualnym i/lub fizycznym.  Wymagane jest dostarczenie licencji dla zabezpieczenie minimum **10** sztuk wirtualnych lub fizycznych serwerów.  Wraz z oprogramowanie wymagane jest dostarczenie wsparcia technicznego i aktualizacyjnego producenta oprogramowania na okres **60 miesięcy**. |

# Biblioteka taśmowa

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla sprzętu** |
| **Obudowa i pojemność** | 1. Wysokość maksymalnie 1U do instalacji w szafie Rack. 2. Co najmniej 8 slotów przeznaczonych na zestaw taśm. |
| **Połączenie** | Co najmniej 1 port SAS o przepustowości co najmniej 12Gb/s w standardzie umożliwiającym podłączenie do serwera backupu |
| **Napęd** | 1. Wyposażony w co najmniej 1 sztukę napędu SAS LTO-8. 2. Kabel SAS o długości min 2m |
| **Nośniki LTO** | Wraz z biblioteką należy dostarczyć:   1. 10 sztuk nośników (taśm) LTO-8 2. 1 sztukę nośnika (taśmy) czyszczącej |
| **Warunki gwarancji** | 1. Okres gwarancji zgodny z ofertą wykonawcy lecz nie krótszy niż 24 miesięcy gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, 2. Uszkodzone nośniki pozostają własnością Zamawiającego 3. Okres gwarancji, wsparcia technicznego i aktualizacyjnego producenta zgodnie ze złożoną ofertą |

# UPS Rack

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla sprzętu** |
| Moc pozorna | 5000 VA |
| Moc rzeczywista | 4500 W |
| Topologia (klasyfikacja IEC 62040-3) | Podwójna konwersja on-line |
| Typ obudowy | Uniwersalna tower/rack |
| Sprawność UPS'a | > 93% w trybie podwójnego przetwarzania on-line przy 100% obciążeniu, 98% w trybie podwyższonej sprawności |
| Liczba, typ gniazd wyjściowych | Zaciski, 8 gniazd C13, 2 gniazda C19 |
| Typ gniazda wejściowego | Listwa zaciskowa |
| Czas podtrzymania dla obciążenia 100% | 20 minut |
| Dodatkowe baterie | Możliwość wydłużenia czasu podtrzymania do 80 minut przy obc. mocą 4500 W poprzez dołożenie dodatkowych modułów baterii zewnętrznych. |
| Napięcie znamionowe | 230 V |
| Tolerancja napięcia prostownika | 176-276 V (100-276 V przy obniżonej mocy) |
| Częstotliwość znamionowa | 50/60 Hz autodetekcja |
| Tolerancja częstotliwości | 40 – 70 Hz |
| Kształt napięcia | Sinusoidalny |
| Napięcie znamionowe wyjściowe | 230 V (domyślnie) / 200/208/220/240 V |
| Zakres zmian napięcia wyjściowego | +/-1% napięcia nominalnego |
| Częstotliwość wyjściowa | 50/60 Hz +/-0,5% |
