**Załącznik Nr 1 do SWZ**

....................................., dnia ................ roku

( miejscowość )

.......................................

.......................................

.......................................

(nazwa i adres firmy – Wykonawcy)

tel. ……………………

e-mail …………………

NIP : …………………..

**Zamawiający:**

**Gmina Rydzyna**

**ul. Rynek 1**

**64-130 Rydzyna**

**O F E R T A**

Niniejszym składam ofertę w postępowaniu o udzielenie zamówienia publicznego na:

**Zakup sprzętu IT wraz z oprogramowaniem w ramach projektu „Cyfrowa Gmina"**

1. Oferuję wykonanie przedmiotu zamówieniaw zakresie **Zadania 1** za łączne wynagrodzenie ryczałtowe w wysokości netto .................................. zł (wpisać pozycję z przedostatniej kolumny) i w wysokości brutto …………………. zł (wpisać pozycję z ostatniej kolumny)\*.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Nazwa** | **Cena jednostkowa netto (1)** | **VAT % (2)** | **Cena jednostkowa brutto (3)** | **Ilość (4)** | **Cena netto ogółem**  **(1) x (4)** | **Cena brutto**  **ogółem**  **(3) x (4)** |
| Serwer |  |  |  | 1 |  |  |
| UPS |  |  |  | 1 |  |  |
| Router i bramka bezpieczeństwa ze zintegrowanym przełącznikiem PoE |  |  |  | 1 |  |  |
| Switch zarządzany SFP+ |  |  |  | 1 |  |  |
| Switch zarządzany |  |  |  | 2 |  |  |
| Punkt dostępowy |  |  |  | 2 |  |  |
| Oprogramowanie zapewniające zintegrowane bezpieczeństwo do zarządzenie infrastrukturą IT wraz z usługą wdrożenia |  |  |  | 1 |  |  |
| Oprogramowanie do wykonywania kopii zapasowych |  |  |  | 1 |  |  |
| Suma: | | | | |  |  |

Ponadto proponuję:

1) gwarancja producenta serwer:

24 miesiące

36 miesięcy\*

2) gwarancja producenta UPS

24 miesiące

36 miesięcy\*

3) gwarancja (**Router i bramka bezpieczeństwa ze zintegrowanym przełącznikiem PoE, Switch zarządzany SFP+, Switch zarządzany, Punkt dostępowy)**

24 miesiące

36 miesięcy\*

\* niepotrzebne skreślić

2. Oferuję wykonanie przedmiotu zamówieniaw zakresie **Zadania 2** za łączne wynagrodzenie ryczałtowe w wysokości netto .................................. zł (wpisać pozycję z przedostatniej kolumny) i w wysokości brutto …………………. zł (wpisać pozycję z ostatniej kolumny i ostatniego wiersza)\*.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Nazwa** | **Cena jednostkowa netto (1)** | **VAT % (2)** | **Cena jednostkowa brutto (3)** | **Ilość (4)** | **Cena netto ogółem**  **(1) x (4)** | **Cena brutto**  **ogółem**  **(3) x (4)** |
| Serwer |  |  |  | 2 |  |  |
| Dysk do serwera |  |  |  | 16 |  |  |
| Dysk kopii zapasowych |  |  |  | 2 |  |  |
| Stacja dokująca |  |  |  | 1 |  |  |
| Suma: | | | | |  |  |

Ponadto proponuję:

1) gwarancja serwer:

24 miesiące

36 miesięcy\*

2) instalacji dysków 3.5"

8

Więcej niż 8\*

3) gwarancja producenta na dyski

36 miesięcy

48 miesięcy

60 miesięcy\*

\* niepotrzebne skreślić

**OPIS PRZEDMIOTU ZAMÓWIENIA (wypełnić odpowiednią część)**

**Zadanie 1**

**1. Serwer**

|  |  |  |
| --- | --- | --- |
| **L.p.** | **Opis parametrów technicznych** | **Podać proponowane parametry** |
| 1 | Producent |  |
| 2 | Model serwera |  |
| 3 | Procesor |  |
| 4 | Model procesora |  |
| 5 | Wynik w teście SPECrate2017\_int\_base, ze strony www.spec.org |  |
| 6 | Obudowa Rack – wysokość |  |
| 7 | Ilość obsługiwanych dysków 2,5” min 24 |  |
| 8 | Pamięć RAM minimum 256 GB |  |
| 9 | Ilość wolnych slotów pamięci RAM |  |
| 10 | Gniazda PCI |  |
| 11 | Interfejs sieciowy Ethernet |  |
| 12 | Interfejs sieciowy SFP+ |  |
| 13 | Model wkładek optycznych zainstalowanych w standardzie min. SFP+ |  |
| 14 | Ilość wkładek optycznych zainstalowanych w standardzie min. SFP+ |  |
| 15 | Ilość zainstalowanych dysków SSD SAS |  |
| 16 | Model dysku SSD SAS |  |
| 17 | Pojemność dysku SSD SAS |  |
| 18 | Rodzaj optymalizacji (zastosowań) dysków SSD SAS |  |
| 19 | Ilość zainstalowanych dysków M.2 SATA |  |
| 20 | Model dysku M.2 SATA |  |
| 21 | Pojemność dysku M.2 SATA |  |
| 22 | Model kontrolera RAID |  |
| 23 | Pamięć cache kontrolera RAID |  |
| 24 | Wbudowane porty |  |
| 25 | Karta video umożliwiająca wyświetlenie rozdzielczości min. 1280x1024 |  |
| 26 | Wentylatory |  |
| 27 | Zasilacze |  |
| 28 | System operacyjny |  |
| 29 | Ilość licencji systemu operacyjny |  |
| 30 | Ilość rdzeni obsługiwanych przez system operacyjny |  |
| 31 | Ilość licencji Cal na użytkownika |  |
| 32 | Środowisko wirtualne producent |  |
| 33 | Środowisko wirtualne wersja |  |
| 34 | Środowisko wirtualne Maks. ilość hostów |  |
| 35 | Środowisko wirtualne Maks. ilość CPU |  |
| 36 | Bezpieczeństwo |  |
| 37 | Diagnostyka (Panel LCD/Diody) |  |
| 38 | Karta Zarządzania model |  |
| 39 | Karta Zarządzania wersja oprogramowania / licencji |  |
| 40 | Gwarancji min. 24 miesiące |  |
| 41 | Możliwość rozszerzenia gwarancji producenta do 7 lat |  |
| 42 | Uszkodzony dysk twardy pozostaje u Zamawiającego (Tak/Nie) |  |

