Znak sprawy: **45/TP/2022**

Załącznik Nr 2 do SWZ

**OPIS PRZEDMIOTU ZAMÓWIENIA**

Spis treści:

[I. Część 1 (Pakiet nr 1): Dostawa sprzętu i oprogramowania 2](#_Toc119581808)

[1. Oprogramowanie do zarządzania infrastrukturą IT – licencja dla 100 stanowisk 2](#_Toc119581809)

[2. Sprzęt komputerowy – komputery PC z systemem operacyjnym – 5 szt. 6](#_Toc119581810)

[3. Serwer dedykowany dla funkcji zarządzania siecią LAN oraz funkcji routera brzegowego wraz zaporą bezpieczeństwa – 1 szt. 12](#_Toc119581811)

[4. Serwer dedykowany dla kopii bezpieczeństwa – 1 szt. 15](#_Toc119581812)

[5. Biblioteka taśmowa wraz z zestawem taśm dla realizacji zadań archiwizacji danych – 1 zestaw 21](#_Toc119581813)

[6. Urządzenie do archiwizacji w technologii RDX – 1 zestaw 23](#_Toc119581814)

[7. Serwer plików NAS dedykowany dla zadań kopii oraz archiwizacji danych – 1 zestaw 24](#_Toc119581815)

[8. Aktualizacja / podniesienie wersji oprogramowania antywirusowego – licencja dla 104 stanowisk 25](#_Toc119581816)

[II. Część 2 (Pakiet nr 2): Dostawa oprogramowania dla backupu systemu dokumentacji medycznej szpitala 30](#_Toc119581817)

[III. Część 3 (Pakiet nr 3): Audyt bezpieczeństwa systemów IT 31](#_Toc119581818)

[Zakres prac 31](#_Toc119581819)

[Obszary Audytu 31](#_Toc119581820)

[Wymagania dla jednostki przeprowadzającej audyt: 31](#_Toc119581821)

[Kryteria Audytu Bezpieczeństwa 31](#_Toc119581822)

**Uwagi i objaśnienia:**

1. Parametry określone jako „TAK” są parametrami granicznymi. Udzielenie odpowiedzi „NIE” lub innej, niestanowiącej jednoznacznego potwierdzenia spełniania warunku, będzie skutkowało bezwzględnym odrzuceniem oferty.
2. Parametry określane jako „TAK/NIE” nie są parametrami wymaganymi. Udzielenie odpowiedzi „NIE”, nie będzie skutkowało odrzuceniem oferty. W przypadku odpowiedzi „TAK”, zamawiający wymaga dla niektórych parametrów podanie nazwy oprogramowania i załączenia oryginalnych materiałów producenta w postaci broszury lub podręcznika użytkowania.
3. Parametry o określonych warunkach liczbowych („≤” lub „≥” ) są warunkami granicznymi, których niespełnienie spowoduje odrzucenie oferty. Wartość podana przy w/w oznaczeniach oznacza wartość wymaganą.
4. Wykonawca zobowiązany jest do podania parametrów w jednostkach wskazanych w niniejszym opisie.
5. Wykonawca gwarantuje niniejszym, że sprzęt jest fabrycznie nowy (wyprodukowany w tym samym roku co dostawa aparatu do Zamawiającego), nieużywany, kompletny i do jego uruchomienia oraz stosowania zgodnie z przeznaczeniem nie jest konieczny zakup dodatkowych elementów i akcesoriów. Żaden aparat ani jego część składowa, wyposażenie dodatkowe, etc. nie jest sprzętem rekondycjonowanym, powystawowym i nie był wykorzystywany wcześniej przez innego użytkownika.