| Całkowite odkształcenia napięcia THDu | < 2% dla obciążenia liniowego |
| Baterie wymieniane przez użytkownika "na gorąco" | Tak |
| Ochrona przed przeładowaniem | Tak (ograniczenie prądu ładowarki, wyłączenie ładowarki / alarm) |
| Ochrona przed głębokim rozładowaniem | Tak |
| Okresowy automatyczny test baterii | Tak (standardowo co tydzień) |
| Zimny start | Tak |
| System zarządzania pracą baterii | System nieciągłego ładowania baterii. Do oferty dołączyć należy opis algorytmu ładowania nieciągłego baterii. W opisie znaleźć się muszą informacje nt. trwania okresów ładowania forsującego, konserwującego i okresu spoczynkowego (tzw. restingu). Okres spoczynkowy w jednym cyklu nie może być krótszy niż 14 dni. Opis powinien być materiałem firmowym producenta lub musi być przez niego potwierdzony. |
| **Interfejsy komunikacyjne** | 1. USB 2. RS232 DB-9 żeński (HID) 3. miniport wyłącznik awaryjny RPO 4. miniport wyłącznik ON/OFF 5. DB-9 port przekaźnikowy 6. karta SNMP |
| **Panel sterowania z wyświetlaczem LCD** | 1. Panel LCD obrotowy (do ułatwienia odczytów przy obu wariantach montażu UPS’a) ze wskazaniami chwilowego poziomu obciążenia i poziomu naładowania baterii, z możliwością sterowania poszczególnymi segmentami odbiorów oraz pomiarem sprawności i zużycia energii przez odbiory (w kWh) 2. Poziomy rząd przycisków sterowania 3. Poziomy rząd wskaźników stanu: trybu online (zielony), trybu bateryjnego (pomarańczowy), trybu bypass (pomarańczowy), usterki (czerwony) |
| **Wymagania dla Karty SNMP** | 1. Cyberbezpieczeństwo (szyfry TLS, MQTT) 2. Wsparcie certyfikatów CA i PKl 3. Prędkość gigabitowa (half-duplex, full-duplex) 4. Różne poziomy nadawania dostępu do konta administratora lub użytkownika |
| **Wyposażenie** | 1. Kabel RS232 2. Kabel USB 3. Gigabitowa Karta SNMP 4. Uchwyty kablowe 5. 2 przewody IEC 10A 6. Dodatkowy Moduł bateryjny 180V 7. Kabel podłączeniowy dodatkowego modułu bateryjnego do UPS 8. Komplet szyn montażowych do szafy 19" do UPS i modułu bateryjnego |
| Protokoły i certyfikaty cyberbezpieczeństwa | UL 2900-2-2/IEC 62443-4-2/HTTPS/MQTT/ /RNDIS/LDAP/NVD//SSH/PKI / pakiet szyfrów TLS 1.2 z minimum SHA256 |
| Maksymalna wysokość | 6U |
| Dodatkowe cetyfikaty | ISO9001 producenta urządzenia |
| Gwarancja producenta | Okres gwarancji zgodny z ofertą Wykonawcy lecz nie krótszy niż 24 miesiące |