**2. UPS**

|  |  |  |
| --- | --- | --- |
| **L.p.** | **Opis parametrów technicznych** | **Podać proponowane parametry** |
| 1 | Producent |  |
| 2 | Model |  |
| 3 | Zakres napięcia wejściowego w trybie podstawowym |  |
| 4 | Typ gniazda wejściowego |  |
| 5 | Moc wyjściowa |  |
| 6 | Napięcie wyjściowe |  |
| 7 | Zniekształcenia napięcia wyjściowego |  |
| 8 | Typ przebiegu |  |
| 9 | Złącza wyjściowe |  |
| 10 | Typ akumulatora |  |
| 11 | Typowy czas ładowania |  |
| 12 | Oczekiwana żywotność akumulatora (lata) |  |
| 13 | Ilość zestawów RBC™ |  |
| 14 | Możliwość podłączenia do 10 zewnętrznych modułów akumulatorowych |  |
| 15 | Akumulatory zewnętrzne typu plug-and-play |  |
| 16 | Akumulatory wymienialne przez użytkownika “na gorąco” bez przerywania pracy systemu |  |
| 17 | Czas podtrzymania przy obciążeniu 100% w trybie podstawowym |  |
| 18 | Czas podtrzymania przy obciążeniu 50% w trybie podstawowym |  |
| 19 | Efektywność urządzenia przy obciążeniu 100% |  |
| 20 | Interfejs Port (s) |  |
| 21 | Moduł SNMP |  |
| 22 | Panel sterowania |  |
| 23 | Okres gwarancji |  |
| 24 | Okres gwarancji baterie |  |

**3. Router i bramka bezpieczeństwa ze zintegrowanym przełącznikiem PoE i sieciowym rejestratorem wideo**

|  |  |  |
| --- | --- | --- |
| **L.p.** | **Opis parametrów technicznych** | **Podać proponowane parametry** |
| 1 | Producent |  |
| 2 | Model |  |
| 3 | Procesor |  |
| 4 | Taktowanie procesora |  |
| 5 | Pamięć systemowa |  |
| 6 | Pamięć wbudowana |  |
| 7 | Zatoka HDD 3,5” |  |
| 8 | Przepustowość IDS/IPS |  |
| 9 | Maks. Pobór mocy (nie licząc wyjścia PoE) |  |
| 10 | Zasilanie |  |
| 11 | Interfejs zarządzania |  |
| 12 | Interfejs sieciowy |  |
| 13 | Interfejs SFP+ |  |
| 14 | PoE |  |
| 15 | Maks. PoE na port 802.3af |  |
| 16 | Maks. PoE na port 802.3at |  |
| 17 | Przyciski Reset |  |
| 18 | Wyświetlacz LCM |  |
| 19 | Model wkładki optycznej zainstalowanej w interfejsie sieciowy LAN w standardzie min. SFP+ |  |
| 20 | Model wkładki optycznej zainstalowanej w interfejsie sieciowy WAN w standardzie min. SFP+ |  |
| 21 | Gwarancja |  |

**4. Switch zarządzany SFP+**

|  |  |  |
| --- | --- | --- |
| **L.p.** | **Opis parametrów technicznych** | **Podać proponowane parametry** |
| 1 | Producent |  |
| 2 | Model |  |
| 3 | Typ przełącznika |  |
| 4 | Przełącznik wielowarstwowy |  |
| 5 | Liczba zainstalowanych modułów |  |
| 6 | Przepustowość rutowania / przełączania |  |
| 7 | Wydajność |  |
| 8 | Prędkość przekazywania |  |
| 9 | Typ obudowy max |  |
| 10 | Maksymalne zużycie mocy |  |
| 11 | Typ przełącznika |  |
| 12 | Okablowanie Patchord (ilość, długość) |  |
| 13 | Model wkładek optycznych zainstalowanych w standardzie min. SFP+ |  |
| 14 | Ilość wkładek optycznych zainstalowanych w standardzie min. SFP+ |  |
| 15 | Gwarancja |  |

**5. Switch zarządzany**

|  |  |  |
| --- | --- | --- |
| **L.p.** | **Opis parametrów technicznych** | **Podać proponowane parametry** |
| 1 | Producent |  |
| 2 | Model |  |
| 3 | Typ przełącznika |  |
| 4 | Przełącznik wielowarstwowy |  |
| 5 | Liczba portów Ethernet (10/100/1000) |  |
| 6 | Liczba zainstalowanych modułów SFP+ |  |
| 7 | Standardy komunikacyjne |  |
| 8 | Obsługa 10G |  |
| 9 | Dublowanie portów |  |
| 10 | Podpora kontroli przepływu |  |
| 11 | Agregator połączenia |  |
| 12 | Kontrola wzrostu natężenia ruchu |  |
| 13 | Protokół drzewa rozpinającego |  |
| 14 | Obsługa sieci VLAN |  |
| 15 | Przepustowość rutowania / przełączania |  |
| 16 | Prędkość przekazywania |  |
| 17 | Typ uwierzytelniania |  |
| 18 | Maksymalne zużycie mocy |  |
| 19 | Obsługa PoE |  |
| 20 | Model wkładek optycznych zainstalowanych w standardzie min. SFP+ |  |
| 21 | Ilość wkładek optycznych zainstalowanych w standardzie min. SFP+ |  |
| 22 | Gwarancja |  |

