**Opis przedmiotu zamówienia (OPZ)**

Spis treści

[1. Nazwa przedmiotu zamówienia 2](#_Toc212644856)

[2. Miejsce realizacji przedmiotu zamówienia 2](#_Toc212644857)

[3. Termin realizacji zamówienia: 2](#_Toc212644858)

[4. Ogólne warunki dostawy sprzętu informatycznego 3](#_Toc212644859)

[5. Pozostałe wymagania dotyczące realizacji przedmiotu zamówienia. 3](#_Toc212644860)

[6. Ogólne zasady równoważności rozwiązań 3](#_Toc212644861)

[7. Ogólne warunki Gwarancji 5](#_Toc212644862)

[8. Ogólne warunki licencjonowania dostarczonych systemów Informatycznych 5](#_Toc212644863)

[9. Wykaz sprzętu 6](#_Toc212644864)

[9.1. Wymagania Techniczne systemu szaf serwerowych 7](#_Toc212644865)

[9.2. Wymagania w zakresie Systemu zabezpieczeń sieciowych UTM – 2 szt. 9](#_Toc212644866)

[9.3. Wymagania w zakresie Analizatora logów z systemu zabezpieczeń sieciowych – 1 szt. 24](#_Toc212644867)

[9.4. Wymagania w zakresie listew zasilających PDU – 16 szt. 27](#_Toc212644868)

[9.5. Wymagania w zakresie Przełączników sieciowych CORE – 2 szt. 29](#_Toc212644869)

[9.6. Wymagania w zakresie Przełączników sieciowych TOR – 2 szt. 31](#_Toc212644870)

[9.7. Wymagania dotyczące przełączników sieciowych dystrybucyjnych 10G/25G – 4 szt. 35](#_Toc212644871)

[9.8. Wymagania dotyczące Serwera – Wirtualizacja – 4 szt. 39](#_Toc212644872)

[9.9. Wymagania dotyczące Macierzy – Wirtualizacja – 2 szt. 46](#_Toc212644873)

[9.10. Wymagania dotyczące Macierzy – Repozytorium – 2 szt. 52](#_Toc212644874)

[9.11. Wymagania dotyczące przełączników SAN – 2 szt. 57](#_Toc212644875)

[9.12. Wymagania dotyczące Biblioteki taśmowej – 1 szt. 59](#_Toc212644876)

[9.13. Wymagania dotyczące Konsoli i przełączniki KVM – 1 szt. 63](#_Toc212644958)

[9.14. Wymagania dotyczące Systemu wirtualizacji wraz z usługą wdrożenia środowiska witalizacyjnego – 1 szt. 64](#_Toc212644959)

[9.15. Wymagania dotyczące systemu monitoringu Infrastruktury IT – 1 szt. 92](#_Toc212644960)

[9.16. Wymagania dotyczące Serwera Kopii Zapasowej – 1 szt. 93](#_Toc212644961)

[9.17. Wymagania dotyczące Oprogramowania do tworzenia kopii zapasowej – 1 szt. 102](#_Toc212644962)

[9.18. Wymagania dotyczące Serwerowych systemów operacyjnych – 7 szt. 115](#_Toc212644963)

[9.19. Wymagania dotyczące Zestawów komputerowych – 54 szt. 119](#_Toc212644964)

[9.19.1. W skład zestawu wchodzi komputer przenośny, monitor, mysz i klawiatura bezprzewodowa, słuchawki oraz torba – 38 szt. 119](#_Toc212644965)

[9.19.2. W skład zestawu wchodzi komputer, monitor, mysz i klawiatura bezprzewodowa oraz słuchawki – 16 szt. 130](#_Toc212644970)

[9.20. Wymagania dotyczące Drukarek biurowych – 10 szt. 137](#_Toc212644971)

[9.21. Wymagania dotyczące Drukarek\urządzeń wielofunkcyjnych – 3 szt. 139](#_Toc212644972)

[9.22. Wymagania dotyczące telefonów Voip – 30 szt. 142](#_Toc212644973)

[9.22.1. Telefon IP Voip typu Desktop – 25 szt. 142](#_Toc212644974)

[9.22.2. Telefon IP Voip typu bezprzewodowy – 5 szt. 145](#_Toc212644975)

[9.23. Wymagania dotyczące subskrypcji oprogramowania biurowego – 40 szt. 146](#_Toc212644976)

[9.24. Wymagania dotyczące urządzenia typu tablet – 2 szt. 148](#_Toc212644977)

[10. Wymagania w zakresie prac montażowo- instalacyjnych 150](#_Toc212644978)

1. **Nazwa przedmiotu zamówienia**

Przedmiotem zamówienia jest dostawa i wdrożenie sprzętu i oprogramowania teleinformatycznego.

1. **Miejsce realizacji przedmiotu zamówienia**

Prace związane z realizacją Przedmiotu zamówienia będą wykonywane w serwerowni zlokalizowanej na terenie miasta Lesznowola zwanej dalej „Serwerownią” lub „Obiektem”. Szczegółowa lokalizacja serwerowni zostanie wskazana przez Zamawiającego na etapie podpisania Umowy.

1. **Termin realizacji zamówienia:**

Wymagane terminy realizacji Przedmiotu zamówienia:

* 1. Przedmiot zamówienia należy zrealizować w terminie zgodnym z zapisami zawartej Umowy.
  2. Dostawę sprzętu należy zrealizować w godzinach pracy Zamawiającego, od poniedziałku do piątku (z wyjątkiem dni ustawowo wolnych od pracy), a w razie konieczności również poza tymi godzinami, zgodnie z potrzebami określanymi na bieżąco przez Zamawiającego.

1. **Ogólne warunki dostawy sprzętu informatycznego**
   1. Dostarczony sprzęt powinien być wolny od wad fizycznych i nie noszący oznak użytkowania.
   2. Dostarczony sprzęt musi być fabrycznie nowy, musi pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski.
   3. Wykonawca zobowiązany jest do instalacji sprzętu informatycznego w lokalizacjach określonych przez Zamawiającego.
   4. Wykonawca zobowiązany jest do skonfigurowania zamawianego sprzętu w uzgodnieniu z Zamawiającym.
   5. Wykonawca jest zobowiązany do zabrania wszystkich kartonów pochodzących od dostarczonego sprzętu.
   6. Wykonawca jest zobowiązany do złożenia dokumentacji powykonawczej, zawierającej w szczególności wszystkie dane dostępu do urządzeń i systemów, które będą wykorzystywane podczas instalacji i konfiguracji sprzętu i systemów, dane wykonanych połączeń sieciowych, schematy fizyczne i logiczne zainstalowanej i skonfigurowanej infrastruktury.
2. **Pozostałe wymagania dotyczące realizacji przedmiotu zamówienia.**

W celu osiągnięcia zakładanych punktów w kredycieENE08 Energy efficient equipment należy wybrać sprzęt, który spełnia następujące kryteria:

* 1. Sprzęt biurowy (drukarki, skanery, komputery, monitory itp.), inne małe urządzenia zasilane elektrycznie (np. urządzenia kuchenne) oraz dodatkowe ogrzewanie elektryczne muszą posiadać dowolną klasę energetyczną zgodną ze standardem Unii Europejskiej (lub klasę wg innego międzynarodowego lub krajowego systemu oznaczeń).

1. **Ogólne zasady równoważności rozwiązań**

W celu uniknięcia wątpliwości, wszędzie, gdziekolwiek w OPZ Zamawiający wskazuje znaki towarowe, patenty lub pochodzenie, źródła lub szczególny proces, który charakteryzuje produkty lub usługi dostarczane przez konkretnego Wykonawcę – Zamawiający zgodnie z art. 99 ust. 5 ustawy Pzp, dopuszcza oferowanie rozwiązań równoważnych. Operowanie przykładowymi nazwami producenta ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania. Posługiwanie się nazwami producentów/produktów ma wyłącznie charakter

przykładowy. Zamawiający, wskazując oznaczenie konkretnego producenta (dostawcy), konkretny produkt lub materiały przy opisie przedmiotu zamówienia, dopuszcza jednocześnie produkty równoważne o parametrach jakościowych i cechach użytkowych co najmniej na poziomie parametrów wskazanego produktu, uznając tym samym każdy produkt o wskazanych lub lepszych parametrach.

Za rozwiązanie równoważne uważa się takie rozwiązanie, które spełni łącznie następujące wymagania:

* zapewnią pełną kompatybilność wszystkich elementów składających się na Przedmiot Umowy,
* zapewnią identyczną lub wyższą funkcjonalność, wydajność i niezawodność,
* będą obsługiwane przez te same narzędzia zarządzania lub równoważne (z poziomu interfejsów API lub GUI),
* będą objęte warunkami gwarancji, wsparciem serwisowym lub technicznym na poziomie nie niższym, co najmniej w takim zakresie i przez co najmniej taki sam okres jak wskazany w OPZ lub PPU,
* nie wpłyną negatywnie na ciągłość pracy, automatyzację zarządzania oraz możliwości utrzymaniowe środowiska informatycznego Zamawiającego.

Dodatkowo, Zamawiający wskazuje, że w odniesieniu do części rozwiązań wskazał inne dodatkowe parametry równoważności, niezbędne do spełnienia.

Wykonawca, który powołuje się na rozwiązania równoważne, ma obowiązek wykazać równoważność oferowanych produktów, w szczególności poprzez przedstawienie:

* specyfikacji technicznych,
* oficjalnych kart katalogowych lub kart produktów,
* dokumentacji producenta lub oświadczenia producenta urządzenia,
* opisów zgodności z wymaganym oprogramowaniem i narzędziami.

Zamawiający zastrzega sobie prawo oceny równoważności na podstawie przedstawionych dowodów, przy czym brak wykazania przez Wykonawcę zgodności na etapie oceny oferty może skutkować jej odrzuceniem na podstawie art. 226 ust. 1 pkt 5 ustawy Pzp.

W przypadkach, w których podane są normy, dopuszcza się rozwiązania równoważne, jednakże Wykonawca, który powoła się na rozwiązania równoważne, jest zobowiązany wykazać, że oferowany przez niego przedmiot dostawy spełnia wymagania określone w wymienionych normach.

1. **Ogólne warunki Gwarancji** 
   1. Okres gwarancji liczony będzie od daty podpisania przez Zamawiającego Protokołu Odbioru Sprzętu.
   2. Czas trwania gwarancji będzie zgodny z oświadczeniem złożonym przez Wykonawcę w ofercie. Nie będzie on jednak krótszy niż wymagany w niniejszym OPZ.
   3. Gwarancja świadczona będzie w siedzibie Zamawiającego.
   4. Świadczenie gwarancji urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta.
   5. Zamawiający ma prawo do dokonywania rozbudowy sprzętu, zgodnie z dokumentacją techniczną, bez utraty gwarancji. Wykonawca nie ponosi odpowiedzialności za uszkodzenia mechaniczne powstałe z winy Zamawiającego.
   6. Minimalne warunki gwarancji sprzętu zostały opisane w Punkcie 9 dla każdego typu urządzenia osobno.
2. **Ogólne warunki licencjonowania dostarczonych systemów Informatycznych**
   1. Licencjobiorcą wszystkich licencji będzie Zamawiający
   2. Oferowane licencje muszą pozwalać na użytkowanie oprogramowania zgodnie z przepisami prawa.
   3. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do rozbudowy, zwiększenia ilości serwerów obsługujących oprogramowanie, przeniesienia danych na osobny serwer aplikacji, osobny serwer plików.
   4. Licencja oprogramowania musi być licencją bez ograniczenia ilości użytkowników, komputerów, serwerów, na których można zainstalować i używać oprogramowanie.
   5. Licencja na oprogramowanie nie może w żaden sposób ograniczać sposobu pracy użytkowników końcowych (np. praca w sieci LAN, praca zdalna poprzez Internet).
   6. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do wykonania kopii bezpieczeństwa oprogramowania w ilości, którą uzna za stosowną.
   7. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do instalacji, użytkowania oprogramowania na serwerach zapasowych uruchamianych w przypadku awarii serwerów podstawowych.
   8. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do korzystania   
      z oprogramowania na dowolnym komputerze klienckim (licencja nie może być przypisana do komputera/urządzenia).
3. **Wykaz sprzętu**

Jeżeli w tabelach nie podano liczby elementów należy rozumieć, że wymagany jest minimum 1 (jeden).

|  |  |  |
| --- | --- | --- |
| **Nr** | **Pozycja** | **Ilość** |
| 1. | System szaf serwerowych wraz z wyposażeniem | 1 |
| 2. | System zabezpieczeń sieciowych UTM | 2 |
| 3. | Analizator logów z systemu zabezpieczeń sieciowych | 1 |
| 4. | Listwy zasilające PDU | 16 |
| 5. | Przełączniki sieciowe CORE | 2 |
| 6. | Przełączniki sieciowe TOR | 2 |
| 7. | Przełączniki sieciowe Dystrybucyjne 10G/25G | 4 |
| 8. | Serwery - wirtualizacja | 4 |
| 9. | Macierz - wirtualizacja | 2 |
| 10. | Macierz - repozytorium | 2 |
| 11. | Przełączniki SAN | 2 |
| 12. | Biblioteka Taśmowa LTO | 1 |
| 13. | Konsola i przełączniki KVM | 1 |
| 14. | System Wirtualizacji wraz z usługą wdrożenia środowiska wirtualizacyjnego | 1 |
| 15. | System monitoringu infrastruktury IT | 1 |
| 16. | Serwer kopii zapasowych | 1 |
| 17. | Oprogramowanie do tworzenia kopii zapasowych | 1 |
| 18. | Serwerowe systemy operacyjne | 7 |
| 19. | Zestaw komputerowy | 54 |
| 20. | Drukarka biurowa | 10 |
| 21. | Drukarka\urządzenie wielofunkcyjne | 3 |
| 22. | Telefony VOIP | 30 |
| 23. | Subskrypcje oprogramowania biurowego | 40 |
| 24. | Urządzenie typu Tablet | 2 |

* 1. **Wymagania Techniczne systemu szaf serwerowych**

Celem zamówienia jest dostawa, instalacja oraz konfiguracja szaf rack w ilości 6 szt. do zastosowań serwerowych i sieciowych. Szafy mają umożliwić bezpieczne i uporządkowane rozmieszczenie urządzeń IT, zapewniając odpowiednią wentylację, dostęp serwisowy oraz możliwość zarządzania okablowaniem.

W ramach realizacji zamówienia Wykonawca zobowiązany będzie do dostarczenia wszystkich niezbędnych materiałów oraz do wykonania prac polegających na dostosowaniu istniejącej instalacji elektrycznej. W szczególności zakres prac obejmuje:

* poprowadzenie przewodów zasilających do lub nad szafy RACK,
* ułożenie przewodów w perforowanych korytach kablowych wykonanych z blachy ocynkowanej,
* montaż wymaganych gniazd zasilających umożliwiających podłączenie listew zasilających oraz urządzeń końcowych.

Dla każdej dostarczonej szafy teleinformatycznej przewidziano:

* 2 szt. gniazd 3-fazowych,
* 2 szt. gniazd 1-fazowych.

|  |  |
| --- | --- |
| **Specyfikacja zamówienia** | **Wymagania** |
| Wymagania ogólne | Zamówienie obejmuje szafy serwerowe o wymiarach **800x1200 mm**, wraz z niezbędnym osprzętem. |
| Dostawa elementów systemu | * + - * 1. Szafy serwerowe: * Wymiary: szerokość 800 mm, głębokość 1200 mm, wysokość dostosowana do potrzeb (standardowo 42U). * Kolor: czarny (RAL 9005) * Wyposażenie:   + Panele zaślepiające dla niewykorzystanych przestrzeni.   + Organizatory kabli   + Wysokiej jakości przepusty kablowe.     - * 1. System monitorowania środowiska (np. temperatury, wilgotności) z możliwością integracji z zewnętrznymi systemami zarządzania IT. |
| Wymagania dotyczące szaf serwerowych: | * + - * 1. Konstrukcja: stalowa, malowana proszkowo, odporna na uszkodzenia mechaniczne.         2. Drzwi: perforowane typu “plaster miodu” z zamkami trzypunktowymi, umożliwiające maksymalny kąt otwarcia 180 stopni.         3. Osłony boczne: Osłony boczne pełne z zamkami jednopunktowymi.         4. Obciążalność: min. 1200 kg ( przy użyciu stopek lub cokołów)         5. Modułowość: możliwość łatwego demontażu i modyfikacji elementów.         6. Montaż: Możliwość ustawienia na stopkach regulacyjnych, kółkach lub cokołach; możliwość zestawienia szaf w zespoły.         7. W płycie dolnej i górnej, fabrycznie zakryte wyłamywanymi zaślepkami otwory kablowe; otwory o szerokości 71 mm pozwalające na wprowadzenie kabli zasilających z wtyczkami trójfazowymi.         8. Dwie pary belek nośnych STANDARD w rozstawie 19”, z możliwością ustawienia w rozstawie 21” w szafach o szerokości 800 mm |
| Wymagania dotyczące monitorowania środowiska: | 1. System monitoringu temperatury, wilgotności i przepływu powietrza w czasie rzeczywistym. 2. Możliwość powiadamiania o przekroczeniu zadanych wartości parametrów. 3. Integracja z systemami zarządzania infrastrukturą IT (np. SNMP, API). |
| Gwarancja | * + 1. Minimum 24 miesiące gwarancji na wszystkie elementy systemu. |
| Wymagania dodatkowe | 1. Możliwość przyszłej rozbudowy systemu o dodatkowe szafy i moduły. 2. System musi być zgodny z normą PN-EN 60529 lub równoważną. |

* 1. **Wymagania w zakresie Systemu zabezpieczeń sieciowych UTM – 2 szt.**

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

Powinna istnieć możliwość dedykowania co najmniej 5 administratorów do poszczególnych instancji systemu.

|  |  |
| --- | --- |
| **Kategoria** | **Wymagania** |
| Funkcje systemu | System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów:   * Routera z funkcją NAT, * transparentnym, * monitorowania na porcie SPAN. |
| Budowa systemu | System umożliwia budowę minimum 10 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie:  Routingu  Firewall’a  IPSec VPN  Antywirus  IPS  Kontroli Aplikacji. |
| Wspierane protokoły | System wspiera protokoły IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego. |
| Redundancja, monitoring i wykrywanie awarii | 1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych. |
| Interfejsy, Dysk, Zasilanie: | 1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:  * 16 portami Gigabit Ethernet RJ-45, * 8 gniazdami SFP 1 Gbps, dostarczone z 4 wkładkami Singlemode oaz 2 wkładkami Multimode dla każdego urządzenia * 4 gniazdami SFP+ 10 Gbps, dostarczone z 3 wkładkami multimode i 1 wkładką singlemode dla każdego urządzenia * gniazdami SFP+ 10 Gbps. Ultra Low, dostarczone z 4 wkładkami multimode dla każdego urządzenia * 2 gniazda zarządzające Gigabit Ethernet RJ-45  1. System Firewall posiada wbudowany port konsoli Rj45 oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB. 2. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q. 3. System jest wyposażony w min. 2 redundantne zasilacze AC. |
| Parametry wydajnościowe: | 1. W zakresie Firewall’a obsługa nie mniej niż 7.8 mln jednoczesnych połączeń oraz 500 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 76 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 26 Gbps. 4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 50 Gbps. 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) - minimum 11 Gbps. 6. Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 9 Gbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 7.2 Gbps. 8. Przepustowość SSL-VPN, nie mniejsza niż 3.5 Gb/s 9. Przepustowość IPS, nie mniejsza niż 10 Gb/s 10. Przepustowość NGF, nie mniejsza niż 10 Gb/s 11. Przepustowość zapory (pakiety na sekundę), nie mniejsza niż 100Mpps |
| Funkcje Systemu Bezpieczeństwa: | W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:   1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. 12. Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system. 13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa). |
| Polityki, Firewall | 1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:  * Translację jeden do jeden oraz jeden do wielu. * Dedykowany ALG (Application-Level Gateway) dla protokołu SIP.  1. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 2. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: adresy URL, adresy IP. 3. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. 4. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. 5. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.  * Amazon Web Services (AWS). * Microsoft Azure. * Cisco ACI. * Google Cloud Platform (GCP). * OpenStack. * VMware NSX. * Kubernetes. |
| Połączenia VPN | 1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:   • Wsparcie dla IKE v1 oraz v2.  • Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode (GCM).  • Obsługa protokołu Diffie-Hellman grup 19, 20.  • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.  • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.  • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.  • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.  • Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.  • Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.  • Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.  • Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.  • Mechanizm „Split tunneling” dla połączeń Client-to-Site.   1. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:   • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.   1. Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji. |
| Routing i obsługa łączy WAN | W zakresie routingu rozwiązanie zapewnia obsługę:   1. Routingu statycznego. 2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego). 3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. 4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. 5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. 6. BFD (Bidirectional Forwarding Detection). 7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu. |
| Funkcje SD-WAN | 1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec). |
| Zarządzanie pasmem | 1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. System daje możliwość określania pasma dla poszczególnych aplikacji. 3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. 4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL. |
| Ochrona przed malware | 1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. 3. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwia konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum. 4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. 5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w usłudze chmurowej realizowanej na terenie Unii Europejskiej. 8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. 9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. 10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu. |
| Ochrona przed atakami | 1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). 7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http. 8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. 9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie. |
| Kontrola aplikacji | 1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. 6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). 7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80). |
| Kontrola WWW | 1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. 4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). 6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. 7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. 8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. 9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji. |
| Uwierzytelnianie użytkowników w ramach sesji | 1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:  * Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. * Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. * Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.  1. System daje możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego. 2. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie. 3. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP. |
| Zarządzanie | 1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. 3. Istnieje możliwość włączenia mechanizmów uwierzytelniania wieloskładnikowego dla dostępu administracyjnego. 4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. 5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. 8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). 9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP. |
| Logowanie | 1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. 4. Możliwość włączenia logowania per reguła w polityce firewall. 5. System zapewnia możliwość logowania do serwera SYSLOG. 6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS. |
| Testy wydajnościowe oraz funkcjonalne | 1. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta lub w przypadku braku parametrów wydajnościowych w dokumentacji, wymagane jest dostarczenie wyników testów wydajnościowych (wykonanych przez producenta rozwiązania w czasie ostatnich 90 dni. |
| Gwarancja oraz wsparcie | 1. System jest objęty serwisem gwarancyjnym producenta przez okres co najmniej 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. Obsługa zgłoszenia w tym zwrot uszkodzonego urządzenia do producenta, bez dodatkowych kosztów po stronie zamawiającego, realizowana przez producenta lub autoryzowanego dystrybutora w języku polskim przez okres wymaganej gwarancji. 2. Dostarczone rozwiązanie musi być objęte rozszerzonym wsparciem technicznym gwarantującym - w przypadku awarii - odbiór i zwrot urządzenia do producenta bez dodatkowych kosztów, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres wymaganej gwarancji. 3. Do zamawianego sprzętu Wykonawca zapewni usługi wsparcia technicznego świadczone przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie:  * obsługa procesu RMA u producenta, * zdalna pomoc w skonfigurowaniu urządzenia do współpracy z aktualnymi bazami funkcji ochronnych i serwisów producenta, * ednorazowa podstawowa konfiguracja platformy realizowana przez inżyniera z najwyższym dostępnym poziomem certyfikacji technicznej producenta, * minimum 3 zdalne konsultacje techniczne z inżynierem posiadającym najwyższy poziom certyfikacji technicznej producenta, \*\*\*\*wymagana wersja PRO\*\*\*\* * jednorazowa usługa hardeningu konfiguracji w formie zdalnej sesji technicznej mającej na celu przegląd konfiguracji urządzenia i przedstawienie zaleceń rekonfiguracji zgodnie z „dobrymi praktykami” producenta, \*\*\*\*wymagana wersja PRO\*\*\*\* * dostęp do szkolenia wideo prezentującego najlepsze praktyki współpracy z suportem producenta systemu realizującego funkcję Firewall.  1. Dostęp do usługi powinien być świadczony przez dedykowaną infolinię (należy podać numer telefonu) oraz przez dedykowany moduł internetowy (należy podać adres). Usługa ta ma być świadczona prze podmiot posiadający certyfikat ISO 9001 lub równoważny w zakresie świadczenia usług serwisowych. 2. Do oferty należy załączyć oświadczenie producenta lub Autoryzowanego Dystrybutora o gotowości świadczenia takiej usługi wraz z certyfikatem ISO 9001 lub równoważny oraz certyfikat potwierdzający posiadany najwyższy poziom certyfikacji technicznej producenta. |
| Rozszerzone wsparcie serwisowe AHB/SOS | 1. System jest objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu najpóźniej w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres co najmniej 36 miesięcy. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący posiada certyfikat ISO 9001 lub równoważny w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe są przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. 2. System jest objęty usługą wsparcia technicznego świadczoną przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie:  * Wsparcie telefoniczne zespołu certyfikowanych inżynierów. * Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu. * Doradztwo w zakresie konfiguracji. * Zdalne wsparcie techniczne. * Pomoc w zakładaniu zgłoszeń serwisowych u producenta. * Pomoc w procesie realizacji naprawy i wymiany w ramach gwarancji producenta (również za granicą). * Przygotowanie urządzenia do zdalnej konfiguracji. * Zdalna konfiguracja urządzenia (połączenia szyfrowane) zgodnie z wymaganiami użytkownika. * Minimum 5 zdalnych rekonfiguracji urządzenia w związku ze zmianą środowiska lub wymagań użytkownika. * Minimum dwa razy w roku zdalny przegląd konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich. * Minimum dwa razy w roku zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich. * Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). * Certyfikat ISO 9001 lub równoważny podmiotu serwisującego. |

* 1. **Wymagania w zakresie Analizatora logów z systemu zabezpieczeń sieciowych – 1 szt.**

W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.

Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi werje: 5.0, 5.1, 5.5, 6.0, 6.5, 6.7; Microsoft Hyper-V wersje: 2008 R2, 2012, 2012 R2, 2016; Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP).

|  |  |
| --- | --- |
| **Specyfikacja zamówienia** | **Wymagania Zamawiającego** |
| Interfejsy, Dysk: | 1.     System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności co najmniej 3 TB. |
| Parametry wydajnościowe: | 1.     System musi być w stanie przyjmować minimum 5 GB logów na dzień. |
| 2.     Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów. |

W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:

|  |  |
| --- | --- |
| **Specyfikacja zamówienia** | **Wymagania Zamawiającego** |
| Logowanie | 1.     Podgląd logowanych zdarzeń w czasie rzeczywistym. |
| 2.     Możliwość przeglądania logów historycznych z funkcją filtrowania. |
| 3.     System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej: a. Listę najczęściej wykrywanych ataków.  b. Listę najbardziej aktywnych użytkowników.  c. Listę najczęściej wykorzystywanych aplikacji.  d. Listę najczęściej odwiedzanych stron www.  e. Listę krajów, do których nawiązywane są połączenia.  f. Listę najczęściej wykorzystywanych polityk Firewall.  g. Informacje o realizowanych połączeniach IPSec. |
| 4.     Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów. |
| 5.     Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514. |
| 6.     System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy. |
| Raportowanie: W zakresie raportowania system musi zapewniać: | 1.     Generowanie raportów co najmniej w formatach: PDF, CSV. |
| 2.     Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników. |
| 3.     Funkcję definiowania własnych raportów. |
| 4.     Możliwość spolszczenia raportów. |
| 5.     Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email. |
| Korelacja logów: W zakresie korelacji zdarzeń system musi zapewniać: | 1.     Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany. |
| 2.     Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa. |
| 3.     Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń: ·       Malware. ·       Aplikacje sieciowe. ·       Email. ·       IPS. ·       Traffic. ·       Systemowe: utracone połączenie vpn, utracone połączenie sieciowe. |
| 4.     Funkcję analizy logów archiwalnych względem aktualnej wiedzy producenta o zagrożeniach, w celu wykrycia potencjalnych stacji - narażonych na zagrożenie w ostatnim czasie. (zapis stosowany, kiedy oferowana jest licencja FortiGuard Indicator of Compromise (IOC)) |
| Zarządzanie | 1.     System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów. a. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI. |
| 2.     System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi. |
| Serwisy i licencje | 1.     System musi być dostarczony w modelu „na własność” tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania. |
| 2.     Wsparcie: System musi być objęty serwisem producenta przez okres 60 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7. |
| Opisy do wymagań ogólnych | 1.     Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (t. j. Dz. U. z 2023 r. poz. 1582 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania. |
| 2.     Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań. |

* 1. **Wymagania w zakresie listew zasilających PDU – 16 szt.**

Szczegółowe wymagania dotyczące listw PDU oraz minimalne parametry techniczne zostały określone w tabeli poniżej i stanowią podstawę do wyceny przedmiotu zamówienia przez Oferentów:

|  |  |
| --- | --- |
| **Kategoria** | **Wymagania** |
| **Typ urządzenia** | Zarządzalna listwa zasilająca PDU umożliwiająca monitorowanie oraz zdalne sterowanie urządzeniami. |
| **Parametry zasilania** | - Napięcie zasilania: 230V (±10%) - Maksymalne obciążenie: co najmniej 32A  - Rodzaj wtyku wejściowego: Odpowiedni do zainstalowanych przez Wykonawcę zakończeń instalacji elektrycznej.  - Gniazda wyjściowe: minimum 20 portów typu C13 oraz 4 porty typu C19 |
| **Funkcjonalność zarządzania** | - Monitorowanie parametrów zasilania w czasie rzeczywistym - Obsługa protokołów: SNMP, Telnet, SSH, HTTPS  - Wbudowany interfejs webowy do zarządzania  - Możliwość integracji z systemami zarządzania infrastrukturą |
| **Konstrukcja i instalacja** | - Montaż w szafie rack 19'' (maks. 1U)  - Obudowa odporna na uszkodzenia mechaniczne i czynniki zewnętrzne  - Złącza i elementy montażowe zgodne ze standardowymi szafami rack  - Obudowę listwy PDU musi stanowić profil aluminiowy zapewniający montaż listwy PDU pomiędzy osłoną boczną a belką rakową, maksymalna szerokość PDU wynosi 44 mm |
| **Bezpieczeństwo** | - Ochrona przed przepięciami i przeciążeniami  - Certyfikaty zgodności z normami bezpieczeństwa i kompatybilności elektromagnetycznej |
| **Dodatkowe wymagania** | - Intuicyjna konfiguracja i wsparcie techniczne producenta - Gwarancja: minimum 60 miesięcy |
| **Dokumentacja i wsparcie** | - Dokumentacja techniczna w języku polskim lub angielskim - Instrukcja instalacji i konfiguracji - Dostępność aktualizacji oprogramowania urządzenia |
| **Zastosowanie** | Instalacja w serwerowniach Zamawiającego, optymalne zarządzanie zasilaniem infrastruktury IT. |

* 1. **Wymagania w zakresie Przełączników sieciowych CORE – 2 szt.**

Wymaga się, aby urządzenie posiadało następujące porty, protokoły oraz spełniało następujące funkcje:

Do wszystkich przełączników sieciowych należy przewidzieć pełne obsadzenie wkładkami SFP+/SFP (singlemode oraz multimode) na każdy przełącznik, w ilości odpowiadającej liczbie portów: 40 wkładek SFP+/SFP dla portów 25Gb/s multimode, 8 wkładek SFP+/SFP dla portów 25Gb/s singemode oraz 8 wkładek QSFP dla portów 100Gb/s. Dodatkowo należy dostarczyć niezbędne okablowanie (patchcordy miedziane i światłowodowe) odpowiedniego typu i długości.

|  |  |
| --- | --- |
| **Kategoria** | **Wymagania** |
| Porty | - 48 portów 25G/10Gb/s - 8 portów 100Gb/s |
| Chłodzenie | Od przodu do tyłu obudowy |
| Tablica MAC | Minimum 32K |
| Bufor | 256Mb |
| Zasilanie | Redundantne wewnętrzne zasilacze AC |
| MTBF | Minimum 289 052 godzin |
| Wydajność | Minimum 4 Tbps |
| Przepustowość | Minimum 2 Bpps |
| Opóźnienia (Latency) | - 25G SFP28: < 0.117μs  - 10G SFP+: < 0.119μs  - 100G QSFP28: < 0.129μs  - 50G QSFP28: < 0.129μs  - 40G QSFP+: < 0.144μs |
| Zarządzanie | - Web GUI  - HTTPs  - CLI  - Telnet  - SSH  - SNMP  - MIB RSPAN |
| Autoryzacja | - RADIUS  - TACACS+ |
| Procesor | CPU: min. 2.20GHz  Cache: min. 8MB  Ilość rdzeni: min. 4 |
| Pamięć RAM | Co najmniej: 8GB DDR3/ECC RAM |
| Pamięć masowa | 128GB SSD |
| Funkcje sieciowe | - Multichassis LAG  - DiffServ  - Harmonogram limitowania przepustowości (min. 1 Kbps)  - IPv4/IPv6 Multicast Filtering |
| Obsługa protokołów multicast | - IGMPv3 MLDv2 Snooping - SSM - IGMPv1, v2 Querier |
| Optymalizacja | iSCSI optimization |
| Routing i QoS | - Policy-based Routing (PBR)  - LLDP-MED  - QoQ (Double VLAN Tagging) |
| Protokoły Spanning Tree | - STP  - MSTP  - RSTP  - BPDU/STRG Root Guard |
| Wirtualizacja VLAN | - VXLAN - Q-in-Q - Private VLAN |
| Zabezpieczenia sieciowe | - DOT1X  - MAB  - DHCP Snooping  - Dynamic ARP Inspection  - IP Source Guard |
| Obsługa VLAN | Minimum 4K |
| sFlow | Tak |
| Interfejsy IP | Minimum 128 |
| Routing multicast | - PIM-SM (IPv4 i IPv6) |
| Obsługa protokołów routingu | - OSPFv2 / GR - BGP4 / AS4 / GR |
| Zabezpieczenia warstwy łącza | UDLD |
| DHCPv6 | DHCPv6 Snooping |
| Listy ACL | - Min. 100 list ACL - Min. 1023 reguły na listę (wejście/wyjście) |
| Gwarancja | Minimum 5 lat.  Urządzenie powinno być objęte usługą szybkiej wymiany w wypadku awarii z wysyłką w następnym dniu roboczym po stwierdzeniu awarii przez okres gwarancji. |

* 1. **Wymagania w zakresie Przełączników sieciowych TOR – 2 szt.**

Wymaga się, aby urządzenie posiadało następujące porty, protokoły oraz spełniało następujące funkcje:

Do wszystkich przełączników sieciowych należy przewidzieć pełne obsadzenie wkładkami SFP+/SFP multimode na każdy przełącznik, w ilości odpowiadającej liczbie portów: 4 wkładki SFP+/SFP dla portów 10Gb/s multimode. Dodatkowo należy dostarczyć niezbędne okablowanie (patchcordy miedziane i światłowodowe) odpowiedniego typu i długości.

|  |  |
| --- | --- |
| **Kategoria** | **Wymagania** |
| Porty | - 48 portów 10GbaseT  - 4 porty SFP+ |
| Chłodzenie | Od przodu do tyłu obudowy |
| Tablice | - MAC: min. 16K  - ARP/NDP: min. 8K |
| Bufor | 56Mb |
| MTBF | Minimum 249 000 godzin |
| Wydajność | Minimum 714 Mp/s |
| Przepustowość | Minimum 960 Gb/s |
| Porty zarządzania | - USB  - miniUSB  - Out-of-band |
| Zarządzanie | - Web GUI  - HTTPs  - CLI  - Telnet  - SSH  - SNMP  - MIB RSPAN |
| Autoryzacja | - RADIUS  - TACACS+ |
| Funkcje QoS | - DiffServ  - Harmonogram limitowania przepustowości (min. 1 Kbps) |
| Multicast | - IPv4/IPv6 Multicast Filtering  - IGMPv3 MLDv2 Snooping  - ASM & SSM  - IGMPv1, v2 Querier |
| Optymalizacje | - Auto-VoIP  - Auto-iSCSI |
| Routing i protokoły | - Policy-based Routing (PBR)  - LLDP-MED  - RIPv1  - RIPv2  - OSPFv2/v3 |
| Spanning Tree | - STP  - MTP  - RSTP  - PV®STP  - BPDU/STRG Root Guard |
| Zarządzanie VLAN | - Q-in-Q  - Private VLAN  - Min. 4K VLAN |
| Zabezpieczenia sieciowe | - DOT1X  - MAB  - Captive Portal  - DHCP Snooping  - Dynamic ARP Inspection  - IP Source Guard |
| Pamięć i CPU | - CPU: min. 800 MHz  - RAM: min. 1GB  - Flash: min. 256MB |
| DHCP | - Serwer DHCP: min. 2K rezerwacji  - DHCPv6 Snooping |
| sFlow | Tak |
| Łączenie w stos | - Min. 8 przełączników  - Interfejsy 10Gb/s  - Konfiguracja: pierścień, podwójny pierścień, mesh |
| Funkcje zaawansowane | - Non-stop Forwarding (NSF)  - Distributed Link Aggregation (LAGs across the stack) |
| Routing multicast | - PIM-DM (IPv4 i IPv6)  - PIM-SM (IPv4 i IPv6) |
| Protokoły routingu | - RFC 2328  - RFC 1583  - Min. 400 sąsiadów OSPFv2/v3  - Min. 100 sąsiadów OSPFv3 na interfejs |
| Standardy bezpieczeństwa | - UDLD  - LLPF |
| Powiadomienia | Wysyłanie alertów na email |
| Standardy zgodności | - CE: EN 55032:2012+AC:2013  - EN 61000-3-2:2014  - EN 61000-3-3:2013  - FCC: 47 CFR FCC Part 15  - ANSI C63.4:2014  - RCM: AS/NZS CISPR 32:2013 Class A  - BSMI: CNS 13438 Class A  lub równoważne |
| Zasilanie | Urządzenie powinno być wyposażone w 2 redundantne zasilacze AC |
| Gwarancja | Minimum 5 lat.  Urządzenie powinno być objęte usługą szybkiej wymiany w wypadku awarii z wysyłką w następnym dniu roboczym po stwierdzeniu awarii przez okres gwarancji. |

* 1. **Wymagania dotyczące przełączników sieciowych dystrybucyjnych 10G/25G – 4 szt.**

Wymaga się, aby urządzenie posiadało następujące porty, protokoły oraz spełniało następujące funkcje:

Do wszystkich przełączników sieciowych należy przewidzieć pełne obsadzenie wkładkami SFP+/SFP singlemode na każdy przełącznik, w ilości odpowiadającej liczbie portów: 4 wkładki SFP+/SFP dla portów 25Gb/s singlemode. Dodatkowo należy dostarczyć niezbędne okablowanie (patchcordy miedziane i światłowodowe) odpowiedniego typu i długości.

|  |  |
| --- | --- |
| **Kategoria** | **Wymagania** |
| Ilość portów | 24 x 1/2,5/5/10G BASE-T PoE+  -4 x SFP28 10/25G |
| Chłodzenie | Od przodu do tyłu obudowy |
| Budżet PoE | Min. 576W |
| Tablica MAC | Min. 16K |
| Tablica ARP/NDP | 4K ARP / 512 NDP |
| Bufor | 32 Mb |
| MTBF | Min. 320552 godzin |
| Wydajność | Min. 505 Mp/s |
| Przepustowość | Min. 680 Gb/s |
| Porty zarządzania | - USB-C  - Out-of-band |
| Interfejsy zarządzania | - Web GUI  - HTTPs  - CLI  - Telnet  - SSH  - SNMP |
| Protokoły zabezpieczeń | - RADIUS  - TACACS+  - DOT1X  - MAB  - Captive Portal |
| Mechanizmy monitorowania | - SNMP  - MIB RSPAN  - sFlow |
| QoS i routing | - DiffServ  - Policy-based routing (PBR)  - QoQ, Double VLAN Tagging |
| Limitowanie przepustowości | Możliwość limitowania przepustowości do 1 Kbps w oparciu o harmonogram |
| Protokoły multicast | - IPv4/IPv6 Multicast filtering  - IGMPv3  - MLDv2 Snooping  - ASM & SSM  - PIM-DM/SM |
| Protokoły routingu | - RIPv1  - RIPv2  - OSPFv2 (RFC 2328, RFC 1583)  - OSPFv3 |
| Spanning Tree | - STP  - MTP  - RSTP |
| Green Ethernet | - EEE (802.3az)  - LLDP-MED  - GVRP/GMRP |
| Bezpieczeństwo sieci | - DHCP Snooping  - Dynamic ARP Inspection  - IP Source Guard |
| Parametry sprzętowe | - ARMv8 1.8 GHz CPU  - 2 GB RAM  - 512 MB Flash |
| VLAN | - Min. 4K obsługiwanych VLAN  - DHCP Server (min. 2K rezerwacji) |
| Stosowanie przełączników | - Min. 8 w stosie  - łączenie interfejsami 25Gb/s, tryby: pierścień, mesh |
| Rozbudowa stosu | Distributed Link Aggregation (LAGs across the stack) |
| Ilość interfejsów IP | 128 |
| Protokoły dodatkowe | - UDLD  - LLPF  - DHCPv6 Snooping  - wysyłanie alertów na email  - MMRP |
| ACL | - Min. 100 list |
| Ilość reguł | - 1023 reguły wejściowe  - 511 reguły wyjściowe |
| Zarządzanie AV | - Automatyczne przypisanie konfiguracji dla  - NVX  - AMX  - NDI  - Dante  - SDVoE  - AES67  - Q-SYS  - Audio Dante  - AVB  - Crestron DigitalMedia AV  - NUCLEUS Converged AV  - Shure  - Sonos  - Visionary AV |
| Szablony AV | Szablony stworzone przez producenta, z jednoznacznym wskazaniem obsługi |
| Aplikacja kontrolera | Dostarczana przez producenta, umożliwiająca przypisanie profili AV automatycznie |
| Obsługa CLI w GUI | Wykonywanie poleceń CLI w GUI bez Telnet/SSH |
| Zasilanie | Urządzenie powinno być wyposażone w 2 redundantne zasilacze AC |
| Gwarancja | Minimum 5 lat  Urządzenie powinno być objęte usługą szybkiej wymiany w wypadku awarii z wysyłką w następnym dniu roboczym po stwierdzeniu awarii przez okres gwarancji. |

* 1. **Wymagania dotyczące** **Serwera – Wirtualizacja – 4 szt.**

Szczegółowe wymagania dotyczące Serwera oraz minimalne parametry techniczne zostały określone w tabeli poniżej i stanowią podstawę do wyceny przedmiotu zamówienia przez Oferentów:

|  |  |
| --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |
| Obudowa | Obudowa Rack o wysokości max 2U z możliwością instalacji min. 16 dysków NVMe 2,5” Hot-Plug z kompletem szyn wraz z organizerem do kabli umożliwiających montaż w szafie rack.  Możliwość instalacji karty umożliwiającej dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI. |
| Płyta główna | Płyta główna z możliwością zainstalowania minimum dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. |
| Chipset | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych. |
| Procesor | Zainstalowane dwa procesory szesnastordzeniowe klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 443 punktów w teście SPECrate2017\_int\_base dostępnym na stronie [www.spec.org](http://www.spec.org). Dla oferowanego serwera. |
| RAM | Min. 1TB DDR5 RDIMM 4800MT/s w modułach min. 128GB RDIMM 4800MT/s, na płycie głównej powinno znajdować się minimum 24 sloty przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać do 6TB pamięci RAM. |
| Gniazda PCIe | Minimum dwa sloty PCIe x8 pełnej wysokości oraz minimum dwa sloty PCIe x16. |
| Interfejsy sieciowe/FC | Wbudowane minimum 2 porty typu Gigabit Ethernet Base-T  Jedna karta dwuportowa 25GbE SFP28. |
| Dyski twarde | Zainstalowane 3 x 1.92TB NVMe i 12 x 3.84TB NVMe |
| Wbudowane porty | min. 2 porty USB 2.0 oraz 1 port USB 3.0, 2 porty RJ45, 1 port VGA na przednim panelu |
| Video | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1600x900. |
| Wentylatory | Redundantne hot-plug |
| Zasilacze | Redundantne, Hot-Plug maksymalnie 1800W. |
| Bezpieczeństwo | TPM 2.0 |
| Karta Zarządzania | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca:   * zdalny dostęp do graficznego interfejsu Web karty zarządzającej * szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika * możliwość podmontowania zdalnych wirtualnych napędów * wirtualną konsolę z dostępem do myszy, klawiatury * wsparcie dla IPv6 * wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH * możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz. * możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer * integracja z Active Directory * możliwość obsługi przez ośmiu administratorów jednocześnie * Wsparcie dla automatycznej rejestracji DNS * wsparcie dla LLDP * wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej * możliwość podłączenia lokalnego poprzez złącze RS-232. * możliwość zarządzania bezpośredniego poprzez złącze microUSB umieszczone na froncie obudowy. * Monitorowanie zużycia dysków SSD * możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi, * Automatyczne zgłaszanie alertów do centrum serwisowego producenta * Automatyczne update firmware dla wszystkich komponentów serwera * Możliwość przywrócenia poprzednich wersji firmware * Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON * Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych * Automatyczne tworzenie kopii ustawień serwera w opraciu o harmonogram. * Możliwość wykrywania odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera * Serwer musi posiadać możliwość uruchomienia funkcjonalności umożliwiającej dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE lub WIFI.   Możliwość rozszerzenia funkcjonalności karty o:   * możliwość wysyłania danych o stanie procesora, kart sieciowych, zasilaczy, kart GPU, lokalnych dysków i urządzeń NVMe, jak również dane wydajnościowe serwera do zewnętrznych * kontrola stanu BIOS pod kątem naruszenia integralności oprogramowania * Automatyczne odświeżanie certyfikatów SSL * możliwość wykorzystania tokenu lub aplikacji SecurID do uwierzytelniania wielkoskładnikowego przy logowaniu do karty zarządzającej * możliwość modyfikacji reguł chłodzenia kart w slotach PCIe, z możliwością własnych ustawień * możliwość ustawienia limitu temperatury powietrza wychodzącego z serwera * możliwość ustawienia dopuszczalnego wzrostu temperatury powietrza przepływającego przez serwer * możliwość ustawienia maksymalnej temperatury powietrza dochodzącego do slotów PCIe   monitorowanie przepływu powietrza na bieżąco |
| Oprogramowanie do zarządzania | Możliwość zainstalowania oporogramowania producenta do zarządznia, spełniające poniższe wymagania:   * Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych * integracja z Active Directory * Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta * Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish * Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram * Szczegółowy opis wykrytych systemów oraz ich komponentów * Możliwość eksportu raportu do CSV, HTML, XLS, PDF * Możliwość tworzenia własnych raportów w opraciu o wszystkie informacje zawarte w inwentarzu. * Grupowanie urządzeń w oparciu o kryteria użytkownika * Tworzenie automatycznie grup urządzeń w opraciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji * Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach * Szybki podgląd stanu środowiska * Podsumowanie stanu dla każdego urządzenia * Szczegółowy status urządzenia/elementu/komponentu * Generowanie alertów przy zmianie stanu urządzenia. * Filtry raportów umożliwiające podgląd najważniejszych zdarzeń * Integracja z service desk producenta dostarczonej platformy sprzętowej * Możliwość przejęcia zdalnego pulpitu * Możliwość podmontowania wirtualnego napędu * Kreator umożliwiający dostosowanie akcji dla wybranych alertów * Możliwość importu plików MIB * Przesyłanie alertów „as-is” do innych konsol firm trzecich * Możliwość definiowania ról administratorów * Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów * Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) * Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta * Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów * Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących aletrów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. * Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstwie weryfikacji środowiska w celu wykrycia rozbieżności. * Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w opraciu o profile * Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. * Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. * Zdalne uruchamianie diagnostyki serwera. * Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarzadzającym. * Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V. |
| Komponenty dodatkowe | - dwa moduły nadawczo-odbiorcze 25GbE SFP28 SR |
| Certyfikaty | Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001 lub równoważną.  Serwer musi posiadać deklaracja CE. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows”. |
| Normy Środowiskowe | Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku *-****Wykonawca złoży dokument potwierdzający spełnianie*wymogu*.***   Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych **w postaci oświadczenia producenta serwera.** |
| Warunki gwarancji | Zamawiający wymaga min. 36 miesięcy gwarancji producenta możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.  Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania.  Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.  Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik ***producenta*** z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi sie na inną formę.  Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowyych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii. Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych.  W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego – wymagane jest dołączenie do oferty oświadczenia podmiotu realizującego serwis lub producenta sprzętu o spełnieniu tego warunku  Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.  Oświadczenie producenta serwera, potwierdzające, że sprzęt pochodzi z oficjalnego kanału dystrybucyjnego producenta.  Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji systemu. |
| Dokumentacja użytkownika | 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. |

* 1. **Wymagania dotyczące Macierzy – Wirtualizacja – 2 szt.**

Szczegółowe wymagania dotyczące Macierzy oraz minimalne parametry techniczne zostały określone w tabeli poniżej i stanowią podstawę do wyceny przedmiotu zamówienia przez Oferentów:

|  |  |
| --- | --- |
| **Nazwa elementu, parametru lub cechy** | **Szczegółowy opis wymagań** |
| Struktura obudowy i dysków | Macierz musi umożliwiać instalację w standardowej szafie RACK 19”. |
| Macierz musi mieć możliwość instalacji kombinacji poniższych nośników dyskowych w ramach jednej obudowy podstawowej (zawierającej kontrolery): - Flash NVMe lub NVMe SSD, gdzie Flash NVMe oznacza dyski autorskie dostawców macierzy wykorzystujące protokół NVMe - SCM (Storage Class Memory) |
| Możliwość zainstalowania co najmniej 12 dysków NVMe o rozmiarze 2,5” cala w obudowie o wysokości 1U. |
| Kontrolery macierzowe muszą komunikować się z nośnikami dyskowymi umieszczonymi w obudowie podstawowej (zawierającej kontrolery) wyłącznie z użyciem protokołu NVMe. |
| Macierz musi być zbudowana z minimum dwóch kontrolerów pracujących w trybie active-active lub dual-active. |
| Architektura macierzy ma być oparta o sprawdzone i powszechnie dostępne procesory technologii x86/x64 |
| Niezawodność i redundancja | Wszystkie krytyczne komponenty macierzy takie jak: kontrolery dyskowe, pamięć cache, zasilacze i wentylatory muszą być zdublowane tak, aby awaria pojedynczego elementu nie wpływała na funkcjonowanie całego systemu. Komponenty te muszą być wymienialne w trakcie pracy macierzy. |
| Macierz musi cechować brak pojedynczego punktu awarii. |
| Wsparcie dla zasilania z dwóch niezależnych źródeł prądu poprzez nadmiarowe zasilacze typu Hot-Swap. Wentylatory typu Hot-Swap. |
| Macierz musi być odporna na zaniki napięcia, tzn. chwilowy zanik napięcia nie powinien przerywać pracy macierzy. |
| Zarządzanie systemem | Macierz musi umożliwiać zarządzanie za pomocą interfejsu Ethernet. Możliwość zarządzania całością dostępnych zasobów dyskowych z jednej konsoli administracyjnej. |
| Funkcjonalność bezpośredniego monitoringu stanu w jakim w danym momencie macierz się znajduje. |
| Urządzenie musi składać się z pojedynczej macierzy dyskowej zarządzanej z jednego wbudowanego w macierz interfejsu GUI (interfejs graficzny), CLI (interfejs tekstowy) oraz zapewniać możliwość tworzenia skryptów użytkownika. Interfejs ten musi być natywnie dostępny na macierzy, bez zastosowania zewnętrznych urządzeń. |
| Ilość portów | Wymagane jest niemniej niż 4 x FC 32Gb/s per kontroler |
| Pojemność macierzy | Całkowita pojemność min. 70TB netto (użyteczne przy założeniu konfiguracji odpornej na awarię minimum 2 dysków (typu RAID-6 lub równoważnego) oraz bez uwzględnienia technik redukcji danych takich jak kompresja, deduplikacja czy thin-provisioning) i musi być zbudowana wyłącznie w oparciu o nośniki NVMe Flash lub NVMe SSD. |
| Macierz musi pozwalać na alokację 99% pojemności użytecznej bez spadku wydajności macierzy (brak zwiększonego czasu odpowiedzi, brak spadku przepustowości macierzy). Wydajność macierzy musi być niezależna od poziomu alokacji przestrzeni macierzy w zakresie od 0% alokacji do wartości wymaganej pojemności użytecznej. Jeżeli oferowane rozwiązanie nie spełnia opisanego wymagania należy dostarczyć conajmniej 20% pojemności użytecznej więcej. |
| Poziomy RAID | Macierz musi obsługiwać poziomy: RAID1, RAID5 i RAID6 (dystrybuowane) i zapewniać zabezpieczenie przed awarią dwóch dysków jednocześnie w ramach jednej grupy raid. |
| Zabezpieczenia danych | Dyski/przestrzeń "spare" muszą zostać skonfigurowane/dostarczone w ilości/pojemności zgodnej z udokumentowanymi rekomendacjami producenta oferowanej macierzy. |
| Macierz musi posiadać wbudowane sprzętowo na nośnikach dyskowych NVMe szyfrowanie AES-256. |
| Kontrolery macierzowe muszą posiadać możliwość szyfrowania danych, uniemożliwiając odczyt danych z usuniętych z macierzy nośników dyskowych. Ta funkcjonalność nie jest to objęta tym postepowaniem. |
| Możliwość rozbudowy systemu | Macierz musi mieć możliwość obsługi min. 200 dysków poprzez dodanie półek rozszerzeń. Macierz musi mieć możliwość rozbudowy poprzez dodanie pojedynczego dysku, dodanie kontrolerów oraz półek dyskowych. |
| Niezależnie od zastosowanych nośników danych, macierz musi umożliwiać granularną rozbudowę grupy RAID w zakresie od co najmniej od 1 do 12 nośników dyskowych, proces rozbudowy nie może powodować niedostępności do danych. |
| Kontrolery macierzy | Macierz musi być wyposażona w minimum 2 kontrolery dyskowe z możliwością rozbudowy do 4 kontrolerów. Każdy z kontrolerów musi udostępniać co najmniej 120GB pamięci Cache. |
| Macierz musi umożliwiać rozbudowę pamięci cache do 1TB w ramach klastra macierzy składającego się z identycznych kontrolerów i zarządzanego z jednego interfejsu GUI, CLI. Zamawiający nie dopuszcza zastosowania dysków SSD/ SSD NVMe lub kart pamięci/modułów FLASH jako rozszerzenia pamięci cache. |
| Zaawansowane funkcje | Funkcjonalność partycjonowania pamięci cache. |
| Funkcjonalność separacji przestrzeni dyskowych pomiędzy różnymi podłączonymi hostami. |
| Funkcjonalność dynamicznego zwiększania rozmiaru wolumenów. |
| Funkcjonalność zarządzania maksymalną ilością operacji wejścia / wyjścia wykonywanych na danym wolumenie - zarządzanie musi być możliwe zarówno poprzez określenie ilości operacji I/O na sekundę jak również przepustowości określonej w MB/s. |
| Macierz musi mieć możliwość kompresji i deduplikacji dla wszystkich rodzajów dysków. Licencja na tą funkcjonalność musi być zawarta w cenie i musi obejmować zaoferowaną w ramach macierzy przestrzeń dyskową Wsparcie dla kompresji danych w trybie inline („na bieżąco” bez potrzeby zapisywania danych na nośnikach danych w formie nie skompresowanej) dla dostępu blokowego. |
| Optymalizacja przestrzeni danych | Macierz musi wspierać kompresję i deduplikację w trybie "inline". |
| Niezawodność działania | Zaoferowane rozwiązanie musi posiadać możliwość implementacji klastra wysokiej dostępności. W ramach architektury klastra wysokiej dostępności musi być wspierane bezprzerwowe migrowanie maszyn wirtualnych pomiędzy ośrodkami. W przypadku awarii jednej z macierzy nastąpi bezprzerwowe przełączenie do lokalizacji zapasowej. Powyższa funkcjonalność musi być realizowana niezależnie od systemu operacyjnego na poziomie przełączania ścieżek do urządzenia logicznego. Licencja na tą funkcjonalność musi być zawarta w cenie i musi obejmować zaoferowaną w ramach macierzy przestrzeń dyskową. |
| Optymalizacja zasobów | Macierz musi optymalizować wykorzystanie dysków SSD/ modułów Flash/ HDD, tak aby w ramach tego samego rodzaju dysków (pojemności/prędkości) wszystkie grupy dysków były utylizowane w równym stopniu. Licencja na tą funkcjonalność musi być zawarta w cenie i musi obejmować całą oferowaną pojemność macierzy. |
| Wirtualne dyski logiczne | Macierz musi mieć możliwość rozłożenia wolumenu logicznego pomiędzy co najmniej dwoma różnymi typami macierzy dyskowych |
| Macierz musi umożliwiać stworzenie mirrorowanych LUN pomiędzy różnymi macierzami, dla których awaria jednej kopii lustra musi być niezauważalna dla systemu hosta. |
| Thin provisioning | Macierz musi obsługiwać funkcjonalność thin provisioning dla wszystkich wolumenów. Należy dostarczyć licencję umożliwiającą korzystanie z funkcji thin provisioning na całą oferowaną pojemność macierzy. |
| Snapshoty danych | Kopie danych typu snapshot (PIT) muszą być tworzone w trybach incremental, multitarget, oraz kopii pełnej oraz kopii wskaźników. Licencja na tą funkcjonalność musi być zawarta w cenie i musi obejmować całą oferowaną pojemność macierzy. |
| Macierz musi posiadać możliwość tworzenia kopii migawkowych w trybie WORM (Write Once Read Many). Kopie powinny być tworzone za pomocą harmonogramu i mieć możliwość ustawienia retencji kopii, po upłynięciu której kopia automatycznie zostanie usunięta z macierzy. |
| Replikacja danych | Macierz musi mieć możliwość wykonywania replikacji synchronicznej i asynchronicznej wolumenów logicznych pomiędzy różnymi typami macierzy dyskowych. Zasoby źródłowe kopii zdalnej oraz docelowe kopii zdalnej mogą być zabezpieczone różnymi poziomami RAID i egzystować na różnych technologicznie dyskach stałych (SAS, SSD, SATA). Licencja na tą funkcjonalność musi być zawarta w cenie i musi obejmować zaoferowaną w ramach macierzy przestrzeń dyskową. |
| Ogólne wymagania | Macierz musi być nowa, nigdy wcześniej nie używana i pochodzić z autoryzowanego kanału dystrybucji producenta a także być objęta serwisem producenta na terenie RP. |
| Kompatybilność z systemami | Wsparcie systemów operacyjnych Macierz musi być wspierana przez systemy operacyjne i wirtualizatory: MS Windows Server 2019, 2022, 2025, Vmware vSphere 7 i nowsze, RedHat Enterprise Server 7.6 i nowsze |
| Zgodność z rozwiązaniami do backupu | Macierz musi zapewniać integrację z oprogramowaniem Veeam Backup & Replication na poziomie umozliwiającym na pełna współprace w zakresie: - backupu z migawek pamięci masowych  - Veeam Explorer for Storage Snapshots  - On-Demand Sandbox for Storage Snapshots  Współpraca z oprogramowaniem Veeam Backup & Replication ma się odbywać bez konieczności instalacji dodatkowych modułów (pluginów). |
| Warunki Gwarancji | Wymagana jest gwarancja świadczona w trybie 24 godziny przez 7 dni w tygodniu na wszystkie elementy macierzy (sprzęt oraz oprogramowanie) na okres 60 miesięcy. Usługi serwisowe będą świadczone przez producenta oferowanego sprzętu.  W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego – wymagane jest dołączenie do oferty oświadczenia podmiotu realizującego serwis lub producenta sprzętu o spełnieniu tego warunku |

