**IF.272.19.2023**

**Załącznik nr 1 do SWZ- AKTUALNY**

**FORMULARZ SPECYFIKACJI TECHNICZNO-CENOWEJ**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Siedziba / miejsce prowadzenia działalności gospodarczej / miejsce zamieszkania: ¹   |  |  | | --- | --- | | Pełna nazwa (firma) Wykonawcy: |  |      |  |  |  | | --- | --- | --- | |  | | | | *NIP/PESEL, KRS/CEIDG:* |  | | | Reprezentowany przez: | | | | *imię i nazwisko, stanowisko:* | |  | | *podstawa do reprezentacji Wykonawcy:* | |  |     ¹niepotrzebne skreślić | Zamawiający  **Powiat Nowosolski**  **Ul. Moniuszki 3**  **67-100 Nowa Sól** |

dot. postępowania o udzielenie zamówienia publicznego w trybie podstawowym bez negocjacji, na podstawie art. 275 pkt 1 ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych, o udzielenie zamówienia publicznego   
o wartości nieprzekraczającej progów unijnych, o jakich stanowi art. 3 ustawy PZP, pod nazwą:

**Zakup sprzętu i oprogramowania w ramach realizacji projektu pn.:**

**„Cyfrowy Powiat”**

|  |  |  |  |
| --- | --- | --- | --- |
| Zawartość formularza: | | | Zamawiana ilość |
| 1 | TABELA A | Opis parametrów techniczno-użytkowych oraz zestawienie cen jednostkowych netto / brutto dla: Serwery | 2 szt. |
| 2 | TABELA B | Opis parametrów techniczno-użytkowych oraz zestawienie cen jednostkowych netto / brutto dla: Klaster UTM | 1 szt. |
| 4 | TABELA C | Opis parametrów techniczno-użytkowych oraz zestawienie cen jednostkowych netto / brutto dla: Serwer NAS | 1 szt. |
|  | TABELA D | Opis parametrów techniczno-użytkowych oraz zestawienie cen jednostkowych netto / brutto dla: Oprogramowanie do backupu | 1 szt. |
|  | TABELA E | Opis parametrów techniczno-użytkowych oraz zestawienie cen jednostkowych netto / brutto dla: Stacja robocza | 5 szt. |
|  | TABELA E1 | Opis parametrów techniczno-użytkowych oraz zestawienie cen jednostkowych netto / brutto dla: Monitor | 5 szt. |
| 5 | TABELA F | Zestawienie cen jednostkowych netto / brutto wraz z wartością brutto |  |

Instrukcja wypełniania:

Załącznik nr 2 należy wypełnić w całości – stanowi on integralną część oferty – deklarację wykonawcy, co do jej treści.

\* (jedna gwiazdka) W przypadku oferowania parametrów zgodnych z wymaganiami Zamawiającego – wykonawca może wpisać: „tak” lub „spełnia” lub „posiada”. W przypadku zaoferowania rozwiązań równoważnych należy je literalnie wskazać.

\*\* (dwie gwiazdki) należy literalnie opisać, wskazać nazwę, określenie lub wartość.

Oferuję dostawę przedmiotu zamówienia w pełnym zakresie, o zaoferowanych poniżej parametrach techniczno-użytkowych i po cenie:

Parametry techniczno-użytkowe oraz zestawienie cen jednostkowych netto / brutto:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| TABELA  A | | Serwery | | | | | | |
| Producent: | | | | \*\* | | |
| Nazwa, Model, Typ, Wersja: | | | | \*\* | | |
| Kod producenta (nr katalogowy): | | | | \*\* | | |
| 1 | 2 | | 3 | | | | 4 | |
| Lp. | ELEMENT / PARAMETR  / CECHA | | MINIMALNE WYMAGANE PARAMETRY TECHNICZNO-UŻYTKOWE | | | | PARAMETRY OFEROWANE PRZEZ  WYKONAWCĘ | |
| 1 | Obudowa | | Obudowa Rack o wysokości max 2U. Możliwość instalacji minimum 24 dysków 2.5”. Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.  Obudowa musi mieć możliwość wyposażenia w kartę umożliwiającą 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/ WIFI. | | | | \* | |
| 2 | Płyta główna | | Płyta główna z możliwością zainstalowania do dwóch procesorów 3rd Generacji Intel Xeon. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. | | | |  | |
| 3 | Chipset | | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych | | | |  | |
| 4 | Procesor | | Zainstalowany jeden procesor min. 8-rdzeniowy klasy x86, min. 2.8GHz, dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 131 w teście SPECrate2017\_int\_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej. | | | | Producent procesora: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\*\*  Pełna nazwa procesora i model: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\*\*  Wynik testu: \_\_\_\_\_\_\_\_\_\*\*pkt z dnia: \_\_\_\_\_\_\_\_\_\_\* | |
| 5 | RAM | | Minimum 256GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 32 sloty przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać do 8TB pamięci RAM. | | | | \*\* | |
| 6 | Funkcjonalność pamięci RAM | | Advanced ECC, Memory Page Retire, Fault Resilient Memory, Memory Self-Healing lub PPR, Partial Cache Line Sparing | | | | \* | |
| 7 | Gniazda PCI | | Min. 3 sloty PCIe generacji 4 | | | | \* | |
| 8 | Interfejsy sieciowe/FC/SAS | | Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 10Gb Ethernet w standardzie SFP+ (porty nie mogą zostać osiągnięte poprzez karty w slotach PCIe)  Dodatkowa, czteroportowa karta 1Gb Ethernet BaseT | | | | \* | |
| 9 | Dyski twarde | | Zainstalowane 4 dyski SSD vSAS/SAS o pojemności min. 960GB, 12Gb, Hot-Plug.  Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 240GB Hot-Plug z możliwością konfiguracji RAID 1.  Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde. | | | | \*\* | |
| 10 | Kontroler RAID | | Sprzętowy kontroler dyskowy, posiadający min. 4GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących. | | | | \* | |
| 11 | Wbudowane porty | | * 4x USB, w tym min. 1 porty USB 3.0 * 2x port VGA (jeden na panelu przednim) * Możliwość rozbudowy o Serial Port | | | | \* | |
| 12 | Video | | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024 | | | | Nazwa karty graficznej: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |
| 13 | Wentylatory | | Redundantne, Hot-Plug | | | | \* | |
| 14 | Zasilacze | | Redundantne, Hot-Plug min. 800W każdy. | | | | \* | |
| 15 | 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. * Moduł TPM 2.0 * 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 | | | | \* | |
| 16 | Diagnostyka | | Serwer wyposażony w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze. | | | | \* | |
| 16 | Karta Zarządzania | | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:   * zdalny dostęp do graficznego interfejsu Web karty zarządzającej; * zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); * 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 WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; * możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; * możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; * integracja z Active Directory; * możliwość obsługi przez dwóch administratorów jednocześnie; * wsparcie dla dynamic DNS; * wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. * możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera * możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera | | | | \* | |
| 17 | Oprogramowanie do zarządzania | | Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego 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 oparciu o wszystkie informacje zawarte w inwentarzu. * Grupowanie urządzeń w oparciu o kryteria użytkownika * Tworzenie automatycznie grup urządzeń w oparciu 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 alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. * Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. * Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu 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 zarządzającym. * Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V. | | | | \* | |
| 17 | Certyfikaty | | Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001  Serwer musi posiadać deklaracja CE.  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](http://www.epeat.net/) potwierdzający spełnienie normy co najmniej Epeat Bronze według normy wprowadzonej w 2019 roku - Wykonawca złoży dokument potwierdzający spełnianie wymogu.  Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server 2022. | | | | \* | |
| 18 | Dokumentacja użytkownika | | Zamawiający wymaga dokumentacji w języku polskim lub angi*e*lskim z tłumaczeniem na język polski.  Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. | | | | \* | |
| 19 | Warunki gwarancji | | 3 lata gwarancji producenta  Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.  Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.  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.  Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera.  Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii.  Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych.  Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.  Możliwość rozszerzenia gwarancji przez producenta do 7 lat.  Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.  Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. | | | | Podać numery telefonów oraz adres e-mail:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_ \*\*  \*Podać nazwę i adres oraz telefony kontaktowe:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_ \*\* | |
| zestawienie cen jednostkowych netto / brutto | | | | | | | | |
| Serwer | | | | Ilość  [szt.] | Cena jednostkowa  (za 1 szt.)  NETTO  obowiązująca przy zawarciu umowy  [zł] | | | Cena jednostkowa  (za 1 szt.)  BRUTTO  obowiązująca przy zawarciu umowy  [zł] |
|  | | | |  |  | | |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| TABELA  B | | Kaster UTM wraz ze szkoleniem dla administratora zamawiającego | | | |
| Producent: | | \*\* | |
| Nazwa, Model, Typ, Wersja: | | \*\* | |
| Kod producenta (nr katalogowy): | | \*\* | |
| 1 | 2 | | 3 | | 4 |
| Lp | ELEMENT / PARAMETR  / CECHA | | MINIMALNE WYMAGANE PARAMETRY TECHNICZNO-UŻYTKOWE | | PARAMETRY OFEROWANE PRZEZ  WYKONAWCĘ |
| 1 | Wymagania Ogólne | | System zbudowany z dwóch urządzeń fizycznych. System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.  System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.  System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.  System wspiera protokoły IPv4 oraz IPv6 w zakresie:   * Firewall. * Ochrony w warstwie aplikacji. * Protokołów routingu dynamicznego. | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* |
| 2 | Redundancja, monitoring i wykrywanie awarii | | * 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. * Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. * Monitoring stanu realizowanych połączeń VPN. * System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych. | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* |

|  |  |  |  |
| --- | --- | --- | --- |
| 3 | 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. * 2 gniazdami SFP+ 10 Gbps.  1. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 2. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q. 3. System jest wyposażony w zasilanie AC. | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* |
| 4 | Parametry wydajnościowe: | 1. W zakresie Firewall’a obsługa nie mniej niż 1.4 mln. jednoczesnych połączeń oraz 52 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.1 Gbps. 4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 11 Gbps. 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 2.5 Gbps. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps. | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* |
| 5 | Funkcje Systemu Bezpieczeństwa: | W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:   1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. 12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. 13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa). | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* |
| 6 | 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: kategorie 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. | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* |

|  |  |  |  |
| --- | --- | --- | --- |
| 7 | 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 Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0. * Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. * 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. | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* |
| 8 | 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, oznaczeń Type of Service w nagłówkach IP). 3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. 4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. 5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. 6. BFD (Bidirectional Forwarding Detection). 7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu. | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* |
| 9 | 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). | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* |
| 10 | 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. | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* |

|  |  |  |  |
| --- | --- | --- | --- |
| 11 | Ochrona przed malware | 1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. 3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości. 4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. 5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze. 8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. 9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. 10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu. | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* |