**6. Punkt dostępowy**

|  |  |  |
| --- | --- | --- |
| **L.p.** | **Opis parametrów technicznych** | **Podać proponowane parametry** |
| 1 | Producent |  |
| 2 | Model |  |
| 3 | Interfejsy sieciowe |  |
| 4 | Anteny |  |
| 5 | Standardy WiFi |  |
| 6 | Tryby POE |  |
| 7 | Tryby POE |  |
| 8 | Maksymalny pobór mocy |  |
| 9 | Moc nadawcza |  |
| 10 | BSSID na radio |  |
| 11 | Maksymalny pobór mocy |  |
| 12 | Oszczędzanie energii |  |
| 13 | Zabezpieczenia |  |
| 14 | Montowanie (uchwyty w zestawie) Tak /Nie |  |
| 15 | VLAN |  |
| 16 | QoS |  |
| 17 | Izolowanie ruchu gości |  |
| 18 | WMM |  |
| 19 | Jednocześni klienci max |  |
| 20 | Wspierane przepustowości (zależnie od modulacji / szerokości kanału) |  |
| 21 | Gwarancja |  |

**7 Oprogramowanie zapewniające zintegrowane bezpieczeństwo do zarządzenie infrastrukturą IT wraz z usługą wdrożenia**

|  |  |  |
| --- | --- | --- |
| **L.p.** | **Parametry / warunki (minimalne)** | **Podać proponowane parametry** |
| **1** | Producent |  |
| **2** | Wersja oprogramowania |  |
| **Wymagania licencyjne** | | |
| **3** | 1. Program będzie dostarczony na licencji bezterminowej, która umożliwia na pełne wykorzystanie oprogramowania bez granicznej daty użytkownika. 2. Program będzie zapewniał możliwość pracy nielimitowanej liczbie administratorów oraz osób odpowiedzialnych za realizację zadań pomocy technicznej. 3. Program będzie zapewniał obsługę minimum 60 stacji roboczych Windows z użyciem agenta. 4. Wsparcie producenta rozwiązania będzie ważne przez min. 12 miesięcy od *,* licząc od daty dostawy oraz podpisania przez Strony protokołu odbioru zdawczo-odbiorczego bez uwag, w zależności od tego, która czynność przypadnie później. |  |
| **Wymagania ogólne:** | | |
| **4** | * 1. Zamawiający wymaga dostarczenia oprogramowania posiadającego budowę modułową, składającego się z serwera zarządzającego, zdalnych konsoli oraz Agentów.   2. Komunikacja pomiędzy Serwerem a Agentami i Konsolami będzie nawiązywana przy użyciu szyfrowanego protokołu TLS w wersji 1.2 lub wyższej.   3. Moduły po będzie umożliwiał kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych oraz pomocy w formie interaktywnego połączenia sieciowego z obsługiwanym użytkownikiem.   4. Dane, które dotyczą działań pracownika na komputerze, a więc: historia aktywności, polityka korzystania z Internetu oraz aplikacji, dostęp do zewnętrznych nośników danych itp., będą odseparowane od danych technicznych. Będą również grupowane w osobnym, dedykowanym oknie. Powinno pozwalać to na, zgodne z RODO, usuwanie danych wybranego użytkownika bez konieczności usunięcia informacji o stacji roboczej.   5. Dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, będzie objęty kontrolą na poziomie wybranych Administratorów – w programie będzie możliwość nadawania kontom administracyjnym różnych poziomów dostępu oraz uprawnień zarówno do funkcji Programu, grup urządzeń, jak i użytkowników. Główny Administrator będzie miał możliwość zarządzania uprawnieniami konfiguracyjnymi programu dla innych kont z rolą administracyjną np. powinien mieć możliwość wyłączenia zdalnej deinstalacji Agenta, ograniczenia dostępu do Opcji programu oraz logów działań innych administratorów   6. Działania administratorów będą logowane, oznacza to, że program będzie posiadał dziennik z listą czynności wykonanych przez administratorów, które zmodyfikowały obiekty znajdujące się w systemie w tym m.in. logowanie dostępu do Opcji programu, logowanie dostępu do informacji o aktywności użytkownika, logowanie poleceń deinstalacji Agenta. Działania administratorów będą automatycznie eksportowane do zewnętrznego kolektora Syslog.   7. Jeżeli oferowane oprogramowanie/system wymaga odrębnych licencji (systemu operacyjnego lub bazodanowego lub działa na licencjonowanym systemie operacyjnym, lub licencjonowane są komponenty wchodzące w skład infrastruktury Zamawiającego, lub licencjonowana jest ilość użytkowników, serwisantów/administratorów) Zamawiający wymaga dostarczenia niezbędnych licencji.   8. Program będzie zabezpieczony hasłem przed ingerencją użytkownika w jego działanie i próbą usunięcia, nawet jeśli użytkownik ma prawa administratora stacji roboczej, na której pracuje.   9. Agent w procesie instalacji ręcznej będzie posiadał możliwość automatycznego wyszukiwania serwera przez oprogramowanie monitorujące stacje robocze.   10. Oprogramowanie będzie posiadać również obszar funkcjonalny w formie platformy WWW, który pozwala na tworzenie wielu interaktywnych paneli informacyjnych (dashboardów) z responsywnymi widgetami, prezentującymi dane ze wszystkich modułów funkcjonalnych oprogramowania:  1. Liczniki wydajności, Alarmy (wraz z filtrowaniem) oraz odpowiedzi serwisów TCP/IP, Ostatnie urządzenia w sieci, 2. Zmiany w konfiguracji sprzętowej urządzeń z Agentami, Zmiany w konfiguracji aplikacyjnej urządzeń z Agentami, Alarmy dla Zasobów, 3. Statystyki z obszaru wydruków, Statystki użycia aplikacji, Użycie łącza, Aktywność WWW, 4. Statystyki z obsługi zgłoszeń, Lista najnowszych nierozwiązanych zgłoszeń, Lista najstarszych nierozwiązanych zgłoszeń, Zgłoszenia z naruszonym SLA, Zgłoszenia, których SLA wkrótce wygaśnie, 5. Ostatnio podłączone nośniki zewnętrzne, Ostatnie operacje na plikach (wraz z filtrowaniem) |  |
| **Wymagania dla funkcjonalności monitorowania infrastruktury obejmującej serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle:** | | |