* 1. **Wymagania dotyczące Macierzy – Repozytorium – 2 szt.**

Szczegółowe wymagania dotyczące Macierzy oraz minimalne parametry techniczne zostały określone w tabeli poniżej i stanowią podstawę do wyceny przedmiotu zamówienia przez Oferentów:

|  |  |
| --- | --- |
| **Typ urządzenia** | **Serwer NAS** |
| Obudowa | Rack 4U |
| Procesor | 2x Dziesięciordzeniowy procesor o taktowaniu 2,4 GHz, maksymalnie 3,2 GHz z technologią Turbo Boost. Pojedynczy procesor musi osiągać w teście Passmark na listopad 2024 min. 15 100 pkt. |
| Sprzętowy mechanizm szyfrowania | Tak (AES-NI) |
| Pamięć RAM | min. 64 GB pamięci DDR4 ECC RDIMM z możliwością rozszerzenia do min. 512 GB |
| Możliwości rozbudowy | Sprzęt powinien być wyposażony w min. 60 kieszeni na dyski twarde typu hot-swap 3.5” SAS oraz 2.5” SATA z możliwością rozszerzenia do 300 dysków za pomocą dedykowanych półek rozszerzających podłączanych do macierzy za pomocą kabla mini-SAS.  Wymaga się dostarczenia urządzenia z dedykowaną półką rozszerzającą celem zapewnienia przestrzeni dyskowej pod wymagania inwestycji – łączna liczba kieszeni nie mniejsza niż 120. |
| Dyski twarde | Urządzenie powinno być wyposażone w 70 szt. dysków twardych 3.5” klasy korporacyjnej przystosowanych do pracy ciągłej z interfejsem SAS 12 Gb/s o pojemności min. 20 TB, prędkości przesyłu danych min. 281 MiB/s tego samego producenta co macierz główna celem zapewnienia pełnej wydajności oraz kompatybilności na poziomie systemu operacyjnego.  68 szt. dysków będzie przewidziane na zapewnienie przestrzeni dyskowej zgodnie ze schematem grup RAID 6 i wolumenów petabajtowych natomiast 2szt. posłużą jako dyski typu global hot-spare |
| Porty zewnętrzne | Minimum:   * 2 porty USB 3.2.1 * 1 port konsoli |
| Porty sieciowe | Minimum:   * 2 porty 1GbE RJ45 (z obsługą funkcji Link Aggregation / przełączania awaryjnego) * 2 porty 10GbE RJ45 (wymogiem jest, aby dostarczane urządzenie posiadało wbudowane porty 10Gbe RJ-45 pozostawiając tym samym wolne gniazdo rozszerzeń PCIe) * 1 port LAN do zarządzania (poza pasmem sieciowym) * 1 karta z 2 portami 25Gbit z wkładkami SR * Możliwość rozszerzania portów sieciowych do min. 15 (łącznie porty sieciowe wbudowane w urządzenie wraz z dodatkowymi kartami sieciowymi) |
| Funkcja Wake on LAN/WAN | Tak |
| Gniazdo rozszerzeń PCIe 3.0 | Min. 2x 8-liniowe gniazdo x16  Min. 2x 8-liniowe gniazdo x8 |
| Wentylator obudowy | Min. 4 wentylatory 80 mm x 80 mm |
| Obsługiwane protokoły sieciowe | Min. SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS Kerberized sessions, iSCSI, Fibre Channel, HTTP, HTTPs, FTP, SNMP, LDAP, CalDAV |
| Obsługiwane systemy plików | Min.:   * Wewnętrzny: Btrfs * Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT |
| Zarządzanie pamięcią masową | * Maksymalny rozmiar pojedynczego wolumenu:   + 1 PB (tylko grupy RAID 6)   + 200 TB * Minimalny liczba wewnętrznych wolumenów: 256 * Minimalny liczba obiektów iSCSI Target: 256 * Minimalny liczba jednostek iSCSI LUN: 512 * Obsługa klonowania/migawek jednostek iSCSI LUN, Windows ODX |
| Obsługiwane typy macierzy RAID | Podstawowy (basic), JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10 |
| Funkcja udostępniania plików | * Minimalna liczba kont użytkowników: 16 000 * Minimalna liczba grup użytkowników: 512 * Minimalna liczba folderów współdzielonych: 512 * Minimalna liczba jednoczesnych połączeń CIFS/AFP/FTP: 10 000 * Minimalna liczba jednoczesnych połączeń protokołu SMB/AFP/FTP (z rozbudową pamięci RAM do maks. wartości): 10 000 |
| Uprawnienia | Uprawnienia aplikacji listy kontroli dostępu systemu Windows (ACL) |
| Wirtualizacja | Obsługa VMware vSphere®, Microsoft Hyper-V®, Citrix® XenServer™, OpenStack® |
| Usługa katalogowa | Integracja z usługami Windows® AD, logowanie użytkowników domeny przez protokoły SMB/NFS/AFP/FTP lub aplikację File Station, integracja z LDAP |
| Bezpieczeństwo | Zapora, szyfrowanie folderu współdzielonego, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne  blokowanie logowania, obsługa Let's Encrypt i HTTPS (mechanizmy szyfrowania z możliwością konfiguracji) |
| Zasilanie | Wymogiem jest dostarczenie sprzętu wyposażonego w nadmiarowy zasilacz. |
| Oprogramowanie | * Oprogramowanie zarządzające na urządzeniu musi obsługiwać deduplikację wolumenów z dysków SSD 2.5” producenta macierzy celem eliminacji nadmiarowych danych oszczędzając znacząco miejsce w pamięci masowej. * Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych CRC a także lustrzanych kopii metadanych, aby zapewnić całkowitą integralność danych biznesowych. Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów udostępnionych * System operacyjny musi wspierać nowoczesne metody zabezpieczenia danych w tym funkcjonalność WORM (WriteOnce, Read Many), niezmienne migawki itd. * Oprogramowanie zarządzające serwerem NAS musi zapewnić darmowe, kompleksowe rozwiązanie do tworzenia kopii zapasowych przeznaczone dla heterogenicznych środowisk IT, umożliwiające zdalne zarządzanie i monitorowanie ochrony komputerów, serwerów i maszyn wirtualnych na jednym, centralnym, przyjaznym dla administratora interfejsie. Ponadto gromadzone dane na urządzeniu mają mieć możliwość replikacji jako lokalne kopie zapasowe, sieciowe kopie zapasowe i kopie zapasowe danych w chmurach publicznych przy użyciu darmowego narzędzia instalowanego z Centrum Pakietów * Wymaga się zapewnienia darmowej aplikacji do realizacji chmury prywatnej bez opłat cyklicznych, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI a także agenty na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS. Usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń a także wspierać algorytm Intelliversioning. Ponadto omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wpierać wersjonowanie oraz edycję tworzonych plików office w czasie rzeczywistym. * Urządzenie musi umożliwiać pracę w trybie klastra wysokiej dostępności (HA) aby zapewnić nieprzerwany, natychmiastowy dostęp do zasobów bez widocznych zmian w użytkowaniu (konfiguracja jako jeden spójny system). Wszystkie dane z powodzeniem zapisane na serwerze aktywnym będą na bieżąco kopiowane do serwera pasywnego zapewniając replikację w czasie rzeczywistym i dostęp do danych oraz usług w przypadku uszkodzenia jednostki aktywnej dając gwarancję ciągłości pracy. Utworzenie klastra HA ma się opierać o 2 identyczne urządzenia. |
| Konserwacja | * Konserwację urządzenia należy przeprowadzać przy użyciu dodatkowych, wygodnych w użyciu przesuwnych szyn rack * Wymiana modułu zasilacza ma przebiegać w szybki i bezpieczny sposób bez wyłączania urządzenia oraz bez użycia narzędzi. * Wymiana wentylatora systemowego musi się odbywać bez wykorzystania narzędzi (poprzez naciśnięcie odpowiednich przycisków na obudowie urządzenia) |
| Gwarancja | * Wykonawca udzieli gwarancji:   + 5 lat na urządzenia główne   + 1 rok na dodatkowe akcesoria montażowe w postaci przesuwnych szyn rack * W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego – wymagane jest dołączenie do oferty oświadczenia podmiotu realizującego serwis lub producenta sprzętu o spełnieniu tego warunku |

* 1. **Wymagania dotyczące przełączników SAN – 2 szt.**

Szczegółowe wymagania dotyczące Przełączników SAN oraz minimalne parametry techniczne zostały określone poniżej i stanowią podstawę do wyceny przedmiotu zamówienia przez Oferentów:

* + - * 1. Przełącznik FC musi być wykonany w technologii FC 32 Gb/s i posiadać możliwość pracy portów FC z prędkościami 16, 8 Gb/s z funkcją autonegocjacji prędkości.
        2. Przełącznik FC musi posiadać minimum 24 sloty na moduły. Wszystkie wymagane funkcje muszą być dostępne dla minimum 16 portów FC przełącznika.
        3. Przełącznik musi być dostarczony wraz z minimum 16 modułami SFP FC 32 Gb/s.
        4. Rodzaj obsługiwanych portów: F, E, M, D
        5. Przełącznik FC musi mieć wysokość maksymalnie 1 RU (jednostka wysokości szafy montażowej) i szerokość 19” oraz zapewniać techniczną możliwość montażu w szafie 19”.
        6. Przełącznik FC musi być wykonany w tzw. architekturze „non-blocking” uniemożliwiającej blokowanie się ruchu wewnątrz przełącznika przy pełnej prędkości pracy wszystkich portów.
        7. Przełącznik musi posiadać mechanizm balansowania ruchu między grupami połączeń tzw. „trunk” oraz obsługiwać grupy połączeń „trunk” o różnych długościach.
        8. Przełącznik FC musi udostępniać usługę Name Server Zoning - tworzenia stref (zon) w oparciu bazę danych nazw serwerów
        9. Przełącznik FC musi posiadać możliwość wymiany i aktywacji wersji firmware’u (zarówno na wersję wyższą jak i na niższą) w czasie pracy urządzenia, bez wymogu ponownego uruchomienia urządzeń w sieci SAN.
        10. Przełącznik FC musi posiadać wsparcie dla następujących mechanizmów zwiększających poziom bezpieczeństwa:
* Listy Kontroli Dostępu definiujące urządzenia (przełączniki i urządzenia końcowe) uprawnione do pracy w sieci Fabric
* Możliwość uwierzytelnienia (autentykacji) przełączników z listy kontroli dostępu w sieci Fabric za pomocą protokołów DH-CHAP i FCAP
* Możliwość uwierzytelnienia (autentykacji) urządzeń końcowych z listy kontroli dostępu w sieci Fabric za pomocą protokołu DH-CHAP
* Kontrola dostępu administracyjnego definiująca możliwość zarządzania przełącznikiem tylko z określonych urządzeń oraz portów
* Szyfrowanie połączenia z konsolą administracyjną. Wsparcie dla SSHv2,
* Wskazanie nadrzędnych przełączników odpowiedzialnych za bezpieczeństwo w sieci typu Fabric.
* Konta użytkowników definiowane w środowisku RADIUS lub LDAP
* Szyfrowanie komunikacji narzędzi administracyjnych za pomocą SSL/HTTPS
* Obsługa SNMP v3
  + - * 1. Przełącznik FC musi posiadać możliwość konfiguracji przez komendy tekstowe w interfejsie znakowym oraz przez przeglądarkę internetową z interfejsem graficznym.
        2. Przełącznik FC musi mieć możliwość instalacji jednomodowych SFP+ umożliwiających bezpośrednie połączenie (bez dodatkowych urządzeń pośredniczących) z innymi przełącznikami na odległość minimum 10km.
        3. Przełącznik FC musi zapewnić możliwość jego zarządzania przez zintegrowany port Ethernet, RS232 oraz inband IP-over-FC, USB port.
        4. Przełącznik FC musi zapewniać wsparcie dla standardu zarządzającego SMI-S v1.1 (powinien zawierać agenta SMI-S zgodnego z wersją standardu v1.1)
        5. Przełącznik FC musi zapewniać możliwość nadawania adresu IP dla zarządzającego portu Ethernet za pomocą protokołu DHCP
        6. Maksymalny dopuszczalny pobór mocy przełącznika FC to 77W
        7. Przełącznik FC musi zapewniać możliwość dynamicznego aktywowania portów za pomocą zakupionych kluczy licencyjnych.
        8. Przełącznik FC musi zapewniać sprzętową obsługę zoningu na podstawie portów i adresów WWN
        9. Możliwość wymiany w trybie „na gorąco”: minimum w odniesieniu do modułów portów Fibre Channel (SFP+).
        10. Wsparcie dla N\_Port ID Virtualization (NPIV).
        11. Zamawiający wymaga min. 60 miesięcy gwarancji producenta możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami:
* telefonicznie,
* przez Internet
* z wykorzystaniem aplikacji.
  + - * 1. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi sie na inną formę.
        2. Produkt musi być fabrycznie nowy i dostarczony przez autoryzowany kanał sprzedaży producenta na terenie kraju.
        3. Szyny do montażu w szafie rack.
  1. **Wymagania dotyczące Biblioteki taśmowej – 1 szt.**

Szczegółowe wymagania dotyczące Biblioteki taśmowej oraz minimalne parametry techniczne zostały określone w tabeli poniżej i stanowią podstawę do wyceny przedmiotu zamówienia przez Oferentów:

|  |  |
| --- | --- |
| **Nazwa elementu, parametru lub cechy** | **Opis minimalnych wymagań** |
| Obudowa | - Biblioteka nie może przekraczać 6U w dostarczonej konfiguracji.  - Montaż w przemysłowej szafie RACK 19”. |
| Obudowa – rozbudowa (opcjonalnie) | - Biblioteka musi skalować się do min. 8 modułów, 6U każdy, 48U łącznie. Niedopuszczalne jest stosowanie okablowania zewnętrznego (np. łączników SCSI) do wykonania rozbudowy, wszelka komunikacja musi odbywać się połączeniami wewnętrznymi. |
| Napędy taśmowe | - Biblioteka taśmowa musi być wyposażona w min. 2 napędy taśmowe LTO9 o natywnym interfejsie FC, pełnej wysokości (Full Height)  - Biblioteka powinna umożliwiać wymianę napędów bez przerywania pracy (napędy typu „hot swap”).  - Żadna funkcjonalność biblioteki taśmowej realizowana przez napędy taśmowe (np. sprawdzanie konsystencji danych) nie może wymuszać łączności napędów taśmowych do innych przełączników niż przełączniki FC.  - Biblioteka musi posiadać możliwość zautomatyzowanego kalibrowania nośników LTO9 z poziomu panelu zarządzania biblioteką taśmową. |
| Napędy taśmowe – rozbudowa (opcjonalnie) | - Biblioteka musi mieć możliwość rozbudowy do 24 napędów taśmowych LTO9 (o natywnych dwóch interfejsach FC, pełnej wysokości (Full Height)), łącznie.  - Musi być możliwość mieszania napędów różnych technologii LTO (od min. LTO-8). |
| Napędy taśmowe - szyfrowanie | - Biblioteka musi mieć możliwość sprzętowego szyfrowania kopii zapasowych z wykorzystaniem napędów taśmowych. Klucze szyfrujące muszą być przechowywane w aplikacji backup.  - Licencja musi być dostarczona wraz z biblioteką. |
| Liczba slotów - storage | - Biblioteka musi mieć min. (fizycznie oraz zalicencjonowanych do dowolnego użytku) 100 kieszeni na nośniki taśmowe. |
| Liczba slotów - storage – rozbudowa (opcjonalnie) | - Biblioteka musi mieć możliwość rozbudowy do min. (fizycznie oraz zalicencjonowanych do dowolnego użytku) 800 kieszeni na nośniki taśmowe. |
| Liczba slotów - mail slot | - Biblioteka musi mieć możliwość zdefiniowania do 50 kieszeni typu „mail slot” w odstępach co 5 (licząc od 0). |
| Ochrona przed ransomware | - Biblioteka musi mieć możliwość stworzenia bezpiecznej przestrzeni dla nośników taśmowych w celu ochrony przed ransomware.  - Partycja musi być skonfigurowana na dostępnych slotach w bibliotece nawet w przypadku, kiedy nie są one za licencjonowane oraz bez możliwości dołączenia do niej napędu taśmowego.  - Biblioteka taśmowa musi przechwytywać operację eksportu nośników taśmowych wykonywanych przez aplikację backup i umieszczać te nośniki w bezpiecznym miejscu a nie w slotach typu “mail”.  - Biblioteka musi mieć możliwość definiowania tzw. “logical lock”, który uniemożliwi użytkownikowi administracyjnemu przesunięcie nośnika taśmowego w inny slot lub napęd biblioteki taśmowej.  - Biblioteka musi mieć możliwość zainstalowanego tzw. “hardware lock”, który uniemożliwi fizyczną ingerencję w bibliotekę taśmową (np. serwisowe wysunięcie magazynków z nośnikami taśmowymi) ale zapewni możliwość skanowania tak zabezpieczonych nośników taśmowych w celach np. inwentaryzacji.  - „Hardware Lock” musi mieć możliwość zdefiniowania po jakiej liczbie nośników taśmowych magazynek ma zostać automatycznie wysunięty. |
| Numery seryjne biblioteki i napędów taśmowych | - Biblioteka taśmowa musi mieć możliwość włączenia adresacji logicznej dla modułu kontrolnego (numer seryjny) oraz napędów taśmowych (WWN), dzięki czemu wymiana tych komponentów nie wpływa na rekonfigurację aplikacji i sieci SAN. |
| Zarządzanie | - Biblioteka musi zarządzana z poziomu panelu dotykowego zabezpieczonego hasłem lub/i numerem PIN oraz zdalnego modułu zarządzania przez panel WWW (HTML5).  - Musi być możliwość tworzenia użytkowników lokalnych oraz integracji z systemem usług katalogowych – Microsoft Active Directory (które Zamawiający obecnie używa).  - Biblioteka musi wspierać Multi-Factor Authentication (MFA) dla min. użytkowników lokalnych.  - Biblioteka musi udostępniać funkcje monitorowania stanu napędów i robota.  - Biblioteka taśmowa powinna mieć również możliwość zdalnego monitorowania stanu urządzenia i wychwytywania błędów bezpośrednio przez inżynierów producenta za pomocą odpowiedniego oprogramowania, dostarczonego razem z biblioteką taśmową. Nie jest dopuszczalne instalowanie żadnych dodatkowych systemów (wirtualnych czy fizycznych) w celu osiągnięcia tej funkcjonalności.  - Obsługa SNMP, Syslog, proxy, definiowanie access list dla adresów IP.  - Biblioteka musi posiadać min. 2 redundantne interfejsy 1GbE do zarządzania. Interfejsy muszą być zlokalizowane na module zarządzania biblioteką oraz posiadać wszystkie mechanizmy zarządzania na obu portach. |
| Partycjonowanie | - Biblioteka powinna być wykonana w technologii umożliwiającej sprzętowy podział na mniejsze biblioteki „logiczne”, a następnie podłączane do różnych serwerów, korzystających z różnego oprogramowania do wykonywania kopii zapasowych i archiwizacji.  - Biblioteka musi wspierać do 24 logicznych bibliotek.  - Biblioteka musi emulować co najmniej następujące biblioteki fizyczne: Quantum i40, i80, i3, i6, i500 oraz i6000. |
| Inwentaryzacja | - Biblioteka musi być wyposażona w czytnik kodów kreskowych a czas jej inwentaryzacji nie powinien przekraczać 7 minut dla pełnej konfiguracji. |
| Zasilanie | - W pełni redundantne dla wszystkich modułów. |
| Kompatybilność | - Oferowane urządzenie musi wspierać, co najmniej następujące aplikacje:   * Acronis Backup, * Arcserve Arcserve Backup, * Archiware P5, * Atempo Time Navigator, * Commvault Simpana/Next Generation Platform, * EMC NetWorker, * IBM Tivoli Storage Manager/Spectrum Protect, * Micro Focus/HP Data Protector, * Microsoft Data Protection Manager, * NovaStor NovaStor DataCenter, * Oracle HSM, * Oracle SecureBackup, * Quest NetVault, * Veeam Backup and Replication, * Veritas Backup Exec, * Veritas NetBackup. |
| Konsystencja danych | - Biblioteka musi posiadać możliwość rozbudowy o system sprawdzania konsystencji danych na nośnikach taśmowych, który działa transparentnie dla systemu operacyjnego i aplikacji wykorzystującej bibliotekę.  - Do realizacji funkcjonalności należy przeznaczyć dedykowany napęd taśmowy.  - Funkcjonalność musi być realizowana bezpośrednio przez oprogramowanie wewnętrzne biblioteki.  - Dodatkowa infrastruktura (maszyny wirtualne, systemy zarządzania) do realizacji tej funkcjonalności jest niedopuszczalne. |
| Gwarancja | - Dostarczona biblioteka musi być fabrycznie nowa oraz pochodzić z oficjalnego kanału sprzedaży w Polsce.  - Biblioteka musi być serwisowana przez producenta lub autoryzowany serwis producenta w języku Polskim ze wsparciem co najmniej 5 lat w trybie 5x9xNBD.  - W przypadku autoryzowanego serwisu producenta na terenie Polski, wymagane jest potwierdzenie kompetencji w zakresie świadczenia usług serwisowych poprzez certyfikat ISO ISO 9001:2015 lub równoważny oraz minimum 3 certyfikowanych inżynierów przez producenta w serwisie dedykowanego urządzenia |
| Taśmy | - Sprzęt powinien być dostarczony z co najmniej 100 taśmami LTO-9 z labelami NIM300, NIM301, NIM302 etc. oraz z co najmniej 5 taśmami czyszczącymi. |
| Inne | - Jeśli do jakiejkolwiek wyżej opisanej funkcjonalności lub rozbudowy fizycznej wymagane jest dostarczenie licencji ta licencje musi być dostarczona w ramach tego postępowania  - Sprzęt musi być dostarczony z kompletnym okablowaniem umożliwiającym pełne uruchomienie systemu. |

* 1. **Wymagania dotyczące Konsoli i przełączniki KVM – 1 szt.**

Szczegółowe wymagania dotyczące konsoli i przełączników KVM oraz minimalne parametry techniczne zostały określone poniżej i stanowią podstawę do wyceny przedmiotu zamówienia przez Oferentów:

1. Konsola musi być przeznaczona do montażu w szafie serwerowej standardu RACK i po złożeniu jej wysokość instalacyjna nie może przekraczać wysokości 1U.
2. Urządzenie musi posiadać wbudowany ekran LCD o przekątnej minimum 18,5”
3. Urządzenie musi posiadać wbudowaną klawiaturę z układem International English (qwerty)
4. Urządzenie musi posiadać wbudowaną mysz minimum trzyprzyciskową w formie touchpad.
5. Urządzenie musi posiadać porty przyłączeniowe do połączenia z przełącznikiem KVM
6. Konsola powinna być wyposażona w szyny montażowe pozwalające na instalację w szafie rack. Szyny powinny umożliwiać korzystanie z konsoli (klawiatura monitor mysz) przy zajętości sąsiednich miejsc instalacyjnych w szafie – pełne wysunięcie oraz otwarcie urządzenia
7. Należy zapewnić niezbędne kable przyłączeniowe do przełącznika KVM oraz okablowanie zasilające do przyłączenia zasilania.
8. Przełącznik musi być przeznaczony do montażu w szafie serwerowej standardu RACK i nie może przekraczać wysokości 1U.
9. Urządzenie musi posiadać 16 portów
10. Dostęp do urządzenia jest realizowany za pośrednictwem TCP/IP. Łącza te obsługują szyfrowanie DES, 3DES, AES i 128-bitowy protokół SSL w ramach sesji KVM i nośników wirtualnych
11. Urządzenie musi posiadać porty (VGA, USB) do podłączenia konsoli KVM LCD
12. Urządzenie musi posiadać redundantne zasilacze
13. Urządzenie musi umożliwiać mapowanie bezpośrednio podłączonych urządzeń do przełącznika KVM (USB DVD-ROM, USB Pendrive) do podłączonych serwerów.
14. Urządzenie musi umożliwiać zestawianie zdalnych połączeń do konsol serwerów (minimum 2 użytkowników pracujących równocześnie)
15. Urządzenia muszą posiadać minimum 60 miesięcy gwarancji producenta
    1. **Wymagania dotyczące Systemu wirtualizacji wraz z usługą wdrożenia środowiska witalizacyjnego – 1 szt.**

Przedmiotem zamówienia jest dostawa instalacja i konfiguracja licencji oprogramowania Vmware vSphere 9 na okres 5 lat wraz z usługą wsparcia gwarancyjnego producenta liczonego od dnia dostarczenia oprogramowania.

Oprogramowanie musi pochodzić bezpośrednio od Producenta lub z oficjalnych i autoryzowanych przez Producenta kanałów dystrybucyjnych. Zamawiający wymaga, aby Wykonawca posiadał kwalifikacje i uprawnienia wymagane do prawidłowej realizacji przedmiotu zamówienia.