|  |  |  |  |
| --- | --- | --- | --- |
| 12 | 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. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. 4. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 5. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). 6. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http. 7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. 8. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie. | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* |
| 13 | Kontrola aplikacji | 1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 3. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 4. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. 5. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). 6. 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). | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* |
| 14 | 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. | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* |
| 15 | 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 dwuskładnikowego. 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. | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 16 | Zarządzanie | 1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. 3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. 5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. 8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). 9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP. | | |  | |
| 17 | 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. | | |  | |
| 18 | Certyfikaty | Poszczególne elementy systemu bezpieczeństwa posiadają następujące certyfikacje:   * ICSA lub EAL4 dla funkcji Firewall. | | |  | |
| 19 | Testy wydajnościowe oraz funkcjonalne | 1. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy. | | |  | |
| 20 | Gwarancja oraz wsparcie | 1. Gwarancja: System jest objęty serwisem gwarancyjnym producenta przez okres 36 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. | | |  | |
| 21 | Rozszerzone wsparcie | Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesięcy. | | |  | |
| 22 | Opisy do wymagań ogólnych | 1. Zaleca się, aby w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), został uzyskany 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 (Dz.U. z 2004, Nr 229, poz. 2315 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. Zaleca się, aby został uzyskany dokument - oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym. | | |  | |
| 23 | Zakres Szkolenia | Szkolenie w ośrodku szkoleniowym producenta lub dystrybutora  Metody zarządzania platformą  Omówienie interfejsu GUI  Omówienie interfejsu CLI  Zmiana hasła  Konfiguracja adresacji interfejsów  Konfiguracja routingu statycznego  Konfiguracja czasu oraz strefy czasowej na urządzeniu  Konfiguracja DNS dla systemu  Konfiguracja kont administracyjnych  Konfiguracja parametrów sesji administracyjnych  Konfiguracja polityki wyjścia do Internetu  Aktualizacja oprogramowania  Techniki balansowania  Konfiguracja VLAN-ów  Zmiana numeru VLAN na interface  Konfiguracja NAT  Backup Konfiguracji  Routing Dynamiczny,  Policy Based Routing (PBR)  IPSec VPN site-to-site  IPSec VPN client-to-site  Konfiguracja SSL VPN:  Webfiltering  White/Black listy  Komunikacja z Supportem producenta | | |  | |
| zestawienie cen jednostkowych netto / brutto | | | | | | |
| Kaster UTM | | | Ilość  [szt.] | Cena jednostkowa  (za 1 szt.)  NETTO  obowiązująca przy zawarciu umowy  [zł] | | Cena jednostkowa  (za 1 szt.)  BRUTTO  obowiązująca przy zawarciu umowy  [zł] |
|  | | |  |  | |  |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| TABELA  C | | Serwer NAS | | | | | | |  |
| Producent: | | | | \*\* | | |  |
| Nazwa, Model, Typ, Wersja: | | | | \*\* | | |  |
| Kod producenta (nr katalogowy): | | | | \*\* | | |  |
| 1 | 2 | | 3 | | | | 4 | |  |
| Lp | ELEMENT / PARAMETR  / CECHA | | MINIMALNE WYMAGANE PARAMETRY TECHNICZNO-UŻYTKOWE | | | | PARAMETRY OFEROWANE PRZEZ  WYKONAWCĘ | |  |
|  | Obudowa | | Obudowa Rack 1U | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | | |
|  | Procesor | | Czterordzeniowy procesor o taktowaniu 2,2 GHz osiągający w teście PassMark na sierpień 2023 co najmniej 4 500 punktów | | | | Producent procesora: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\*\*  Pełna nazwa procesora i model: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\*\*  Wynik testu: \_\_\_\_\_\_\_\_\_\*\*pkt z dnia: \_\_\_\_\_\_\_\_\_\_\* | | |
|  | Sprzętowy mechanizm szyfrowania | | Tak (AES-NI) | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | | |
|  | RAM | | min. 8 GB pamięci ECC SODIMM z możliwością rozszerzenia do min. 32 GB | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | | |
|  | Możliwości rozbudowy | | Sprzęt powinien być wyposażony w min. 4 kieszenie na dyski twarde typu hot-swap z możliwością rozszerzenia do 8 dysków łącznie przy użyciu dodatkowych jednostek rozszerzających podłączanych do jednostki głównej za pomocą portu eSATA. | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | | |
|  | Porty zewnętrzne | | Minimum:  • 2 porty USB 3.2.1  • 1 port eSATA (jako gniazdo rozszerzenia) | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | | |
|  | Porty sieciowe | | Minimum:  • 4 porty 1GbE RJ45 (z obsługą funkcji Link Aggregation / przełączania awaryjnego) | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | | |
|  | Funkcja Wake on LAN/WAN | | Tak | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | | |
|  | Gniazdo rozszerzeń PCIe 2.0 | | Min. 1x 4-liniowe gniazdo x8 gen. 3 | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | | |
|  | Wentylator obudowy | | Min. 2 wentylatory (40 × 40 × 20 mm) | | | | * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | | |
|  | Obsługiwane protokoły sieciowe | | Min. SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS Kerberized sessions, iSCSI, HTTP, HTTPs, FTP, SNMP, LDAP, CalDAV | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | | |
|  | Obsługiwane systemy plików | | Min.:  • Wewnętrzny: Btrfs, ext4  • Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | | |
|  | Zarządzanie pamięcią masową | | Zainstalowane min. 4 dyski min. 8TB  • Maksymalny rozmiar pojedynczego wolumenu: 108 TB  • Minimalny liczba wewnętrznych wolumenów: 64  • Minimalny liczba obiektów iSCSI Target: 128  • Minimalny liczba jednostek iSCSI LUN: 256  • Obsługa klonowania/migawek jednostek iSCSI LUN | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | | |
|  | Obsługiwane typy macierzy RAID | | * Min. SHR, Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10 | | | | * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | | |
|  | Funkcja udostępniania plików | | Minimalna liczba kont użytkowników: 2 048  • Minimalna liczba grup użytkowników: 256  • Minimalna liczba folderów współdzielonych: 512  • Minimalna liczba jednoczesnych połączeń CIFS/AFP/NFS/FTP: 500\*  *\*Liczba jednoczesnych połączeń może zostać zwiększona do 2 000 po zainstalowaniu co najmniej 8 GB pamięci RAM.* | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | | |
|  | Uprawnienia | | * Uprawnienia listy kontroli dostępu systemu Windows® (ACL) i aplikacji | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | | |
|  | Wirtualizacja | | * Obsługa VMware vSphere with VAAI, Microsoft Hyper-V®, Citrix®, OpenStack® | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | | |
| Serwer NAS | | | | Ilość  [szt.] | Cena jednostkowa  (za 1 szt.)  NETTO  obowiązująca przy zawarciu umowy  [zł] | | | Cena jednostkowa  (za 1 szt.)  BRUTTO  obowiązująca przy zawarciu umowy  [zł] |  |
|  | | | |  |  | | |  |  |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| TABELA  D | | Oprogramowanie do Backupu | | | | | | | |
| Producent: | | | | \*\* | | | |
| Nazwa, Model, Typ, Wersja: | | | | \*\* | | | |
| Kod producenta (nr katalogowy): | | | | \*\* | | | |
| 1 | 2 | | 3 | | | | 4 | | |
| Lp | ELEMENT / PARAMETR  / CECHA | | MINIMALNE WYMAGANE PARAMETRY TECHNICZNO-UŻYTKOWE | | | | PARAMETRY OFEROWANE PRZEZ  WYKONAWCĘ | | |
| 1 |  | | Rozwiązanie musi zapewniać wsparcie backupu dla następujących platform wirtualizacyjnych, środowisk chmurowych i maszyn fizycznych, przy czym obsługa poszczególnych z nich może być uwarunkowana wybranym typem licencji | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| Microsoft Server z rolą Hyper-V min. w wersjach 2022, 2019, 2016, 2012R2, 2012 | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| Vmware vSphere min. w wersjach v5.5-7.0.3 | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| Nutanix AHV 5.15, 5.20 (LTS) | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| Maszyny fizyczne: Windows Server 2022, 2019, 2016, 2012R2, 2012 | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| Microsoft 365 (Exchange online, One Drive for Business, Sharepoint) | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| Oprogramowanie musi wspierać wszystkie systemy operacyjne gościa, które są obsługiwane przez natywny backup środowisk VMware vSphere, MS Hyper-V | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| Oprogramowanie musi być niezależne sprzętowo i posiadać możliwość uruchomienia: | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| na serwerze Windows lub Linux | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| jako maszyna wirtualna Vmware | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| jako maszyna wirtualna Amazon | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| na serwerze NAS: ASUSTOR, NETGEAR, QNAP, Synology i Western Digital | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| Oprogramowanie do backupu musi pozwalać na wykorzystanie dowolnego serwera oraz przestrzeni dyskowej (nie dedykowanych), za pośrednictwem protokołów CIFS lub NFS | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| Oprogramowanie nie może wymagać instalacji dedykowanego agenta wewnątrz maszyny wirtualnej w celach backupu/przywracania | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| Oprogramowanie nie może wymagać dodatkowej instalacji zewnętrznych aplikacji lub baz danych (jeżeli oprogramowanie wymaga bazy danych musi ona być instalowana automatycznie z paczki opracowanej przez producenta i nie wymagać dodatkowych licencji). | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| 2 | Licencjonowanie | | Wszystkie funkcje i komponenty oprogramowania dla środowisk Vmware i Hyper-V powinny być licencjonowane per gniazdo procesora w hostach wirtualizacyjnych służących za źródło backupu lub replikacji. Licencjonowanie powinno być realizowane w wariancie wieczystym, w którym licencja nie ma terminu ważności | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| Dopuszczalne jest dostarczenie oprogramowania w wersji umożliwiającej ograniczoną rozbudowę środowiska, wersja ta powinna jednak umożliwiać rozbudowę do nie mniej niż 6 gniazd procesorów w obrębie środowiska | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| W ramach dostarczonej licencji na określoną ilość gniazd procesorów wymagane jest zapewnienie 1 roku wsparcia technicznego producenta, zapewniającego dostęp do aktualizacji i poprawek oprogramowania oraz umożliwiającego kontakt z działem technicznym producenta w zakresie oferowanego oprogramowania | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| W ramach dostawy wymagane jest dostarczenie licencji na ochronę 4 gniazd procesorów w hostach Vmware lub Hyper-V | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| Licencjonowanie innych środowisk może być realizowane na zasadzie wymagającej zakupu dedykowanej licencji dla środowiska | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| 3 | Ochrona danych | | Oprogramowanie musi posiadać funkcje backupu i replikacji: | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| Backup maszyn wirtualnych Vmware | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| Replikacja maszyn wirtualnych Vmware (tworzenie I aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych). Replikacja nie może wymagać utworzenia backupu | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| Backup maszyn wirtualnych Hyper-V | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| Replikacja maszyn wirtualnych Hyper-V (tworzenie I aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych). Replikacja nie może wymagać utworzenia backupu | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| Możliwość przesłania pierwszych kopii za pośrednictwem dysków zewnętrznych do lokalizacji docelowej oraz późniejsze wznowienie ochrony maszyn wirtualnych | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| Możliwość określania pasma wykorzystywanego przez oprogramowanie do backupu globalnie lub per zadanie | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| Możliwość tworzenia do 1000 punktów przywracania dla każdej z maszyn wirtualnych w ramach zadania backupu | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| Obsługa retencji zgodnie z zasadą Grandfather-father-son – oprogramowanie musi pozwalać na rotację punktów przywracania w trybie dziennym, tygodniowym, miesięcznym oraz rocznym | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| Kopia backupu (replikacja) do innych repozytoriów backupu lokalnych oraz zdalnych  Oprogramowanie musi pozwalać na utworzenie kopii źródłowego repozytorium backupu oraz tylko wybranych backupów. Kopia tworzona jest zgodnie z określonym harmonogramem | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| Oprogramowanie musi pozwalać na określenie kolejności, w jakiej są backupowane lub replikowane maszyny wirtualne w ramach zadania | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| 4 | Optymalizacja wykorzystania miejsca na dane | | Oprogramowanie musi posiadać poniższe funkcje pozwalające na ograniczenie wielkości backupowanych danych: | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| Deduplikacja backupu, która działa w ramach całego repozytorium backupu oraz obejmuje wszystkie dane, które są w tym repozytorium przechowywane | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| Kompresja backupu, w tym konfigurowalny stopień kompresji | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| Automatyczne pomijanie plików i partycji wymiany w systemach Windows i Linux działających jako maszyny wirtualne | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| 5 | Przywracanie danych | | Oprogramowanie musi posiadać poniższe funkcje: | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| Przywracanie pełnych maszyn wirtualnych z backupu do oryginalnego lub innego serwera wirtualizacji | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| Uruchomienie maszyny wirtualnej bezpośrednio z plików backupu w środowisku VMware (bez wcześniejszego przywracania maszyny wirtualnej) | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| Przywracanie pojedynczych plików czy folderów bezpośrednio z plików backupu (bez wcześniejszego przywracania całej maszyny wirtualnej) | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| Przywracanie pojedynczych obiektów z poniższych aplikacji, bezpośrednio z plików backupu (bez wcześniejszego przywracania całej maszyny wirtualnej z backupu czy rozpakowywania plików backupu): | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| Microsoft Exchange | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| Active Directory | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| MS SQL | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| Migracja dysków maszyn wirtualnych pomiędzy środowiskami wirtualizacji Vmware i Hyper-V i odwrotnie. | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| 6 | Wydajność | | Oprogramowanie do backupu musi pozwalać na: | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| Tworzenie backupu I replik przyrostowo przy wykorzystaniu VMware CBT oraz Hyper-V RCT | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| Wykonywanie backupów przyrostowych bez wymogu okresowego tworzenia kopii pełnych | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| Backup z pominięciem sieci lan dzięki opcjom dostępu bezpośredniego w sieciach SAN | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| Akcelerację sieciową umożliwiającą redukcję ilości danych przesyłanych w sieci | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| 7 | Zarządzanie | | Oprogramowanie musi pozwalać na następujące formy zarządzania: | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| Być wyposażone w interfejs web do zarządzania wszystkimi aspektami związanymi z backupem i przywracaniem danych | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| Umożliwiać wysyłanie powiadomień w formie email dotyczących wykonywanych zadań backupu, błędów, cyklicznych raportów oraz wiadomości email z załącznikami potwierdzającymi poprawność odtworzenia maszyn wirtualnych dla wybranych zadań w formie zrzutów ekranu z uruchomionej z backupu maszyny wirtualnej | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| Zadanie backupu musi mieć możliwość uruchamiania zgodnie z harmonogramem, z opcją dodawania wielu harmonogramów dla pojedynczego zadania | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| Pliki backupu muszą mieć możliwość eksportu z opcją wyboru rodzaju dysków do których będzie robiony eksport. | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| Oprogramowanie musi pozwalać na eksportowanie oraz importowanie konfiguracji na cele reinstalacji czy migracji | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| zestawienie cen jednostkowych netto / brutto | | | | | | | | | |
| Oprogramowanie do backupu | | | | Ilość  [szt.] | Cena jednostkowa  (za 1 szt.)  NETTO  obowiązująca przy zawarciu umowy  [zł] | | | Cena jednostkowa  (za 1 szt.)  BRUTTO  obowiązująca przy zawarciu umowy  [zł] | |
|  | | | |  |  | | |  | |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| TABELA  E | | Stacja robocza wraz z monitorem | | | | | | | |
| Producent: | | | | \*\* | | | |
| Nazwa, Model, Typ, Wersja: | | | | \*\* | | | |
| Kod producenta (nr katalogowy): | | | | \*\* | | | |
| 1 | 2 | | 3 | | | | 4 | |  |
| Lp | ELEMENT / PARAMETR  / CECHA | | MINIMALNE WYMAGANE PARAMETRY TECHNICZNO-UŻYTKOWE | | | | PARAMETRY OFEROWANE PRZEZ  WYKONAWCĘ | |  |