| **5** | 1. Wykrywanie urządzeń w sieci poprzez skanowanie ping oraz arp-ping. 2. Wykrywanie urządzeń na podstawie informacji odczytanych z Active Directory (wraz z informacją o OU). 3. Wizualizacja stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci. 4. Wizualizacja map urządzeń poprzez tworzenie spersonalizowanych map z możliwością wyboru koloru tła. 5. Wizualizacja map urządzeń poprzez tworzenie spersonalizowanych map z wykorzystaniem jako tła zaimportowanych obrazków np. schematu rozmieszczenia pomieszczeń w budynku. 6. Wizualizacji map urządzeń poprzez grupowanie urządzeń i przedstawianie ich za pomocą kształtu graficznego. 7. Wizualizacji map urządzeń poprzez wstawianie dowolnego tekstu na mapie. 8. Wizualizacja połączeń pomiędzy urządzeniami a przełącznikami za pomocą linii i informacji, do którego portu przełącznika podłączone jest dane urządzenie w sposób manualny oraz automatyczny. 9. Zablokowanie mapy urządzeń przed przypadkową edycją. 10. Serwisy TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program powinien monitorować czas ich odpowiedzi i procent utraconych pakietów. 11. Serwer pocztowy:     1. monitorowanie czasu logowania do serwisu odbierającego oraz czasu wysyłania poczty;     2. możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie (np. gdy ważne parametry znajdą się poza zakresem);     3. możliwość wykonywania operacji testowych;     4. możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa. 12. Monitorowanie serwerów WWW i adresów URL. 13. Cykliczne monitorowanie czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS. 14. Obsługa szyfrowania SSL/TLS w powiadomieniach e-mail. 15. Obsługa urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją, (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.) – monitorowanie wartości za pomocą nazw zmiennych oraz OID. 16. Obsługa komunikatów syslog i pułapek SNMP i ewidencjonowanie odebranych z nich danych. 17. Monitoring routerów i przełączników wg: 18. zmian stanu interfejsów sieciowych; 19. ruchu sieciowego; 20. podłączonych stacji roboczych – graficzna prezentacja panelu switcha; 21. ruchu generowanego przez podłączone do portów stacje robocze. 22. Serwis Windows: monitor serwisów Windows powinien alarmować gdy serwis przestanie działać oraz pozwalać na jego uruchomienie/zatrzymanie/zrestartowanie. 23. Wyświetlanie statystyk przy każdym urządzeniu na mapie takich jak: czas odpowiedzi urządzenia, czas od ostatniej poprawnej odpowiedzi, nazwa DNS, adres IP, status zarządzalności SNMP, ostrzeżenie o zdarzeniu na urządzeniu. 24. Wydajność systemów Windows: obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy. 25. Kompilacja plików MIB, umożliwiająca dodawanie definicji dla modułów SNMP. 26. Nakładanie na urządzenia liczników wydajności WMI oraz SNMP wg szablonów. 27. Definiowanie alarmów z wykorzystaniem akcji związanych ze zdarzeniami w systemie, m.in.: wysłanie komunikatu pulpitowego, wysłanie wiadomości e-mail, wysłanie SMS, uruchomienie programu, wysłanie pułapki SNMP, wysłanie pakietu Wake-On-LAN, zatrzymanie/restart usługi Windows, wyłączenie/restart komputera. 28. Budowanie alarmów przez administratora z wykorzystaniem ciągu przyczynowo skutkowego (możliwość samodzielnego wskazania przez administratora dowolnego zdarzenia z listy, którego wykrycie wzbudzi alarm oraz dowolnej liczby akcji wybranych z listy, które zostaną wykonane jako reakcja na wykryte zdarzenie). 29. Integracja ze sprzętową bramką GSM w celu wysyłania powiadomień SMS z wykorzystaniem protokołu netGSM (SOAP). |  |
| **Wymagania dla funkcjonalności inwentaryzacji:** | | |
| **6** | * 1. Automatycznie gromadzenie informacje o sprzęcie i oprogramowaniu na stacjach roboczych.   2. Prezentacja szczegółów dotyczących sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp.   3. Prezentacja zestawień posiadanych konfiguracji sprzętowych, wolnego miejsca na dyskach, średniego wykorzystanie pamięci, informacji pozwalających na wytypowanie systemów, dla których konieczny jest upgrade.   4. Informowanie o zainstalowanych aplikacjach oraz aktualizacjach Windows (możliwość audytowania i weryfikacji użytkowania licencji.   5. Zbieranie informacji w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itp.   6. Wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera.   7. Możliwość odczytania numeru seryjnego (klucze licencyjne).   8. Automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych.   9. Przegląd informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp.   10. Tworzenie listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI) znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem metadanych plików użytkownika: obrazów (wymiary obrazka), video (długość filmu), audio (długość nagrania), archiwów (liczba plików w środku, rozmiar po wypakowaniu).   11. Wymiana plików „do” i „ze” stacją roboczą poprzez funkcję Menedżera plików. Działania administratorów wykonywane w tej funkcji powinny być logowane.   12. Tworzenie powiązań między zasobami a urządzeniami.   13. Tworzenie powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak i zsynchronizowanymi z Active Directory), wskazywanie osób odpowiedzialnych.   14. Wskazywanie osób uprawnionych do użycia zasobów.   15. Definiowanie własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości - dla danego urządzenia lub oprogramowania z możliwością dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer dokumentu zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu gwarancji, termin kolejnego przeglądu (data, po której administrator otrzyma powiadomienie e-mail o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, lub własny komentarz   16. Określenie atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów.   17. Określenie atrybutów dodatkowych tylko dla wybranych typów zasobów.   18. Definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie.   19. Import danych z zewnętrznego źródła (.CSV).   20. Przechowywanie dowolnych dokumentów (np. pliki .DOCX, .XLSX, .PDF), np.: skan faktury zakupu, gwarancji, dowolnego dokumentu itp.   21. Tworzenie powiązań między zasobami a dokumentami.   22. Oznaczanie statusów zasobów, np. w użyciu, w naprawie, zutylizowany itp.   23. Ewidencja czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie, konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie czynności.   