**Zamawiający wymaga spełnienia przez oprogramowanie minimalnych wymagań   
w zakresie funkcjonalności określonych poniżej (warunki równoważności):**

**Wirtualizacja mocy obliczeniowej**

1. Zaoferowane oprogramowanie do wirtualizacji musi być instalowane bezpośrednio na sprzęcie fizycznym i nie może być ono częścią innego systemu operacyjnego
2. W zaoferowanym oprogramowaniu warstwa wirtualizacji nie może dla własnych celów alokować więcej niż 200MB pamięci operacyjnej RAM serwera fizycznego
3. Zaoferowane oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym musi potrafić obsłużyć i wykorzystać procesory fizyczne tego serwera wyposażone w 768 logicznych wątków, 16TB pamięci fizycznej RAM tego serwera oraz 16 procesorów fizycznych tego serwera
4. Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z ilością od 1 do 256 procesorów wirtualnych
5. Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 6 TB pamięci operacyjnej RAM
6. Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia od 1 do 10 wirtualnych kart sieciowych dla każdej z nich. Dodatkowo, oprogramowanie musi posiadać możliwość utworzenia maszyny wirtualnej bez przydzielonej wirtualnej karty sieciowej.
7. Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowe, 3 porty równoległe i 20 urządzeń USB
8. Zaoferowane oprogramowanie musi wspierać następujące systemy operacyjne: Windows Server 2016, Windows Server 2019, Windows Server 2022, Windows Server 2025, Windows 7, Windows 8, Windows 10, Windows 11, Debian, CentOS, Ubuntu, Photon OS, Oracle Linux
9. W celu osiągnięcia maksymalnego współczynnika konsolidacji, zaoferowane oprogramowanie musi umożliwiać przydzielenie łącznie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera, na którym maszyny te są posadowione
10. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie dostępne na zasobach dyskowych
11. Zaoferowane oprogramowanie musi zapewniać sprzętowe wsparcie dla wirtualizacji zagnieżdżonej, w szczególności instalacji wszystkich funkcjonalności w tym Microsoft Hyper-V pakietu Microsoft Windows Server 2012 na maszynie wirtualnej
12. Zaoferowane oprogramowanie musi umożliwiać integrację z rozwiązaniami antywirusowymi firm trzecich w zakresie skanowania maszyn wirtualnych z poziomu warstwy wirtualizacji bez ingerencji w systemy operacyjne maszyn wirtualnych (bezagentowość)
13. Zaoferowane oprogramowanie musi zapewniać zdalny i lokalny dostęp administracyjny do wszystkich serwerów fizycznych poprzez protokół SSH, z możliwością nadawania uprawnień do takiego dostępu nazwanym użytkownikom bez konieczności wykorzystania konta „root”
14. Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość powielania maszyn wirtualnych wraz z ich pełną konfiguracją i danymi
15. Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy z możliwością konieczności zachowania stanu pamięci pracującej maszyny wirtualnej.
16. Konsola zarządzająca zaoferowanego oprogramowania musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi, minimalnie z: Microsoft Active Directory i Open LDAP
17. Zaoferowane oprogramowanie musi zapewniać możliwość dodawania zasobów w czasie pracy maszyny wirtualnej, w szczególności w zakresie ilości procesorów, pamięci operacyjnej i przestrzeni dyskowej
18. Zaoferowane oprogramowanie musi posiadać funkcjonalność tworzenia wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta (hypervisora wirtualizacyjnego) i pozwalającego połączyć tym przełącznikiem maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji minimum 4000 portów
19. Pojedynczy wirtualny przełącznik w zaoferowanym oprogramowaniu, w celu zapewnienia bezpieczeństwa połączenia ethernetowego w razie awarii fizycznej karty sieciowej, musi posiadać możliwość przyłączania do niego minimum dwóch fizycznych kart sieciowych
20. Wirtualne przełączniki w zaoferowane oprogramowaniu muszą posiadać funkcjonalność obsługi wirtualnych sieci lokalnych (VLAN)
21. Zaoferowane oprogramowanie musi zapewniać możliwość konfigurowania polityk separacji sieci w warstwie trzeciej, tak aby zapewnić oddzielne grupy wzajemnej komunikacji pomiędzy maszynami wirtualnymi
22. Zaoferowane oprogramowanie musi umożliwiać wykorzystanie technologii przepustowości sieci komputerowych do 100GbE w tym agregację połączeń fizycznych do minimalizacji czasu przenoszenia maszyny wirtualnej pomiędzy serwerami fizycznymi
23. Zaoferowane oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek LAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieże
24. Zaoferowane oprogramowanie musi zapewnić możliwość zdefiniowania alertów informujących o przekroczeniu wartości progowych
25. Zaoferowane oprogramowanie, musi zapewniać możliwość replikacji maszyn wirtualnych z dowolnej pamięci masowej w tym z dysków wewnętrznych serwerów fizycznych na dowolną pamięć masową w tym samym lub oddalonym ośrodku przetwarzania.
26. Zaoferowane oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek
27. Zaoferowane oprogramowanie musi mieć możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami fizycznymi bez przerywania pracy usług na przenoszonych maszynach wirtualnych.
28. Wymaga się wsparcia natywnego szyfrowania ruchu sieciowego dla maszyn wirtualnych podczas ich przenoszenia między serwerami fizycznymi
29. Zaoferowane oprogramowanie w środowisku z więcej niż pojedynczym wirtualizatorem, musi umożliwiać automatyczne, ponowne uruchomienie maszyn wirtualnych w przypadku awarii jednego z wirtualizatorów na kolejnym, działającym w tym samym klastrze wirtualizatorze (funkcjonalność HA) (ang. high availability)
30. Zaoferowane oprogramowanie w środowisku z minimalnie dwoma wirtualizatorami oraz w przypadku potrzeby wgrania aktualizacji do warstwy wirtualizacji, musi posiadać możliwość w przypadku wywołania startu aktualizacji, automatycznego przeniesienia bezprzerwowego działających maszyn wirtualnych do innego wirtualizatora nie objętego aktualizacją, przed rozpoczęciem samej aktualizacji
31. Zaoferowane oprogramowanie musi posiadać co najmniej 2 niezależne mechanizmy wzajemnej komunikacji między serwerami z zainstalowanym wirtualizatorem oraz z serwerem zarządzającym, gwarantujące właściwe działanie mechanizmów wysokiej dostępności na wypadek izolacji sieciowej serwerów fizycznych lub partycjonowania sieci
32. Zaoferowane oprogramowanie w środowisku z minimum dwoma wirtualizatorami musi zapewniać pracę bez przestojów dla wybranych maszyn wirtualnych (o maksymalnie dwóch procesorach wirtualnych), niezależnie od systemu operacyjnego oraz aplikacji, podczas awarii wirtualizatora, bez utraty danych i dostępności danych na maszynach wirtualnych objętych ochroną
33. Zaoferowane oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości 62 TB
34. Zaoferowane oprogramowanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjne
35. Producent zaoferowanego oprogramowania do wirtualizacji musi wspierać rozwiązania do automatyzacji procesów oraz wirtualizacji sieci (SDN, ang. software defined network).
36. Zaoferowane oprogramowanie musi wspierać mechanizmy zaawansowanego uwierzytelniania do systemu operacyjnego wirtualnej maszyny za pomocą technologii Smart Card Reader
37. Zaoferowane oprogramowanie musi wspierać TPM 2.0. Minimalne wymaganie Zamawiającego dla TPM oznacza, że TPM zapewnia mechanizm gwarantujący, że serwer fizyczny, na którym zainstalowane jest zaoferowane oprogramowanie, uruchomił się z włączoną opcją Secure Boot. Po potwierdzeniu, że Secure Boot jest włączone, system gwarantuje, poprzez weryfikację podpisu cyfrowego, że hypervisor uruchomił się w niezmienionej formie
38. Wirtualizator w zaoferowanym oprogramowaniu musi mieć możliwość włączenia funkcji “Microsoft virtualization-based security”, tzw. Microsoft VBS dla systemów operacyjnych maszyn wirtualnych opartych o system operacyjny Microsoft Windows 10, Microsoft Windows Server 2022 oraz Microsoft Windows Server 2025.
39. Zaoferowane oprogramowanie musi posiadać certyfikację FIPS-140-2 min. dla modułu jądra wirtualizatora odpowiedzialnego za szyfrowanie danych
40. Zaoferowane oprogramowanie musi posiadać funkcjonalność szybkiego uruchamiania wirtualizatora po przeprowadzonym procesie jego aktualizacji. Zamawiający wymaga aby w procesie aktualizacji wirtualizatora, jeśli wymagany jest jego restart, funkcjonalność szybkiego uruchamiania powodowała eliminację czasochłonnej fazy inicjalizacji serwera fizycznego
41. Zaoferowane oprogramowanie musi posiadać możliwość aktualizacji i kontroli wersji oprogramowania do wirtualizacji w ramach klastra serwerów z poziomu centralnej konsoli zarządzającej. Dodatkowo centralna konsola zarządzająca musi posiadać funkcjonalność aktualizacji firmware komponentów serwera fizycznego (dyski, kontrolery, karty sieciowe) z poziomu konsoli zarządzającej wirtualizatora. Konsola zarządzająca musi mieć możliwość automatycznej weryfikacji, czy zainstalowane komponenty serwera posiadają rekomendowaną wersję sterowników i firmware, eliminując ryzyko pracy na nieaktualnych wersjach. Taka funkcjonalność powinna być dostępna dla minimum dwóch producentów serwerów
42. Zaoferowane oprogramowanie musi posiadać wsparcie dla natywnych dysków 4K
43. Zaoferowane oprogramowanie musi wspierać protokół precyzyjnej synchronizacji czasu PTP
44. Zaoferowane oprogramowanie musi posiadać mechanizm, który ogranicza dostęp do indywidualnego zarządzania warstwą wirtualizacji na serwerach fizycznych w ramach klastra serwerów w celu utwardzenia/hardening (maksymalnego zwiększenia bezpieczeństwa dostępu) systemu wirtualizacji.
45. Zaoferowane oprogramowanie musi mieć funkcjonalność migracji w trybie rzeczywistym dysków działających maszyn wirtualnych z jednego podsystemu dyskowego do innego bez konieczności przerywania pracy maszyny wirtualnej, której dysk jest migrowany
46. Zaoferowane oprogramowanie podczas pracy w klastrze musi umożliwiać automatyczne równoważenie obciążenia CPU/MEM serwerów fizycznych pracujących jako platforma dla infrastruktury wirtualnej
47. Zaoferowane oprogramowanie do wirtualizacji musi zapewniać mechanizm pozwalający tworzyć profil (szablon konfiguracji) wybranego serwera wirtualizacyjnego (Hypervisora), a następnie wymuszać ten profil/konfigurację na innych serwerach fizycznych lub sprawdzać zgodność konfiguracji pomiędzy zdefiniowanym wcześniej profilem a wskazanym serwerem fizycznym
48. Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, musi umożliwiać utworzenie w nim jednorodnego, wirtualnego przełącznika sieciowego, rozproszonego na wszystkie serwery fizyczne istniejące w tym klastrze. Przełącznik taki musi zapewniać możliwość konfiguracji parametrów sieciowych maszyny wirtualnej z granulacją na poziomie portu tego przełącznika. Pojedyncza maszyna wirtualna musi mieć możliwość wykorzystania jednego lub wielu portów przełącznika z niezależną od siebie konfiguracją. Przełącznik rozproszony musi współpracować z protokołem NetFlow
49. Zaoferowane oprogramowanie do wirtualizacji, w ramach zaimplementowanego w nim rozproszonego przełącznika sieciowego, powinno zapewniać możliwość integracji z produktami (przełącznikami wirtualnymi) firm trzecich, tak aby umożliwić granularną delegację zadań w zakresie zarządzania konfiguracją sieci do zespołów sieciowych
50. Zaimplementowany w zaoferowanym oprogramowaniu przełącznik rozproszony musi umożliwiać funkcjonalność duplikowania ruchu sieciowego dowolnego jego portu wirtualnego na inny port
51. Zaimplementowany w zaoferowanym oprogramowaniu przełącznik rozproszony musi mieć wbudowane mechanizmy składowania kopii konfiguracji, przywracania tej kopii a także mechanizmy automatycznie zapobiegające niewłaściwej konfiguracji sieciowej, które w całości lub w części mogą eliminować błędy ludzkie i utratę łączności sieciowej
52. Zaoferowane oprogramowanie musi mieć wbudowany mechanizm kontrolowania i monitorowania ruchu sieciowego oraz ustalania priorytetów w zależności od jego rodzaju na poziomie konkretnych maszyn wirtualnych
53. Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, musi mieć możliwość uruchamiania fizycznych serwerów z centralnie przygotowanego obrazu poprzez protokół PXE
54. Zaoferowane oprogramowanie, musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane maksymalnie sprzed roku
55. Zaoferowane oprogramowanie, musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi, pamięciami masowymi niezależnie od dostępności współdzielonej przestrzeni dyskowej, różnymi rodzajami wirtualnych przełączników sieciowych oraz pomiędzy różnymi Centrami Przetwarzania Danych platformami wirtualnej
56. Zaoferowane oprogramowanie w środowisku z minimum dwoma wirtualizatorami, musi zapewniać pracę bez przestojów dla wybranych maszyn wirtualnych (o maksymalnie czterech procesorach wirtualnych), niezależnie od systemu operacyjnego oraz aplikacji, podczas awarii wirtualizatora, bez utraty danych i dostępności danych na maszynach wirtualnych objętych ochroną
57. Zaoferowane oprogramowanie musi mieć wbudowany mechanizm kontrolowania i monitorowania ruchu do pamięci masowych oraz ustalania priorytetów dostępu do nich na poziomie konkretnych wirtualnych maszyn
58. Zaoferowane oprogramowanie musi mieć możliwość grupowania pamięci masowych o podobnych parametrach w grupy i przydzielania ich do wirtualnych maszyn zgodnie z ustaloną przez administratora polityką
59. Zaoferowane oprogramowanie musi umożliwiać udostępnianie pojedynczego urządzenia fizycznego (PCIe) jako logicznie separowanego wirtualnego urządzenia dedykowanego dla poszczególnych maszyn wirtualnych
60. Zaoferowane oprogramowanie, musi mieć możliwość równoważenia obciążenia i zajętości pamięci masowych wraz z pełną automatyką i przenoszeniem plików wirtualnych maszyn z bardziej zajętych na mniej zajęte przestrzenie dyskowe lub/i z przestrzeni dyskowych bardziej obciążonych operacjami I/O na mniej obciążone
61. Zaoferowane oprogramowanie musi umożliwiać uruchamianie kontenerów zbudowanychw topologii Docker Image w wirtualnych maszynach
62. Zaoferowane oprogramowanie musi wspierać technologię rozproszonego udostępniania procesora graficznego Nvidia Grid vGPU zainstalowanego w serwerze fizycznym do maszyn wirtualnych
63. Zaoferowane oprogramowanie musi wspierać funkcjonalność trwałej, nieulotnej pamięci (ang. Persistent Memory)
64. Zaoferowane oprogramowanie musi wspierać protokół Remote Direct Memory Access (RDMA) poprzez konwergentny Ethernet, lub RoCE (“rocky”) v2, Fiber Channel over Ethernet (FCoE) adapter i iSCSI rozszerzenie dla RDMA (iSER). Wymaga się, aby maszyny wirtualne można było konfigurować z wykorzystaniem protokołu RDMA
65. Zaoferowane oprogramowanie musi wspierać możliwość eksportu konfiguracji centralnej konsoli zarządzającej przez API i umożliwiać wykorzystanie jej jako szablonu przy kreowaniu kolejnych instancji centralnej konsoli zarządzającej oraz do weryfikacji poprawności konfiguracji zainstalowanych już instancji
66. Centralna konsola zarządzająca musi wspierać możliwość wcześniejszego i automatycznego przetestowania wpływu jej aktualizacji na pozostałe podłączone do niej komponenty klastra oraz uruchomione na nim funkcjonalności. Musi również wspierać proces aktualizacji całego klastra poprzez automatyczne raportowanie kolejności aktualizacji podłączonych do niej komponentów i rekomendowanej ich wersji
67. Dodatkowo zaoferowane oprogramowanie musi wspierać funkcjonalność bezpośredniego tworzenia kontenerów oraz klastrów Kubernetes na hiperwizorze (warstwie wirtualizatora) za pomocą dostarczonej konsoli zarządzającej Kubernetes (Kubectl) – włączenie tej funkcji w warstwie wirtualizatora może wymagać dodatkowej licencji/subskrypcji, która nie jest wymagana
68. Zaoferowana licencja na oprogramowanie spełniające powyższe wymagania musi posiadać możliwość swobodnego przeniesienia na dowolny serwer fizyczny będący w posiadaniu Zamawiającego (bez ograniczeń licencji OEM). Licencje dostępne w modelu licencjonowania na procesor fizyczny.

**Moduł wirtualizacji przestrzeni dyskowej**

Zamawiający wymaga dostarczenia oprogramowania spełniającego poniższe funkcjonalności:

* 1. Zaoferowane oprogramowanie musi umożliwiać zbudowanie współdzielonej przestrzeni dyskowej w oparciu o dyski wewnętrzne serwerów fizycznych. System powinien wspierać następujące konfiguracje: hybrydowa w oparciu o dyski SSD i HDD oraz allflash w oparciu o dyski SSD (SAS/SATA/NVMe).
  2. Każdy serwer fizyczny, na którym zostanie zainstalowane zaoferowane oprogramowane, musi dostarczać zarówno moc obliczeniową do klastra (CPU i RAM) jak również przestrzeń dyskową definiowaną programowo (eng. Software Defined Storage). Powyższa funkcjonalność musi dać możliwość utworzenia przestrzeni dyskowej złożonej z 64 hostów.
  3. W przypadku potrzeby wykonania rozwiązania, opartego na zaoferowanym oprogramowaniu, posiadającego wyłącznie dyski SSD, zaoferowane oprogramowanie musi zapewniać możliwość optymalizacji wydajności poprzez wbudowaną funkcjonalność „cache’owania” operacji zapisu.
  4. W przypadku potrzeby wykonania rozwiązania opartego na zaoferowanym oprogramowaniu, posiadającego dyski mieszane, tj. SSD i HDD, zaoferowane oprogramowanie musi zapewniać możliwość optymalizacji wydajności poprzez wbudowaną funkcjonalność „cache’owania” operacji zapisu i odczytu z możliwością
  5. W przypadku potrzeby wykonania rozwiązania opartego na zaoferowanym oprogramowaniu posiadającego dyski mieszane, tj. SSD i HDD, oprogramowanie musi posiadać funkcjonalność rezerwacji, dla poszczególnych maszyn wirtualnych, części dysku „cache” wykonującego funkcję odczytu
  6. Zaoferowane rozwiązanie musi wspierać technologie NVMe i “cache’owanie” operacji zapisu z wykorzystaniem dysków NVMe
  7. Zaoferowane rozwiązanie musi umożliwiać konfigurację serwerów all-NVMe
  8. W przypadku zastosowania dysków NVMe zaoferowanie rozwiązanie musi wspierać ich wymianę w trybie hot-plug dla dodawania i wyjmowania dysków “na gorąco”. Taka funkcjonalność musi być dostępna dla minimum dwóch producentów serwerów
  9. Zaoferowane oprogramowanie musi posiadać możliwość aktualizacji i kontroli wersji oprogramowania do wirtualizacji pamięci masowej w ramach klastra serwerów z poziomu centralnej konsoli zarządzającej. Dodatkowo centralna konsola zarządzająca musi posiadać funkcjonalność aktualizacji firmware komponentów serwera fizycznego (dyski, kontrolery, karty sieciowe) z poziomu konsoli zarządzającej wirtualizatora. Konsola zarządzająca musi mieć możliwość automatycznej weryfikacji, czy zainstalowane komponenty serwera posiadają rekomendowaną wersję sterowników i firmware, eliminując ryzyko pracy na nieaktualnych wersjach. Taka funkcjonalność powinna być dostępna dla minimum dwóch producentów serwerów
  10. Zaoferowane oprogramowanie musi zapewniać możliwość zmniejszania lub zwiększenia przestrzeni dyskowej (odjęcie lub dodanie pojedynczego dysku, odjęcie lub dodanie serwera fizycznego) w sposób niewymagający przestoju i przerwy w dostępie do działających na zmienianym środowisku maszyn wirtualnych
  11. Zaoferowane oprogramowanie musi być zintegrowane z warstwą wirtualizacji w sposób bezpośredni, niewymagający instalacji lub konfiguracji dodatkowych komponentów sprzętowych oraz dodatkowego oprogramowania lub dodatkowych maszyn wirtualnych.
  12. Konfiguracja, zarządzanie i monitoring przestrzeni dyskowej, w zaoferowanym oprogramowaniu, muszą być zintegrowane z centralną konsolą zarządzającą platformą wirtualizacyjną
  13. Zaoferowane oprogramowanie musi zapewniać możliwość obsługiwania dysków wirtualnych maszyn do rozmiaru min. 62TB
  14. Funkcjonalności zaoferowanego oprogramowania nie może w żaden sposób ograniczać lub niwelować żadnej funkcjonalności platformy wirtualizacyjnej między innymi w warstwie mechanizmów niezawodnościowych, wydajnościowo-optymalizacyjnych jak i zarządzania.
  15. Zaoferowane oprogramowanie musi zapewniać funkcjonalność konfigurowalnych mechanizmów zabezpieczania danych na wypadek awarii sprzętowej w ramach lokalizacji lub szafy rack w taki sposób, aby poszczególne kopie dysków maszyny wirtualnej nie były umieszczane na hostach w ramach tej samej szafy rackowej lub w ramach tej samej lokalizacji
  16. Zaoferowane oprogramowanie musi posiadać, na oficjalnej stronie producenta tego oprogramowania, listę wspieranych i certyfikowanych konfiguracji serwerowych. Wymagane jest wsparcie dla min. 5 niezalenych producentów sprzętu serwerowego dostępnego na terenie Unii Europejskiej.
  17. Zaoferowane oprogramowanie nie może wprowadzać ograniczenia, aby na etapie rozbudowy przestrzeni dyskowej wymagana była rozbudowa jedynie o serwery fizyczne producenta wykorzystane na etapie przed rozbudową. W przypadku rozbudowy o kolejne serwery fizyczne, wytworzone na podstawie zaoferowanego oprogramowania, rozwiązanie nie może wprowadzać wymogu, aby w dostarczanych, kolejnych serwerach fizycznych, wymagana była instalacja komponentów sprzętowych oferowanych tylko przez jednego dostawce/producenta (np. dyski, adaptery, specjalizowane karty i kontrolery)
  18. Zaoferowane oprogramowanie musi zapewniać funkcjonalność możliwości rozbudowy i skalowania zarówno mocy obliczeniowej, pojemności przestrzeni cache, jak i pojemności przestrzeni dyskowej (w ramach istniejącej infrastruktury serwerów fizycznych) bez konieczności dodawania kolejnych serwerów fizycznych
  19. Zaoferowane oprogramowanie musi zapewniać możliwość rozbudowy oferowanej przestrzeni dyskowej poprzez dodanie pojedynczego dysku lub dodanie jednego lub więcej serwera fizycznego w sposób niewymagający przestoju i przerwy w dostępie do działających usług wirtualnych
  20. Zaoferowane oprogramowanie musi zapewniać możliwość ochrony danych przed utratą ich integralności za pomocą weryfikacji sum kontrolnych. Suma kontrolna musi być liczona w momencie wykonania przez maszynę wirtualną operacji IO write już na poziomie wirtualizatora
  21. Zaoferowane oprogramowanie musi umożliwiać zarządzanie warstwą wirtualizacji mocy obliczeniowej i pamięci masowej bez potrzeby otwierania dostępu poprzez protokół SSH.
  22. Zaoferowane oprogramowanie musi umożliwiać utworzenie wysokodostępnego klastra przestrzeni dyskowej w scenariuszu dla tzw. „oddziału zdalnego”, zbudowanego w oparciu o min. 2 serwery fizyczne i min. dwie lokalizacje. Architektura systemu musi mieć możliwość dołączania kolejnych lokalizacji „oddziałów zdalnych” w ilości min. 64.
  23. Zaoferowane oprogramowanie musi zapewniać możliwość tworzenia i konfigurowania polityk niezawodnościowych, wydajnościowych i pojemnościowych przypisanych z granulacją na poziomie dysków maszyn wirtualnych tak, aby można było określić min.: liczbę serwerów fizycznych, które mogą ulec awarii jednocześnie, liczbę operacji I/O, użycie funkcji thin-provisioning, stripe
  24. Zaoferowane oprogramowanie musi posiadać możliwość udostępniania przestrzeni dyskowej również dla fizycznych systemów operacyjnych w oparciu o technologię iSCSI i umożliwiać zarządzanie dostępnością, pojemnością i wydajnością bez konieczności wyłączania systemów na tej przestrzeni posadowionych („w locie”)
  25. Zaoferowane oprogramowanie musi posiadać interfejs API umożliwiający automatyzowanie wdrażania lub modyfikacji konfiguracji systemu
  26. Zaoferowane oprogramowanie musi umożliwiać funkcjonalność automatycznego odzyskiwania pojemności dyskowej (przestrzeni dyskowej) zwolnionej na poziomie systemu operacyjnego tj. TRIM/UNMAP (ang. storage space reclamation)
  27. Zaoferowane oprogramowanie musi mieć możliwość włączania na żądanie i wyłączania na żądanie dostępnej w ramach funkcjonalności zaoferowanego oprogramowania dedupikacji i kompresji
  28. Zaoferowane oprogramowanie musi zapewniać mechanizmy optymalizacji wykorzystania przestrzeni dyskowych (ang. ereasure coding) dla RAID 5 I RAID 6 konfigurowane per dysk maszyny wirtualnej
  29. Zaoferowane oprogramowanie musi umożliwiać rozciągnięcie zdefiniowanej przestrzeni dyskowej pomiędzy dwiema fizycznymi lokalizacjami oddalonymi z czasem RTT wynoszącym nie więcej niż 5ms dla warstw sieci L2 lub L3 w ten sposób, by zapis danych następował synchronicznie do obu lokalizacji.
  30. Zaoferowane oprogramowanie musi zapewniać możliwość tworzenia i konfigurowania polityk niezawodnościowych, wydajnościowych i pojemnościowych przypisanych z granulacją na poziomie dysków maszyn wirtualnych tak, aby można było określić min.: liczbę serwerów fizycznych, które mogą ulec awarii jednocześnie, liczbę operacji I/O, użycie funkcji thin-provisioning, stripe, replikację lub jej brak w ramach rozciągniętego klastra. Funkcjonalność klastra opisana została w poprzedzającym punkcie.
  31. Zaoferowane oprogramowanie musi posiadać konfigurowalne mechanizmy zabezpieczania danych na wypadek awarii jednego z dwóch centrów danych (klaster rozciągnięty) w taki sposób, aby poszczególne kopie maszyn wirtualnych były umieszczane zarówno na hostach w ramach tej samej lokalizacji (lokalna protekcja) oraz w ramach dwóch lokalizacji (protekcja na poziomie lokalizacji)
  32. Zaoferowane oprogramowanie musi umożliwiać szyfrowanie przestrzeni dyskowej przydzielonej do serwerów wirtualnych. Szyfrowanie nie może być realizowane poprzez dyski samo szyfrujące (ang. Self Encrypting Drives).
  33. Zaoferowane oprogramowanie musi posiadać możliwość uruchomienia usługi NFS w wersji 1oraz 4. Ta usługa musi być zintegrowana z warstwą wirtualizacji oraz uruchamiania i zarządzana wyłącznie z poziomu centralnej konsoli zarządzającej klastrem wirtualizacyjnym bez potrzeby manualnej instalacji dodatkowych komponentów zewnętrznych
  34. Zaoferowane oprogramowanie musi zapewniać możliwość tworzenia i konfigurowania polityk niezawodnościowych, wydajnościowych i mechanizmy optymalizacji wykorzystania przestrzeni dyskowych (ang. ereasure coding) dla RAID 5 I RAID 6 konfigurowane granularnie per zasób NFS/NFS share.
  35. Funkcjonalność usługi NFS w zaoferowanym oprogramowaniu musi współpracować z Kubernetes CSI driver (Container Storage Interface) w ten sposób, że zasoby NFS kreowane są i usuwane automatyczne z poziomu kontenerów
  36. Zaoferowana licencja na oprogramowanie spełniające powyższe wymagania musi posiadać możliwość swobodnego przeniesienia na dowolny serwer fizyczny będący w posiadaniu Zamawiającego (bez ograniczeń licencji OEM). Licencje dostępne w modelu licencjonowania na procesor fizyczny.