**Formularz parametrów technicznych (specyfikacja przedmiotowa)**

# Część 1 (Pakiet nr 1): Dostawa sprzętu i oprogramowania

# Oprogramowanie do zarządzania infrastrukturą IT – licencja dla 100 stanowisk

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **Parametr** | **Parametr graniczny** | **Parametry oferowane /podać zakres lub opisać**/ | **Punktacja dodatkowa** |
| **Wymagania** | | | | |
|  | Oferowany oprogramowanie/ producent / kraj pochodzenia / | Podać |  | Bez oceny |
|  | Oprogramowanie musi posiadać polski oraz angielski interfejs językowy. | TAK |  | Bez oceny |
|  | Oprogramowanie musi posiadać architekturę trójwarstwową składającą się z Bazy Danych, Serwera Aplikacji, Agenta/Konsoli zarządzającej. | TAK |  | Bez oceny |
|  | Odczyt informacji dotyczących parametrów sprzętowych komputera musi odbywać się za pośrednictwem agenta systemu instalowanego na komputerach użytkowników. | TAK |  | Bez oceny |
|  | Oprogramowanie musi umożliwiać wybór instalacji agenta w trybie standardowym oraz bezpiecznym tj. braku wkompilowanych funkcji takich jak zdalne zarządzanie, transfer plików, zdalny pulpit. | TAK |  | Bez oceny |
|  | Oprogramowanie musi posiadać procedurę uwierzytelnienia i autoryzacji kont operatorów w konsoli zarządzającej poprzez fizyczne zabezpieczenie sprzętowe (lokalne lub sieciowe) wraz z hasłem, który umożliwia jednoczesną prace wielu administratorom. Logowanie użytkowników konsoli zarządzającej musi umożliwiać integrację z kontami Active Directory. Wymagane zabezpieczenie sprzętowe musi posiadać mechanizm szyfrowania danych AES w obrębie przechowywania danych wrażliwych. | TAK |  | Bez oceny |
|  | Oprogramowanie musi posiadać moduł zarządzania uprawnieniami do poszczególnych funkcjonalności systemu dla operatorów konsoli zarządzającej zgodny z modelem RBAC (Role Based Access Control). | TAK |  | Bez oceny |
|  | Oprogramowanie musi umożliwiać nadawanie oraz odbieranie uprawnień w czasie rzeczywistym (brak konieczności przelogowania użytkownika konsoli systemu). | TAK |  | Bez oceny |
|  | Oprogramowanie musi umożliwiać blokadę wybranych uprawnień konkretnego użytkownika niezależnie od uprawnień wynikających z przypisanych ról. | TAK |  | Bez oceny |
|  | Oprogramowanie musi współpracować z serwerem MSSQL Server 2008R2-2019 | TAK |  | Bez oceny |
|  | Oprogramowanie, w zakresie wszystkich warstw, nie może wymagać do prawidłowej pracy komponentów Java. | TAK |  | Bez oceny |
|  | Oprogramowanie serwera aplikacji musi posiadać funkcjonalność centralnego wysyłania wybranych powiadomień mailowych. | TAK |  | Bez oceny |
|  | Oprogramowanie musi posiadać moduł zarządzania uprawnieniami do danych w zakresie przypisywania wybranych jednostek organizacyjnych, Jednostek lokalizacyjnych oraz typów zasobów do poszczególnych użytkowników konsoli. Wszelkie raporty, zestawienia oraz funkcje obejmują wtedy tylko w/w przypisane obiekty. | TAK |  | Bez oceny |
|  | Oprogramowanie musi być podpisane cyfrowo przez Producenta ważnym certyfikatem, z prawidłową ścieżką certyfikacji, w której główny urząd certyfikacji (Root CA) jest uczestnikiem programu certyfikatów głównych systemu Windows. Podpis cyfrowy dotyczy składników Producenta systemu w zakresie plików wykonywalnych (\*.exe), plików bibliotek współdzielonych (\*.dll), plików sterowników (\*.sys) oraz pakietów instalacyjnych oprogramowania (\*.msi). | TAK |  | Bez oceny |
|  | Oprogramowanie agentów musi posiadać obsługę sesji terminalowych Windows. | TAK |  | Bez oceny |
|  | Oprogramowanie musi zapewniać dowolną konfigurację pracy wszystkich agentów, jednostek organizacyjnych, pojedynczego agenta, poprzez dziedziczenie definiowanych przez administratora parametrów. Zmiany konfiguracji agentów następują w trybie natychmiastowym (online). | TAK |  | Bez oceny |
|  | Oprogramowanie musi posiadać raport przedstawiający różnice w konfiguracji poszczególnych agentów w stosunku do konfiguracji globalnej. | TAK |  | Bez oceny |
|  | Oprogramowanie musi posiadać mechanizm logowania zmian w konfiguracji agentów przez użytkowników konsoli (data, czas, login, poprzednia i nowa wartość). | TAK |  | Bez oceny |
|  | Oprogramowanie musi posiadać mechanizm analizy czasu pracy komputera, informujący użytkownika (alert oraz wymuszone działanie – restart) o przekroczeniu zadanego czasu pracy bez restartu systemu operacyjnego. | TAK |  | Bez oceny |
|  | Oprogramowanie musi zapewniać automatyczny import drzewiastej struktury organizacyjnej zamawiającego (bez ograniczeń ilości zagnieżdżeń z kontenera Active Directory/OpenLDAP), kont użytkowników i komputerów z zachowaniem ich oryginalnego położenia wg. OU. | TAK |  | Bez oceny |
|  | Oprogramowanie musi zapewniać w obrębie synchronizacji z Active Directory/OpenLDAP tworzenie listy filtrów zawężających węzły danych wraz z możliwością wskazania docelowej gałęzi struktury organizacyjnej lub lokalizacyjnej Zamawiającego. | TAK |  | Bez oceny |
|  | Oprogramowanie musi posiadać kreator powiązań (mapowanie atrybutów) dowolnych atrybutów obiektów z usługi katalogowej do wskazanych atrybutów zasobów systemowych. | TAK |  | Bez oceny |
|  | Oprogramowanie musi umożliwiać współpracę z nieograniczoną ilością kontrolerów domen z zachowaniem podległej struktury drzewiastej. | TAK |  | Bez oceny |
|  | Oprogramowanie musi umożliwiać automatyczny import informacji dotyczących przynależności użytkowników oraz stanowisk komputerowych do grup struktury katalogowej. | TAK |  | Bez oceny |
|  | Oprogramowanie musi posiadać raport przedstawiający informacje nt. grup struktury katalogowej wraz przynależącymi do nich użytkownikami. | TAK |  | Bez oceny |
|  | Oprogramowanie musi umożliwiać tworzenie dynamicznych grup stanowisk w oparciu o kreator zawierający filtry (AND, OR) w zakresie min. wersja OS, nazwa oraz wersja wybranej aplikacji, RAM, CPU, HDD, jednostka organizacyjna, jednostka lokalizacyjna, architektura (x32, x64), zainstalowane oprogramowanie, wersja oprogramowania, lista usług systemowych, producent oraz model komputera, poziom uprawnień, predefiniowane atrybuty komputera. | TAK |  | Bez oceny |
|  | Oprogramowanie musi umożliwiać prezentację widoku zarządzanych stanowisk komputerowych w postaci listy stanowisk, drzewiastej struktury wg jednostek organizacyjnych, jednostek lokalizacyjnych, struktury Active Directory, struktury sieciowej (pule IP) oraz grup dynamicznych. | TAK |  | Bez oceny |
|  | Oprogramowanie musi umożliwiać dynamiczne zawężanie wyników wyszukiwania ww. widoków na podstawie prezentowanych w nich atrybutów. | TAK |  | Bez oceny |
|  | Oprogramowanie musi umożliwiać graficzną prezentację aktualnego stanu aktywności agenta (online/offline) z dokładnością do 1 minuty. | TAK |  | Bez oceny |
|  | Oprogramowanie musi umożliwiać zapisywanie w bazie danych informacji o uruchomieniu i wyłączeniu komputera oraz zalogowaniu i wylogowaniu użytkownika. | TAK |  | Bez oceny |
|  | Szkolenie personelu w zakresie eksploatacji i obsługi w miejscu instalacji. | TAK |  | Bez oceny |
|  | Okres gwarancji | Gwarancja min. 24 miesiące |  | Punktacja za okres gwarancji w kryterium oceny oferty:  „Okres gwarancji (G)” |