24. Generowanie zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania;   25. Przygotowanie wielu szablonów generowanych dokumentów i protokołów przekazania zasobów wraz z konfigurowalną sekcją zawierającą dane i logo Zamawiającego.   26. Konfiguracja stylu automatycznego numerowania dodawanych zasobów wg zdefiniowanego wzorca.   27. Konfiguracji stylu automatycznego numerowania dodawanych dokumentów i protokołów wg zdefiniowanego wzorca.   28. Archiwizacja i porównywanie audytów zasobów.   29. Tworzenia kodów kreskowych dla zasobów.   30. Drukowanie kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów, które posiadają numer inwentarzowy.   31. Inwentaryzacja zasobów posiadających kody kreskowe za pomocą aplikacji mobilnej dla systemu Android poprzez wyszukiwanie zasobów, skanowanie etykiet, dodawanie i edycję zasobów, dodawanie czynności serwisowych, drukowanie etykiet.   32. Inwentaryzacja stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline).   33. Definiowanie alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data” z atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnie licencja/gwarancja”).   34. Agent inwentaryzacji na system Android który powinien zapewniać funkcjonalność pozyskiwania informacji o oprogramowaniu i audycie licencji w zakresie:  1. Skanowania plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP. 2. Informacji o aplikacjach używanych u Zamawiającego; 3. Tworzenia własnych wzorców aplikacji; 4. Tworzenia dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp. 5. Informacji o komputerach, na których aplikacja została wykryta; 6. Zarządzania posiadanymi licencjami; 7. Wskazywania osób odpowiedzialnych za licencję; 8. Wskazania użytkowników licencji; 9. Tworzenia powiązań między licencjami a dokumentami; 10. Zarządzania licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu; 11. Audyt legalności oprogramowania oraz powiadomień w razie przekroczenia liczby posiadanych licencji - z możliwością wykonania aktualnych raportów audytowych; 12. Raport zgodności licencji; 13. Możliwości przypisania do programów numerów seryjnych, wartości itp. |  |
| **Wymagania dla funkcjonalności obsługi użytkowników:** | | |
| **7** | 1. Monitorowanie aktywności użytkowników pracujących na komputerach z systemem Windows. 2. Monitorowanie faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy). 3. Monitorowanie procesów (każdy proces powinien mieć możliwość podania całkowitego czasu działania oraz czasu aktywności użytkownika) wraz informacją o uruchomieniu na podwyższonych uprawnieniach. 4. Monitorowanie rzeczywistego użytkowania programów (m.in. procentowej wartoś wykorzystania aplikacji, obrazującej czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność. 5. Monitorowanie informacji o edytowanych przez użytkownika dokumentach. 6. Monitorowanie historii pracy (cykliczne zrzuty ekranowe). 7. Monitorowanie listy odwiedzanych stron WWW (liczba odwiedzin stron z nagłówkami, liczbą i czasem wizyt). 8. Monitorowanie transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika). 9. Monitorowanie wydruków m.in. przekazywania informacji o dacie wydruku, informacji o wykorzystaniu drukarek, raportów dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek. Monitorowanie kosztów wydruków. 10. Monitorowanie nagłówków przesyłanej w aplikacjach Zamawiającego poczty e-mail. 11. Blokowanie stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla stacji roboczej, na której zalogowany jest użytkownik, z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen (np. \*.domena.pl). Reguły w postaci listy domen tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami. 12. Blokowanie ruchu na wskazanych portach TCP/IP 13. Blokowanie pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem. 14. Wysyłanie powiadomień gdy użytkownik: odwiedzi stronę z określonej grupy domeny; pobierze lub wyśle określoną ilość danych w ciągu dnia w sieci lokalnej lub Internet; wydrukuje określoną ilość stron w ciągu dnia. 15. Przygotowanie zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu (który można dołączyć np. do akt pracownika). 16. Definiowanie godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone. 17. Generowanie raportów dla użytkowników Active Directory niezależnie od tego, na jakich komputerach pracowali w danym czasie. 18. Blokowanie uruchamiania aplikacji wg maski nazwy oraz lokalizacji pliku. Reguły w postaci listy blokowanych plików lub lokalizacji powinny być tworzone dla użytkownika lub grupy użytkowników i powinny być kopiowane pomiędzy grupami lub kontami. 19. Możliwość uzyskania dostępu z prywatnego komputera tylko do swojego komputera firmowego, który pozostał w Szpitalu, za pomocą funkcji zdalnego dostępu przez każdego pracownika |  |
| **Wymagania dla funkcjonalności ochrony danych przed wyciekiem:** | | |
| **8** | * 1. Możliwość blokowania urządzeń i nośników danych.   2. Możliwość zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny.   3. Możliwość blokowania urządzeń i interfejsów fizycznych: USB, FireWire, gniazd kart pamięci, SATA, dysków przenośnych, napędów CD/DVD, stacji dyskietek.   4. Możliwość blokowania interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA.   5. Możliwość blokownia tylko urządzeń służących do przenoszenia danych (inne urządzenia (drukarka, klawiatura, mysz itp.) mogą być podłączane).   6. Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych.   7. Wsparcie bezpieczeństwa systemu:  1. integracja i zarządzanie ustawieniami Windows Defender; 2. integracja z Windows Defender w zakresie odczytu stanu ochrony, włączenia i wyłączenia ochrony, tworzenia reguł ruchu; 3. monitorowanie stanu szyfrowania dysków BitLocker; 4. monitorowanie stanu modułu TPM.    1. Zarządzanie prawami dostępu do urządzeń: 5. możliwość definiowania praw użytkowników/grup do odczytu, zapisu czy wykonania plików; 6. możliwość autoryzowania urządzeń firmowych (przykładowo szyfrowanych): pendrive’ów, dysków itp. - urządzenia prywatne są blokowane; 7. możliwość całkowitego zablokowania określonych typów urządzeń dla wybranych użytkowników; 8. możliwość całkowitego zablokowania określonych typów urządzeń dla wybranych użytkowników; 9. możliwość usuwania z listy znanych urządzeń nośników, które np. zostały zutylizowane.    1. Audyt operacji na plikach na urządzeniach przenośnych: 10. zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych; 11. podłączenie/odłączenie urządzenia przenośnego.     1. Możliwość monitorowania operacji na plikach w lokalnych folderach komputera użytkownika.     2. Możliwość integracji z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych. Możliwość przydzielania uprawnień do kont użytkowników lokalnych. |  |