**Moduł wirtualizacji funkcji sieciowych**

1. Zaoferowane oprogramowanie musi oferować możliwość budowy sieci komunikacyjnych (IP) w oparciu o środowiska wirtualne.
2. Zaoferowane oprogramowanie musi zapewniać funkcjonalność tworzenia wirtualnych sieci w sposób niezależny od topologii sieci fizycznej i używanych w obrębie tej sieci w protokołów sieciowych
3. Zaoferowane oprogramowanie realizujące usługi wirtualnych sieci musi być zarządzane przez narzędzie do zarządzania warstwą wirtualizacji serwerów. Wyklucza się używanie skryptów lub wtyczek (ang. plugin’ów) nie wspieranych przez dostawcę platformy wirtualizacji serwerów
4. Zaoferowane oprogramowanie musi posiadać funkcję tworzenia rozproszonego, wirtualnego przełącznika instalowanego bezpośrednio w jądrze wirtualizatora serwerów (Hypervisor), umożliwiającego tworzenie logicznych segmentów sieci w warstwie L2. Wirtualny przełącznik musi być wspierany bezpośrednio przez producenta platformy wirtualizacyjnej serwerów
5. Zaoferowane oprogramowanie musi posiadać funkcję tworzenia rozproszonego, wirtualnego routera instalowanego bezpośrednio w jądrze wirtualizatora serwerów (Hypervisor), zapewniającego funkcję bramy domyślnej dla środowiska serwerów wirtualnych. Brama domyślna musi działać w trybie rozproszonym. Przełączanie pakietów w warstwie sieci L3 musi odbywać się w obrębie fizycznego serwera, bez wynoszenia ruchu do fizycznych przełączników (tj. poza środowisko wirtualizacyjne)
6. Zaoferowane oprogramowanie musi posiadać możliwość kreowania segmentów sieci wirtualnej przy użyciu technologii GENEVE (Generic Network Virtualization Encapsulation)
7. Zaoferowane oprogramowanie musi zapewnić funkcjonalność łączenia (ang. bridging) środowiska zwirtualizowanego opartego o technologię GENEVE oraz niezwirtualizowanego zdefiniowanego za pomocą technologii VLAN-ów
8. Zaoferowane oprogramowanie musi zapewniać funkcjonalność wirtualnego routera wspierającego protokół BGP. Routing statyczny oraz BGP musi być możliwy do wykonania poprzez tunel GRE
9. Zaoferowane oprogramowanie musi zapewniać funkcjonalność łączenia segmentów sieci w warstwie L2 VLAN i GENVE poprzez zastosowanie wirtualnej bramy (ang. bridge)
10. Zaoferowane oprogramowanie musi zapewniać funkcjonalność translowania adresów IP zarówno dla ruchu wychodzącego ze środowiska wirtualnego (SNAT) jak i przychodzącego do środowiska wirtualnego (DNAT)
11. Zaoferowane oprogramowanie musi posiadać funkcjonalność serwera DHCP w celu dynamicznego nadawania adresów IP dla środowiska obiektów w środowisku zwirtualizowanym
12. Zaoferowane oprogramowanie musi posiadać jednocześnie zarówno funkcjonalność bezpieczeństwa (m. in. firewall) oraz funkcjonalność sieci komputerowej (m.in. switching) przy czym wymienione powyżej muszą być zarządzane oraz instalowane w ramach jednego interfejsu graficznego (pojedynczej konsoli)
13. Zaoferowane oprogramowanie musi posiadać funkcjonalność API umożliwiającą automatyzowanie wdrażania lub modyfikację konfiguracji
14. Aktualizacje zaoferowanego oprogramowania powinny odbywać się poprzez portal służący do ich planowania i uruchamiania, dostarczany przez tego samego producenta oprogramowania. Portal musi umożliwiać przegląd wszystkich elementów systemu pod kątem ich aktualnej oraz przygotowanej do aktualizacji wersji. Portal musi oferować wskaźniki postępu aktualizacji, umożliwiać tworzenie planów aktualizacji oraz zapewniać mechanizmy sprawdzenia konsystencji działania systemu przed oraz po aktualizacji
15. Oprogramowanie musi zapewniać wsparcie dla wykorzystania plików danych JSON oraz XML
16. Licencjonowanie zaoferowanego oprogramowania lub zapewnienie udzielenia licencji na zaoferowane oprogramowanie spełniające wymagania Standardowe musi posiadać możliwość swobodnego przeniesienia praw do użytkowania na dowolny podmiot wymieniony w umowie ramowej i dowolny serwer fizyczny będący w posiadaniu Zamawiającego (bez ograniczeń licencji OEM). Licencje dostępne w modelu licencjonowania na procesor fizyczny
17. Zaoferowane oprogramowanie musi zapewnić bezpieczeństwo transmisji danych (filtracja pakietów) na poziomie wirtulanego interfejsu sieciowego (vNIC) w hipervisorze wirtualizacyjnym, dla całości transmisji danych (włączając w to transmisję pomiędzy wirtualnymi maszynami w tym samym wirtualnym segmencie sieci) bez wynoszenia ruchu do fizycznych przełączników lub firewalli na zewnątrz hypervisora
18. Zaoferowane oprogramowanie musi posiadać funkcję rozproszonego, stanowego firewall'a instalowanego bezpośrednio w jądrze wirtualizatora (Hypervisor) serwerów umożliwiającego tworzenie polityk bezpieczeństwa w warstwach 2, 3 i 4 modelu sieciowego OSI. Nie dopuszcza się stosowania filtracji ruchu sieciowego typu "reflexive".
19. Zaoferowane oprogramowanie musi zapewniać możliwość tworzenia reguł firewall’a w trybie bezstanowym (ang. stateless) dla różnych grup wirtualnych serwerów
20. Zaoferowane oprogramowanie musi zapewniać możliwość tworzenia granularnych polityk bezpieczeństwa na poziomie wirtualnego portu maszyny wirtualnej, włączając ruch pomiędzy wirtualnymi maszynami w ramach tego samego segmentu sieci i na tym samym fizycznym serwerze (hoście)
21. Zaoferowane oprogramowanie musi zapewniać możliwość tworzenia granularnych polityk bezpieczeństwa dostępnych do wykorzystania w celu ochrony maszyn wirtualnych oraz serwerów fizycznych (ang. Bare metal) działających pod kontrolą systemu operacyjnego Linux (Red Hat Enterprise Linux, min. 7.6 ) oraz Microsoft Windows 2016
22. Zaoferowane oprogramowanie, do tworzenia reguł polityk bezpieczeństwa, musi umożliwiać wykorzystanie, oprócz parametrów takich jak adres IP, porty i protokoły, dodatkowych obiektów, m in.: nazwa maszyny wirtualnej, nazwa switcha wirtualnego, nazwa grupy maszyn wirtualnych, system operacyjny wirtualnej maszyny
23. Zaoferowane oprogramowanie musi zabezpieczać środowisko wirtualne przed nieautoryzowaną zmianą adresu IP wirtualnej maszyny, poprzez zablokowanie ruchu z i do tej wirtualnej maszyny po zmianie jej adresu IP w sposób nieautoryzowany
24. Zaoferowane oprogramowanie musi posiadać możliwość terminowania tuneli IPSeC site-to- site z uwierzytelnieniem za pomocą współdzielonego klucza (pre shared key) lub certyfikatu
25. Zaoferowane oprogramowanie musi umożliwiać natywną integrację z produktami firm trzecich oferującymi rozwiązania klasy antywirus/antymalware w postaci bezagentowej. Poprzez bezagentowość Zamawiający rozumie instalacje na poziomie wirtualizatora (hypervisora) serwerów, bez ingerencji w maszynę wirtualną
26. Zaoferowane oprogramowanie musi umożliwiać natywną integrację z minimum trzema produktami firm trzecich oferującymi rozwiązania typu Next Generation Firewall w warstwie 7 modelu ISO OSI, w celu dodatkowej filtracji i inspekcji ruchu
27. Zaoferowane oprogramowanie musi umożliwiać przekierowanie wybranego ruchu warstwy 2
28. modelu ISO OSI do rozwiązania firm trzecich z obszaru bezpieczeństwa
29. Zaoferowane oprogramowanie musi posiadać funkcję łączenia segmentów sieci w warstwie 2 ISO OSI (ang. bridge) dla VLAN i VXLAN poprzez zastosowanie fizycznego przełącznika firm trzecich
30. Zaoferowane oprogramowanie musi posiadać możliwość tworzenia reguł bezpieczeństwa uwzględniających nazwy użytkowników, poprzez integrację z Microsoft Active Directory z obsługą selektywnej synchronizacji
31. W ramach inspekcji warstwy 7 modelu ISO OSI funkcjonalność równoważenia ruchu (ang.
32. Load Balancer) musi oferować funkcję blokowania i modyfikacji URL
33. Rozwiązanie równoważenia ruchu (ang. Load Balancer) w zaoferowanym oprogramowaniu musi posiadać możliwość wstrzykiwania w nagłówek znacznika XFF (X-Fowarder- For)
34. Funkcja wirtualnego równoważenia ruchu (ang. Load Balancing) musi być zarządzana oraz instalowana w ramach jednego interfejsu graficznego (pojedynczej konsoli) w ramach zaoferowanego oprogramowania
35. Zaoferowane oprogramowanie musi posiadać funkcjonalność typu Identity Firewall umożliwiające obsługę sesji użytkowników na pulpitach wirtualnych (VDI) oraz serwerach aplikacji (RDSH) współdzielących pojedynczy adres IP
36. Zaoferowane oprogramowanie musi posiadać funkcjonalność identyfikacji aplikacji, np. MySQL, http, DNS, DHCP, Active Directory, TLS, itp. na poziomie sieciowym modelu ISO OSI w warstwach 5, 6 i 7, a następnie móc wykorzystać wynik identyfikacji w rozproszonym, wewnętrznym firewall w celu kontroli dostępu nie tylko na poziomie adresów IP oraz portów, ale również w połączeniu adresów IP, portów oraz zidentyfikowanej aplikacji
37. Zaoferowane oprogramowanie musi umożliwiać włączenie funkcjonalności rozproszonego Systemu Wykrywania Włamań (and. Intrusion Detection System) za pomocą licencji instalowanego na serwerach dedykowanych wirtualizacji (Hypervisor) umożliwiającego realizację wykrywania włamań za pomocą dedykowanych sygnatur ataków
38. Zaoferowane oprogramowanie musi mieć możliwość analizowania przepływów sieciowych (w tym IPFIX) w warstwie sieciowej wirtualizacji.
39. Zaoferowane oprogramowanie musi mieć możliwość tworzenia raportów przepływów z informacją uwzględniającą adresy IP oraz porty TCP/UDP dla środowiska wirtualnego. Poprzez raporty przepływów Zamawiający rozumie informację o ruchu sieciowym z konkretnej maszyny wirtualnej do innej konkretnej maszyny wirtualnej
40. Zaoferowane oprogramowanie musi mieć możliwość posiadania wbudowanego kolektora zebranego ruchu sieciowego możliwego do użycia w celu analizy ruchu
41. Zaoferowane oprogramowanie musi mieć możliwość generowania rekomendacji dla reguł serwerów klasy ściana ogniowa na bazie zebranych wcześniej informacji o przepływach
42. Zaoferowane oprogramowanie musi mieć możliwość przeanalizowania ruchu powiązanego z wybraną grupą maszyn wirtualnych w zadanym okresie i na tej podstawie zarekomendowania reguł bezpieczeństwa.
43. Zaoferowane oprogramowanie musi dawać możliwość przeprowadzenia symulacji jak będzie wyglądała komunikacja w ramach danej aplikacji po zastosowaniu rekomendowanych reguł bezpieczeństwa.
44. Zaoferowane oprogramowanie musi umożliwiać implementację zarekomendowanych reguł bezpieczeństwa na poziomie rozproszonego, stanowego firewalla bezpośrednio w jądrze wirtualizatora, po uprzednim zatwierdzeniu ich przez administratora systemu.
45. Zaoferowane oprogramowanie musi mieć możliwość wizualizacji (przedstawienia w postaci graficznej) ścieżki logicznej i przejść w relacji maszyna wirtualna do maszyny wirtualnej, wskazania komponentów sieciowych w topologii logicznej i fizycznej uwzględniając przełączniki, routery, firewall’e oraz połączenia między nimi z uwzględnieniem komponentów wirtualnych (minimum host i maszyna wirtualna)
46. Zaoferowane oprogramowanie musi mieć możliwość wizualizacji w formie graficznej przepływów pomiędzy minimum sieciami wirtualnymi, podsieciami, aplikacjami oraz grupami bezpieczeństwa
47. Zaoferowane oprogramowanie musi mieć możliwość informowania o maskowanych regułach firewalla, czyli regułach, które nie są wykorzystywane ze względu na reguły, które w ciągu analizy ruchu znajdują się w kolejce analizy je poprzedzają
48. Zaoferowane oprogramowanie musi mieć możliwość automatycznego wykrycia aplikacji działających w sieci klienta oraz wizualizacji zależności zarówno, pomiędzy maszynami wirtualnymi należącymi do tej aplikacji jak i ruchem zewnętrznym, wychodzącym i wchodzącym do maszyn wirtualnych odpowiedzialnych za tą aplikacje
49. Zaoferowane oprogramowanie musi mieć możliwość zarządzania polityką sieciową oraz polityką bezpieczeństwa dla wielu lokalizacji w sposób jednolity, utrzymując stan synchronizacji pomiędzy lokalizacjami.
50. Zaoferowane oprogramowanie musi posiadać funkcjonalność API umożliwiającą automatyzowanie wdrażania lub modyfikację konfiguracji
51. Zaoferowana licencja na oprogramowanie spełniające powyższe wymagania musi posiadać możliwość swobodnego przeniesienia na dowolny serwer fizyczny będący w posiadaniu Zamawiającego (bez ograniczeń licencji OEM). Licencje dostępne w modelu licencjonowania na procesor fizyczny.

**Moduł monitorowania funkcji sieci wirtualnej**

* 1. Zaoferowane oprogramowanie musi mieć możliwość analizowania przepływów sieciowych w warstwie sieciowej wirtualizacji.
  2. Zaoferowane oprogramowanie musi mieć możliwość tworzenia raportów przepływów z informacją uwzględniającą adresy IP oraz porty TCP/UDP dla środowiska wirtualnego. Poprzez raporty przepływów Zamawiający rozumie informację o ruchu sieciowym z konkretnej maszyny wirtualnej do innej konkretnej maszyny wirtualnej
  3. Zaoferowane oprogramowanie musi mieć możliwość posiadania wbudowanego kolektora zebranego ruchu sieciowego możliwego do użycia w celu analizy ruchu
  4. Zaoferowane oprogramowanie musi mieć możliwość generowania rekomendacji dla reguł serwerów klasy ściana ogniowa na bazie zebranych wcześniej informacji o przepływach
  5. Zaoferowane oprogramowanie musi mieć możliwość wizualizacji (przedstawienia w postaci graficznej) ścieżki logicznej i przejść w relacji maszyna wirtualna do maszyny wirtualnej, wskazania komponentów sieciowych w topologii logicznej i fizycznej uwzględniając przełączniki, routery, firewall’e połączenia między nimi z uwzględnieniem komponentów wirtualnych (minimum host i maszyna wirtualna)
  6. Zaoferowane oprogramowanie musi mieć możliwość wizualizacji w formie graficznej przepływów pomiędzy minimum sieciami wirtualnymi, podsieciami, aplikacjami oraz grupami bezpieczeństwa
  7. Zaoferowane oprogramowanie musi mieć możliwość informowania o maskowanych regułach firewalla, czyli regułach, które nie są wykorzystywane ze względu na reguły, które w ciągu analizy ruchu znajdują się w kolejce analizy je poprzedzają
  8. Zaoferowane oprogramowanie musi mieć możliwość automatycznego wykrycia aplikacji działających w sieci klienta oraz wizualizacji zależności zarówno, pomiędzy maszynami wirtualnymi należącymi do tej aplikacji jak i ruchem zewnętrznym, wychodzącym i wchodzącym do maszyn wirtualnych odpowiedzialnych za tą aplikacje
  9. Zaoferowane oprogramowanie musi posiadać funkcjonalność API umożliwiającą automatyzowanie wdrażania lub modyfikację konfiguracji
  10. Zaoferowana licencja na oprogramowanie spełniające powyższe wymagania musi posiadać możliwość swobodnego przeniesienia na dowolny serwer fizyczny będący w posiadaniu Zamawiającego (bez ograniczeń licencji OEM). Licencje dostępne w modelu licencjonowania na procesor fizyczny.

**Moduł monitorowania i zarządzania pojemnością i efektywnością platformy**

* + 1. Zaoferowane oprogramowanie musi posiadać mechanizm, który ogranicza dostęp do indywidualnego zarządzania warstwą wirtualizacji na serwerach fizycznych w ramach klastra serwerów w celu utwardzenia/hardening (maksymalnego zwiększenia bezpieczeństwa dostępu) systemu wirtualizacji.
    2. Zaoferowane oprogramowanie musi uzyskiwać informacje na temat wydajności środowiska wirtualnego pod kątem zarządzania pojemnością
    3. Zaoferowane oprogramowanie musi za pomocą wbudowanych inteligentnych algorytmów przewidywać trendy związane z pojemnością środowiska wirtualnego.
    4. Zaoferowane oprogramowanie musi posiadać funkcjonalność dającą możliwość analizy środowiska wirtualnego pod kątem optymalizacji wykorzystania zasobów (CPU, RAM, zasoby dyskowe)
    5. Zaoferowane oprogramowanie musi mieć możliwość tworzenia unikalnego zbioru obiektów korespondujących funkcjami z obiektami Datacenter, tzn. musi być możliwe grupowanie obiektów w logiczne zbiory, dla których będzie istniała możliwość informowania o alertach, pojemności, ryzykach zgromadzonych w zbiorze obiektów. Obiekty mogą pochodzić z różnych Data Center objętych tym rozwiązaniem.
    6. Zaoferowane oprogramowanie musi mieć możliwość tworzenia unikalnego/dedykowanego profilu pojemności, tzn. będzie możliwe grupowanie obiektów z Data Center w logiczne zbiory, dla których będzie istniała możliwość informowania o alertach, pojemności, ryzykach zgromadzonych w zbiorze obiektów.
    7. Zaoferowane oprogramowanie musi mieć funkcjonalność tworzenia scenariuszy predykcyjnego obliczania pojemności na zasadzie: "co jeśli" dla minimum: co jeśli dodamy kolejne maszyn wirtualne. Rozwiązanie będzie umożliwiało definiowanie poziomów buforów potrzebnych do zachowania wysokiej dostępności. Analiza pojemności musi odnosić się zarówno do średniego obciążenia środowiska, jak również do tzw. skoków obciążenia
    8. Zaoferowane oprogramowanie, w obrębie monitorowania, będzie posiadało rozwiązanie generowania alertów na podstawie korelacji wykrytych w środowisku wirtualnym anomalii i symptomów, a nie pojedynczych monitorowanych metryk
    9. Zaoferowane oprogramowanie musi posiadać funkcjonalność dostarczania informacji na temat rekomendowanych przez producenta posiadanego środowiska działań, mających na celu prawidłowe działanie środowiska
    10. Zaoferowane oprogramowanie musi posiadać wbudowane komponenty integracyjne obsługujące zewnętrzne kolektory logów i zdarzeń
    11. Zaoferowane oprogramowanie musi posiadać bazę wiedzy eksperckiej, która będzie używana przez administratorów, jako źródło dobrych praktyk, sugestii, opisu typowych problemów i błędów związanych ze środowiskiem zwirtualizowanym
    12. Zaoferowane oprogramowanie musi wizualizować w trybie online obciążenie środowiska wirtualnego wraz z tzw. funkcjonalnością „drill down” do minimum 2 poziomów zagnieżdzenia
    13. Zaoferowane oprogramowanie musi posiadać funkcjonalność graficznej prezentacji wyników (ang. dashboard)
    14. Zaoferowane oprogramowanie musi posiadać funkcjonalność aktywnych map graficznych ukazujących elementy lub całe środowisko wirtualne bez konieczności korzystania z usługi wsparcia technicznego producenta do ich dodatkowego wytwarzania podczas używania oprogramowania
    15. Zaoferowane oprogramowanie powinno dokonywać automatycznej predykcji wykorzystania zasobów maszyn fizycznych na podstawie analiz zebranych danych, informacji pochodzących z modułu zarządzania cyklem życia maszyn wirtualnych (wbudowanego w zaoferowane oprogramowanie) oraz planów uruchomienia kolejnych serwerów wirtualnych
    16. Zaoferowane oprogramowanie musi umożliwiać przeglądanie linii trendu monitorowanych parametrów
    17. Zaoferowane oprogramowanie musi umożliwiać tworzenie raportów pojemnościowych dla monitorowanego środowiska, zarówno dla urządzeń wirtualnych jak i fizycznych, związanych z wirtualiztorem oraz fizycznymi zasobami dyskowymi poza środowiskiem wirtualnym
    18. Zaoferowane oprogramowanie musi umożliwiać monitorowanie środowisk w czasie rzeczywistym (przeglądane informacje powinny ukazywać się w trybie rzeczywistym – dopuszczane jest maksymalne opóźnienie nie większe niż 5 minut)
    19. Zaoferowane oprogramowanie musi pozyskiwać oraz prezentować, w formie wykresów oraz tabelaryczno-tekstowej, zbiorczo oraz osobno, dla każdego systemu operacyjnego, aktualne i historyczne dane dotyczące utylizacji CPU, RAM, zasobów dyskowych oraz interfejsów sieciowych
    20. Zaoferowane oprogramowanie musi umożliwiać przeglądanie wszystkich zbieranych statystyk w dowolnie wybranym zakresie czasu w postaci wykresów
    21. Zaoferowane oprogramowanie musi umożliwiać szczegółowe monitorowanie komponentów serwerów fizycznych (CPU, Ethernet, RAM, zasoby dyskowe)
    22. Zaoferowane oprogramowanie musi umożliwiać definiowanie progów wydajności i pojemności w celu identyfikacji przypadków wąskich gardeł
    23. Zaoferowane oprogramowanie musi posiadać funkcjonalność zmiany parametrów maszyn wirtualnych, minimum CPU i RAM, za pomocą wygenerowanego w tym oprogramowaniu zadania. Dodatkowo, wymagana jest funkcjonalność odkładania w czasie w/w zadania, po wygenerowaniu (zadanie może być uruchamiane w momencie utworzenia lub w dowolnie skonfigurowanym przez użytkownika czasie)
    24. Zaoferowane oprogramowanie musi posiadać możliwość kasowania, wykonywania kopii migawkowych (ang. snapshot), włączania oraz wyłączania maszyn wirtualnych posadowionych na monitorowanym środowisku wirtualnym
    25. Zaoferowane oprogramowanie musi automatycznie przeszukiwać i analizować zebrane dane w celu wynajdywania nadmiarowości oraz niedoborów przyznanych zasobów (CPU, RAM, HDD) w monitorowanym środowisku
    26. Zaoferowane oprogramowanie musi posiadać funkcjonalność automatycznego alarmowania w sytuacji nietypowych (system monitoringu obserwuje i analizuje zachowanie platformy wirtualnej, na tej podstawie podnosi alarmy o minimum nie normalnym w tym dniu zwiększonym obciążeniu elementu platformy wirtualnej)
    27. Zaoferowane oprogramowanie musi posiadać możliwość dowolnego przypisywania powiadamiania o alertach w środowisku dla różnych grup odbiorców (także z użyciem alertów stworzonych we własnym zakresie przez użytkownika)
    28. Zaoferowane oprogramowanie musi pozwalać na odczyt wyświetlanych alarmów dotyczących monitorowanego środowiska wirtualnego wraz z powiązanymi z nimi poradami eksperckim
    29. Zaoferowane oprogramowanie musi umożliwiać definiowanie alertów związanych z: zarządzaniem pojemnością, zarządzaniem wydajnością, anomaliami w środowisku, zarządzaniu dostępnością dla monitorowanego środowiska
    30. Zaoferowane oprogramowanie musi mieć posiadać funkcjonalność przypisania alertu do administratora/operatora rozwiązującego problem
    31. Zaoferowane oprogramowanie musi mieć możliwość realizacji funkcji półautomatycznego równoważenia obciążenia serwerów fizycznych w obrębie klastra, jak również pomiędzy logicznymi klastrami
    32. Zaoferowane oprogramowanie musi mieć możliwość generowania gotowych, predefiniowanych raportów o stanie środowiska monitorowanego
    33. Licencjonowanie zaoferowanego oprogramowania lub zapewnienie udzielenia licencji na zaoferowane oprogramowanie spełniające wymagania Standardowe musi posiadać możliwość swobodnego przeniesienia praw do użytkowania na dowolny podmiot wymieniony w umowie ramowej i dowolny serwer fizyczny będący w posiadaniu Zamawiającego (bez ograniczeń licencji OEM). Licencje dostępne w modelu licencjonowania na procesor fizyczny
    34. Zaoferowane oprogramowanie musi posiadać funkcjonalność gotowego pulpitu kierowniczego (ang. dashboard) za pomocą którego administrator będzie posiadał gotowe trzy kolumny z następującymi informacjami:
    - Zdarzenia jakie wystąpiły w zadanym okresie dla analizowanego problemu, min. dla: wirtualnych maszyn, sieci wirtualnej, wirtualnej przestrzeni dyskowej
    - Anomalie, jakie wystąpiły w zadanym okresie dla analizowanego problemu
    - Zmiany w konfiguracji monitorowanej infrastruktury jakie wystąpiły w zadanym okresie czasu dla analizowanego problemu

Analiza danych ukazująca powyższe wyniki prezentowane w dashboard musi odbywać się automatycznie poprzez mechanizmy uczenia się maszynowego zaoferowanego oprogramowania do monitorowania na podstawie zakresu czasowego definiowanego przez użytkownika tego Dashborad. Dodatkowo użytkownik musi mieć możliwość definiowania, dla którego obiektu, np. wybranej maszyny wirtualnej należy przeprowadzić analizę, a następnie wyświetlić jej wyniki.

* 1. Zaoferowane oprogramowanie musi posiadać możliwość zastosowania dodatkowych adapterów umożliwiających integrację z systemami firm trzecich monitorującymi infrastrukturę
  2. Zaoferowane oprogramowanie musi posiadać możliwość zastosowania dodatkowych paczek monitorujących dla rozwiązań firm trzecich
  3. Zaoferowane oprogramowanie musi umożliwiać konfiguracje trybu wysokiej dostępności (ang. HA) dla każdego swojego komponentu w celu unikania awarii pojedynczego elementu
  4. Zaoferowane oprogramowanie musi posiadać możliwość zastosowania dodatkowych adapterów odpowiadających za monitorowanie systemów zewnętrznych takich jak m.in: macierze dyskowe, chmury obliczeniowe, serwery fizyczne, przełączniki LAN/SAN, umożliwiając tym samym wykorzystanie dedykowanych dodatkowych mechanizmów monitorujących określone komponenty
  5. Zaoferowane oprogramowanie musi umożliwiać elastyczne dostosowanie wyglądu interfejsu użytkownika w zależności od indywidualnych potrzeb
  6. Zaoferowane oprogramowanie musi posiadać funkcję tzw. konfiguratora własnych widoków zgromadzonych danych, który musi umożliwiać tworzenie zaawansowanych widoków dotyczących wszystkich monitorowanych metryk
  7. Zaoferowane oprogramowanie musi posiadać funkcję tzw. konfiguratora własnych pulpitów kierowniczych (ang. dashboard) na podstawie zgromadzonych danych w rozwiązaniu. Za pomocą tej funkcjonalności rozwiązanie musi umożliwiać tworzenie zaawansowanych pulpitów kierowniczych (dashborad)
  8. Zaoferowane oprogramowanie musi posiadać funkcjonalność monitorowania systemów operacyjnych (m.in. Windows, Linux) za pomocą zainstalowanego agenta w monitorowanym systemie operacyjnym
  9. Zaoferowane oprogramowanie musi posiadać funkcjonalność integracji z rozwiązaniem VMware vRealize Automation
  10. Zaoferowane oprogramowanie musi posiadać gotowe paczki do monitorowania (ang. management packs) dla produktów VMware vRealize Orchestrator, VMware SDDC, VMware NSX, VMware vRealize Automation
  11. Zaoferowane oprogramowanie musi mieć funkcjonalność tworzenia scenariuszy pojemnościowych na zasadzie: "co jeśli" dla minimum: CPU, RAM, oraz przestrzeni dyskowej dla następujących elementów:
* Dodawania nowych serwerów fizycznych
* Dodawania dodatkowych elementów rozproszonych przestrzeni dyskowych SDS
  1. Zaoferowane oprogramowanie musi posiadać możliwość matematycznego wyliczania wartości super metryki na podstawie innych, gromadzonych i monitorowanych metryk podstawowych. Super metryka to formuła matematyczna, która zawiera jedną lub więcej metryk. Jest to niestandardowa metryka, którą można zaprojektować w rozwiązaniu, aby pomóc śledzić kombinacje metryk, z jednego obiektu lub z wielu obiektów
  2. Zaoferowane oprogramowanie musi wykrywać usługi uruchomione na monitorowanych maszynach wirtualnych, a następnie budować relacje lub zależności między usługami z różnych maszyn wirtualnych na podstawie komunikacja sieciowej
  3. Zaoferowane oprogramowanie musi posiadać możliwość, po uruchomieniu alarmu, wykonywać na podstawie tego alarmu, automatyczne działania dotyczących akcji naprawczych
  4. Zaoferowane oprogramowanie musi posiadać funkcjonalność monitorowania urządzeń firm trzecich typu macierze dyskowe, urządzenia sieciowe, a także wirtualizatorów za pomocą specjalnie przygotowanych paczek do monitorowania
  5. Licencjonowanie zaoferowanego oprogramowania lub zapewnienie udzielenia licencji na zaoferowane oprogramowanie spełniające wymagania Zaawansowane musi posiadać możliwość swobodnego przeniesienia praw do użytkowania na dowolny podmiot wymieniony w umowie ramowej i dowolny serwer fizyczny będący w posiadaniu Zamawiającego (bez ograniczeń licencji OEM). Licencje dostępne w modelu licencjonowania na procesor fizyczny
  6. Zaoferowane oprogramowanie musi posiadać funkcjonalność monitorowania aplikacji, serwerów aplikacyjnych oraz baz danych firm trzecich, m.in. baz danych Oracle DB, Microsoft SQL, MySQL, za pomocą specjalnie przygotowanych paczek (ang. management packs) firm trzecich
  7. Zaoferowane oprogramowanie musi mieć możliwość monitorowania zmian na poziomie systemów operacyjnych w tym konfiguracji tych systemów oraz procesu zarządzania aktualizacjami (ang. patch management)
  8. Zaoferowane oprogramowanie musi mieć gotowe paczki (ang. management packs) do monitorowania platform typu Multi-Cloud, tj. AWS (Amazon Web Services) , Microsoft Azure, OpenStack i rozwiązań kontenerowych, tj. Kubernetes
  9. Zaoferowane oprogramowanie musi mieć gotową funkcjonalność (tzw. Out-of-the-Box) do wykrywania, monitorowania i rozwiązywania problemów dla aplikacji firm trzecich tj.: Tomcat, MySQL, NGINX, RabbitMQ, Apache http, Postgresql, MongoDB, Elastic Search, ActiveMQ
  10. Rozwiązanie musi posiadać portal typu „Self-Service” do automatycznego tworzenia i uruchamiania wirtualnych systemów operacyjnych, platform aplikacyjnych i całych zestawów/systemów maszyn wirtualnych
  11. Interfejs graficzny tzw. UI musi być dostępny poprzez przeglądarkę internetową i wspierać technologię opartą o HTML5
  12. Musi też posiadać możliwość katalogowania widoku poszczególnych typów usług według własnego wzorcaRozwiązanie musi posiadać możliwość modyfikacji właściwości obiektów w katalogu (w tym w szczególności konfiguracji wirtualnego sprzętu: CPU, RAM, STORAGE,NETWORK), zarówno przed provisioningiem usługi jak i po provisioningu
  13. Rozwiązanie musi oferować w ramach katalogu usług informacje o kosztach danej usługi - modyfikowana na bieżąco w zależności od konfiguracji wirtualnego sprzętu (np. ilość instancji, ilość pamięci RAM, ilość CPU)
  14. Rozwiązanie musi prezentować informacje w postaci wykresów o kluczowych metrykach maszyny wirtualnej, wytworzonej w ramach procesu takich jak CPU, pamięć, IOPS, sieć
  15. Rozwiązanie musi umożliwiać modyfikację wirtualnego sprzętu po "provisioningu" danego obiektu z katalogu
  16. Rozwiązanie musi posiadać zestaw wbudowanych procesów/czynności automatyzacji dostarczania usług wraz z możliwością ich edycji, zmiany konfiguracji i tworzenia nowych „kroków” w procesie cyklu życia konkretnej usługi
  17. Rozwiązanie musi informować o statusie usługi w czasie rzeczywistym np. (usługa zaakceptowana, zakolejkowana, odrzucona, w trakcie akceptacji itp.) dodatkowo rozwiązanie musi mieć możliwość wysłania informacji poprzez pocztę elektroniczną o zmianie statusu usługi
  18. Rozwiązanie musi posiadać możliwość definiowania sieci wirtualnych, które łączą maszyny wirtualne w ramach zarządzanej platformy (w każdym z Data Center będącym elementem projektu) – rozwiązanie musi wspierać natywnie nie mniej niż dwa rozwiązania typu SDN
  19. Administrator rozwiązania musi posiadać możliwość definiowania sieci wewnętrznych jak i sieci zewnętrznych połączonych do sieci fizycznej - pozwalającej na komunikację np. do Internetu za pomocą np. NAT – rozwiązanie musi wspierać natywnie nie mniej niż dwa rozwiązania typu SDN
  20. Administrator rozwiązania musi posiadać możliwość definiowania fizycznych zasobów (mocy obliczeniowej) oraz zmiany ich wielkości poprzez powiększenie lub pomniejszenie obiektu) bez wpływu na działanie usług - tj. Obiekt musi być dostępny podczas dokonywanych operacji
  21. Rozwiązanie musi posiadać możliwość definiowania logicznych obiektów zawierających wiele wirtualnych elementów w tym wiele maszyn wirtualnych powiązanych ze sobą zależnościami, tak aby w rezultacie administrator systemu mógł stworzyć wielowarstwowy serwis (np. aplikacja CRM (Load Balansowany Web Front-End, Middelware oraz sklastrowany Back End- Baza Danych)
  22. Administrator rozwiązania musi posiadać możliwość wyboru, które obiekty z katalogu mogą ulegać modyfikacji przez użytkownika końcowego. Wymaga się aby lista obiektów była nie mniejsza niż: liczba wirtualnych procesorów, wielkość pamięci operacyjnej, ilość i wielkość dysków oraz typ wolumenu, ilość kart sieciowych i typy sieci, czas dzierżawy, polityka archiwizacji, hasło administracyjne systemu operacyjnego) przy czym zmiana parametrów przez użytkownika może wymagać dodatkowych akceptacji przy procesie uruchomienia serwisu
  23. Posiadanie wsparcia dla platform: KVM, Hyper-V (SCVMM), XenServer, VMwar
  24. Rozwiązanie niezależne od producenta sprzętu, możliwy provisioning na bare-metal ze wsparciem dla min. takich producentów jak: Dell, HP, Cisco
  25. Rozwiązanie musi realizować model: "Projektuj usługę raz, wdrażaj gdziekolwiek"
  26. Rozwiązanie musi umożliwiać rezerwację zasobów fizycznych dla wybranych grup użytkowników oraz pełną kontrolę tych zasobów w obrębie wskazanej grupy użytkowników
  27. Rozwiązanie musi mieć możliwość tworzenia wielu logicznych, izolowanych od siebie grup maszyn wirtualnych, określania dla nich zasobów fizycznych, grup użytkowników, wzorców usług a także procesów tworzenia, zarzadzania cyklem życia usług
  28. Automatyczne wdrażanie wszelakich usług IT w jak najkrótszym czasie: Infrastructure as a Service - wdrażanie instancji OS w maszynie wirtualnej lub fizycznej (szablon)