# Sprzęt komputerowy – komputery PC z systemem operacyjnym – 5 szt.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Lp.** | | **Parametr** | **TAK/NIE** | **Parametry oferowane /podać zakres lub opisać**/ | **Punktacja dodatkowa** |
| Oferowany model sprzętu/ producent | | | Podać |  | Bez oceny |
| **Wymagania podstawowe** | | | | |
|  | | Obudowa | Typu SFF z obsługą kart PCI Express o niskim profilu.  Fabrycznie umożliwiająca montaż min. 2 kieszeni: 1 szt. na napęd optyczny (dopuszcza się stosowanie napędów slim) zewnętrzna, 1 szt. 3,5”na standardowy dysk twardy. Wolna zatoka do rozbudowy o dysk 3,5”/2,5”  Wyposażona w czytnik kart multimedialnych  - Obudowa trwale oznaczona nazwą producenta, nazwą komputera, numerem MTM, PN, numerem seryjnym  - Wyposażona w budowany głośnik o mocy min. 1W |  | Bez oceny |
|  | | Zasilacz | Zasilacz maksymalnie 260W o sprawności minimum 90% |  | Bez oceny |
|  | | Chipset | Dostosowany do zaoferowanego procesora |  | Bez oceny |
|  | | Płyta główna | Zaprojektowana i wyprodukowana przez producenta komputera.  Wyposażona w złącza min.:   * 1 x PCI Express 3.0 x16, * 1 x PCI Express 3.0 x1, * 2 x M.2 z czego min. 1 przeznaczona dla dysku SSD z obsługą PCIe NVMe |  | Bez oceny |
|  | | Wydajność | Procesor o wydajności osiągającej w teście PassMark PerformanceTest co najmniej wynik 19 500 punktów PassMark CPU Mark <http://www.cpubenchmark.net>.  Wydruk testu załączyć do oferty. |  | Bez oceny |
|  | | Pamięć operacyjna | Min. 8GB DDR4 3200MHz z możliwością rozszerzenia do 64 GB  Ilość banków pamięci: min. 2 szt.  Ilość wolnych banków pamięci: min. 1 szt. |  | Bez oceny |
|  | | Dysk twardy | Min 512GB SSD M.2 PCIe NVMe zawierający RECOVERY umożliwiające odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii. |  | Bez oceny |
|  | | Napęd optyczny | Nagrywarka DVD +/-RW |  | Bez oceny |
|  | | Karta graficzna | Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki w trybie UMA (Unified Memory Access) – z możliwością dynamicznego przydzielenia pamięci. |  | Bez oceny |
|  | | Audio | Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition. |  | Bez oceny |
|  | | Karta sieciowa | LAN 10/100/1000 Mbit/s z funkcją PXE,Wake on LAN  WiFi 802.11ac 2x2 + BT 5.0 |  | Bez oceny |
|  | | Porty/  złącza | Wbudowane porty/złącza:  Wideo różnego typu umożliwiające elastyczne podłączenie urządzenia bez stosowania przejściówek lub adapterów za pomocą min:  - 1 x VGA,  - 1 x HDMI 2.1,  - 1 x DisplayPort 1.4,  Pozostałe porty/złącza:  - 7 x USB w tym:  - z przodu obudowy min.3 x USB 3.2, w tym min. 1 x USB typ C  - z tyłu obudowy min. 4 x USB, w tym min. 2 x USB 3.2  - port sieciowy RJ-45,  - porty słuchawek i mikrofonu na przednim lub tylnym panelu obudowy  - czytnik kart pamięci min. SD  Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp. |  | Bez oceny |
|  | | Klawiatura/mysz | Klawiatura przewodowa w układzie US  Mysz przewodowa (scroll) |  | Bez oceny |
|  | | System operacyjny | System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:   1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: 2. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, 3. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 4. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego 5. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim 6. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 7. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 8. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 9. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 10. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim 11. Wbudowany system pomocy w języku polskim. 12. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 13. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego. 14. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 15. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. 16. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 17. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze. 18. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk". 19. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy. 20. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 21. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 22. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 23. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 24. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 25. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)." 26. Wbudowany mechanizm wirtualizacji typu hypervisor." 27. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego. 28. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 29. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 30. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). 31. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi. 32. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne. 33. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. 34. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM 35. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych. 36. Możliwość tworzenia wirtualnych kart inteligentnych. 37. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) 38. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL. 39. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 40. Mechanizmy logowania w oparciu o: 41. Login i hasło, 42. Karty inteligentne i certyfikaty (smartcard), 43. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), 44. Certyfikat/Klucz i PIN 45. Certyfikat/Klucz i uwierzytelnienie biometryczne 46. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5 47. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej. 48. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach 49. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń 50. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń |  | Bez oceny |
|  | | BIOS | BIOS zgodny ze specyfikacją UEFI  Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych informacji o:   1. modelu komputera, PN 2. numerze seryjnym, 3. AssetTag, 4. MAC Adres karty sieciowej, 5. wersja Biosu wraz z datą produkcji, 6. zainstalowanym procesorze, jego taktowaniu i ilości rdzeni 7. ilości pamięci RAM wraz z taktowaniem, 8. stanie pracy wentylatora na procesorze 9. napędach lub dyskach podłączonych do portów SATA oraz M.2 (model dysku i napędu optycznego) 10. wersji systemu operacyjnego preinstalowanego na komputerze   Możliwość z poziomu Bios:   1. wyłączania/włączania portów USB zarówno z przodu jak i z tyłu obudowy 2. wyłączenia selektywnego (pojedynczego) portów SATA, 3. wyłączenia karty sieciowej, karty audio, czytnika kart pamięci 4. możliwość ustawienia portów USB w jednym z dwóch trybów: 5. użytkownik może kopiować dane z urządzenia pamięci masowej podłączonego do pamięci USB na komputer ale nie może kopiować danych z komputera na urządzenia pamięci masowej podłączone do portu USB 6. użytkownik nie może kopiować danych z urządzenia pamięci masowej podłączonego do portu USB na komputer oraz nie może kopiować danych z komputera na urządzenia pamięci masowej 7. ustawienia hasła: administratora, Power-On, HDD, 8. blokady aktualizacji BIOS bez podania hasła administratora 9. wglądu w system zbierania logów (min. Informacja o update Bios, błędzie wentylatora na procesorze, wyczyszczeniu logów) z możliwością czyszczenia logów 10. alertowania zmiany konfiguracji sprzętowej komputera 11. załadowania optymalnych ustawień Bios 12. obsługa Bios za pomocą klawiatury i myszy 13. możliwość ustawienia polityki dotyczącej haseł (długość i trudność hasła) 14. możliwość włączenia/wyłączenia Device Guard 15. możliwość włączenia/wyłączenia uruchomienia komputera za pomocą kombinacji klawiszy na podłączonej klawiaturze |  | Bez oceny |
|  | | Zintegrowany System Diagnostyczny | Wizualny system diagnostyczny producenta działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera umożliwiający na wykonanie diagnostyki następujących podzespołów:   * wykonanie testu pamięci RAM * test dysku twardego lub SSD * test monitora * test magistrali PCI-e * test portów USB * test płyty głównej * test procesora   Wizualna lub dźwiękowa sygnalizacja w przypadku błędów któregokolwiek z powyższych podzespołów komputera.  Ponadto system powinien umożliwiać identyfikacje testowanej jednostki i jej komponentów w następującym zakresie:   * PC: Producent, model * BIOS: Wersja oraz data wydania Bios * Procesor: Nazwa, taktowanie, ilość pamięci CACHE * Pamięć RAM: Ilość zainstalowanej pamięci RAM, producent oraz numer seryjny poszczególnych kości pamięci * Dysk: model, numer seryjny, wersja firmware, pojemność, temperatura pracy * Monitor: producent, model, rozdzielczość   System Diagnostyczny działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera. |  | Bez oceny |
|  | | Certyfikaty i standardy | * Certyfikat ISO9001 dla producenta sprzętu (należy załączyć do oferty) * Deklaracja zgodności CE (załączyć do oferty) * Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki   TCO Certified 9.0 |  | Bez oceny |
|  | | Waga/rozmiary urządzenia | Waga urządzenia poniżej 4.7 kg  Suma wymiarów nie przekraczająca 69 cm |  | Bez oceny |
|  | | Bezpieczeństwo i zdalne zarządzanie | * Złącze typu Kensington Lock * Oczko na kłódkę * TPM 2.0 |  | Bez oceny |
|  | | Okres gwarancji | Gwarancja min. 24 miesiące |  | Punktacja za okres gwarancji w kryterium oceny oferty:  „Okres gwarancji (G)” |
|  | | Warunki gwarancji | Usługi gwarancyjne świadczone w miejscu użytkowania sprzętu (on-site)  Oświadczenie producenta komputera, że w przypadku niewywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem. |  | Bez oceny |
|  | | Wsparcie techniczne producenta | Dedykowany numer oraz adres email dla wsparcia technicznego i informacji produktowej.  - możliwość weryfikacji u producenta konfiguracji fabrycznej zakupionego sprzętu  - Naprawy gwarancyjne urządzeń muszą być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta. |  | Bez oceny |