| **Wymagania dla funkcjonalności realizacji zdalnej pomocy użytkownikom, poprzez:** | | |
| **9** | * 1. podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli wraz z możliwością zdefiniowania czy użytkownik powinien zostać zapytany o zgodę na połącznie i opcją odrzucenia takiego połącznia przez użytkownika (np. w przypadku pracowników wysokiego szczebla);   2. zablokowanie w trakcie zdalnego dostępu działania myszy oraz klawiatury dla użytkownika;   3. zdefiniowanie bazy zgłoszeń umożliwiającej użytkownikom zgłaszanie problemów technicznych, które z kolei są przetwarzane i przyporządkowywane odpowiednim administratorom/serwisantom, otrzymującym automatycznie powiadomienie o przypisanym im problemie;   4. możliwość przetwarzania zgłoszeń w trybie anonimowym (wsparcie w realizacji wymogów „Dyrektywy o sygnalistach”) oraz posiadanie dokumentów prawnych dot. ochrony sygnalistów w tym szablonów regulaminu zgłoszeń wewnętrznych wymagany przez Dyrektywę;   5. umożliwienie użytkownikom monitorowania procesu rozwiązywania zgłoszonych przez nich problemów i ich aktualnych statusów, jak również możliwość wymiany informacji z administratorem/serwisantem poprzez komentarze, które są wpisywane i widoczne dla obu stron;   6. wbudowany komunikator (czat), który umożliwia przesyłanie wiadomości pomiędzy zalogowanymi użytkownikami i administratorami/serwisantami (wraz z wyszukiwarką wiadomości oraz automatycznym oczyszczaniem historii rozmów) oraz bazę wiedzy pomagającą użytkownikom samodzielnie rozwiązywać najprostsze, powtarzające się problemy;   7. umożliwienie informowania pracowników o zdarzeniach, np. planowanych przestojach w dostępie do usług, przez komunikaty z graficznym formatowaniem treści oraz łączami do artykułów w bazie wiedzy;   8. dedykowany portal w oparciu o przeglądarkę internetową, który jest dostępem do systemu zgłoszeń oraz bazy wiedzy,   9. pobieranie listy użytkowników z Active Directory;   10. zarządzania lokalnymi kontami Windows w zakresie: tworzenia, usuwania, aktywacji, edycji uprawnień, resetu hasła, edycji kont;   11. zarządzanie dostępem Administratorów/Serwisantów do zgłoszeń poprzez system zarządzania regułami widoczności zgłoszeń;   12. zarządzanie dostępem do czatu w 3 poziomach uprawnień: pełny dostęp, brak dostępu lub dostęp ograniczony wyłącznie do pomocy technicznej;   13. tworzenie własnego drzewa kategorii zgłoszeń wraz z możliwością grupowania kategorii w folderach (do 4 poziomów kategorii), opisami kategorii oraz klauzulą RODO;   14. automatyczne przypisywanie konkretnych pracowników helpdesk do zgłoszeń w określonych kategoriach lub pochodzących od określonych grup użytkowników;   15. procesowanie zgłoszeń użytkowników z wiadomości e-mail;   16. wykonywanie operacji na wielu zgłoszeniach równocześnie;   17. dołączanie załączników do zgłoszeń;   18. szybki dostęp do ostatnich zgłoszeń, artykułów bazy wiedzy i załączników;   19. wprowadzenie komentarza oraz informacji o czasie poświęconym na rozwiązanie w kreatorze wyświetlanym przy zamykaniu zgłoszenia;   20. dystrybucję oprogramowania przez Agenta;   21. dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików MSI);   22. zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecania operacji powinno następować kolejkowanie zadania dystrybucji pliku;   23. możliwość skonfigurowania automatyzacji procesowania zgłoszeń wraz z powiadomieniami e-mail wysyłanymi do określonych użytkowników w zgłoszeniu;   24. planowanie nieobecności Administratorów/Serwisantów;   25. obsługę umów o gwarantowanym poziomie świadczenia usług (SLA) wraz z raportami np. przekroczeń SLA wraz z podsumowaniem;   26. generowanie raportów obsługi helpdesk;   27. zarządzanie procesami systemu Windows (w zakresie: zakończ proces, zakończ drzewo procesu, uruchom nowy proces w sesji użytkownika wraz z parametrami);   28. wymiany plików do i ze stacji roboczej poprzez funkcję Menedżera plików. |  |
| **Wymagania dla prac wdrożeniowo-szkoleniowych:** | | |
| **10** | 1. Zakres minimalnych prac w obszarze przeprowadzenia szkolenia dla pracowników Działu Informatyki Zamawiającego pełniącego rolę pracownika pomocy technicznej wdrażanego systemu:    1. Zakres szkolenia:       1. Ogólne omówienie rozwiązania i jego struktury;       2. Praca w obszarze obsługi zgłoszeń w przypadku pełnienia roli osoby obsługującej zgłoszenie;       3. Praca w obszarze obsługi zgłoszeń w przypadku pełnienia roli osoby obserwującej zgłoszenie;       4. Praca w obszarze obsługi zgłoszeń w przypadku pełnienia roli osoby zgłaszającej problem czy potrzebę;       5. Możliwości pomocy zdalnej i komunikacji ze zgłaszającym;       6. Mechanizmy raportowania i generowania statystyk w zgłoszeniach;       7. Rozwiązywanie najczęstszych problemów;       8. Egzamin certyfikujący.    2. Czas trwania szkolenia:       1. Minimum 5 godziny dla pracowników Działu Informatyki odpowiedzialnych za obsługę systemu zgłoszeń;       2. Szkolenie powinno się kończyć egzaminem oraz wydaniem certyfikatu.   **Prace wdrożeniowo-szkoleniowe powinny być przeprowadzone przez inżyniera certyfikowanego przez producenta oferowanego rozwiązania.** |  |