Rozwiązanie musi się integrować z innymi systemami zewnętrznymi typu: CMDB, DNS, IPAM, Load Balancer, Servcie Desk, Monitoring, Web Services, BMC Blade Logic, HP Server Automation, Puppet, Chef, SaltStack, MS SCCM i wiele innych gotowych jako plug-iny lub napisanych od początku w języku programowania. Efektem powyższej integracji musi być w pełni automatyczny proces tworzenia i zarządzania usługą niewymagający czynności ręcznych

* 1. Rozwiązanie musi umożliwiać tworzenie nowych usług wraz z określeniem ilości i rodzaju zasobów dostępnych dla danej usługi zarówno na etapie tworzenia jak i późniejszej rekonfiguracji danej usługi
  2. Rozwiązanie musi posiadać jedno narzędzie do projektowania usługi opartej na OS, aplikacjach, usług sieciowych tj.: Load Balancing, Routing, Switching oraz tworzenia reguł bezpieczeństwa w locie podczas provisioningu - w sieciowym aspekcie rozwiązanie musi mieć wsparcie dla microsegmentacji tj. filtrowania ruchu pomiędzy dowolnymi maszynami wirtualnymi również w obrębie tej samej sieci - rozwiązanie musi wspierać natywnie nie mniej niż dwa rozwiązania typu SDN
  3. Rozwiązanie musi umożliwiać z zbudowanie zunifikowanego Katalogu Usług dla aplikacji, infrastruktury i danych,
  4. Rozwiązanie musi posiadać interfejs typu „drag-drop” przeznaczony do tworzenia dowolnej aplikacji na podstawie utworzonych wcześniej komponentów, aplikacji, systemów, sieci i polityk bezpieczeństwa oraz innych skryptów pomocnych w automatyzacji
  5. Rozwiązanie musi umożliwiać graficzną edycję przebiegu procesu realizacji usług, definiowanie poszczególnych kroków oraz ich danych wejściowych i wyjściowych. Przebiegi procesów mogą być sekwencyjne lub składać się z wielu sekwencji zadań realizowanych równocześnie, musi istnieć możliwość testowania zdefiniowanych procesów realizacji usług przy użyciu debugger-a, który pozwala analizować postęp procesu krok po kroku ze śledzeniem przekazywanych danych
  6. Rozwiązanie musi umożliwiać export/import zdefiniowanych procesów realizacji usług do/z pliku w celu przeniesienia definicji pomiędzy różnymi środowiskami
  7. Rozwiązanie musi umożliwiać integrację z Active Directory oraz Open LDAP, i wieloma ich domenami w tym samym czasie
  8. użytkownik REQUESTER musi mieć możliwość wykonywania wszystkich operacji na swojej usłudze z jednej konsoli tj. Self-Service portalu, bez konieczności posługiwania się innymi narzędziami administracyjnymi
  9. Rozwiązanie musi posiadać możliwość granularnego zarządzania uprawnieniami dla poszczególnych użytkowników w zależności od pełnionej roli, opartego na rolach: np.: Tenant Admin, Service Architect, Network Architect, Application Architect
  10. Rozwiązanie służące do automatyzacji musi standaryzować wdrażanie usług IT oraz eliminować w ten sposób błędy czynnika ludzkiego
  11. Rozwiązanie musi dostarczać mechanizmy monitorowania statusów zdarzeń, notyfikacji o tych zdarzeniach, umożliwiać śledzenie i kontrolę zmian w konfiguracji wszystkich usług, za pomocą min. portalu Self-Service i powiadomień e-mail
  12. Rozwiązanie musi mieć możliwość zgłaszania przez Administratora potrzeby odzyskania poszczególnych zasobów od użytkowników w przypadku ich niewłaściwego wykorzystywania
  13. Oferowane oprogramowanie musi udostępniać funkcjonalność zarządzania poprzez ustandaryzowany interfejs tj. API
  14. Zaoferowana licencja na oprogramowanie spełniające powyższe wymagania musi posiadać możliwość swobodnego przeniesienia na dowolny serwer fizyczny będący w posiadaniu Zamawiającego (bez ograniczeń licencji OEM). Licencje dostępne w modelu licencjonowania na procesor fizyczny.

**Moduł zbierania zbieranie logów z infrastruktury**

1. Zaoferowane oprogramowanie musi zapewniać możliwość centralnego gromadzenia i analizy wszystkich logów z urządzeń fizycznych wykorzystujących technologię „Syslog”
2. Zaoferowane oprogramowanie musi umożliwiać personalizację i wizualizację logów w postaci wykresów minimum: liniowych, kołowych oraz słupkowych
3. Zaoferowane oprogramowanie musi w pełni integrować się z platformą posiadana przez Zamawiającego. tj. VMware vSphere wraz z VMware vCenter.
4. Zaoferowane oprogramowanie musi zapewniać monitorowanie urządzeń typu „Real Time”
5. Zaoferowane oprogramowanie musi posiadać wbudowaną bazę wiedzy dotycząca logów oraz zdarzeń
6. Zaoferowane oprogramowanie musi posiadać możliwość udostępniania raportów za pomocą URL kierującego do systemu logowania wysyłanego do odbiorcy
7. Zaoferowane oprogramowanie musi umożliwiać łatwą korelację wybranych zdarzeń w infrastrukturze fizycznej/wirtualnej oraz ich graficzną prezentację
8. Zaoferowane oprogramowanie musi posiadać możliwość personalizacji interfejsu graficznego w zależności od użytkownika/operatora
9. Zaoferowane oprogramowanie musi umożliwiać łatwe i szybkie przeszukiwanie logów w oparciu o zdefiniowane przez użytkownika kryteria
10. Zaoferowane oprogramowanie musi posiadać funkcjonalność implementacji dedykowanych modułów do analizy logów innych urządzeń fizycznych np. macierzy dyskowych, przełączników LAN, itp., tak aby analiza i korelacja wszystkich wiadomości systemowych mogła odbywać się z jednej konsoli zarządzającej
11. Zaoferowane oprogramowanie musi posiadać mechanizmy efektywnej analizy wszystkich rodzajów logów, takich jak np. logi aplikacji, logi sieciowe, pliki konfiguracyjne, informacje, dane wydajnościowe, zrzuty awaryjne itp., a także logów ‘nieustrukturyzowanych”
12. Zaoferowane oprogramowanie musi umożliwiać definiowanie struktury dla logów nieustrukturyzowanych
13. W zaoferowanym oprogramowaniu uprawnienia do interfejsu prezentacji i analizy logów muszą dopuszczać rozłączność z uprawnieniami do infrastruktury, z której zbierane są logi
14. Zaoferowane oprogramowanie musi umożliwiać generowanie i eksportowanie dowolnych raportów związanych z zarejestrowanymi zdarzeniami i logami
15. Zaoferowane oprogramowanie musi zapewniać możliwość stworzenie klastra składającego się co najmniej 18 węzłów, z którego każdy ma wydajność 15 000 EPS (ang. Events Per Second), co sumarycznie daje 270 000 EPS
16. Zaoferowane oprogramowanie musi posiadać możliwość logowania zdarzeń z platformy Kubernetes i Tanzu
17. Zaoferowane oprogramowanie musi mieć możliwość określania czasu retencji danych, tzn. Administrator w konsoli graficznej do zarządzania platformą do zbierania i korelacji logów musi mieć możliwość określenia czasu po jaki zebrane logi będą archiwizowane (eksportowane) na zewnętrznej macierzy dyskowej po protokole NFS. Dodatkowo wymaga się aby retencja mogła być ustawiana granularnie, tj. np. inny czas retencji dla logów z urządzeń klasy firewall a inny czas retencji dla logów z hyperwizorów
18. Zaoferowana licencja na oprogramowanie spełniające powyższe wymagania musi posiadać możliwość swobodnego przeniesienia na dowolny serwer fizyczny będący w posiadaniu Zamawiającego (bez ograniczeń licencji OEM). Licencje dostępne w modelu licencjonowania na procesor fizyczny

**Usługi Gwarancyjne**

* + - * 1. Usługa gwarancyjna musi umożliwiać zgłaszanie problemów 7 dni w tygodniu bez ograniczeń czasowych (7/24).
        2. Usługa musi zapewnić:
* Nieograniczoną ilość zgłoszeń serwisowych.
* Dostęp do materiałów producenta takich jak: dokumentacja techniczna, internetowa baza wiedzy, forum internetowe producenta Oprogramowania.
* Gwarancję poufności w zarządzaniu przekazanymi informacjami (usługa świadczona bez możliwości i wymogu przesyłania logów oraz informacji o zgłoszeniach serwisowych poza system procesowania zgłoszeń zarządzany i administrowany przez producenta Oprogramowania).
* Dostęp do poprawek i uaktualnień Oprogramowania objętego usługą gwarancyjną,
* Dostęp do portalu www producenta Oprogramowania umożliwiającego zarządzanie posiadanymi licencjami, założenie zgłoszenia awarii u producenta, podniesienie lub obniżenie (jeśli producent oficjalnie wspiera poprzednie wersje) wersji Oprogramowania.
* Dostęp do rejestru licencji (dostępnego przez portal www producenta Oprogramowania).
* Dostęp do narzędzia Producenta pozwalającego na automatyczne zbieranie danych o statusie i działaniu produktów objętych usługą gwarancyjną.
  1. **Wymagania dotyczące systemu monitoringu Infrastruktury IT – 1 szt.**

System monitoringu Infrastruktury IT, zarządzania użytkownikami, zarządzania zasobami IT i helpdesku W ramach licencji producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne na okres minimum 60 miesięcy.

Oprogramowanie ma zawierać centralną konsolę do zarządzania instalowaną lokalnie. Oprogramowanie ma zawierać funkcje takie jak:

|  |  |
| --- | --- |
| **Nazwa wymagania** | **Opis wymagań** |
| Wykrywanie i wizualizacja sieci | * automatyczne wykrywanie komputerów znajdujących się w całej sieci (uwzględniając podsieci), * skanowanie i wykrywanie serwisów działających na wykrytych komputerach, * możliwość cyklicznego uruchamiania skanera sieci, * możliwość tworzenia dowolnej liczby sieci i map; przy dodawaniu każda sieć ma być skanowana przy użyciu definiowalnych parametrów, * możliwość prezentowania na mapach wszelkich krytycznych informacji o działaniu urządzeń (czas odpowiedzi podstawowego serwisu, czas, w którym serwisy i komputer nie działały, wystąpienia alarmów itp.), * możliwość tworzenia map o dowolnym układzie oraz zawierających tło w postaci bitmapy. |
| Monitorowanie sieci | * identyfikowanie i monitorowanie systemów operacyjnych (w tym systemów Windows, Linux) oraz urządzeń SNMP v1/2/3, * identyfikowanie i monitorowanie predefiniowanych serwisów TCP/IP z możliwością tworzenia własnych, * identyfikowanie i monitorowanie serwerów pocztowych, stron WWW i adresów URL, * identyfikowanie i monitorowanie routerów i switch’y; posiadanie funkcjonalności MRTG, * monitorowanie wydajności urządzeń SNMP (w tym transfer sieciowy), * identyfikowanie i monitorowanie switch’y zarządzalnych - informacja o podłączonych urządzeniach do każdego portu, stanie portów (włączony, wyłączony) i ruchu na każdym porcie, * identyfikowanie i monitorowanie serwisów i wydajności systemu Windows (poprzez pomiar CPU, pamięci, przestrzeni dyskowej), * możliwość automatycznego restartu serwisów, które przestały działać, lub działają niewłaściwie, * identyfikowanie i monitorowanie aplikacji takich jak MS SQL, Exchange, IIS, Oracle i innych poprzez monitorowanie liczników wydajności udostępnianych przez producenta aplikacji, * wykrywanie ruchu sieciowego wynikającego np. ze źle działających urządzeń, * blokowanie działania w sieci urządzeń np. pamięci flash, które wcześniej w firmie nie były zarejestrowane (ochrona antywirusowa), * generowanie alarmów, które przekazywane będą za pośrednictwem różnych kanałów (w tym e-mail, ICQ, SMS), * automatyczne wykonywanie akcji korekcyjnych (np. restart serwisu, komputera; uruchomienie programów; skryptów). |
| Inwentaryzacja sprzętu i oprogramowania | * gromadzenie informacji o sprzęcie występującym w sieci: min. model sprzętu, CPU, pamięci, płytę główną, dyski, karty, * gromadzenie informacji o oprogramowaniu występującym w sieci: min. nazwa, wersja, typ oprogramowania, * porównywanie użytkowanego oprogramowania z posiadanymi licencjami, zdefiniowanymi przez administratora, * zarządzanie posiadanymi licencjami (typami licencji), * tworzenie raportu zgodności licencji, |

* 1. **Wymagania dotyczące Serwera Kopii Zapasowej – 1 szt.**

Szczegółowe wymagania dotyczące Serwera kopii zapasowej oraz minimalne parametry techniczne zostały określone w tabeli poniżej i stanowią podstawę do wyceny przedmiotu zamówienia przez Oferentów:

|  |  |
| --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |
| Obudowa | Obudowa Rack o wysokości max. 2U, umożliwiającą instalację min. 12 dysków 3,5” z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. |
| Płyta główna | Płyta główna z możliwością zainstalowania dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. |
| Chipset | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych |
| Procesor | Zainstalowane dwa procesory min. dwunastordzeniowe klasy x86 do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 216 punktów w teście SPECrate2017\_int\_base dostępnym na stronie www.spec.org dla dwóch procesorów. Dla oferowanego serwera. |
| RAM | Min. 64GB DDR5 RDIMM 5600MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM. |
| Zabezpieczenia pamięci RAM | Demand Scrubbing, Patrol Scrubbing, Permanent Fault Detection (PFD) |
| Sloty PCIe | Trzy sloty PCIe x16 oraz jeden slot PCIe x8. |
| Interfejsy sieciowe/FC/SAS | Wbudowane dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT  Dwa interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 nie zajmujące slotów PCIe.  Dodatkowo zainstalowane:  - Jedna karta dwuportowa FC 32Gb/s |
| Dyski twarde | Zainstalowane 2 x 480GB SSD SATA oraz 10 x 20TB NearLine SAS.  Możliwość instalacji dwóch dysków hot-swap M.2 NVMe o pojemności min. 960GB z możliwością konfiguracji RAID 1. |
| Kontroler RAID | Sprzętowy kontroler dyskowy z pojemnością cache 8GB, możliwe konfiguracje poziomów RAID: 0,1,5,6,10,50,60, non-RAID (JBOD). |
| Wbudowane porty | min. port USB 2.0 oraz dwa porty USB 3.0, port VGA, |
| Video | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1600x900 |
| Wentylatory | Redundantne |
| Zasilacze | Min. dwa zasilacze Hot-Plug maksymalnie 1100W Titanium. |
| Bezpieczeństwo | Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.  Możliwość wyłączenia w BIOS funkcji przycisku zasilania.  BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła  Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą  Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera  Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem.  Możliwość integracji z RSA SecurID  Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania. |
| Karta Zarządzania | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca:   * zdalny dostęp do graficznego interfejsu Web karty zarządzającej * szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika * możliwość podmontowania zdalnych wirtualnych napędów * wirtualną konsolę z dostępem do myszy, klawiatury * wsparcie dla IPv6 * wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH * możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz. * możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer * integracja z Active Directory * możliwość obsługi przez ośmiu administratorów jednocześnie * Wsparcie dla automatycznej rejestracji DNS * wsparcie dla LLDP * wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej * możliwość podłączenia lokalnego poprzez złącze RS-232. * możliwość zarządzania bezpośredniego poprzez złącze microUSB umieszczone na froncie obudowy. * Monitorowanie zużycia dysków SSD * możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi, * Automatyczne zgłaszanie alertów do centrum serwisowego producenta * Automatyczne update firmware dla wszystkich komponentów serwera * Możliwość przywrócenia poprzednich wersji firmware * Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON * Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych * Automatyczne tworzenie kopii ustawień serwera w opraciu o harmonogram. * Możliwość wykrywania odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera * Serwer musi posiadać możliwość uruchomienia funkcjonalności umożliwiającej dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE lub WIFI.   Karta powinna umożliwiać rozszerzenie funkcjonalności o:   * możliwość wysyłania danych o stanie procesora, kart sieciowych, zasilaczy, kart GPU, lokalnych dysków i urządzeń NVMe, jak również dane wydajnościowe serwera do zewnętrznych * kontrola stanu BIOS pod kątem naruszenia integralności oprogramowania * Automatyczne odświeżanie certyfikatów SSL * możliwość wykorzystania tokenu lub aplikacji SecurID do uwierzytelniania wielkoskładnikowego przy logowaniu do karty zarządzającej * możliwość modyfikacji reguł chłodzenia kart w slotach PCIe, z możliwością własnych ustawień * możliwość ustawienia limitu temperatury powietrza wychodzącego z serwera * możliwość ustawienia dopuszczalnego wzrostu temperatury powietrza przepływającego przez serwer * możliwość ustawienia maksymalnej temperatury powietrza dochodzącego do slotów PCIe * monitorowanie przepływu powietrza na bieżąco |
| Oprogramowanie | Serwer musi być wyposażony w licencję Windows Serwer 2025 |
| Oprogramowanie do zarządzania | Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniające poniższe wymagania:   * Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych * integracja z Active Directory * Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta * Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish * Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram * Szczegółowy opis wykrytych systemów oraz ich komponentów * Możliwość eksportu raportu do CSV, HTML, XLS, PDF * Możliwość tworzenia własnych raportów w opraciu o wszystkie informacje zawarte w inwentarzu. * Grupowanie urządzeń w oparciu o kryteria użytkownika * Tworzenie automatycznie grup urządzeń w opraciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji * Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach * Szybki podgląd stanu środowiska * Podsumowanie stanu dla każdego urządzenia * Szczegółowy status urządzenia/elementu/komponentu * Generowanie alertów przy zmianie stanu urządzenia. * Filtry raportów umożliwiające podgląd najważniejszych zdarzeń * Integracja z service desk producenta dostarczonej platformy sprzętowej * Możliwość przejęcia zdalnego pulpitu * Możliwość podmontowania wirtualnego napędu * Kreator umożliwiający dostosowanie akcji dla wybranych alertów * Możliwość importu plików MIB * Przesyłanie alertów „as-is” do innych konsol firm trzecich * Możliwość definiowania ról administratorów * Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów * Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) * Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta * Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów * Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących aletrów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. * Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstwie weryfikacji środowiska w celu wykrycia rozbieżności. * Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w opraciu o profile * Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. * Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. * Zdalne uruchamianie diagnostyki serwera. * Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarzadzającym. * Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V. |
| Certyfikaty | Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001 lub równoważnymi.  Serwer musi posiadać deklaracja CE.  Urządzenia wyprodukowane są przez producenta, zgodnie z normą PN-EN ISO 50001 lub równoważną lub oświadczenie producenta o stosowaniu w fabrykach polityki zarządzania energią, która jest zgodna z obowiązującymi przepisami na terenie Unii Europejskiej.   Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows”. |
| Normy Środowiskowe | Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami rozporządzenia nr 1272/2008WE. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku *-****Wykonawca złoży dokument potwierdzający spełnianie*wymogu*.***  Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych **w postaci oświadczenia producenta serwera** |
| Warunki gwarancji | Zamawiający wymaga min. 60 miesięcy gwarancji producenta możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.  Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy.  Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania.  Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.  Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.  Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik ***producenta*** z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi sie na inną formę.  Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii. Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych  W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego – wymagane jest dołączenie do oferty oświadczenia podmiotu realizującego serwis lub producenta sprzętu o spełnieniu tego warunku  Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.  Oświadczenie producenta serwera, potwierdzające, że sprzęt pochodzi z oficjalnego kanału dystrybucyjnego producenta.  Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji systemu. |
| Dokumentacja użytkownika | Zamawiający wymaga dokumentacji w języku polskim lub angi*e*lskim.  Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |

* 1. **Wymagania dotyczące Oprogramowania do tworzenia kopii zapasowej – 1 szt.**

Szczegółowe wymagania dotyczące oprogramowania oraz minimalne parametry techniczne zostały określone w tabeli poniżej i stanowią podstawę do wyceny przedmiotu zamówienia przez Oferentów:

|  |  |
| --- | --- |
| **Specyfikacja zamówienia** | **Wymagania Zamawiającego** |
| Wymagania Ogólne | 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, |
| Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 6.x, 7.x i 8.0 oraz Microsoft Hyper-V 2012, 2012R2, 2016, 2019, 2022 i 2025. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej |
| Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux. |
| Całkowite koszty posiadania | Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej |
| Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków |
| Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji |
| Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu. |
| Oprogramowanie musi 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. |
| Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier. |
| Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie. |
| Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania |
| Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time) |
| Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu |
| Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API |
| Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji |
| Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji |
| Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania |
| Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych. |
| Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej |
| Wymagania RPO | Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej |
| Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych. |
| Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych z dokładnością do pojedynczego datastoru |
| 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. |
| Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware. |
| Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy. |
| Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son) |
| Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard. |
| Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019, 2022 lub 2025 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS. |
| Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN. |
| Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji. |
| Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO. |
| Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik |
| Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding) |
| Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN) |
| Wymagania RTO | Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage’u użytego do przechowywania kopii zapasowych. |
| Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna) |
| Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami |
| Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre |
| Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL i Oracle bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne. |
| Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków |
| Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform. |
| Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików |
| Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V. |
| Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell |
| Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces. |
| Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej. |
| Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA, elementów AD Sites oraz pozwalać na odtworzenie haseł. |
| Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2013SP1 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego. |
| Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur. |
| Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2013 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji. |
| Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux. |
| Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux. |
| Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN |
| Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle |
| Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI |
| Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN |
| Ograniczenie ryzyka | Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna) |
| Dla VMware’a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach. |
| Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem |
| Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32. |
| Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego. |
| Środowisko fizyczne | Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego |
| Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych |
| Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE |
| Rozwiązanie musi wspierać system operacyjny macOS |
| Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix |
| Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą) |
| Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster |
| Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów |
| Rozwiązanie musi wspierać backup podłączonych dysków USB |
| Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym |
| Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury) |
| Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone |
| Rozwiązanie musi wspierać kontrolę pasma sieciowego |
| Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych |
| Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN |
| Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft |
| Rozwiązanie musi wspierać technologię BitLocker |
| Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania |
| Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla Microsoft Exchange 2013SP1 i nowszych, Microsoft Active Directory 2008 i nowszych, Microsoft Sharepoint 2013 i nowszych, Microsoft SQL 2008 i nowszych, Oracle 11g i nowszych oraz PostgreSQL 12 i nowszych |
| Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych |
| Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL i Oracle poprzez bezpośrednie uruchomienie ich z pliku backupu. |
| Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere, Hyper-V, Nutanix AHV, Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform |
| Rozwiązanie musi wspierać szyfrowanie |
| Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne |
| Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego |
| Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej |
| Rozwiązanie musi wspierać tworzenie wielu zadań backupowych |
| Monitoring | System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich |
| System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie |
| System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019, 2022 oraz 2025 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie. |
| System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter |
| System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn |
| System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel |
| System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk |
| System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora |
| System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów |
| System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard) |
| System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna |
| System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego |
| System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta |
| System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych. |
| System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu. |
| System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy Vmware |
| System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji od 10.x do 10.4 |
| Raportowanie | System musi umożliwiać raportowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie |
| System musi umożliwiać raportowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019, 2022 oraz 2025 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie. |
| System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów. |
| System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V |
| System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF |
| System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc |
| System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach |
| System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów |
| System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych |
| System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych |
| System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury |
| System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta |
| System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych. |
| System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach ‘what-if’. |
| System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy Vmware |
| System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots) |
| System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie |
| Licencjonowanie i wsparcie techniczne | Oferowane oprogramowanie musi być dostarczone z licencją bezterminową lub z licencją abonamentową obejmującą cały okres użytkowania zgodny z umową, z zapewnieniem wszystkich funkcjonalności opisanych w niniejszej specyfikacji. |
| Licencja musi obejmować prawo do wykonywania nielimitowanej liczby kopii zapasowych, replikacji oraz odzyskiwania danych w ramach zakupionych funkcjonalności. |
| Oprogramowanie musi być objęte wsparciem technicznym producenta przez okres co najmniej 5 lat, liczonych od dnia podpisania protokołu odbioru rozwiązania. Wsparcie techniczne musi obejmować:   * prawo do aktualizacji i uaktualnień oprogramowania (w tym nowe wersje i łatki bezpieczeństwa), * dostęp do portalu wsparcia producenta, * pomoc techniczną w trybie 24x7 dla zgłoszeń krytycznych, * możliwość kontaktu z dedykowanym inżynierem wsparcia w przypadku eskalacji. |
| Licencjonowanie musi umożliwiać korzystanie z wszystkich funkcjonalności opisanych w specyfikacji, bez potrzeby zakupu dodatkowych modułów, komponentów, agentów czy rozszerzeń funkcjonalnych. W przypadku zastosowania modelu licencjonowania na hosty, rdzenie CPU, liczbę VM lub wolumen danych – wszystkie te elementy muszą być jasno wyspecyfikowane i zawarte w ofercie wykonawcy. |
| System musi posiadać możliwość replikacji danych z posiadanym przez zamawiającego systemem Veeam backup i umożliwiać odtwarzanie kopii zapasowych z nośników taśmowych utworzonych przez w/w system. |