|  | Typ | | Komputer stacjonarny. W ofercie wymagane jest podanie modelu, symbolu oraz producenta. | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
|  | Zastosowanie | | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna. | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
|  | Procesor | | Procesor dedykowany do pracy w komputerach stacjonarnych. Procesor osiągający w teście Passmark CPU Mark, w kategorii Average CPU Mark wynik co najmniej .32450 pkt. według wyników opublikowanych na stronie <http://www.cpubenchmark.net/cpu_list.php> na dzień 20.07.2023r. | | | | Producent procesora: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\*\*  Pełna nazwa procesora i model: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\*\*  Wynik testu: \_\_\_\_\_\_\_\_\_\*\*pkt z dnia: \_\_\_\_\_\_\_\_\_\_\* | |  |
|  | Pamięć RAM | | 8GB DDR4 3200MHz. Możliwość rozbudowy do min 64GB, minimum jeden slot DIMM wolny. | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
|  | Pamięć masowa | | Min. 256GB SSD PCIe NVMe Obudowa musi umożliwać montaż dodatkowego dysku 2.5” lub 3.5”. | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
|  | Karta graficzna | | Zintegrowana z procesorem | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
|  | Wyposażenie multimedialne | | Karta dźwiękowa min. dwukanałowa zintegrowana z płytą główną, zgodna z High Definition, wewnętrzny głośnik 2W w obudowie komputera. Port słuchawek i mikrofonu na przednim panelu, dopuszcza się rozwiązanie port combo. | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
|  | Obudowa | | Typu Small Form Factor z obsługą kart wyłącznie o niskim profilu. Umożliwiająca montaż 1 x dysku 3.5” lub 1 x dysku 2.5” wewnątrz obudowy. Obudowa fabrycznie przystosowana do pracy w orientacji poziomej i pionowej. Otwory wentylacyjne usytuowane wyłącznie na przednim oraz tylnym panelu obudowy. Suma wymiarów obudowy nieprzekraczająca 680 mm.  Zasilacz o mocy min. 180W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 85% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności min. 82% przy obciążeniu zasilacza na poziomie 100%. Zasilacz w oferowanym komputerze musi się znajdować na stronie <http://www.plugloadsolutions.com/80pluspowersupplies.aspx>, do oferty należy dołączyć wydruk potwierdzający spełnienie wymogu 80plus.  Moduł konstrukcji obudowy w jednostce centralnej komputera powinien pozwalać na demontaż kart rozszerzeń bez konieczności użycia narzędzi (wyklucza się użycia wkrętów, śrub motylkowych). Obudowa w jednostce centralnej musi być otwierana bez konieczności użycia narzędzi (wyklucza się użycie standardowych wkrętów, śrub motylkowych) oraz posiadać czujnik otwarcia obudowy współpracujący z oprogramowaniem zarządzająco – diagnostycznym. Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej oraz kłódki (oczko w obudowie do założenia kłódki). Wbudowany wizualny system diagnostyczny oparty o sygnalizację LED np. włącznik POWER, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, sygnalizacja oparta na zmianie statusów diody LED (zmiana barw oraz miganie). System usytuowany na przednim panelu. System diagnostyczny musi sygnalizować: uszkodzenie lub brak pamięci RAM, uszkodzenie płyty głównej, awarię BIOS’u, awarię procesora. Oferowany system diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów na płycie głównej, wymaganych wnęk zewnętrznych w specyfikacji i dodatkowych oferowanych przez wykonawcę, oraz nie może być uzyskany przez konwertowanie, przerabianie innych złączy na płycie głównej nie wymienionych w specyfikacji a które nie są dedykowane dla systemu diagnostycznego. Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, oraz musi być wpisany na stałe w BIOS. | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
|  | Bezpieczeństwo | | Ukryty w laminacie płyty głównej układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Próba usunięcia dedykowanego układu doprowadzi do uszkodzenia całej płyty głównej. System diagnostyczny z graficznym interfejsem użytkownika zaszyty w tej samej pamięci flash co BIOS, dostępny z poziomu szybkiego menu boot lub BIOS, umożliwiający przetestowanie komputera a w szczególności jego składowych. System zapewniający pełną funkcjonalność, a także zachowujący interfejs graficzny nawet w przypadku braku dysku twardego oraz jego uszkodzenia, nie wymagający stosowania zewnętrznych nośników pamięci masowej oraz dostępu do internetu i sieci lokalnej.  Procedura POST traktowana jest jako oddzielna funkcjonalność. | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
|  | BIOS | | BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera lub nazwę modelu oferowanego komputera. Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy. BIOS wyposażony w automatyczną detekcję zmiany konfiguracji, automatycznie nanoszący zmiany w konfiguracji w szczególności: procesor, wielkość pamięci, pojemność dysku. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania (w tym również systemu diagnostycznego) i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: wersji BIOS, nr seryjnym komputera, ilości zainstalowanej pamięci RAM, prędkości zainstalowanych pamięci RAM, technologii wykonania pamięci, sposobie obsadzeniu slotów pamięci z rozbiciem na wielkości pamięci i banki, typie zainstalowanego procesora, ilości rdzeni zainstalowanego procesora, typowej prędkości zainstalowanego procesora, minimalnej i maksymalnej osiąganej prędkości zainstalowanego procesora, pojemności zainstalowanego lub zainstalowanych dysków twardych, wszystkich urządzeniach podpiętych do dostępnych na płycie głównej portów SATA, MAC adresie zintegrowanej karty sieciowej, zintegrowanym układzie graficznym, kontrolerze audio.  Do odczytu wskazanych informacji nie mogą być stosowane rozwiązania oparte o pamięć masową (wewnętrzną lub zewnętrzną), zaimplementowane poza systemem BIOS narzędzia, np. system diagnostyczny, dodatkowe oprogramowanie.  Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń, możliwość ustawienia hasła użytkownika umożliwiającego uruchomienie komputera (zabezpieczenie przed nieautoryzowanym uruchomieniem) przy jednoczesnym zdefiniowanym haśle administratora. Użytkownik po wpisaniu swojego hasła jest wstanie zidentyfikować ustawienia BIOS. Możliwość ustawienia haseł użytkownika i administratora składających się z cyfr, małych liter, dużych liter oraz znaków specjalnych. Możliwość włączenia/wyłączenia kontrolera SATA (w tym w szczególności pojedynczo), Możliwość ustawienia portów USB w trybie „no BOOT” (podczas startu komputer nie wykrywa urządzeń bootujących typu USB). Możliwość wyłączania portów USB pojedynczo.  Możliwość dokonywania backup’u BIOS wraz z ustawieniami na dysku wewnętrznym. Oferowany BIOS musi posiadać poza swoją wewnętrzną strukturą menu szybkiego boot’owania które umożliwia m.in.: uruchamianie systemu zainstalowanego na dysku twardym, uruchamianie systemu z urządzeń zewnętrznych, uruchamianie systemu z serwera za pośrednictwem zintegrowanej karty sieciowej, uruchomienie graficznego systemu diagnostycznego, wejście do BIOS, upgrade BIOS. | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
|  | Wirtualizacja | | Sprzętowe wsparcie technologi wirtualizacji realizowane łącznie w procesorze, chipsecie płyty główej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu). | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
|  | System operacyjny | | Zainstalowany system operacyjny Windows 11 Professional, musi być zapisany trwale w BIOS i umożliwiać reinstalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego. | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
|  | Certyfikaty i standardy | | Certyfikat ISO9001 oraz ISO 50001 dla producenta sprzętu (załączyć dokument potwierdzający spełnianie wymogu)  Deklaracja zgodności CE (załączyć do oferty)  Certyfikat EPEAT Gold dla Polski – do oferty należy załączyć wydruk ze strony <https://epeat.net/>  Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych”, pkt. 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gram. | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
|  | Wymagania dodatkowe | | Wymagane porty; porty video wlutowane i wyprowadzone bezpośrednio z płyty głównej: 2 x HDMI 1.4, 1 x DisplayPort 1.4a, 8 portów USB wyprowadzonych na zewnątrz obudowy, na panelu przednim 2 x USB 3.2 gen 1 Typu A oraz 2 x USB 2.0, na panelu tylnym 2 x USB 3.2 gen 1 Typu A oraz 2 x USB 2.0,  Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) wszystkich portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek lub przewodów połączeniowych itp. Zainstalowane porty wlutowane w płytę główną i bezpośrednio wyprowadzone na panel przedni i tylny obudowy, dodatkowo nie mogą blokować instalacji kart rozszerzeń w złączach wymaganych w opisie płyty głównej.  Karta sieciowa 10/100/1000 zintegrowana z płytą główną, wspierająca obsługęWoL (funkcja włączana przez użytkownika),  Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona na etapie produkcji logiem producenta oferowanej jednostki, dedykowana dla danego urządzenia, wyposażona w: 1 x PCIe x16 Gen.3, 1 x PCIe x1, 2 x DIMM z obsługą do 64 GB DDR4 RAM, 2 x SATA w tym min. 1 szt SATA 3.0., Jedno złącze M.2 dla dysków oraz złącze M.2 bezprzewodowej karty sieciowej.  Klawiatura USB w układzie polski programisty  Mysz optyczna USB  Opakowanie musi być wykonane z materiałów podlegających powtórnemu przetworzeniu. | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
|  | Ergonomia | | Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji obserwatora w trybie IDLE wynosząca maksymalnie 25dB (załączyć oświadczenie producenta). | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
|  | Warunki gwaranc wsparcie techniczne producenta ji i | | 3-letnia gwarancja producenta świadczona na miejscu u klienta  Czas reakcji serwisu - do końca następnego dnia roboczego  Firma serwisująca musi posiadać ISO 9001: 2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty.  Oświadczenie producenta komputera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem  W przypadku awarii dysk twardy zostaje u Zamawiającego – do oferty załączyć oświadczenie podmiotu realizującego serwis lub producenta o spełnieniu tego warunku  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)  Zamawiający wymaga narzędzia do zarządzania zgłoszeniami serwisowymi samodzielnie przez portal internetowy lub inne narzędzie nie wymagające działań po stronie dostawcy. Narzędzie powinno umożliwiać:  - samodzielne wystawianie zgłoszeń serwisowych, śledzenie stanu zgłoszenia, komunikację z serwisem producenta przez edycję zlecenia i stanu zlecenia  - dostęp do materiałów serwisowych - co najmniej podręczników serwisowych i not serwisowych  - dostęp do materiałów szkoleniowych  - możliwości dodawania plików do otwieranego lub otwartego zlecenia (zdjęcia uszkodzeń, opisy etc.)  - śledzenie historii zleceń - raporty ze zleceń, historia - dla poszczególnych zleceń lub dla poszczególnych komputerów  - możliwość samodzielnego zarządzania wysyłką części (decyzja o zamówieniu części zamiennych i diagnostyka po stronie zamawiającego)  - możliwość rejestrowania i zarządzania zdarzeniami serwisowymi - agregowania zdarzeń z oprogramowania zarządzającego dostarczonego przez producenta, możliwość konwertowania zdarzeń na zgłoszenia serwisowe do producenta - z poziomu narzędzia.  - możliwość spięcia systemu serwisowego producenta z systemem helpdesk zamawiającego (dostępność API co najmniej dla opcji wystawienie zlecenia, sprawdzenie stanu zlecenia, raport zleceń)  - tworzenia kont dla inżynierów serwisu z możliwością sprawdzenia statystyk wydajności / jakości ich pracy. | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