# Serwer dedykowany dla funkcji zarządzania siecią LAN oraz funkcji routera brzegowego wraz zaporą bezpieczeństwa – 1 szt.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **Parametr** | **Parametr graniczny** | **Parametry oferowane /podać zakres lub opisać**/ | **Punktacja dodatkowa** |
| **Wymagania podstawowe** | | | | |
| Oferowany model/ producent | | Podać |  |  |
|  | Wydajność obliczeniowa procesora | Zainstalowany minimum 1 procesor posiadający min. 4 rdzenie, min.8 MB cache, współczynnik mocy nie więcej niż 70W. Procesor osiąga wynik min. 12,5 pkt w teście Spec speed 2017int base (spec cpu 2017 Integer Speed Result), na wskazanym w ofercie modelu serwera. Wyniki muszą być dostępne na stronach internetowych organizacji spec.org |  | Bez oceny |
|  | Pamięć RAM | Min. 2 x 32GB DDR4, Dual Rank, ECC. Minimalny rozmiar jednej kości to 32GB. |  | Bez oceny |
|  | Sloty rozszerzeń | Min. 2 x PCI-E gen 4 |  | Bez oceny |
|  | Dyski i kontrolery | 2. Dwa dyski HDD min. 1000 GB pracujące w układzie RAID 1 |  | Bez oceny |
|  | Obudowa/  Zasilanie | 1. RACK 19’’, maks wysokość 1U, miejsce na 4 dysków 2,5’’.  2. szyny rack do montażu serwera w szafie przemysłowej  3. Zasilacz o mocy maksymalnej 500W każdy. |  | Bez oceny |
|  | Karty sieciowe | 1. Zintegrowana karta sieciowa 2x RJ-45, 1Gb/s, 1000Base-T nie zajmująca slotów PCIe  2. Karta sieciowa na PCIe 2x SFP+, 10Gb/s. |  | Bez oceny |
|  | Moduł zarządzający | Niezależna od system operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować zmniejszenia mininmalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność:   * monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe * wparcie dla agentów zarządzających oraz możliwość pracy w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP * dostęp do karty zarządzającej poprzez * dedykowany port RJ45 z tyłu serwera lub * przez współdzielony port zintegrowanej karty sieciowej serwera * dostęp do karty możliwy * z poziomu przeglądarki webowej (GUI) * z poziomu linii komend zgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SM CLP) * z poziomu skryptu (XML/Perl) * poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface) * wbudowane narzędzia diagnostyczne * zdalna konfiguracji serwera(BIOS) i instalacji systemu operacyjnego * obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie * wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników * przesyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough) * obsługa zdalnego serwera logowania (remote syslog) * wirtualna zadalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i i wirtualnych folderów * mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego startu serwera a także nagrywanie na żądanie * funkcja zdalnej konsoli szeregowej przez SSH (wirtualny port szeregowy) z funkcją nagrywania i odtwarzania sekwencji zdarzeń i aktywności * monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji * konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping) * zdalna aktualizacja oprogramowania (firmware) * zarządzanie grupami serwerów, w tym: * tworzenie i konfiguracja grup serwerów * sterowanie zasilaniem (wł/wył) * ograniczenie poboru mocy dla grupy (power caping) * aktualizacja oprogramowania (firmware) * wspólne wirtualne media dla grupy * możliwość równoczesnej obsługi przez min. 2 administratorów * autentykacja dwuskładnikowa (Kerberos) * wsparcie dla Microsoft Active Directory * obsługa SSL i SSH * enkrypcja AES/3DES dla zdalnej konsoli * wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API * możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP) |  | Bez oceny |
|  | Gwarancja i wsparcie dla dostarczonego sprzętu | Gwarancja w miejscu instalacji w następny dzień roboczy, serwis w miejscu instalacji lub w sposób zdalny, naprawa lub wymiana producenta uszkodzonego sprzętu maksymalnie w następnym dniu roboczym. Wsparcie techniczne realizowane jest przez serwis producenta oferowanego serwera. |  | Bez oceny |
|  | Okres gwarancji | Gwarancja min. 24 miesiące |  | Punktacja za okres gwarancji w kryterium oceny oferty:  „Okres gwarancji (G)” |
|  | Wsparcie techniczne producenta | Dedykowany numer oraz adres email dla wsparcia technicznego i informacji produktowej.  - możliwość weryfikacji u producenta konfiguracji fabrycznej zakupionego sprzętu  - Naprawy gwarancyjne urządzeń muszą być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta. |  | Bez oceny |
|  | Inne | Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta.  Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001.  Deklaracja zgodności CE. |  | Bez oceny |