* 1. **Wymagania dotyczące Serwerowych systemów operacyjnych – 7 szt.**

Szczegółowe wymagania dotyczące oprogramowania oraz minimalne parametry techniczne zostały określone w tabeli poniżej i stanowią podstawę do wyceny przedmiotu zamówienia przez Oferentów:

|  |  |
| --- | --- |
| **Specyfikacja**  **zamówienia** | **Wymagania Zamawiającego** |
| Opis rozwiązania | Przedmiotem zamówienia jest zakup dedykowanego systemu Windows Server Standard 2025 (16-rdzeniowy) w modelu licencjonowania CSP (Cloud Solution Provider) |
| Rodzaj licencjonowania | Windows Server Standard 16 Core 2025 w modelu licencjonowania CSP (Cloud Solution Provider) - nowa licencja |
| Zastosowanie licencji | Licencja ma zostać udzielona jako licencja jednorazowa (one-time purchase), bez ograniczeń terytorialnych. |
| Zarządzanie systemem | Możliwość zarządzania wbudowaną w oprogramowanie relacyjną bazą danych w środowisku systemu operacyjnego Windows. |
| Dostępność usługi | Możliwość zdalnego dostępu do oprogramowania z wykorzystaniem narzędzi zdalnej komunikacji i/lub dostęp do odpowiednich zasobów. |
| Instalacja oprogramowania | Możliwość instalacji oprogramowania na systemach operacyjnych Windows Server 2025 w środowisku wirtualnym i lokalnym. |
| Aktualizacja oprogramowania | Bezpłatne uaktualnienie do najnowszej wersji licencji dla przedmiotowego oprogramowania. |
| Wsparcie producenta | Wsparcie producenta na oprogramowanie Windows Server Standard 16 Core 2025 powinno być świadczone bez ograniczeń terytorialnych dla oprogramowania objętego przedmiotową licencją i zgodnie z warunkami jak w pakiecie Microsoft Software Assurance. |
| Rozwiązania równoważne | 1. Zamawiający dopuszcza zastosowanie rozwiązania równoważnego o parametrach nie gorszych niż wymienione w Opisie Przedmiotu Zamówienia, w tym:  1) System operacyjny dla komputerów typu serwer, z graficznym interfejsem użytkownika,  2) Interfejsy użytkownika dostępne w wielu językach do wyboru – w tym polskim i angielskim,  3) Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim,  4) Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta systemu z możliwością wyboru instalowanych poprawek oraz mechanizmem sprawdzającym, które z poprawek są potrzebne,  5) Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego,  6) Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6;  7) Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami,  8) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi),  9) Tworzenie i zarządzanie kontrolerami domeny (Active Directory Domain Services),  10) Obsługę usług DNS, DHCP, File Services i Hyper-V,  11) Zarządzanie uprawnieniami i użytkownikami,  12) Możliwość instalacji w środowisku fizycznym lub wirtualnym (VMware/Hyper-V),  13) Zarządzanie zdalne (Windows Admin Center, PowerShell),  14) System posiadający zlokalizowane w języku polskim i angielskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe oraz umożliwiający:  • wykorzystanie pamięci RAM powyżej 4GB,  • wykorzystanie graficznego środowiska instalacji i konfiguracji,  • darmową aktualizację i pobieranie sterowników i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek,  • zarządzanie komputerami, kontami i grupami użytkowników, dostępem do plików i drukarek,  • zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe,  • możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych,  • obsługę usługi Active Directory bez wykorzystania dodatkowego oprogramowania,  • przyłączanie do domeny oraz określanie zasad grupy, zasad zabezpieczeń i korzystania z sieci dla użytkowników i urządzeń,  • szyfrowanie urządzeń,  • wykorzystanie wbudowanych funkcji bezpieczeństwa, w tym zapory i zabezpieczeń internetowych do ochrony przed wirusami oraz złośliwym oprogramowaniem,  • określenie polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji,  • wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi),  • zabezpieczenie hasłem dostęp do systemu, konta i profilu użytkowników,  • zdalnie zarządzane,  • pracę systemu w trybie ochrony kont użytkowników,  • wyszukiwanie informacji (plików) dostępne z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego,  • system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,  • uzyskanie pomocy poprzez wbudowany system pomocy w języku polskim,  • możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących),  • zdalną pomoc i współdzielenie aplikacji, w tym możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem,  • skanowanie i przywracanie plików systemowych z poziomu konsoli,  • wsparcie dla Oracle Java i .NET Framework w najnowszej wersji oraz możliwość uruchomienia aplikacji działających we wskazanych środowiskach. Wymagane jest by klucz produktu był na stałe zapisany w BIOS-ie komputera, zapewniając poprawną aktywację systemu operacyjnego po reinstalacji bez konieczności ręcznego wpisywania klucza produktu.  2. Obowiązek zachowania równoważności spoczywa na Wykonawcy, który w przypadku zaoferowania rozwiązań równoważnych powinien dołączyć dane techniczne elementów równoważnych. 3.  Pod pojęciem rozwiązań równoważnych Zamawiający rozumie takie oprogramowanie, które w równoważnym stopniu spełnia warunki wyszczególnione w OPZ. Dla jednoznacznej identyfikacji oferowanego produktu należy podać co najmniej nazwę producenta, nazwę oferowanego oprogramowania, rodzaj licencji oraz parametry techniczne zgodne z oznaczeniem producenta. 4.    Licencje muszą pochodzić z legalnego i akceptowanego przez producenta oprogramowania kanału dystrybucji oraz pozwalać na swobodne przenoszenie pomiędzy serwerami (w tym maszynami wirtualnymi) przy zachowaniu wymagań sprzętowych jakie stawia dana licencja. 5. System serwerowy musi spełniać wszystkie wymagania jak dla Windows Server Standard 16 Core 2025 lub równoważne, zgodne z opisem zamieszczonym na stronie internetowej dla wersji standard: https://www.microsoft.com/en-us/windows-server/pricing 6. W razie wątpliwości co do równoważności poszczególnych elementów, Zamawiający wezwie Wykonawcę do złożenia dodatkowych wyjaśnień lub dokumentów potwierdzających prawidłową realizację usługi. |

* 1. **Wymagania dotyczące Zestawów komputerowych – 54 szt.** 
     1. **W skład zestawu wchodzi komputer przenośny, monitor, mysz i klawiatura bezprzewodowa, słuchawki oraz torba – 38 szt.**

Szczegółowe wymagania dotyczące zestawów komputerowych oraz minimalne parametry techniczne zostały określone w tabeli poniżej i stanowią podstawę do wyceny przedmiotu zamówienia przez Oferentów.

|  |  |
| --- | --- |
| **Nazwa** | **Wymagane parametry techniczne komputera przenośnego** |
| Zastosowanie | Komputer mobilny będzie wykorzystywany dla potrzeb aplikacji biurowych, edukacyjnych, obliczeniowych, dostępu do Internetu oraz poczty elektronicznej. |
| Matryca | 14” FHD (1920 x 1080), matryca IPS, powłoka przeciwodblaskowa, bez dotyku, jasność 250 cd/m2.  14” FHD (1920 x 1080), matryca IPS, powłoka przeciwodblaskowa, bez dotyku, jasność 400 cd/m2, kontrast 1000:1, pokrycie barw 100% sRGB.  14” FHD (1920 x 1080), matryca dotykowa IPS, powłoka przeciwodblaskowa, jasność 300 cd/m2, kontrast 700:1, NTSC 72%. |
| Bezpieczeństwo wyświetlanych treści | Komputer mobilny wyposażony we wbudowany sprzętowy mechanizm umożliwiający wykrywanie osób trzecich, uniemożliwiając tym samym dostęp do wyświetlanych danych poprzez automatyczne rozmycie lub blokowanie wyświetlanych treści. |
| Wydajność | Oferowany komputer przenośny musi osiągać w teście wydajności:  SYSMARK 25  MobileMARK 25  CrossMark  Wymagane testy wydajnościowe wykonawca musi przeprowadzić na automatycznych ustawieniach konfiguratora dołączonego przez firmę BAPCO i przy natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzaniach. Nie dopuszcza się stosowanie overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS (tzn. wyłączanie urządzeń stanowiących pełną konfigurację) jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.).  Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzonych wszystkich wymaganych testów Oferent musi dostarczyć Zamawiającemu oprogramowanie testujące, komputer do testu oraz dokładny opis metodyki przeprowadzonego testu wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od Zamawiającego |
| Procesor | Procesor osiągający w teście PassMark Performance Test, co najmniej 14 000 punktów w kategorii Average CPU Mark. Wynik dostępny na stronie: <https://www.cpubenchmark.net/cpu_list.php> |
| Pamięć RAM | 16GB DDR5 5200 MT/s, możliwość rozbudowy do min. 64GB RAM, jeden slot na pamięć wolny. |
| Pamięć masowa | 1TB NVMe SSD M.2 |
| Karta graficzna | Wynik karty graficznej w teście PassMark Performance Test co najmniej 2683 punktów w kategorii Average G3D Rating. Dostępny na stronie: <http://www.videocardbenchmark.net/gpu_list.php> |
| Klawiatura | Klawiatura w układzie US – QWERTY, z wbudowanym podświetleniem, min 78 klawiszy. Wszystkie klawisze funkcyjne typu: mute, regulacja głośności, print screen dostępne w ciągu klawiszy F1-F12. Dedykowany klawisz dla Microsoft Copilot. |
| Multimedia | Karta dźwiękowa zintegrowana z płytą główną, wbudowane dwa głośniki stereo o mocy 2W każdy.  Dwa kierunkowe, cyfrowe mikrofony z funkcją redukcji szumów i poprawy mowy wbudowane w obudowę matrycy.  Kamera internetowa FHD RGB 2 MPIX, trwale zainstalowana w obudowie matrycy opatrzona wbudowaną mechaniczną przysłonę.  Kamera internetowa FHD RGB 2 MPIX z kamerą IR, trwale zainstalowana w obudowie matrycy opatrzona wbudowaną mechaniczną przysłonę.  1 port audio typu combo (słuchawki i mikrofon) |
| Łączność bezprzewodowa | Karta Wi-Fi 6E AX z transferem do 2400 Mbps + Bluetooth 5.3  Modem LTE / 5G eSIM |
| Bateria i zasilanie | Bateria o pojemności min. 54WH, z obsługą technologii szybkiego ładowania, umożliwiającą szybkie naładowanie baterii do poziomu 80% w czasie 1 godziny.  Zasilacz o mocy min. 65W ze złączem Typu – C |
| Waga i wymiary | Waga maks. 1.5kg z oferowaną baterią  Suma wymiarów notebooka nie większa niż 535 mm mierzona po krawędziach obudowy. |
| Obudowa | Komputer spełniający normy MIL-STD-810H załączyć do oferty oświadczenie wykonawcy opatrzone numerem postępowania oraz poparte oświadczeniem producenta. |
| BIOS | BIOS producenta oferowanego komputera zgodny ze specyfikacją UEFI, wymagana pełna obsługa za pomocą klawiatury i urządzenia wskazującego (wmontowanego na stałe) oraz samego urządzenia wskazującego. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji, oraz posiadać: datę produkcji komputera (data produkcji nieusuwalna), o kontrolerze audio, procesorze, a w szczególności min. i maks. osiągana prędkość, pamięci RAM z informacją o taktowaniu i obsadzeniu w slotach. Niezmazywalne (nieedytowalne) pole asset tag z możliwością wpisywania min. znaków specjalnych. Funkcje logowania się do BIOS na podstawie hasła systemowego/użytkownika, administratora (hasła niezależne), Blokowanie hasłem systemowym/użytkownika rozruch dysku twardego. Funkcja umożliwiająca założenie hasła na dysk, informację o stanie naładowania baterii (stanu użycia), podpiętego zasilacza, zarządzanie trybem ładowania baterii (np. określenie docelowego poziomu naładowania). Możliwość nadania numeru inwentarzowego z poziomu BIOS bez wykorzystania dodatkowego oprogramowania, jak i konieczności aktualizacji BIOS.  Możliwość włączenia/wyłączenia funkcji automatycznego tworzenia recovery BIOS na dysku twardym. |
| Certyfikaty | Certyfikat ISO9001 dla producenta sprzętu  Certyfikat ISO 14001 dla producenta sprzętu  Certyfikat ISO 50001 dla producenta sprzętu  Certyfikat TCO, wymagana certyfikacja na stronie:  Certyfikat EPEAT Gold dla Polski lub kraju członkowskiego UE, dla oferowanego modelu komputera. Wymagana certyfikacja na stronie: https://www.epeat.net/search-computers-and-displays - załączyć do oferty wydruk ze strony. Deklaracja zgodności CE  Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki  - lub certyfikaty równoważne  Potwierdzenie kompatybilności komputera z oferowanym systemem operacyjnym (wydruk ze strony) |
| Ergonomia | Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 lub równoważną oraz wykazana zgodnie z normą ISO 9296 lub równoważną w pozycji obserwatora w trybie pracy dysku twardego (IDLE) wynosząca maksymalnie 23dB (załączyć do oferty oświadczenie wykonawcy opatrzone numerem postępowania oraz poparte oświadczeniem producenta) |
| Diagnostyka | System diagnostyczny z graficznym interfejsem użytkownika zaszyty w tej samej pamięci flash co BIOS, dostępny z poziomu szybkiego menu boot lub BIOS, umożliwiający przetestowanie komponentów komputera takich jak:  - procesor  - pamięć RAM  - dysk twardy  - zasilanie/ładowanie  - klawiatura  - matryca  - audio  - układ graficzny/video  - kamera internetowa  - bateria  - wentylator  - porty USB  Testy możliwe do wykonania w formie szybkiej i zaawansowanej lub dedykowanej formie dla danego komponentu, Pełna obsługa systemu diagnostycznego za pomoca samej klawiatury, urządzenia wskazującego, myszy i jednocześnie za pomocą klawiatury i myszy. System zapewniający zachowujący pełną funkcjonalność nawet w przypadku braku dysku twardego oraz jego uszkodzenia, niewymagający stosowania zewnętrznych nośników pamięci masowej oraz dostępu do internetu i sieci lokalnej. Procedura POST traktowana jest jako oddzielna funkcjonalność. |
| Bezpieczeństwo | Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Próba usunięcia układu powoduje uszkodzenie płyty głównej. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Weryfikacja wygenerowanych przez komputer kluczy szyfrowania musi odbywać się w dedykowanym chipsecie na płycie głównej.  Wbudowany czyunik otwarcia obudowy (dolnej pokrywy)  Wbudowana w obudowę matrycy kamera IR umożliwiająca autentykację na poziomie oferowanego systemu operacyjnego  Czytnik linii papilarnych  Czytnik SmartCard  Czytnik SmartCard kontaktowy |
| System operacyjny | Zainstalowany system operacyjny Windows 11 Professional, klucz licencyjny zapisany trwale w BIOS, umożliwiać instalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego. |
| Rozwiązania równoważne | Zamawiający dopuszcza rozwiązania równoważne o parametrach nie gorszych niż wymienione w Opisie Przedmiotu Zamówienia, w tym spełniające następujące wymagania:  − pełna integracja z domeną Active Directory Microsoft Windows,  − pełna integracja z Windows Management Instrumentation (WMI) – zestawem protokołów i rozszerzeń systemu Windows umożliwiającym zarządzanie i dostęp do zarządzalnych zasobów komputera, takich jak adaptery sieciowe, aktualnie otwarte programy, lista procesów, odczyty z wbudowanych czujników temperatury,  − zarządzanie komputerami za pomocą Zasad grupy (GPO – Group Policy Object) Active Directory Microsoft Windows,  − niewymaganie aktywacji instalowanego systemu w firmie producenta oprogramowania innej od aktywacji za pomocą serwera KMS (Key Management Software) będącego w posiadaniu Zamawiającego,  − możliwość uruchamiania aplikacji 32-bitowych i 64-bitowych napisanych natywnie dla systemu Microsoft Windows,  − możliwość natywnej obsługa pamięci RAM komputera powyżej 4GB,  − możliwość zarządzania komputerem poprzez protokół Remote Desktop Protocol (Pulpit Zdalny),  − natywne wsparcie dla usługi Azure Active Directory (możliwość używania tych samych poświadczeń logowania dla Windows 10, Office 365 i innych usług Microsoft),  − wbudowana zapora sieciowa umożliwiająca kontrolę nad niepowołanym dostępem do komputera oraz zapewniającą ochronę połączeń internetowych,  − dostęp do bezpłatnych aktualizacji bezpieczeństwa oraz poprawek związanych z działaniem systemu operacyjnego,  − wbudowana ochrona antywirusowa oraz przeciw złośliwemu oprogramowaniu,  − wszystkie w/w funkcjonalności nie mogą być realizowane za pomocą jakiegokolwiek rodzaju emulacji i wirtualizacji oferowanego sytemu operacyjnego. |
| Oprogramowanie dodatkowe | Dołączone do oferowanego komputera oprogramowanie z nieograniczoną licencją czasowo na użytkowanie umożliwiające:  - upgrade i instalacje wszystkich sterowników, dostarczonych w obrazie systemu operacyjnego producenta, BIOS’u z certyfikatem zgodności producenta do najnowszej dostępnej wersji,  - możliwość przed instalacją sprawdzenia każdego sterownika, BIOS’u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji:                  a. o poprawkach i usprawnieniach dotyczących aktualizacji                  b. dacie wydania ostatniej aktualizacji                  c. priorytecie aktualizacji                  d. zgodność z systemami operacyjnymi                  e. jakiego komponentu sprzętu dotyczy aktualizacja                  f.  wszystkie poprzednie aktualizacje z informacjami jak powyżej od punktu a do punktu e.  - wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne  - możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku, kiedy jest wymagany przy instalacji sterownika, aplikacji, która tego wymaga.  - rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację, kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty (dd-mm-rrrr)  - sprawdzenia historii upgrade’u z informacją jakie sterowniki były instalowane z dokładną datą (dd-mm-rrrr) i wersją (rewizja wydania)  - dokładny wykaz wymaganych sterowników, aplikacji, BIOS’u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu \*.xml  - raport uwzględniający informacje o: sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach, zainstalowanych aktualizacjach z dokładnym rozbiciem jakich komponentów to dotyczyło, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu do pliku \*.xml. Raport musi zawierać z dokładną datą (dd-mm-rrrr) i godziną z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku. |
| Porty i złącza | Wbudowane porty i złącza: 1 x HDMI 2.1, 2 x USB 3.2 typ A, 2 x Thunderbolt 4, port audio combo, gniazdo linki zabezpieczającej |
| Bezpieczeństwo łańcucha dostaw | Producent zaoferowanego komputera musi posiadać wdrożony proces zapewniający bezpieczny łańcuch dostaw.  Rozwiązanie to musi chronić urządzenie przed niepowołaną ingerencją osób trzecich w integralność podzespołów komputera, zagrażającą bezpieczeństwu danych organizacji.  Producent komputera zapewni możliwość weryfikacji dostarczonej konfiguracji sprzętowej pod kątem zgodności z konfiguracją fabryczną w zakresie podzespołów takich jak:   * Procesor * Moduł TPM * Dysk * Karta sieciowa * Pamięć RAM * Płyta główna   Sprawdzenie konfiguracji musi odbywać się na portalu internetowym producenta komputera, poprzez weryfikację zgodności unikalnego dla konkretnej części numeru nadanego i przechowywanego przez producenta komputera.  W przypadku zidentyfikowania niezgodności któregokolwiek z ww. komponentów, informacja o naruszeniu integralności podzespołów będzie widoczna na portalu internetowym producenta sprzętu.  Proces weryfikacji komponentów musi być zaprojektowany w zgodnie z zaleceniami NIST.  Wymaga się dołączenia oświadczenia producenta komputera potwierdzającego spełnienie powyższych wymagań. |
| Warunki gwarancyjne, wsparcie techniczne | * Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. * Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, Rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego). * Minimum 3-letnia gwarancja producenta świadczona na miejscu u klienta, * Czas reakcji serwisu - do końca następnego dnia roboczego. * W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego – wymagane jest dołączenie do oferty oświadczenia podmiotu realizującego serwis lub producenta sprzętu o spełnieniu tego warunku   Gwarancja musi oferować przez cały okres:  - usługi serwisowe świadczone w miejscu instalacji urządzenia  oraz możliwość szybkiego zgłaszania usterek przez portal internetowy  - opiekę kierownika technicznego ds. Eskalacji  - dostępność wsparcia technicznego przez 24 godziny 7 dni w tygodniu przez cały rok (w języku polskim w dni robocze)  - dostęp do portalu technicznego producenta, który umożliwi zamawianie części zamiennych i/lub wizyt technika serwisowego, mający na celu przyśpieszenie i procesu diagnostyki i skrócenia czasu uśnięcia usterki  - szybkie wsparcie telefoniczne świadczone przez wykwalifikowanych konsultantów, a nie przez call center bazujące na skryptach rozmów telefonicznych  - wsparcie techniczne dla problemów z fabrycznie zainstalowanym oprogramowaniem OEM |
| Wyposażenie dodatkowe | 1. Torba przystosowana do wielkości zamawianego sprzętu (nie większa niż 15,6 cala), wykonana z materiałów odpornych na uszkodzenia mechaniczne i warunki atmosferyczne, umożliwiająca bezpieczny transport komputera przenośnego wraz z akcesoriami. Torba musi posiadać przegrodę lub system organizacji przestrzeni umożliwiający przenoszenie zasilacza, myszy oraz dokumentów formatu A4. 2. Przewodowe słuchawki nagłowne z mikrofonem, przeznaczone do pracy biurowej oraz prowadzenia rozmów głosowych i wideokonferencji.  * Podłączenie za pomocą złącza USB typu A. * Wbudowany mikrofon z funkcją redukcji szumów otoczenia. * Obsługa dźwięku szerokopasmowego (wideband audio) zapewniająca czysty i wyraźny przekaz głosu. * Regulowany, wyściełany pałąk na głowę oraz miękkie nauszniki dla komfortu użytkowania. * Zintegrowany pilot sterowania na kablu umożliwiający odbieranie i kończenie połączeń, regulację głośności oraz wyciszenie mikrofonu.  1. Zestaw składający się z bezprzewodowej klawiatury pełnowymiarowej oraz bezprzewodowej myszy.  * Podłączenie za pomocą jednego odbiornika USB do obsługi obu urządzeń * Zasięg działania minimum 10 metrów * Układ klawiatury, QWERTY, układ polski programisty z pełnym blokiem numerycznym * Klawiatura membranowa lub niskoprofilowa, typu wyspowego, odpowiednia do pracy biurowej * Klawiatura powinna posiadać klawisze funkcyjne multimedialne, z możliwością programowania skrótów, klawisze szybkiego dostępu (np. do poczty, kalkulatora) * Mysz bezprzewodowa, ergonomiczna, z minimum 5 przyciskami, w tym przyciskami bocznymi (wstecz/dalej), oraz rolką przewijania * Czułość myszy regulowana, min.1000-1600 DPI * Klawiatura i mysz powinny być zasilane za pomocą baterii (które powinny być w zestawie) lub akumulatorów * Zestaw powinien być w pełni kompatybilny z systemami Windows 10/11 bez konieczności instalowania dodatkowego oprogramowania * Zestaw w kolorze czarnym, grafitowym lub ciemnoszarym * Gwarancja na zestaw: Minimum 36 miesięcy door-to-door lub realizowana w miejscu użytkowania sprzętu |

|  |  |
| --- | --- |
| **Nazwa** | **Wymagane parametry techniczne Monitora** |
| Przekątna ekranu | Min. 27 cali |
| Typ matrycy | IPS z powłoką Anti-Glare lub równoważna |
| Rozdzielczość | Min. 3840 x 2160 (Ultra HD 4K) |
| Format obrazu | 16:9 |
| Częstotliwość odświeżania | Min. 60 Hz |
| Jasność | Min. 350 cd/m² |
| Kontrast statyczny | Min. 1000:1 |
| Kąty widzenia (pion/poziom) | Min. 178° / 178° |
| Czas reakcji | Najniższy: min. 5 ms; Standardowy: min. 8ms |
| Złącza | Min. 1x HDMI 2.0, 1x DisplayPort 1.4, 1x USB-C 3.2 Gen 1, 4x USB 3.2, 1 x RJ45 lub równoważne |
| Zasilanie przez USB-C | Tak, min. 90W |
| Regulacja położenia | Regulacja wysokości: min. 15 cm  Pochylenie: min. -5° do 21°  Obrotowa podstawa: min. -45° do 45°  pivot (obrót do pionu): min. -90° do 90° |
| Standard montażu VESA | Tak, min. 100 x 100 mm |
| Kolor obudowy | Czarny, szary lub zbliżony |
| Akcesoria w zestawie | Przewód zasilający  Przewód DisplayPort - DisplayPort  Przewód USB-C - USB-C |
| Gwarancja | Min. 3 lata gwarancji typu on-site lub door-to-door |

* + 1. **W skład zestawu wchodzi komputer, monitor, mysz i klawiatura bezprzewodowa oraz słuchawki – 16 szt.**

Szczegółowe wymagania dotyczące zestawów komputerowych oraz minimalne parametry techniczne zostały określone w tabeli poniżej i stanowią podstawę do wyceny przedmiotu zamówienia przez Oferentów

|  |  |
| --- | --- |
| **Nazwa** | **Wymagane parametry techniczne komputera** |
| Zastosowanie | Komputer stacjonarny będzie wykorzystywany do zastosowań biurowych, edukacyjnych, obliczeniowych, dostępu do Internetu oraz obsługi poczty elektronicznej. |
| Obudowa | Typ SFF (Small Form Factor), umożliwiająca montaż w ograniczonych przestrzeniach. W zestawie podstawka pionowa. |
| Procesor | Min. 14-rdzeniowy (6P+8E), 20-wątkowy, taktowanie bazowe min. 2.6 GHz, turbo do 5.0 GHz. Wynik w teście PassMark CPU Mark: ≥ 29 000 punktów (https://www.cpubenchmark.net). |
| Pamięć RAM | Min. 16 GB DDR5 4800 MHz z możliwością rozbudowy do min. 64 GB, co najmniej jeden wolny slot. |
| Dysk SSD | Min. 1TB SSD M.2 NVMe. Możliwość zamontowania drugiego nośnika danych. |
| Karta graficzna | Zintegrowana Intel UHD Graphics 770. Wynik PassMark G3D Rating ≥ 2683 punktów (https://www.videocardbenchmark.net). |
| Łączność | Karta Wi-Fi 6E AX (do 2400 Mbps), Bluetooth 5.3. |
| System operacyjny | Windows 11 Professional PL, klucz licencyjny zapisany trwale w BIOS. |
| Rozwiązania równoważne | Zamawiający dopuszcza rozwiązania równoważne o parametrach nie gorszych niż wymienione w Opisie Przedmiotu Zamówienia, w tym spełniające następujące wymagania:  − pełna integracja z domeną Active Directory Microsoft Windows,  − pełna integracja z Windows Management Instrumentation (WMI) – zestawem protokołów i rozszerzeń systemu Windows umożliwiającym zarządzanie i dostęp do zarządzalnych zasobów komputera, takich jak adaptery sieciowe, aktualnie otwarte programy, lista procesów, odczyty z wbudowanych czujników temperatury,  − zarządzanie komputerami za pomocą Zasad grupy (GPO – Group Policy Object) Active Directory Microsoft Windows,  − niewymaganie aktywacji instalowanego systemu w firmie producenta oprogramowania innej od aktywacji za pomocą serwera KMS (Key Management Software) będącego w posiadaniu Zamawiającego,  − możliwość uruchamiania aplikacji 32-bitowych i 64-bitowych napisanych natywnie dla systemu Microsoft Windows,  − możliwość natywnej obsługa pamięci RAM komputera powyżej 4GB,  − możliwość zarządzania komputerem poprzez protokół Remote Desktop Protocol (Pulpit Zdalny),  − natywne wsparcie dla usługi Azure Active Directory (możliwość używania tych samych poświadczeń logowania dla Windows 10, Office 365 i innych usług Microsoft),  − wbudowana zapora sieciowa umożliwiająca kontrolę nad niepowołanym dostępem do komputera oraz zapewniającą ochronę połączeń internetowych,  − dostęp do bezpłatnych aktualizacji bezpieczeństwa oraz poprawek związanych z działaniem systemu operacyjnego,  − wbudowana ochrona antywirusowa oraz przeciw złośliwemu oprogramowaniu,  − wszystkie w/w funkcjonalności nie mogą być realizowane za pomocą jakiegokolwiek rodzaju emulacji i wirtualizacji oferowanego sytemu operacyjnego. |
| Porty i złącza | * Min. 1 x HDMI 1.4b * Min. 1 x DisplayPort 1.4 * Min. 4 x USB 3.2 Gen1 * Min. 2 x USB 2.0 * Min. 1 x USB-C (opcjonalnie z przodu) * 1 x RJ-45 * 1 x audio combo (przód) * 1 x port zasilania * 1 x port blokady Kensington. |
| BIOS | * UEFI BIOS, obsługa z poziomu klawiatury i myszy * dostęp do informacji o konfiguracji sprzętowej * możliwość ustawień haseł użytkownika, administratora * blokada rozruchu dysku * Funkcja Asset Tag * numer inwentarzowy * kontrola stanu baterii (jeśli dotyczy) * możliwość tworzenia recovery BIOS. |
| Bezpieczeństwo | * TPM 2.0 zintegrowany z płytą główną * czujnik otwarcia obudowy * wsparcie dla BitLocker. |
| Ergonomia i hałas | Maksymalny poziom hałasu w trybie IDLE ≤ 23 dB (zgodnie z ISO 7779/9296). |
| Zasilanie | Zasilacz 180W zewnętrzny lub wewnętrzny (w zależności od wersji), certyfikat 80 PLUS. |
| Certyfikaty | ISO 9001, ISO 14001, ISO 50001 dla producenta, EPEAT Gold (PL), TCO Certified – lub równoważne, CE, zgodność z dyrektywą RoHS. |
| Diagnostyka | * Wbudowane narzędzie diagnostyczne dostępne z poziomu BIOS/UEFI. * Testowanie procesora, RAM, dysku, grafiki, wentylatora, portów USB. * Obsługa za pomocą klawiatury i myszy. Funkcjonalność bez potrzeby zewnętrznych nośników i dostępu do Internetu. |
| Oprogramowanie dodatkowe | Oprogramowanie producenta umożliwiające:   * aktualizacje BIOS i sterowników * przegląd historii aktualizacji * identyfikację modelu * eksport konfiguracji do pliku XML * automatyczne raportowanie stanu systemu. |
| Bezpieczeństwo łańcucha dostaw | Producent zapewnia możliwość weryfikacji zgodności komponentów (CPU, RAM, TPM, dysk, karta sieciowa, płyta główna) z konfiguracją fabryczną na portalu internetowym, zgodność z NIST. Wymagane oświadczenie producenta. |
| Warunki gwarancyjne, wsparcie techniczne | * Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. * Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, Rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego). * Minimum 3-letnia gwarancja producenta świadczona na miejscu u klienta, * Czas reakcji serwisu - do końca następnego dnia roboczego. * W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego – wymagane jest dołączenie do oferty oświadczenia podmiotu realizującego serwis lub producenta sprzętu o spełnieniu tego warunku   Gwarancja musi oferować przez cały okres:  - usługi serwisowe świadczone w miejscu instalacji urządzenia  oraz możliwość szybkiego zgłaszania usterek przez portal internetowy  - opiekę kierownika technicznego ds. Eskalacji  - dostępność wsparcia technicznego przez 24 godziny 7 dni w tygodniu przez cały rok (w języku polskim w dni robocze)  - dostęp do portalu technicznego producenta, który umożliwi zamawianie części zamiennych i/lub wizyt technika serwisowego, mający na celu przyśpieszenie i procesu diagnostyki i skrócenia czasu uśnięcia usterki  - szybkie wsparcie telefoniczne świadczone przez wykwalifikowanych konsultantów, a nie przez call center bazujące na skryptach rozmów telefonicznych  - wsparcie techniczne dla problemów z fabrycznie zainstalowanym oprogramowaniem OEM |
| Wyposażenie dodatkowe | 1. Przewodowe słuchawki nagłowne z mikrofonem, przeznaczone do pracy biurowej oraz prowadzenia rozmów głosowych i wideokonferencji.  * Podłączenie za pomocą złącza USB typu A. * Wbudowany mikrofon z funkcją redukcji szumów otoczenia. * Obsługa dźwięku szerokopasmowego (wideband audio) zapewniająca czysty i wyraźny przekaz głosu. * Regulowany, wyściełany pałąk na głowę oraz miękkie nauszniki dla komfortu użytkowania. * Zintegrowany pilot sterowania na kablu umożliwiający odbieranie i kończenie połączeń, regulację głośności oraz wyciszenie mikrofonu.  1. Zestaw składający się z bezprzewodowej klawiatury pełnowymiarowej oraz bezprzewodowej myszy.  * Podłączenie za pomocą jednego odbiornika USB do obsługi obu urządzeń * Zasięg działania minimum 10 metrów * Układ klawiatury, QWERTY, układ polski programisty z pełnym blokiem numerycznym * Klawiatura membranowa lub niskoprofilowa, typu wyspowego, odpowiednia do pracy biurowej * Klawiatura powinna posiadać klawisze funkcyjne multimedialne, z możliwością programowania skrótów, klawisze szybkiego dostępu (np. do poczty, kalkulatora) * Mysz bezprzewodowa, ergonomiczna, z minimum 5 przyciskami, w tym przyciskami bocznymi (wstecz/dalej), oraz rolką przewijania * Czułość myszy regulowana, min.1000-1600 DPI * Klawiatura i mysz powinny być zasilane za pomocą baterii (które powinny być w zestawie) lub akumulatorów * Zestaw powinien być w pełni kompatybilny z systemami Windows 10/11 bez konieczności instalowania dodatkowego oprogramowania * Zestaw w kolorze czarnym, grafitowym lub ciemnoszarym * Gwarancja na zestaw: Minimum 36 miesięcy door-to-door lub realizowana w miejscu użytkowania sprzętu |

|  |  |
| --- | --- |
| **Nazwa** | **Wymagane parametry techniczne Monitora** |
| Przekątna ekranu | Min. 27 cali |
| Typ matrycy | IPS z powłoką Anti-Glare lub równoważna |
| Rozdzielczość | Min. 3840 x 2160 (Ultra HD 4K) |
| Format obrazu | 16:9 |
| Częstotliwość odświeżania | Min. 60 Hz |
| Jasność | Min. 350 cd/m² |
| Kontrast statyczny | Min. 1000:1 |
| Kąty widzenia (pion/poziom) | Min. 178° / 178° |
| Czas reakcji | Najniższy: min. 5 ms; Standardowy: min. 8ms |
| Złącza | Min. 1x HDMI 2.0, 1x DisplayPort 1.4, 1x USB-C 3.2 Gen 1, 4x USB 3.2, 1 x RJ45 lub równoważne |
| Zasilanie przez USB-C | Tak, min. 90W |
| Regulacja położenia | Regulacja wysokości: min. 15 cm  Pochylenie: min. -5° do 21°  Obrotowa podstawa: min. -45° do 45°  pivot (obrót do pionu): min. -90° do 90° |
| Standard montażu VESA | Tak, min. 100 x 100 mm |
| Kolor obudowy | Czarny, szary lub zbliżony |
| Akcesoria w zestawie | Przewód zasilający  Przewód DisplayPort - DisplayPort  Przewód USB-C - USB-C |
| Gwarancja | Min. 3 lata gwarancji typu on-site lub door-to-door |