**8 Oprogramowanie do wykonywania kopii zapasowych.**

|  |  |  |
| --- | --- | --- |
| **L.p.** | **Parametry / warunki (minimalne)** | **Podać proponowane parametry** |
| **1** | Producent |  |
| **2** | Wersja oprogramowania |  |
| **Wymagania licencyjne** | | |
| **3** | 1. Oprogramowanie będzie zapewniać obsługę minimum 15 obciążeń (maszyn wirtualnych, fizycznych) 2. Wsparcie producenta rozwiązania będzie uprawniać do wykonywania aktualizacji i przejścia na nową wersję przez okres min. 60 miesięcy 3. Oprogramowanie będzie można rozszerzyć do minimum 50 obciążeń (maszyn wirtualnych, fizycznych |  |
| **Wymagania ogólne** | | |
| **4** | 1. Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner: https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions i spełniać minimalne wymaganie : - minimalna liczba referencji 150, - minimalna ocena z referencji 4,5, 2. Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 5.5, 6.0, 6.5, 6.7 and 7.0 oraz Microsoft Hyper-V 2008R2SP1, 2012, 2012 R2 i 2019. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej 3. Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami. 4. Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manger, klastrami hostów oraz pojedynczymi hostami. 5. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux. |  |
| **Całkowite koszty posiadania** | | |
| **5** | 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 pozwalać na tworzenie kopii zapasowych w trybach: Pełny, pełny syntetyczny, przyrostowy i odwrotnie przyrostowy (tzw. reverse-inremental) 4. 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 5. 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. 6. 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. 7. Oprogramowanie musi pozwalać na rozszerzenie lokalnej przestrzeni backupowej poprzez integrację z Microsoft Azure Blob, Amazon S3 oraz z innymi kompatybilnymi z S3 macierzami obiektowymi. Proces migracji danych powinien być zautomatyzowany. Jedynie unikalne bloki mogą być przesyłane w celu oszczędności pasma oraz przestrzeni na przechowywane dane. Funkcjonalność ta nie może mieć wpływu na możliwości odtwarzania danych. 8. Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania 9. Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota. 10. Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL oraz Oracle (w tym odtwarzanie point-in-time) 11. Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu 12. Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API 13. Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji 14. 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 15. Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania 16. Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX) 17. Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych. |  |
| **Wymagania RPO** | | |
| **6** | 1. Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej 2. Oprogramowanie musi wykorzystywanać mechnizmy 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 4. Oprogramowanie musi oferować ten mechanizm z dokładnością do pojedynczego datastoru 5. Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora 6. 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 i być dostępna dla następujących macierzy: HPE, Dell EMC, NetApp, Cisco, IBM, Lenovo, Fujitsu, Huawei, INFINIDAT, Pure Storage. 7. Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware. 8. Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn 9. Oprogramowanie musi posiadać wsparcie dla NDMP 10. Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son) 11. Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku, gdy repozytorium backupów jest umiejscowione na Dell EMC DataDomain. Funkcjonalność powinna wspierać łącze sieciowe lub FC. 12. Oprogramowanie musi umieć korzystać z protokołu Catalyst (w tym Catalyst Copy) w przypadku, gdy repozytorium backupów jest umiejscowione na HPE StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC. 13. Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 lub 2019 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS. 14. Repozytoria oparte o XFS muszą pozwalać na zmiezmienność danych przez określoną ilość czasu (tzw Immutability) 15. Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN. 16. 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. 17. Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwośc zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO. 18. Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik 19. Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding) 20. Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN) |  |
| **Wymagania RTO** | | |
| **7** | 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 oraz Hyper-V niezależnie od rodzaju storage’u użytego do przechowywania kopii zapasowych. 2. Dodatkowo dla środowiska vSphere i Hyper-V 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 umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków 6. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2. 7. Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików 8. Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V. 9. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z następujących systemów plików:  * Linux: ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs * BSD: UFS, UFS2 * Solaris: ZFS, UFS * Mac: HFS, HFS+ * Windows: NTFS, FAT, FAT32, ReFS * Novell OES: NSS  1. Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces. 2. Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej. 3. Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników oraz pozwalać na odtworzenie haseł. 4. Oprogramowanie musi wspierać granularne odtwarzanie dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA oraz elementów AD Sites. 5. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"), 6. Oprogramowanie musi wspierać przywracanie danych Exchange do oryginalnego środowiska 7. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowszych 8. Oprogramowanie musi wspierać odtworzenie point-in-time wraz z możliwością przywrócenia bazy do oryginalnego środowiska 9. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowszych 10. Oprogramowanie musi wspierać odtworzenia elementów, witryn, uprawnień dla witryn Sharepoint. 11. 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. 12. Oprogramowanie musi pozwalać na zaprezentowanie oraz migrację online baz MS SQL oraz Oracle bezpośrednio z pliku kopii zapasowej do działającego serwera bazodanowego 13. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN 14. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA 15. Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN |  |
| **Ograniczenie ryzyka** | | |
| **8** | 1. Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. 2. Dla VMware’a oprogramowanie musi pozwalać na uruchomienie takiego środowiska 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 mieć podobne mechanizmy dla replik w środowisku vSphere 5. Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32. 6. Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego. |  |
| **Monitoring** | | |
| **9** | 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 5.5, 6.0, 6.5, 6.7 and 7.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie 3. System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016 oraz 2019 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 mieć status „VMware Ready” i być przetestowany i certyfikowany przez VMware 5. System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter 6. System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn 7. System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel 8. System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk 9. System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora 10. System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów 11. System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard) 12. System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna 13. System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego 14. System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta 15. System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych. 16. 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. 17. System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware 18. System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji 8.x i 9.x |  |
| **Raportowanie** | | |
| **8** | 1. System raportowania musi umożliwić tworzenie raportów z infrastruktury wirtualnej bazującej na VMware ESX/ESXi 5.5, 6.0, 6.5, 6.7 and 7.0 vCenter Server 5.x oraz 6.x jak również Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016 oraz 2019 2. System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów. 3. System musi być certyfikowany przez VMware i posiadać status „VMware Ready” 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 |  |