# UTM klasy korporacyjnej

|  |  |
| --- | --- |
| Cecha | Wymagania minimalne |
| Wymagania ogólne | System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.  System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.  System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.  System wspiera protokoły IPv4 oraz IPv6 w zakresie:   1. Firewall. 2. Ochrony w warstwie aplikacji. 3. Protokołów routingu dynamicznego. |
| Redundancja, monitoring I wykrywanie awarii | 1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych. |
| Interfejsy, dysk i zasilanie | 1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: 2. 18 portami Gigabit Ethernet RJ-45. 3. 8 gniazdami SFP 1 Gbps. 4. 4 gniazdami SFP+ 10 Gbps.   wraz z urządzeniem należy dostarczyć 4 szt. wkładek 10GB MM SR LC   1. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 2. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q. 3. System jest wyposażony w zasilanie 2x AC. |
| Parametry wydajnościowe | 1. W zakresie Firewall’a obsługa nie mniej niż 3 mln. jednoczesnych połączeń oraz 140 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 39 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 6.5 Gbps. 4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 35 Gbps. 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 5 Gbps. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 2.8 Gbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 3 Gbps. |
| Funkcje systemu bezpieczeństwa | W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:   1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. 12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. 13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa). |
| Polityki, Firewall | 1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz: 3. Translację jeden do jeden oraz jeden do wielu. 4. Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 5. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 6. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP. 7. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. 8. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. 9. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu. 10. Amazon Web Services (AWS). 11. Microsoft Azure. 12. Cisco ACI. 13. Google Cloud Platform (GCP). 14. OpenStack. 15. VMware NSX. 16. Kubernetes. |
| Połączenia VPN | 1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: 2. Wsparcie dla IKE v1 oraz v2. 3. Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). 4. Obsługa protokołu Diffie-Hellman grup 19, 20. 5. Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. 6. Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. 7. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. 8. Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. 9. Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. 10. Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. 11. Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. 12. Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. 13. Mechanizm „Split tunneling” dla połączeń Client-to-Site. 14. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia: 15. Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. 16. Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji. |
| Routing i obsługa łączy WAM | W zakresie routingu rozwiązanie zapewnia obsługę:   1. Routingu statycznego. 2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP). 3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. 4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. 5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. 6. BFD (Bidirectional Forwarding Detection). 7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu. |
| Funkcje SD-WAM | 1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec). |
| Zarządzanie pasmem | 1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. System daje możliwość określania pasma dla poszczególnych aplikacji. 3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. 4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL. |
| Ochrona przed malware | 1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. 3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości. 4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. 5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze. 8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. 9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. 10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu. |
| Ochrona przed atakami | 1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków zawiera minimum 2000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). 7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http. 8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. 9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie. |
| Kontrola aplikacji | 1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. 6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). 7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80). |
| Kontrola WWW | 1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. 4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). 6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. 7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. 8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. 9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji. |
| Uwierzytelnianie użytkowników w ramach sesji | 1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą: 2. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. 3. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. 4. Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 5. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego. 6. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie. 7. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP. |
| Zarządzanie | 1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. 3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. 5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. 8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). 9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP. |
| Logowanie | 1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania, raportowania, korelacji zdarzeń, powiadamiania o incydentach) udostępnianej w chmurze lub musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej 3. W przypadku kiedy usługa logowania, raportowania, korelacji zdarzeń realizowana jest w chmurze, wykonawca musi dostarczyć stosowne licencje upoważniające do składowania logów przez okres co najmniej jednego roku. 4. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 5. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. 6. Możliwość włączenia logowania per reguła w polityce firewall. 7. System zapewnia możliwość logowania do serwera SYSLOG. 8. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS. |
| Serwisy i licencje | Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:   1. Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), 2. Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen 3. Logowane, raportowanie, korelacja zdarzeń, powiadamiania o incydentach   na okres 60 miesięcy. |
| Gwarancja oraz wsparcie | Gwarancja: System jest objęty serwisem gwarancyjnym producenta przez okres Zgodny z ofertą Wykonawcy lecz nie krótszy niż 24 miesiące, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. |