* 1. **Wymagania dotyczące Drukarek biurowych – 10 szt.**

Szczegółowe wymagania dotyczące drukarek biurowych oraz minimalne parametry techniczne zostały określone w tabeli poniżej i stanowią podstawę do wyceny przedmiotu zamówienia przez Oferentów:

|  |  |
| --- | --- |
| **Parametr** | **Szczegóły** |
| Połączenie | Sieć przewodowa, USB |
| Lokalny interfejs | Hi-Speed USB 2.0, USB 2.0Host (Przód | Tył) |
| NFC | Obsługiwane standardy NFC:(ISO14443 Typ A lub równoważny) MIFAREStandard/Plus/Ultralight/Ultralight C/DESfire my-d move, Tag-it (ISO15693 Typ B lub równoważny) |
| Interfejs sieci przewodowej | GigE (10Base-T/100Base-TX/1000Base-T) |
| Kopiowanie 2-stronne | Tak |
| Rozdzielczość | Co najmniej 600 x 600 dpi |
| Szybkość | Co najmniej 40 kopii na minutę |
| Współczynnik powiększenia/zmniejszenia | Urządzenie zmniejsza lub powiększa rozmiar dokumentu w zakresie od 25% do 400% co 1% |
| Faks-modem | 33.6 kb/s |
| Faks internetowy | Tak |
| PC Fax | Tak |
| Warunki pracy: wilgotność | 20 - 80% |
| Warunki pracy: temperatura | 10°C - 32°C |
| Warunki przechowywania: wilgotność | 10 - 90% |
| Warunki przechowywania: temperatura | 0°C - 40°C |
| Moc dźwięku | Maksymalna moc dźwięku: podczas drukowania 6,79 BA; W trybie gotowości 3,06 BA; W trybie cichej pracy 6.37 BA; W trybie głębokiego uśpienia 3,06 BA; |
| Poziom hałasu | Maksymalny poziom hałasu: Podczas drukowania 55 dBA; W trybie gotowości 17,2 dBA; W trybie cichej pracy 52 dBA; |
| Zużycie energii | Podczas drukowania 770 W (430 W w trybie cichej pracy); Podczas kopiowania 730 W (420 W w trybie cichej pracy); W trybie gotowości 85 W; W trybie uśpienia 16,8 W; W trybie głębokiego uśpienia 1,1 W; Urządzenie wyłączone 0,04 W; |
| Typowe zużycie energii | 0,687 kWh / tydzień |
| Typy i gramatury papieru | (Podajnik 1): Letter, Legal, Executive, A4, A5, A5 (długa krawędź), A6, B5(ISO), Mexico Legal , India Legal , Folio, 16K(195 x 270 mm); Podajnik uniwersalny Szerokość: 76,2 - 215,9 mm; Długość: 127 - 355,6 mm; Koperty; C5, Com 10, DL, Monarch Podajniki opcjonalne (2-5): Letter, Legal Executive, A4, A5, Mexico Legal, India Legal Folio, 16 K 195 x 270 mm); |
| Rozmiary | Podajnik 1: 60 - 230 g/m2; Podajnik uniwersalny: 60 - 230 g/m2; Automatyczny podajnik dokumentów (ADF):45 - 120 g/m2; Podajniki opcjonalne (2-5):60 - 105 g/m2; |
| Pojemność papieru (arkusze) | Podajnik standardowy (Podajnik 1): 520 arkuszy; Podajnik uniwersalny: 100 arkuszy, 15 kopert; Automatyczny podajnik dokumentów (ADF): 100 arkuszy; |
| Rozdzielczość drukowania | 2400 dpi (2400 x 600 dpi), 600 x 600 dpi |
| Szybkość kolorowego drukowania 2-stronnego A4 | Co najmniej 28 strony na minutę |
| Szybkość standardowego drukowania kolorowego A4 | Co najmniej 40 strony na minutę |
| Automatyczne drukowanie 2-stronne | Tak |
| Obsługiwane języki drukowania | PCL5e, PCL5c, PCL6 (PCL XL Class3.0), BR Script3, PDF v. 1.7, XPS v. 1.0 |
| Czas wykonania pierwszego wydruku | Mniej niż 10 sekundy |
| Skanowanie 2-stronne | Tak |
| Rozdzielczość skanowania | Co najmniej 600 x 600 dpi (szyba i ADF); Do 19 200 x 19 200 dpi (Interpolowana) |
| Funkcje skanowania | Skanowanie do folderu sieciowego (SMB), FTP, SFTP, serwera E-mail, platformy SharePoint (lokalnie); |
| Szybkość skanowania | Co najmniej 100 ipm (obrazów na minutę) |
| Typ skanera | Podwójny CIS |
| Funkcje sieciowe | 802.1x; Active Directory LDAP Authentication; Automatic Intrusion Detection |
| Funkcje zabezpieczeń | Cloud Secure Print |
| Gwarancja | Co najmniej 3-lata gwarancji (po rejestracji na stronie producenta) |

* 1. **Wymagania dotyczące Drukarek\urządzeń wielofunkcyjnych – 3 szt.**

Szczegółowe wymagania dotyczące urządzeń wielofunkcyjnych oraz minimalne parametry techniczne zostały określone w tabeli poniżej i stanowią podstawę do wyceny przedmiotu zamówienia przez Oferentów:

|  |  |
| --- | --- |
| **Parametr** | **Szczegóły** |
| Typ | Urządzenie wielofunkcyjne (MFP) |
| Funkcje | Drukowanie, kopiowanie, skanowanie, faksowanie |
| Technologia druku | Laserowa |
| Maksymalna prędkość druku | Co najmniej 45 stron na minutę (A4) |
| Prędkość druku w kolorze | Co najmniej 45 stron na minutę (A4) |
| Prędkość druku mono A3 | Co najmniej 22 str./min. |
| Powiększenie | 25­-400% w odstępach 0,1%; automatyczny zoom |
| Pierwsza strona w czerni | 3,8 sekundy |
| Pierwsza strona w kolorze | 7,5 sekundy |
| Czas nagrzewania | ok. 15 sekund |
| Rozdzielczość druku | 1800 x 600 dpi; 1200 x 1200 dpi |
| Rozdzielczość kopiowania i skanowania | Co najmniej 600 x 600 dpi |
| Wydajność miesięczna | Co najmniej 200 000 stron |
| Rekomendowane obciążenie miesięczne | Co najmniej 40 000 stron |
| Wydajność tonera czarno-białego | Co najmniej 24 000 stron |
| Wydajność sekcji obrazowania czarno-białego | 260 000 stron/1 000 000 stron (Bęben/Wywoływacz) |
| Szybkość skanowania w kolorze i w czerni | Co najmniej 140/140 obr./min. w trybie simplex (mono/kolor) co najmniej 280/280 obr./min. w trybie duplex (mono/kolor) |
| Rozdzielczość skanowania (dpi) | Co najmniej 600 x 600 dpi |
| Formaty plików | JPEG; TIFF; PDF; Kompaktowy PDF; Szyfrowany PDF; XPS; Kompaktowy XPS; PPTX opcjonalnie: Przeszukiwalny PDF; PDF/A 1a i 1b; Przeszukiwalny DOCX/PPTX/XLSX |
| Automatyczny podajnik dokumentów | Co najmniej 300 oryginałów; A6-A3; 35-163 g/m²; dostępność funkcji Dualscan |
| Format Papieru | A6-SRA3; papier do banerów max. 1200 x 297 mm, rozmiary niestandardowe |
| Gramatura Papieru | 52-300 g/m² |
| Pojemność papieru (arkusze) | Standard 1150 arkuszy maks. 6650 arkuszy |
| Funkcje drukowania | Bezpośredni wydruk plików PCL; PS; TIFF; XPS; PDF (wer. 1.7); szyfrowanych plików PDF i OOXML (DOCX; XLSX; PPTX); Mixmedia i Mixplex; programowanie zadań „Easy Set”; nakładka; znak wodny’ ochrona kopii; tryb „carbon copy” |
| Automatyczny druk dwustronny | A6–SRA3; 52–256 g/m² |
| Dysk twardy | 250 GB SSD (wbudowany, możliwość szyfrowania) |
| Złącza | USB 3.0, Ethernet (10/100/1000Base-T), opcjonalnie Wi-Fi |
| Protokoły sieciowe | TCP/IP (IPv4/IPv6); SMB; LPD; IPP; SNMP; HTTP(S) |
| Zużycie energii | 220-240 V / 50/60 Hz; Poniżej 1,58 kW (system) |
| Panel sterujący | 10,1-calowy ekran dotykowy |
| Interfejs użytkownika | Możliwość dostosowywania; obsługuje różne języki |
| Możliwości skanowania | Skanowanie do e-maila, FTP, SMB, USB; skanowanie w kolorze |
| Funkcje zabezpieczeń | Wspólne kryteria ISO 15408 HCD-PP lub równoważny (w trakcie oceny); Filtrowanie IP i blokowanie portów; Komunikacja sieciowa SSL3 and TLS1.0/1.1/1.2; Obsługa IPsec; Obsługa IEEE 802.1x; Uwierzytelnianie użytkownika; Dziennik uwierzytelniania; Bezpieczny wydruk; Kerberos; Nadpisywanie dysku; Szyfrowanie danych na dysku (AES 256); Odbiór faksów poufnych; Szyfrowanie danych użytkownika drukarki opcjonalnie: Skanowanie antywirusowe w czasie rzeczywistym (Bitdefender®); Ochrona przed kopiowaniem (funkcje Copy Guard, Password Copy) |

* 1. **Wymagania dotyczące telefonów Voip – 30 szt.**

Szczegółowe wymagania dotyczące telefonów IP typu VOIP oraz minimalne parametry techniczne zostały określone w tabeli poniżej i stanowią podstawę do wyceny przedmiotu zamówienia przez Oferentów:

* + 1. **Telefon IP Voip typu Desktop – 25 szt.**

|  |  |
| --- | --- |
| **Przedmiot**  **zamówienia** | **Wymagane przez Zamawiającego minimalne parametry techniczne**  **aparatów telefonicznych do obsługi numerów VoIP** |
| Aparat telefoniczny do obsługi numerów VoIP | 1. **Wyświetlacz:**  * 4.3-calowy Kolorowy wyświetlacz LCD z podświetlaniem: 480x272 px  1. **Przyciski:**  * 7 przycisków funkcyjnych (Transfer/ Hold / Redial / Wyciszenie / Słuchawka nagłowna / Tryb głośnomówiący / Wiadomości) * Głośność: długie przyciski +/- * Przyciski kontekstowe: 4 kontekstowe klawisze LCD * Diody dual LED programowalne do 27 różnych funkcji * 3-stronna konferencja: dedykowany przycisk na klawiaturze telefonu * Diody LED do wyboru linii i nawigacji: 10 diod dual LED  1. **Funkcje telefonu:**  * Szybkie wybieranie * SMS * Ponowne wybieranie * Wybór dzwonka * BLA (Bridged Line Apperance) * BLF (Busy lamp field) * Czarna lista * Historia połączeń * Hot-desking * Anonimowe wykonywanie połączeń * Wstrzymanie połączenia * Wyciszanie połączenia * Funkcja „nie przeszkadzać” DND * Anonimowe odrzucanie połączeń * 16 kont SIP * Lokalna książka telefoniczna do 1000 wpisów * Dziesięciostronne konferencje * Identyfikator dzwoniącego z nazwą i numerem * Obsługa aparatu w języku Polskim  1. **Konfiguracja i parametry sieciowe:**  * Ręczna: lokalna przez telefon / interfejs www * Wersja IP: Ipv4 / Ipv6 * Przydzielanie adresu IP: DHCP / Statyczny * Obsługiwane protokoły: HTTP / Klient czasu SNTP / DNS / 802.1Q / QoS * Trawersowanie NAT (Tryb STUN) * Obsługa SRTP / TLS * Kompatybilność SIP: SIP v1 (RFC2543) / v2 (RFC3261) * Szyfrowanie AES dla pliku konfiguracyjnego * Uwierzytelniane szyfrowanie * Konfiguracja z OpenVPN, IEEE802.1X * IPv6, LLDP/CDP/DHCP VLAN, ICE  1. **Parametry Audio:**  * Kodeki Audio: G.711 aLaw, G.711 μLaw / G.722 (szerokopasmowy) / G.726 / G.729 / iLBC * Eliminacja echa * Słuchawka kompatybilna z aparatami słuchowymi (HAC)  1. **Porty wyjścia:**  * Porty Ethernet: 2 x 1000 Mb/s * Słuchawka nagłowna 1 x RJ9 * Mikrofon 1 x RJ9 * 2 x USB port (2.0 compliant)  1. **Zasilanie:**  * Obsługa PoE (Power over Ethernet) zgodnie ze standardem IEEE 802.3 af klasy 3 * Sieciowe zasilacz DC 5V 2A (Opcjonalnie)  1. **Wymagania dodatkowe:**  * Pobór mocy przy pracy na zasilaczu nie więcej niż 3W. * Pobór mocy przy pracy poprzez POE, nie więcej niż 3.8W * Wilgotność dopuszczalna do poprawnej pracy aparatu 10 – 95 % Temperatura dopuszczalna do poprawnej pracy aparatu od 0 – 40 °C * Wymiary (szer. × gł. × wys.): 244× 213× 185 mm  1. **Fabrycznie nowy aparat telefoniczny, nieużywany w oryginalnym opakowaniu, pochodzący z bieżącej produkcji.** 2. **Gwarancja min. 24 miesiące.** |

* + 1. **Telefon IP Voip typu bezprzewodowy – 5 szt.**

|  |  |
| --- | --- |
| **Przedmiot**  **zamówienia** | **Wymagane przez Zamawiającego minimalne parametry techniczne aparatów telefonicznych do obsługi numerów VoIP** |
| Typ urządzenia | Bezprzewodowy telefon IP do komunikacji VoIP |
| Łączność bezprzewodowa | Wi-Fi w standardach IEEE 802.11 a/b/g/n/ac; obsługa pasm 2,4 GHz oraz 5 GHz |
| Obsługiwane konta | Minimum 2 niezależne konta SIP |
| Ekran | Kolorowy wyświetlacz LCD o przekątnej co najmniej 2,4 cala |
| Bateria | Wbudowana bateria zapewniająca minimum 40 godzin rozmów oraz minimum 400 godzin czuwania |
| Port ładowania | Złącze USB typu C umożliwiające ładowanie urządzenia |
| Klasa odporności | Obudowa o stopniu ochrony minimum IP65 (odporność na kurz i strumień wody) |
| Jakość dźwięku | Obsługa technologii HD Voice (dźwięk szerokopasmowy) |
| Funkcje dodatkowe | Wbudowana funkcja Push-to-Talk (PTT); przycisk alarmowy (panic button) |
| Głośnik | Wbudowany głośnik o podwyższonej głośności, umożliwiający pracę w środowiskach hałaśliwych |
| Zarządzanie urządzeniem | Możliwość zdalnego zarządzania i konfiguracji urządzenia za pomocą systemu Device Management System |
| Zasilanie | Możliwość ładowania poprzez port USB-C lub opcjonalną stację dokującą |
| Wsparcie dla systemów | Współpraca z serwerami telefonii IP kompatybilnymi z protokołem SIP |
| Wymagania certyfikacyjne | Urządzenie posiadające wymagane deklaracje zgodności CE lub równoważne |
| Warunki Gwarancyjne | Okres gwarancji: minimum 24 miesiące od daty dostawy. Warunki realizacji serwisu: naprawa lub wymiana urządzenia na nowe w przypadku wystąpienia wad fabrycznych. Czas reakcji serwisowej: maksymalnie 5 dni roboczych od momentu zgłoszenia usterki. Forma zgłoszenia awarii: zgłoszenia telefoniczne lub elektroniczne (e-mail, formularz online). Koszty napraw: wszelkie koszty transportu i naprawy w okresie gwarancyjnym po stronie Wykonawcy. |
| Uwagi dodatkowe | Dopuszczenie urządzeń równoważnych: Zamawiający dopuszcza składanie ofert na urządzenia równoważne, pod warunkiem zapewnienia parametrów technicznych, funkcjonalnych i użytkowych nie gorszych niż wskazane w niniejszym opisie przedmiotu zamówienia.  - Dostarczenie instrukcji: Wykonawca zobowiązany jest do dostarczenia wraz z urządzeniami instrukcji obsługi w języku polskim w wersji papierowej lub elektronicznej.  - Wymogi formalne: Wszystkie oferowane urządzenia muszą być fabrycznie nowe, wolne od wad fizycznych i prawnych oraz nieużywane przed dostawą do Zamawiającego. |

* 1. **Wymagania dotyczące subskrypcji oprogramowania biurowego – 40 szt.**

Przedmiotem zamówienia jest dostawa licencji oprogramowania Microsoft 365 A5 for faculty na okres 60 miesięcy subskrypcji pakietu usług hostowanych - subskrypcja na użytkownika (przypisanie dodatkowych licencji do obecnego konta zamawiającego).

Oprogramowanie musi pochodzić bezpośrednio od Producenta lub z oficjalnych i autoryzowanych przez Producenta kanałów dystrybucyjnych. Zamawiający wymaga, aby Wykonawca posiadał kwalifikacje i uprawnienia wymagane do prawidłowej realizacji przedmiotu zamówienia.

1. Licencje muszą pozwalać na swobodne przenoszenie pomiędzy komputerami (np. w przypadku wymiany sprzętu).
2. Gwarancja dostępności najnowszej wersji oprogramowania oraz bieżące jego poprawki i uaktualnienia w trakcie trwania umowy.
3. Możliwość wykorzystania wspólnych i jednolitych procedur masowej instalacji, uaktualniania, zarządzania, monitorowania i wsparcia technicznego.
4. Zamawiający dopuszcza oferowanie produktów o szerszej niż opisana funkcjonalności.
5. W ramach procedury odbiorczej Wykonawca w terminie wskazanym przez Zamawiającego zapewni dostęp do spersonalizowanej strony pozwalającej upoważnionym ze strony Zamawiającego osobom na:
   1. pobieranie oprogramowania,
   2. pobieranie kluczy aktywacyjnych do oprogramowania,
   3. sprawdzanie liczby zakupionych licencji w wykazie oprogramowania.

**Tabela warunków równoważności – Microsoft 365**

| **Obszar** | **Minimalny warunek** | **Równoważność** |
| --- | --- | --- |
| **Licencje** | Licencje Microsoft 365 w planie A5 (zgodnie z wymaganiami). | Oferowane rozwiązanie musi zapewniać funkcjonalność nie mniejszą niż odpowiadający plan Microsoft 365 A5. |
| **Poczta (Exchange)** | Skrzynki pocztowe użytkowników w Exchange Online, z obsługą kalendarzy i reguł. | System musi zapewniać pocztę, kalendarze i reguły transportowe co najmniej równoważne do Exchange Online |
| **Przechowywanie plików** | SharePoint Online i OneDrive for Business – współdzielenie, wersjonowanie, praca w czasie rzeczywistym. | Rozwiązanie musi umożliwiać współdzielenie i edycję plików online z mechanizmami kontroli wersji oraz możliwością edycji/pracy grupowej bezpośrednio w edytorze zainstalowanym na komputerze |
| **Komunikacja (Teams)** | Microsoft Teams – czat, wideokonferencje, współdzielenie ekranu, integracja z Office. | System komunikacyjny musi umożliwiać te same formy komunikacji i współpracy |
| **Bezpieczeństwo** | MFA, Conditional Access, szyfrowanie danych w spoczynku i transmisji, DLP. | Rozwiązanie musi posiadać mechanizmy ochrony danych i dostępów na poziomie nie niższym niż dla oprogramowania referencyjnego. |
| **Integracje** | Integracja z Azure AD i Intune, możliwość SSO i zarządzania urządzeniami. | Musi istnieć możliwość integracji z tożsamością i zarządzania urządzeniami na poziomie równoważnym. |
| **Zgodność** | Zgodność z RODO i normami branżowymi (ISO 27001, ISO 27018). | Rozwiązanie musi spełniać wymagania zgodności co najmniej na takim samym poziomie. |
| **SLA i dostępność** | Gwarancja dostępności usług zgodna z SLA Microsoft 365 (99,9%). | Dostępność usług nie może być niższa niż SLA Microsoft 365. |

* 1. **Wymagania dotyczące urządzenia typu tablet – 2 szt.**

Szczegółowe wymagania dotyczące tabletów multimedialnych oraz minimalne parametry techniczne zostały określone w tabeli poniżej i stanowią podstawę do wyceny przedmiotu zamówienia przez Oferentów:

|  |  |
| --- | --- |
| **Parametr** | **Wymagane minimalne parametry techniczne** |
| Typ urządzenia | Tablet multimedialny z wbudowanym modemem 5G |
| Ekran | Przekątna ekranu: minimum 10,9 cala; rozdzielczość minimum 2304×1440 pikseli; technologia: TFT lub AMOLED |
| Procesor | Ośmiordzeniowy procesor o częstotliwości co najmniej 2,0 GHz |
| Pamięć RAM | Minimum 8 GB RAM |
| Pamięć wewnętrzna | Minimum 128 GB pamięci wewnętrznej; możliwość rozszerzenia kartą microSD do 1 TB |
| Łączność | Obsługa 5G, 4G LTE, Wi-Fi 802.11 a/b/g/n/ac/ax (2,4 GHz i 5 GHz), Bluetooth min. 5.3 |
| System operacyjny | Android w najnowszej stabilnej wersji wspieranej przez producenta |
| Aparat | Tylny: minimum 8 MP; Przedni: minimum 12 MP |
| Złącza | Minimum jedno złącze USB typu C |
| Bateria | Pojemność minimum 8000 mAh; szybkie ładowanie minimum 25W |
| Funkcje dodatkowe | Obsługa rysika; rysik w zestawie |
| Funkcje zabezpieczeń | Czytnik linii papilarnych lub rozpoznawanie twarzy |
| Obudowa | Wytrzymała konstrukcja; minimalna odporność IP68 dla rysika |
| Waga | Maksymalnie 520 g |
| Akcesoria | Rysik w zestawie, kabel USB, ładowarka sieciowa  Dedykowane zamykane etui |
| Język | Menu urządzenia w języku polskim |
| Certyfikaty | Deklaracja zgodności CE |
| Warunki gwarancji | Urządzenia muszą być objęte gwarancją producenta lub dostawcy na okres minimum 24 miesięcy od daty dostawy. Serwis gwarancyjny realizowany w trybie door-to-door lub w autoryzowanym punkcie serwisowym. Czas naprawy: maksymalnie 14 dni kalendarzowych od zgłoszenia. Koszty serwisowe (transport, diagnostyka, naprawa) ponosi Wykonawca. Forma zgłoszenia awarii: telefonicznie lub elektronicznie. Trzecia poważna awaria w okresie gwarancji skutkuje wymianą urządzenia na nowe. |
| Uwagi dodatkowe | Zamawiający dopuszcza składanie ofert na urządzenia równoważne, spełniające wszystkie minimalne wymagania techniczne, funkcjonalne i użytkowe określone w opisie przedmiotu zamówienia.  Wraz z dostarczonym sprzętem należy dostarczyć instrukcję obsługi w języku polskim (papierową lub elektroniczną).  Urządzenia muszą być fabrycznie nowe, wolne od wad fizycznych i prawnych, nieużywane przed dostawą. |

1. **Wymagania w zakresie prac montażowo- instalacyjnych**

W ramach zamówienia Wykonawca zobowiązany jest do:

1. zamontowania i uruchomienia wszystkich dostarczonych rozwiązań we wskazanych przez Zamawiającego miejscach.
2. uruchomienia i skonfigurowania wszystkich dostarczonych rozwiązań, urządzeń i systemów w sposób umożliwiający rozpoczęcie ich wykorzystywania zgodnie z przeznaczeniem. Sposób konfiguracji zostanie ustalony w porozumieniu z Zamawiającym.
3. skonfigurowania wszystkich urządzeń sieciowych w sposób uzgodniony z Zamawiającym uwzględniając m.in. segmentacje sieci, oraz najlepsze praktyki w zakresie konfiguracji urządzeń sieciowych
4. skonfigurowania wszystkich urządzeń i systemów bezpieczeństwa IT w sposób uzgodniony z Zamawiającym uwzględniając m.in. najlepsze praktyki w zakresie konfiguracji urządzeń i systemów bezpieczeństwa IT.
5. skonfigurowania wszystkich urządzeń pamięci masowych w sposób uzgodniony z Zamawiającym uwzględniając m.in. konfigurację pól dyskowych, oraz najlepsze praktyki w zakresie konfiguracji urządzeń pamięci masowych
6. skonfigurowania wszystkich urządzeń serwerowych w sposób uzgodniony z Zamawiającym uwzględniając m.in. najlepsze praktyki w zakresie konfiguracji serwerów.
7. instalacji okablowania sieciowego niezbędnego do uzyskania pełnej funkcjonalności środowiska IT z uwzględnieniem redundancji połączeń, w sposób uzgodniony z Zamawiającym.
8. przeprowadzenia testów m.in. funkcjonalnych, wydajnościowych i redundancji wdrożonego środowiska uzgodnionych z Zamawiającym.

W trakcie prowadzenia prac montażowych Wykonawca jest zobowiązany do:

1. zorganizowania niezbędnego zaplecza technicznego,
2. skoordynowania wszystkich prac związanych z realizacją przedmiotu zamówienia w sposób umożliwiający pełną kontrolę ruchu osobowo-materiałowego na terenie serwerowni,
3. w przypadku wykonywaniu robót generujących drgania mogące mieć negatywny wpływ na infrastrukturę serwerowni, Wykonawca jest zobowiązany wykonywać prace z zastosowaniem odpowiedniego sprzętu, niewywołującego takich drgań,
4. dostawy w ramach wynagrodzenia z tytułu realizacji przedmiotu zamówienia wszystkich materiałów instalacyjnych niezbędnych do realizacji przedmiotu zamówienia zgodnie z wymaganiami Zamawiającego wskazanych w niniejszym Zapytaniu ofertowym,
5. prowadzenie prac z zachowaniem bezprzerwowej pracy pozostałych obwodów elektrycznych w obiekcie,
6. zorganizowania wywozu nieczystości,
7. zagospodarowania odpadów z godnie z Ustawą o odpadach,
8. dostarczenia atestów, certyfikatów i aprobat technicznych na wszystkie materiały użyte do budowy i wyposażenia obiektu jeszcze przed rozpoczęciem montażu,
9. przygotowania pełnej, aktualnej dokumentacji powykonawczej,
10. udziału w odbiorze.