**Zadanie 2**

**1. Serwer**

|  |  |  |
| --- | --- | --- |
| **L.p.** | **Opis parametrów technicznych** | **Podać proponowane parametry** |
| 1 | Producent |  |
| 2 | Model serwera |  |
| 3 | Procesor |  |
| 4 | Model procesora |  |
| 5 | Wynik w teście dostępnym na stronie internetowej www.cpubenchmark.net dla konfiguracji Multiple CPU |  |
| 6 | Obudowa Rack – wysokość |  |
| 7 | Ilość obsługiwanych dysków 3,5” min. 8 |  |
| 8 | Pamięć RAM minimum 256 GB |  |
| 9 | Ilość wolnych slotów pamięci RAM |  |
| 10 | Interfejs sieciowy Ethernet |  |
| 11 | Interfejs sieciowy SFP+ |  |
| 12 | Model wkładek optycznych zainstalowanych w standardzie min. SFP+ |  |
| 13 | Ilość wkładek optycznych zainstalowanych w standardzie min. SFP+ |  |
| 14 | Ilość zainstalowanych kieszeni na dyski |  |
| 15 | Model kontrolera RAID |  |
| 16 | Pamięć cache kontrolera RAID |  |
| 17 | Wbudowane porty |  |
| 18 | Wentylatory |  |
| 19 | Zasilacze |  |
| 20 | Bezpieczeństwo |  |
| 21 | Diagnostyka (Panel LCD/Diody) |  |
| 22 | Karta Zarządzania model |  |
| 23 | Karta Zarządzania wersja oprogramowania / licencji |  |
| 24 | Gwarancji min. 24 miesiące |  |

**2. Dysk do serwer**

|  |  |  |
| --- | --- | --- |
| **L.p.** | **Opis parametrów technicznych** | **Podać proponowane parametry** |
| 1 | Producent |  |
| 2 | Model |  |
| 3 | Dedykowany do |  |
| 4 | Rodzaj dysku |  |
| 5 | Typ |  |
| 6 | Format |  |
| 7 | Interfejs |  |
| 8 | Pojemność |  |
| 9 | Prędkość obrotowa |  |
| 10 | Pamięć cache |  |
| 11 | Szybkość transmisji interfejsu dysku twardego |  |
| 12 | Transfer zewnętrzny |  |
| 13 | Wytrzymałość na wstrząsy w czasie pracy |  |
| 14 | Niezawodność MTBF |  |
| 15 | Gwarancja min. 36 |  |

**3. Dysk do kopii zapasowych**

|  |  |  |
| --- | --- | --- |
| **L.p.** | **Opis parametrów technicznych** | **Podać proponowane parametry** |
| 1 | Producent |  |
| 2 | Model |  |
| 3 | Dedykowany do |  |
| 4 | Rodzaj dysku |  |
| 5 | Typ |  |
| 6 | Format |  |
| 7 | Interfejs |  |
| 8 | Pojemność |  |
| 9 | Prędkość obrotowa |  |
| 10 | Pamięć cache |  |
| 11 | Szybkość transmisji interfejsu dysku twardego |  |
| 12 | Transfer zewnętrzny |  |
| 13 | Wytrzymałość na wstrząsy w czasie pracy |  |
| 14 | Niezawodność MTBF |  |
| 15 | Gwarancja min. 36 |  |

**4. Stacja dokująca na dwa dyski**

|  |  |  |
| --- | --- | --- |
| **L.p.** | **Opis parametrów technicznych** | **Podać proponowane parametry** |
| 1 | Producent |  |
| 2 | Model |  |
| 3 | Typ obudowy |  |
| 4 | Rozmiar |  |
| 5 | Interfejs obudowy |  |
| 6 | Interfejs dysku |  |
| 7 | Transfer zapisu dla USB 3.1 |  |
| 8 | Dodatkowe informacje |  |
| 9 | Dołączone akcesoria |  |
| 10 | Gwarancja min. 24 |  |