# Serwer dedykowany dla kopii bezpieczeństwa – 1 szt.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **Parametr** | **Parametr graniczny** | **Parametry oferowane /podać zakres lub opisać**/ | **Punktacja dodatkowa** |
| **Wymagania podstawowe** | | | | |
| Oferowany model/ producent | | Podać |  |  |
|  | Obudowa | Maksymalnie 1U RACK 19 cali (wraz z szynami montażowymi, umożliwiającymi serwisowanie serwera w szafie rack bez wyłączania urządzenia) |  | Bez oceny |
|  | Procesor | Dwa procesory min. dziesięciordzeniowe x86 - 64 bity lub procesory równoważne, osiągające w teście SPECrate2017\_int\_base wynik nie gorszy niż 113 punktów, na wskazanym w ofercie modelu serwera, w konfiguracji 2 procesorowej. Wyniki muszą być dostępna na stronach internetowych organizacji spec.org  Płyta główna wspierająca zastosowanie procesorów od 4 do 28 rdzeniowych, mocy do min. 205W i taktowaniu CPU do min. 3.6 GHz. |  | Bez oceny |
|  | Liczba procesorów | Min. 2 procesory |  | Bez oceny |
|  | Pamięć operacyjna | 256 GB RDIMM DDR4 2933 MT/s w modułach o pojemności min.16GB każdy.  Płyta główna z minimum 24 slotami na pamięć i umożliwiająca instalację do minimum 3TB (przy zastosowaniu odpowiednich proceosrów).  Obsługa zabezpieczeń: min.Advanced ECC i Online Spare.  FnSerwer z obsługą pamięci typu NVDIMM |  | Bez oceny |
|  | Sloty rozszerzeń | 3 aktywne gniazda PCI-Express generacji 3, w tym min. 2 slot x16 (szybkość slotu – bus width) oraz jeden slot x8. |  | Bez oceny |
|  | Dysk twardy | Zatoki dyskowe gotowe do zainstalowania 8 dysków typu Hot Swap, SAS/SATA/SSD,  Serwer wyposażony w cztery dyski, każdy min. 2,4TB SAS 10k 2.5” |  | Bez oceny |
|  | Kontroler | Serwer wyposażony w kontroler sprzętowy, wyposażony w min. 2 porty zewnętrzne, zapewniający obsługę zewnętrznej macierzy dyskowej SAS, kontroler obsługujący poziomy: RAID 0/1/10/5.  Serwer wyposażony w kontroler sprzętowy z min. 2GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, zapewniający obsługę 8 napędów dyskowych SAS oraz obsługujący poziomy: RAID 0/1/10/5/50/6/60.  Serwer umożliwiający rozbudowę/wymianę na sprzętowy kontroler RAID zapewniający obsługę RAID 0/1/10/5/50/6/60 z 4GB pamięci cache z podtrzymywaniem bateryjnym.  Kontroler umożliwiający pracę z dyskami w trybach RAID i JBOD jednocześnie |  | Bez oceny |
|  | Interfejsy sieciowe | Minimum 4 porty Ethernet 100/1000/10000 Mb/s RJ-45 z funkcjonalnościami 802.3, 802.3x, 802.2x, 802.3ad, 802.1Qaz, 802.1Qau, 802.1Qbb, 802.1Qbg, 802.1ax, które nie zajmuje gniazd PCIe opisanych w sekcji „Sloty rozszerzeń”. |  | Bez oceny |
|  | Karta graficzna | Zintegrowana karta graficzna |  | Bez oceny |
|  | Porty | 5 x USB 3.0 (w tym min. 1 porty wewnętrzne), 1x VGA  Wewnętrzny slot na kartę micro SD.  Możliwość rozbudowy o:   * dodatkowy port video typu DisplayPort/HDMI/VGA, dostępny z przodu serwera * port szeregowy typu DB9/DE-9 (9 pinowy), wyprowadzony na zewnątrz obudowy bez pośrednictwa portu USB/RJ45 oraz bez konieczności instalowania kart w slotach PCI-Express |  | Bez oceny |
|  | Zasilacz | 2 szt., typu Hot-plug, redundantne, każdy o mocy max. 500W. |  | Bez oceny |
|  | Chłodzenie | Zestaw wentylatorów redundantnych typu hot-plug |  | Bez oceny |
|  | Napęd | Możliwość rozbudowy/rekonfiguracji o  wewnętrzny napęd DVD-ROM lub DVD-RW |  | Bez oceny |
|  | Diagnostyka | Możliwość zainstalowania elektronicznego panelu diagnostycznego dostępnego z przodu serwera pozwalającego uzyskać informacje o stanie: procesora, pamięci, wentylatorów, kary sieciowej, zasilaczy, kartach rozszerzeń, temperaturze. |  | Bez oceny |
|  | Karta/moduł zarządzający | Niezależna od system operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować zmniejszenia mininmalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność:   * monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe * wparcie dla agentów zarządzających oraz możliwość pracy w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP * dostęp do karty zarządzającej poprzez   + dedykowany port RJ45 z tyłu serwera lub   + przez współdzielony port zintegrowanej karty sieciowej serwera   dostęp do karty możliwy:   * + z poziomu przeglądarki webowej (GUI)   + z poziomu linii komend zgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SM CLP)   + z poziomu skryptu (XML/Perl)   + poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface) * wbudowane narzędzia diagnostyczne * zdalna konfiguracji serwera(BIOS) i instalacji systemu operacyjnego * obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie * wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników * przesyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough) * obsługa zdalnego serwera logowania (remote syslog) * wirtualna zadalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i i wirtualnych folderów * mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego startu serwera a także nagrywanie na żądanie * funkcja zdalnej konsoli szeregowej przez SSH (wirtualny port szeregowy) z funkcją nagrywania i odtwarzania sekwencji zdarzeń i aktywności * monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji * konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping) * zdalna aktualizacja oprogramowania (firmware) * zarządzanie grupami serwerów, w tym:   + tworzenie i konfiguracja grup serwerów   + sterowanie zasilaniem (wł/wył)   + ograniczenie poboru mocy dla grupy (power caping)   + aktualizacja oprogramowania (firmware)   + wspólne wirtualne media dla grupy * możliwość równoczesnej obsługi przez min. 2 administratorów * autentykacja dwuskładnikowa (Kerberos) * wsparcie dla Microsoft Active Directory * obsługa SSL i SSH * enkrypcja AES/3DES dla zdalnej konsoli * wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API * możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP) |  | Bez oceny |
|  | Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych | * Microsoft Windows Server 2012 R2, 2016, 2019, 2022 * Red Hat Enterprise Linux (RHEL) 7.X * SUSE Linux Enterprise Server (SLES) 12 * CentOS * VMware ESXi 6.5 oraz U1 |  | Bez oceny |
|  | Serwerowy system operacyjny zwany dalej SSO, spełniający wymagania: | Licencja musi uprawniać do uruchamiania SSO w środowisku fizycznym lub min. dwóch SSO w środowisku wirtualnym (jako maszyny wirtualne) za pomocą wbudowanych mechanizmów wirtualizacji.  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 do 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, możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading),   8. wbudowane wsparcie instalacji i pracy na wolumenach, które:      1. pozwalają na zmianę rozmiaru w czasie pracy systemu,      2. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,      3. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,      4. umożliwiają zdefiniowanie list kontroli dostępu (ACL),   9. wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość,   10. wbudowane szyfrowanie dysków   11. możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET,   12. możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów,   13. wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych,   14. graficzny interfejs użytkownika,   15. zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,   16. wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play),   17. możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu,   18. dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa,   19. możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:       1. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,       2. usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:   1) podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,  2) ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,  3) odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,   * + 1. zdalna dystrybucja oprogramowania na stacje robocze,     2. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej,     3. centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:        1. dystrybucję certyfikatów poprzez http,        2. konsolidację CA dla wielu lasów domeny,        3. automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,     4. szyfrowanie plików i folderów,     5. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),     6. możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów,     7. serwis udostępniania stron WWW,     8. wsparcie dla protokołu IP w wersji 6 (IPv6),     9. 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:   1. dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,   2. obsługi ramek typu jumbo frames dla maszyn wirtualnych,   3. obsługi 4-KB sektorów dysków,   4. nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,   5. możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model),      1. 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,      2. wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath),      3. możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego,      4. mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty,      5. możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. |  | Bez oceny |
|  | Wsparcie techniczne | 3-letnia gwarancja producenta w miejscu instalacji w następny dzień roboczy. Wsparcie techniczne realizowane jest przez serwis producenta oferowanego serwera. |  | Bez oceny |
|  | Okres gwarancji | Gwarancja min. 24 miesiące |  | Punktacja za okres gwarancji w kryterium oceny oferty:  „Okres gwarancji (G)” |
|  | Inne | Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta.  Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001.  Deklaracja zgodności CE. Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |  | Bez oceny |