# Punkt dostępowy

|  |  |
| --- | --- |
| Cecha | Wymagania minimalne |
| Ogólne | Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej.   1. Obudowa urządzenia musi umożliwiać montaż na suficie lub ścianie wewnątrz budynku i zapewniać prawidłową pracę urządzenia w następujących warunkach klimatycznych:    1. Temperatura 0–50°C,    2. Wilgotność 5–90%. 2. Urządzenie musi być dostarczone z elementami mocującymi. Obudowa musi być fabrycznie przystosowana do zastosowania linki zabezpieczającej przed kradzieżą i być wyposażone w złącze typu Kensington. 3. Urządzenie musi być wyposażone w trzy niezależne moduły radiowe pracujące w podanych poniżej pasmach i obsługiwać następujące standardy:    1. 2.4 GHz 802.11b/g/n,    2. 5 GHz 802.11a/n/ac/ax,    3. 5/6 GHz 802.11a/n/ac/ax 4. Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 24 SSID. 5. Urządzenie musi być wyposażone w moduł BLE. 6. Urządzenie musi być wyposażone w dwa interfejsy Ethernet 100/1000/2500/5000 Base-T 7. Urządzenie powinno być zasilane poprzez interfejs ETH w standardzie 802.3bt lub zewnętrzny zasilacz. 8. Punkt dostępowy musi umożliwiać następujące tryby przesyłania danych:    1. Tunnel,    2. Bridge,    3. Mesh. 9. Wsparcie dla QoS: 802.11e, konfigurowalne polityki QoS per użytkownik/aplikacja. 10. Wsparcie dla poniższych metod uwierzytelnienia: WEP, WPA, WPA2, WPA3, Web Captive Portal, MAC blacklist & whitelist, 802.1X (EAP-TLS, EAP-TTLS/MSCHAPv2, EAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, EAP-FAST). 11. Interfejs radiowy urządzenia powinien wspierać następujące funkcje:     1. MIMO – 4x4,     2. Wymagana maksymalna przepustowość dla poszczególnych modułów radiowych:        1. 1147 Mbps;        2. 2402 Mbps;        3. 4803 Mbps     3. Wymagana moc nadawania:        1. min. 26 dBm dla pasma 2.4GHz z możliwością zmiany co 1dBm;        2. min. 26 dBm dla pasma 5GHz z możliwością zmiany co 1dBm;        3. min. 24 dBm dla pasma 6GHz z możliwością zmiany co 1dBm     4. Wsparcie dla 802.11n 20/40Mhz HT,     5. Wsparcie dla kanałów 80 i 160 MHz,     6. Anteny – wbudowane dla nadajników standardu 802.11 o zysku min. 4dBi dla pasma 2.4GHz, 6dBi dla pasma 5GHz, 5.5dBi dla pasma 6GHz.     7. Nieużywany moduł radiowy może zostać wyłączony programowo w celu obniżenia poboru mocy, 12. Maksymalna deklarowana liczba klientów na każdy moduł radiowy – 512 13. Funkcje dodatkowe:     1. OFDMA UL i DL     2. Spatial Reuse (BSS Coloring)     3. UL-MU-MIMO     4. DL-MU-MIMO     5. Enhanced Target Wake Time (TWT)     6. Wbudowany analizator widma     7. Wbudowane mechanizmy WIPS/WIDS |
| Zasilanie | Wraz z urządzeniami należy dostarczyć 2 szt. tzw. Injectory POE umożliwiające ich zdalne zasilanie poprzez kable typu „skrętka” |
| Gwarancja oraz wsparcie | Urządzenie musi mieć zapewnioną dożywotnią ograniczoną gwarancję producenta tzw. LifeTime do 5 lat od zaprzestania produkcji oraz być objęte serwisem gwarancyjnym producenta przez okres zgodny z ofertą wykonawcy lecz nie krótszy niż 24 miesiące, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. |