|  | Dodatkowe oprogramowanie | | Oprogramowanie zarządzającego produkowanego przez producenta i instalowanego przez producenta na etapie produkcji komputera. Program ma umożliwiać przynajmniej:  - monitorowanie komputera i generowanie zgłoszeń o błędach / nieprawidłowym działaniu w zakresie pracy komponentów i wydajności systemów  - powiadamiania o nowych wersjach sterowników i umożliwienie użytkownikowi wykonania upgrade systemu  - powiadamianie o problemach wydajnościowych i diagnozowanie / rozwiązywanie takich problemów  - śledzenia kluczowych komponentów i przewidywanie awarii przed ich wystąpieniem.  Oprogramowanie producenta komputera z nieograniczoną licencją czasowo na użytkowanie umożliwiające:   * upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS’u z certyfikatem zgodności producenta do najnowszej dostępnej wersji, * możliwość przed instalacją sprawdzenia każdego sterownika, każdej aplikacji, BIOS’u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji o:   + poprawkach i usprawnieniach dotyczących aktualizacji   + dacie wydania ostatniej aktualizacji   + priorytecie aktualizacji   + zgodności z systemami operacyjnymi   + jakiego komponentu sprzętu dotyczy aktualizacja   + wszystkich poprzednich aktualizacjach z informacjami jak powyżej. * 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. | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |  |
| zestawienie cen jednostkowych netto / brutto | | | | | | | | | |
| Stacja robocza | | | | Ilość  [szt.] | Cena jednostkowa  (za 1 szt.)  NETTO  obowiązująca przy zawarciu umowy  [zł] | | | Cena jednostkowa  (za 1 szt.)  BRUTTO  obowiązująca przy zawarciu umowy  [zł] | |
|  |  | | |  | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| TABELA  E1 | | Monitor | | | | | | |
| Producent: | | | | \*\* | | |
| Nazwa, Model, Typ, Wersja: | | | | \*\* | | |
| Kod producenta (nr katalogowy): | | | | \*\* | | |
| 1 | 2 | | 3 | | | | 4 | |
| Lp | ELEMENT / PARAMETR  / CECHA | | MINIMALNE WYMAGANE PARAMETRY TECHNICZNO-UŻYTKOWE | | | | PARAMETRY OFEROWANE PRZEZ  WYKONAWCĘ | |
| 1 | Typ ekranu | | Ekran ciekłokrystaliczny z aktywną matrycą IPS 24” | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |
| 2 | Rozmiar plamki (maksymalnie) | | 0,27 mm x 0,27 mm | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |
| 3 | Jasność | | 300 cd/m2 | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |
| 4 | Kontrast | | 1000:1 | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |
| 5 | Kąty widzenia (pion/poziom) | | 178/178 stopni | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |
| 6 | Czas reakcji matrycy  (maksymalnie) | | 8ms | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |
| 7 | Rozdzielczość maksymalna | | 1920 x 1200 przy 60Hz | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |
| 8 | Gama koloru | | min. 99% sRGB | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |
| 9 | Częstotliwość odświeżania poziomego | | 30 – 83 kHz | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |
| 10 | Częstotliwość odświeżania pionowego | | 56 – 76 Hz | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |
| 11 | Pochylenie monitora | | W zakresie 26 stopni | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |
| 12 | Wydłużenie w pionie | | Tak, min 150 mm | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |
| 13 | PIVOT | | Tak | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |
| 14 | Obrót lewo/prawo | | Min. 90 stopni | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |
| 15 | Powłoka powierzchni ekranu | | Antyodblaskowa | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |
| 16 | Podświetlenie | | System podświetlenia LED | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |
| 17 | Zużycie energii | | Maksymalne 48W, czuwanie mniej niż 0,3W | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |
| 18 | Bezpieczeństwo | | Monitor musi być wyposażony dedykowany slot na linkę zabezpieczającą | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |
| 19 | Waga bez podstawy | | Maksymalnie 3,6kg | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |
| 20 | Złącze | | 1x HDMI (v1.4),  1x DisplayPort (v1.2)  1x DVI  1x VGA  4 x USB 3.2 | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |
| 21 | Gwarancja | | 3 letnia gwarancja producenta świadczona na miesjcu u klienta, możliwość zgłaszania awarii przez ogólnopolską linię telefoniczną oraz stronę internetową producenta  Czas reakcji serwisu - do końca następnego dnia roboczego  Firma serwisująca musi posiadać ISO 9001:20015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta – dokumenty potwierdzające załączyć do oferty.  Oświadczenie producenta, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie zobowiązania związane z serwisem zgodnie z udzielonym wsparciem.  Gwarancja zero martwych pikseli | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |
| 22 | Certyfikaty | | EPEAT Gold dla Polski  Energy Star  Monitor musi się znajdować na stronie TCO :  http://tcocertified.com/product-finder/ | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |
| 23 | Inne | | Podstawa odłączana bez użycia narzędzi  VESA 100mm.  Możliwość podłączenia dedykowanych głośników producenta monitora lub głosniki wbudowane | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\* | |
| zestawienie cen jednostkowych netto / brutto | | | | | | | | |
| Monitor | | | | Ilość  [szt.] | Cena jednostkowa  (za 1 szt.)  NETTO  obowiązująca przy zawarciu umowy  [zł] | | | Cena jednostkowa  (za 1 szt.)  BRUTTO  obowiązująca przy zawarciu umowy  [zł] |
|  |  | | |  |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| TABELA  F | | | Zestawienie cen jednostkowych netto / brutto wraz z wartością brutto (ceną ofertową): | | | | | | |
| a | b | | | c | d | e | f | | g |
| kol. d x kol. f |
| L.p. | Wyszczególnienie | | | J.m. | Ilość | Cena jednostkowa  (za 1 szt.) NETTO  obowiązująca przy zawarciu umowy  [zł] | Cena jednostkowa (za 1 szt.)  BRUTTO  obowiązująca przy zawarciu umowy  [zł] | | Wartość BRUTTO  obowiązująca przy zawarciu umowy  [zł] |
| 1. | Dane z Tabeli A | | | szt. | 2 |  |  | |  |
| RAZEM Tabela A: | | |
| 2. | Dane z Tabeli B | | | szt. | 1 |  |  | |  |
| RAZEM Tabela B: | | |
| 3. | | Dane z Tabeli C | | szt. | 1 |  |  | |  |
| RAZEM Tabela C: | | |
| 4. | | Dane z Tabeli D | | szt. | 1 |  | |  |  |
| RAZEM Tabela D: | | |
| 5. | | Dane z Tabeli E | | szt. | 5 |  | |  |  |
| RAZEM Tabela E: | | |
| 6. | | Dane z Tabeli E1 | | szt. | 5 |  | |  |  |
| RAZEM Tabela E1: | | |
| RAZEM WARTOŚĆ BRUTTO (CENA OFERTOWA): | | | | | | | | |  |