# Biblioteka taśmowa wraz z zestawem taśm dla realizacji zadań archiwizacji danych – 1 zestaw

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **Parametr** | **Parametr graniczny** | **Parametry oferowane /podać zakres lub opisać**/ | **Punktacja dodatkowa** |
| **Wymagania podstawowe** | | | | |
| Oferowany model/ producent | | Podać |  |  |
|  | Obudowa | Obudowa typu Rack o wysokości max 2U |  | Bez oceny |
|  | Typ napędu LTO | Min. LTO8 |  | Bez oceny |
|  | Ilość napędów | Min. 1, możliwość rozbudowy do min. 2 napędów LTO |  | Bez oceny |
|  | Technologie napędów | Min. LTO6,7,8,9 |  | Bez oceny |
|  | Interfejs komunikacyjny | FC SAN min. 8 Gbps |  | Bez oceny |
|  | Maksymalna, możliwa pojemność danych | Min. 270 TB natywnie oraz 710 TB z użyciem kompresji danych |  | Bez oceny |
|  | Maksymalny transfer danych w oferowanej konfiguracji | Min. 270 mb/s |  | Bez oceny |
|  | Ilość slotów na taśmy | Min. 24 |  | Bez oceny |
|  | Panel diagnostyczny | Panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie urządzenia |  | Bez oceny |
|  | Możliwość szyfrowania danych | Min. Kluczem AES256 |  | Bez oceny |
|  | Złącza | Min. 1 x LC optyczne, min 1 x RJ45 oraz min. 1x USB |  | Bez oceny |
|  | Zasilacz | Min. 1 x 170W |  | Bez oceny |
|  | Zarządzanie | - komunikacja poprzez interfejs RJ45  - wbudowana diagnostyka  - wsparcie dla IPv4 i Ipv6  - sterowniki do Windows Serwer 2008/2012 R2/2016/2019 |  | Bez oceny |
|  | Wyposażenie | Wraz z urządzeniem należy dostarczyć min. 8 taśm LT08 RW z zestawem etykiet oraz 1 taśmę czyszczącą, kabel połączeniowe zasilające oraz kabel LC-LC min. OM4 o długości min. 3mb do połączenia z siecią SAN |  | Bez oceny |
|  | Wsparcie techniczne | 3-letnia gwarancja producenta w miejscu instalacji w następny dzień roboczy. Wsparcie techniczne realizowane jest przez serwis producenta oferowanego serwera. |  | Bez oceny |
|  | Okres gwarancji | Gwarancja min. 24 miesiące |  | Punktacja za okres gwarancji w kryterium oceny oferty:  „Okres gwarancji (G)” |
|  | Inne | Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta.  Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001.  Deklaracja zgodności CE. Oferowany napęd LTO musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Windows Server 2008 R2. Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |  | Bez oceny |

# Urządzenie do archiwizacji w technologii RDX – 1 zestaw

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **Parametr** | **Parametr graniczny** | **Parametry oferowane /podać zakres lub opisać**/ | **Punktacja dodatkowa** |
| **Wymagania podstawowe** | | | | |
| Oferowany model/ producent | | Podać |  |  |
|  | Rodzaj urządzenia: | Napęd RDX – zewnętrzny |  | Bez oceny |
|  | Interfejs: | SuperSpeed USB 3.0 |  | Bez oceny |
|  | Szerokość: | Maks 12 cm |  | Bez oceny |
|  | Głębokość: | Maks 18 cm |  | Bez oceny |
|  | Wysokość: | Maks 6 cm |  | Bez oceny |
|  | Waga: | Maks 700 g |  | Bez oceny |
|  | Wyposażenie dodatkowe | Kartridż min. 4 TB – 2 sztuki |  | Bez oceny |
|  | **Pamięć wymienialna** | |  |  |
|  | Typ: | Kartridż RDX |  | Bez oceny |
|  | Typ nośnika: | Kartridż RDX |  | Bez oceny |
|  | Szybkość transmisji danych: | Min. 260 MBps (wewnętrzna) |  |  |
|  | Średni czas dostępu: | Maks. 15 ms |  |  |
|  | Wyposażenie | Min. 2 kartridże, min. 5 TB każdy |  |  |
|  | **Rozszerzenie / połączenie** | |  |  |
|  | Interfejsy: | Min 1 x USB 3.0 |  |  |
|  | **Różne** | |  |  |
|  | MTBF: | Min. 550,000 godzina(y) |  |  |
|  | Zgodność z normami: | VCCI, C-Tick, CISPR 22 Class B, CISPR 24, EN 60950, EN 61000-3-2, IEC 60950, EN 61000-3-3, EN55024, UL 60950, CSA 22.2 No. 60950, EN55022 Class B, ICES-003 Class B, FCC CFR47 Part 15 B |  |  |
|  | **Oprogramowanie / Wymagania systemowe** | |  |  |
|  | Obsługa systemów operacyjnych: | Microsoft Windows XP, SUSE Linux Enterprise Server, Microsoft Windows Server 2003, Red Hat Enterprise Linux, Microsoft Windows 7, Microsoft Windows Server 2008 R2, Red Hat Fedora Core 5, Microsoft Windows Server 2003 R2, Microsoft Windows Server 2008, Microsoft Windows Vista SP1, Microsoft Windows Small Business Server 2008, CentOS, Microsoft Windows Small Business Server 2011, Windows 8, Microsoft Windows Server 2012, Microsoft Windows Server 2012 R2 |  |  |
|  | **Parametry środowiska** | |  |  |
|  | Min. temperatura pracy: | 10 °C |  |  |
|  | Maks. temperatura pracy: | 40 °C |  |  |
|  | **Warunki gwarancji** | |  |  |
|  | Okres gwarancji | Gwarancja producenta min. 24 miesiące |  | Punktacja za okres gwarancji w kryterium oceny oferty:  „Okres gwarancji (G)” |

# Serwer plików NAS dedykowany dla zadań kopii oraz archiwizacji danych – 1 zestaw

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **Parametr** | **Parametr graniczny** | **Parametry oferowane /podać zakres lub opisać**/ | **Punktacja dodatkowa** |
| **Wymagania podstawowe** | | | | |
| Oferowany model/ producent | | Podać |  |  |
|  | Procesor | Min. 2 rdzeniowy z częstotliwością zwiększaną dynamicznie do 2,8GHz |  | Bez oceny |
|  | Obudowa | Obudowa wolnostojąca |  |  |
|  | Wnęki dyskowe | Min. 4 dyski 3,5” lub 2,5”, zainstalowane 4 dyski o pojemności min 8TB każdy |  |  |
|  | Gniazdo M.2 | Obsługa dla min. 2 dysków M.2 |  |  |
|  | Pamięć systemowa | Min. 2 GB |  | Bez oceny |
|  | Rozbudowa pamięci | Do min. 16GB |  |  |
|  | Pamięć flash | Min. 3GB |  |  |
|  | Sloty rozszerzeń | Min. 1 x PCI-E gen 3 |  | Bez oceny |
|  | Interfejsy sieciowe | Min. 1 o prędkości 2,5GB/1GB |  | Bez oceny |
|  | Porty USB | Min. 2 X USB 3.2 oraz 2 porty USB 2.0 |  |  |
|  | Złącze video | Min. 1 x HDMI |  |  |
|  | Pobór mocy | Maks. 26W |  | Bez oceny |
|  | Okres gwarancji | Gwarancja producenta min. 24 miesiące |  | Punktacja za okres gwarancji w kryterium oceny oferty:  „Okres gwarancji (G)” |
|  | Inne | Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta.  Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001.  Deklaracja zgodności CE. |  | Bez oceny |