# Wdrożenie i konfiguracja dostarczonego sprzętu

|  |  |
| --- | --- |
| **Serwer z systemem operacyjnym i macierzą** | 1. Podłączenie przewodów sieciowych i zasilających zgodnie z dokumentacją techniczną. 2. Wykonanie połączeń przy użyciu niezbędnych kabli, uruchomienie urządzeń. 3. Instalacja dostępnych na dzień wdrożenia aktualizacji. 4. Instalacja i konfiguracja platformy zarządzającej środowiskiem wirtualnym, utworzenie interfejsów sieciowych, konfiguracja pul dyskowych. 5. Zabezpieczenie serwera i środowiska wirtualizacyjnego przed nieautoryzowanym dostępem. 6. Migracja istniejącego środowiska Zamawiającego na nowy sprzęt. |
| **Oprogramowanie backupowe z deduplikatorem** | 1. Instalacja oprogramowania kopii zapasowej na wskazanej przez Zamawiającego maszynie wirtualnej. 2. Konfiguracja systemu kopii zapasowych zgodnie z polityką zaakceptowaną w projekcie. 3. Testy sprawnościowe wdrożonych usług. 4. Opracowanie raportu z testów. 5. Ustalenie reguł dostępu i okien synchronizacji danych. 6. Wdrożenie modułu raportowania dla klienta. |
| Biblioteka taśmowa LTO | 1. Podłączenie i konfiguracja biblioteki taśmowej w infrastrukturze Zamawiającego. 2. Integracja urządzenia z serwerem kopii zapasowych oraz oprogramowaniem backupowym zgodnie z polityką ochrony danych zaakceptowaną w projekcie. 3. Przeprowadzenie testów sprawnościowych, obejmujących zapis i odczyt danych na nośnikach taśmowych. 4. Ustalenie reguł retencji, harmonogramu backupu oraz polityki przechowywania i rotacji taśm. 5. Wdrożenie mechanizmu raportowania dla klienta. 6. Dostarczenie instrukcji dotyczącej obsługi biblioteki taśmowej. |
| **Wdrożenie zapory sieciowej UTM** | 1. Konfiguracja interfejsów sieciowych. 2. Ustawienie podstawowych polityk bezpieczeństwa, takich jak filtrowanie ruchu sieciowego, ochrona przed atakami zewnętrznymi i wewnętrznymi. 3. Aktywacja oraz konfiguracja usług związanych z ochroną (firewall, VPN, antywirus, kontrola aplikacji, systemy detekcji i zapobiegania włamaniom -IPS/IDS). 4. Ustawienie zaawansowanych polityk bezpieczeństwa zgodnie z wymaganiami Zamawiającego, w tym dostosowanie polityk dostępu do Internetu oraz konfiguracja kontroli dostępu dla różnych działów lub grup użytkowników. 5. Konfiguracja monitorowania i raportowania zdarzeń sieciowych oraz zapewnienie dostępu do tych danych dla administratorów sieci danej jednostki. 6. Przeprowadzenie testów funkcjonalności urządzenia po instalacji i konfiguracji, w tym testy przepustowości, skuteczności polityk bezpieczeństwa oraz poprawności działania usług (VPN, firewall, IPS/IDS). |
| Rekonfiguracja szafy | 1. W ramach instalacji nowego sprzętu należy zoptymalizować przestrzeń w szafie rack. Zamawiającego poprzez zmianę kolejności zainstalowanych urządzeń. 2. **Montaż urządzeń** (w tym UPS, modułów bateryjnych oraz osprzętu towarzyszącego) musi zostać wykonany w dostarczonej lub wskazanej przez Zamawiającego szafie rack 42U, z zachowaniem właściwego rozmieszczenia zapewniającego:  * odpowiednią wentylację, * łatwy dostęp serwisowy, * bezpieczeństwo eksploatacji.  1. **Ułożenie okablowania w szafie rack musi spełniać następujące wymagania:**  * Przewody zasilające i sygnałowe należy prowadzić **oddzielnie**, zgodnie z zasadą rozdziału okablowania energetycznego i logicznego. * Przewody muszą być prowadzone w sposób **uporządkowany**, z wykorzystaniem **poziomych i pionowych organizatorów kabli**, uchwytów kablowych, rzepów lub opasek z możliwością szybkiego demontażu. * Niedopuszczalne jest prowadzenie przewodów luzem, ich skręcanie lub blokowanie cyrkulacji powietrza w szafie. * Wszystkie przewody muszą być **trwale oznakowane** z opisem ich funkcji (np. zasilanie UPS, połączenie bateryjne, SNMP, RS232, EPO).  1. **Wymagane jest zastosowanie kanałów lub organizerów kablowych** również w górnej i dolnej części szafy, jeżeli prowadzenie przewodów wymaga ich poprowadzenia poza standardowe uchwyty boczne. 2. Wszystkie urządzenia muszą zostać **zamocowane w szafie na dostarczonych przez producenta szynach montażowych** lub innych dedykowanych uchwytach, zapewniających ich bezpieczne mocowanie i łatwość demontażu. 3. Po zakończeniu montażu, Wykonawca zobowiązany jest do sporządzenia i przekazania Zamawiającemu:  * **schematu montażowego szafy rack** z wyszczególnieniem umiejscowienia urządzeń i przebiegu przewodów, |