# Aktualizacja / podniesienie wersji oprogramowania antywirusowego – licencja dla 104 stanowisk

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Lp.** | **Parametr** | | **Parametr graniczny** | **Parametry oferowane /podać zakres lub opisać**/ | **Punktacja dodatkowa** |
| **Wymagania** | | | | | |
| Zamawiający użytkuje oprogramowanie ESET PROTECT Essential ON-PREM na 104 stanowiska  (licencja ważna do 2023-11-29). Zakup ma na celu podniesienie wersji oprogramowania do wersji Enterprise.  Zamawiający dopuszcza dostawę rozwiązania równoważnego spełniającego poniższe funkcjonalności. | | | | | |
| **Oferowane oprogramowanie/ producent** | |  | | | |
| **Funkcjonalności** | | | | | |
| **Administracja zdalna** | | | | | |
|  | Rozwiązanie musi wspierać instalację na systemach Windows Server (od 2012), Linux oraz w postaci maszyny wirtualnej w formacie OVA lub dysku wirtualnego w formacie VHD. | | TAK |  | Bez oceny |
|  | Rozwiązanie musi zapewniać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL. | | TAK |  | Bez oceny |
|  | Rozwiązanie musi zapewniać pobranie wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta. | | TAK |  | Bez oceny |
|  | Rozwiązanie musi zapewniać dostęp do konsoli centralnego zarządzania w języku polskim z poziomu interfejsu WWW zabezpieczony za pośrednictwem protokołu SSL. | | TAK |  | Bez oceny |
|  | Rozwiązanie musi zapewniać zabezpieczoną komunikację pomiędzy poszczególnymi modułami serwera za pomocą certyfikatów. | | TAK |  | Bez oceny |
|  | Rozwiązanie musi zapewniać utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi. | | TAK |  | Bez oceny |
|  | Rozwiązanie musi wspierać zarządzanie urządzeniami z systemem iOS i Android. | | TAK |  | Bez oceny |
|  | Rozwiązanie musi zapewniać centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, antyspyware, które działają na stacjach roboczych w sieci. | | TAK |  | Bez oceny |
|  | Rozwiązanie musi zapewniać weryfikację podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe). | | TAK |  | Bez oceny |
|  | Rozwiązanie musi zapewniać instalowanie i odinstalowywanie oprogramowania firm trzecich dla systemów Windows oraz MacOS oraz odinstalowywanie oprogramowania zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT. | | TAK |  | Bez oceny |
|  | Rozwiązanie musi zapewniać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. | | TAK |  | Bez oceny |
|  | Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. | | TAK |  | Bez oceny |
|  | Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera. | | TAK |  | Bez oceny |
|  | Rozwiązanie musi zapewniać korzystanie z minimum 100 szablonów raportów, przygotowanych przez producenta oraz musi zapewniać tworzenie własnych raportów przez administratora. | | TAK |  | Bez oceny |
|  | Rozwiązanie musi zapewniać wysłanie powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog. | | TAK |  | Bez oceny |
|  | Rozwiązanie musi zapewniać podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami. | | TAK |  | Bez oceny |
| **Ochrona stacji roboczych** | | | | | |
|  | Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 7/Windows 8/Windows 8.1/Windows 10/Windows 11). | |  |  |  |
|  | Rozwiązanie musi wspierać architekturę ARM64. | | TAK |  | Bez oceny |
|  | Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. | | TAK |  | Bez oceny |
|  | Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet. | | TAK |  | Bez oceny |
|  | Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. | | TAK |  | Bez oceny |
|  | Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. | | TAK |  | Bez oceny |
|  | Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. | | TAK |  | Bez oceny |
|  | Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych. | | TAK |  | Bez oceny |
|  | Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku. | | TAK |  | Bez oceny |
|  | Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). | | TAK |  | Bez oceny |
|  | Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. | | TAK |  | Bez oceny |
|  | Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. | | TAK |  | Bez oceny |
|  | Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. | | TAK |  | Bez oceny |
|  | Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia. | | TAK |  | Bez oceny |
|  | Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:  • tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,  • tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,  • tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,  • tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,  • tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach. | | TAK |  | Bez oceny |
|  | Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników. | | TAK |  | Bez oceny |
|  | Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa. | |  |  |  |
|  | Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. | |  |  |  |
|  | Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). | |  |  |  |
|  | Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. | |  |  |  |
|  | Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego MS Outlook. | |  |  |  |
|  | Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:  • tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,  • tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,  • tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,  • tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu. | |  |  |  |
|  | Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki. | |  |  |  |
|  | Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika. | |  |  |  |
|  | Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki. | |  |  |  |
|  | Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych. | |  |  |  |
|  | Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii. | |  |  |  |
| **Ochrona serwera** | | | | | |
|  | Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 7 i 8, CentOS 7 i 8, Ubuntu Server 16.04 LTS i nowsze, Debian 9, Debian 10, SUSE Linux Enterprise Server (SLES) 12, SUSE Linux Enterprise Server (SLES) 15, Oracle Linux oraz Amazon Linux. | |  |  |  |
|  | Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. | |  |  |  |
|  | Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. | |  |  |  |
|  | Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS. | |  |  |  |
|  | Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. | |  |  |  |
|  | Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji. | |  |  |  |
|  | Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów. | |  |  |  |
|  | Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty. | |  |  |  |
|  | **Dodatkowe wymagania dla ochrony serwerów Windows:** | |  |  |  |
|  | Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive. | |  |  |  |
|  | Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS). | |  |  |  |
|  | Rozwiązanie musi wspierać skanowanie magazynu Hyper-V. | |  |  |  |
|  | Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. | |  |  |  |
|  | Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. | |  |  |  |
|  | Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. | |  |  |  |
|  | Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. | |  |  |  |
|  | Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. | |  |  |  |
|  | Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu. | |  |  |  |
|  | **Dodatkowe wymagania dla ochrony serwerów Linux:** | |  |  |  |
|  | Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej. | |  |  |  |
|  | Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web. | |  |  |  |
|  | Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon. | |  |  |  |
|  | Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu. | |  |  |  |
| **Ochrona urządzeń mobilnych opartych o system Android** | | | | | |
|  | Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie. | |  |  |  |
|  | Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne. | |  |  |  |
|  | Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki). | |  |  |  |
|  | Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM. | |  |  |  |
|  | Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:   * 1. a. usunięcie zawartości urządzenia,   2. b. przywrócenie urządzenie do ustawień fabrycznych,   3. c. zablokowania urządzenia,   4. d. uruchomienie sygnału dźwiękowego,   5. e. lokalizację GPS. | |  |  |  |
|  | Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji. | |  |  |  |
|  | Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:  a. nazwę aplikacji,  b. nazwę pakietu,  c. kategorię sklepu Google Play,  d. uprawnienia aplikacji,  e. pochodzenie aplikacji z nieznanego źródła. | |  |  |  |
|  | **Okres gwarancji** | | Gwarancja min. 24 miesiące |  | Punktacja za okres gwarancji w kryterium oceny oferty:  „Okres gwarancji (G)” |

# Część 2 (Pakiet nr 2): Dostawa oprogramowania dla backupu systemu dokumentacji medycznej szpitala

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **Parametr** | **Parametr graniczny** | **Parametry oferowane /podać zakres lub opisać**/ | **Punktacja dodatkowa** |
| **Wymagania podstawowe** | | | | |
| Oferowany model/ producent | | Podać |  |  |
|  | Funkcjonalności | 1. System zapewnia możliwość wykonywania dziennej kopii bezpieczeństwa kart leków wszystkich pacjentów znajdujących się na oddziałach  2. Funkcjonalność zabezpiecza informacje dotyczących podań leków na wypadek awarii uniemożliwiającej przejrzenie tych informacji bezpośrednio z poziomu systemu  3. Funkcjonalność zabezpiecza informacje dotyczące planu terapie  4. Funkcjonalność zabezpiecza informacje dotyczące listy operacyjnej  5. Funkcjonalność zabezpiecza treści kart wizyt  6. Funkcjonalność zabezpiecza historię choroby  7. System zapewnia możliwość zaplanowania wykonania kopii zapasowej według wprowadzonego harmonogramu  8. System zapewnia możliwość automatycznego zrzutu dokumentów do plików .pdf na dany dzień harmonogramu  9. System zapewnia możliwość określenia docelowej lokalizacji zapisanych plików kopii uwzględniając lokalizacje sieciowe  10. System zapewnia możliwość organizacji dokumentów w folderach odpowiadających datom kolejnych zrzutów  11. Zrzut bezpieczeństwa karty leków w obrębie pacjenta zawiera nagłówek prezentujący minimum następujące informacje:  a. Imię, nazwisko pacjenta  b. Płeć  c. Nr księgi głównej  d. Nr księgi oddziałowej  e. Data przyjęcia  f. PESEL  12. W ramach zrzutu karty leków prezentowane są informacje dotyczące podań leków zorganizowane w tabelę zawierającą minimum następujące informacje:  a. Nazwa leku,  b. Droga podania  c. Dawka  d. Godzina planowanego podania  e. Podpis zlecającego  13.W przypadku zleceń leków w pompie infuzyjnej bądź wlewie kroplowym w ramach zrzutu karty leków tabela zawiera minimum następujące informacje:  a. Nazwa leku,  b. Droga podania  c. Dawka  d. Przepływ (prędkość podawania leku)  e. Bolus  f. Godzina planowanego podania  g. Podpis zlecającego |  | Bez oceny |

# Część 3 (Pakiet nr 3): Audyt bezpieczeństwa systemów IT

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Parametr** |  |
| **Zakres prac** | | |
|  | Przeprowadzenie audytu bezpieczeństwa, którego celem jest wykazanie podniesienia poziomu bezpieczeństwa teleinformatycznego po zrealizowaniu czynności w odniesieniu do stanu na dzień przeprowadzenia badania poziomu dojrzałości cyberbezpieczeństwa i oceny podniesienia poziomu bezpieczeństwa teleinformatycznego, zgodnie z Zarządzeniem nr 68/2022/BBIICD Prezesa Narodowego Funduszu Zdrowia z dnia 20 maja 2022 r. w sprawie finansowania działań w celu podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców. | |
| **Obszary Audytu** | | |
|  | 1. Ocena skuteczności działania infrastruktury w zakresie urządzeń i konfiguracji w zakresie: ochrony poczty, ochrony sieci, systemów serwerowych, stacji roboczych, systemów bezpieczeństwa, 2. Zarządzanie bezpieczeństwem informacji:  * nośniki wymienne - udokumentowany sposób postępowania, * zarządzanie tożsamością/dostęp do systemów w zakresie: przydzielanie dostępu, odbieranie dostępu, * pomieszczenie/pomieszczenia w dyspozycji Zespołu IT  1. Monitorowanie i reagowanie na incydenty bezpieczeństwa:  * procedury zarządzania incydentami, * raportowanie poziomów pokrycia scenariuszami znanych incydentów, * dokumentacja dotycząca przekazywania informacji do właściwego zespołu CSIRT poziomu krajowego/ sektorowego zespołu cyberbezpieczeństwa, * monitorowanie i wykrycie incydentów bezpieczeństwa, * Identyfikacja i dokumentowanie przyczyn wystąpienia incydentów.  1. Zarządzanie ciągłością działania:  * konfiguracja oraz polityki systemów do wykonywania kopii bezpieczeństwa, * raport z przeglądów i testów odtwarzania kopii bezpieczeństwa, * procedury wykonywania i przechowywania kopii zapasowych, * strategia i polityka ciągłości działania, awaryjne oraz odtwarzania po katastrofie (DRP), * procedury utrzymaniowe.  1. Utrzymanie systemów informacyjnych:  * harmonogramy skanowania podatności, * aktualny status realizacji postępowania z podatnościami, * procedury związane ze z identyfikowaniem (wykryciem) podatności, * współpraca z osobami odpowiedzialnymi za procesy zarządzania incydentami.  1. Zarządzanie bezpieczeństwem i ciągłością działania łańcucha usług:  * polityka bezpieczeństwa w relacjach z dostawcami, * standardy i wymagania nakładane na dostawców w umowach w zakresie cyberbezpieczeństwa, * dostęp zdalny, * metody uwierzytelnienia. | |
| **Wymagania dla jednostki przeprowadzającej audyt:** | | |
| Zamawiający wymaga, aby jednostka przeprowadzająca audyt spełniała wymagania określone w Załączniku nr 2 do Zarządzenia nr 68/2022/BBIICD Prezesa Narodowego Funduszu Zdrowia z dnia 20 maja 2022 r. w sprawie finansowania działań w celu podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców,  oraz Ustawie z dnia 5 lipca 2018r. o Krajowym Systemie Cyberbezpieczeństwa (Dz. U. 2018 poz. 1560). | | |
| **Kryteria Audytu Bezpieczeństwa** | | |
| Kryteria Audytu Bezpieczeństwa oparte będą o:   * Ankietę weryfikacji pod kątem dojrzałości cyberbezpieczeństwa. * Wymagania normatywne PN-EN ISO/IEC 27001:2017-06. * Wymagania normatywne PN-EN ISO 22301:2020-04. * Wewnętrzną dokumentację Zamawiającego. * Przepisy o Krajowym Systemie Cyberbezpieczeństwa. * Standardy Krajowych Ram Interoperacyjności (KRI).   Audytowi poddany zostanie wpływ przeprowadzonych inwestycji na podniesienie poziomu cyberbezpieczeństwa Szpitala. | | |