*Załącznik nr 5 do SWZ – opis/specyfikacja przedmiotu zamówienia*

**Wykonawca:**

*(pełna nazwa/firma)*

*(adres)*

w zależności od podmiotu: NIP/PESEL

REGON

*(KRS/CEiDG)*

reprezentowany przez:

*(imię, nazwisko)*

*(stanowisko/podstawa do reprezentacji)*

**Specyfikacja przedmiotu Zamówienia**

Nr postępowania: IR.272.2.**43**.2025

Dotyczy zamówienia pn.: **Dostawa sprzętu komputerowego, sieciowego z wdrożeniem oraz podniesieniem poziomu bezpieczeństwa dla Urzędu Gminy w Skrzyszowie oraz jednostki Centrum Usług Społecznych w Skrzyszowie w związku z realizacją projektu „Cyberbezpieczny Samorząd”**

**UWAGA:** niniejszy załącznik należy uzupełnić o ceny jednostkowe poszczególnych elementów dostawy oraz informację o spełnieniu/niespełnieniu minimalnych parametrów.

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Wymagane minimalne parametry** | **Oferowane parametry** | **Spełnie/ niespełnia minimalne parametry**  \*WŁAŚCIWE PODKREŚLIĆ |
| **1.** | **DOSTAWA SPRZĘTU I OPROGRAMOWANIA NA POTRZEBY URZĘDU GMINY SKRZYSZÓW ORAZ CENTRUM USŁUG SPOŁECZNYCH W SKRZYSZOWIE** | | |
|  | **Przełączniki Sieciowe Zarządzalne –**  **Urząd Gminy w Skrzyszowie (5 szt.),**  **Centrum usług Społecznych w Skrzyszowie (2 szt.) fabrycznie nowe urządzenia/** | |  |
| **Cena jednostkowa:**  **brutto zł za sztukę** | |  |
|  | Marka/Model przełącznika |  | TAK/NIE\* |
|  | Przełącznik dostępowy gigabitowy |  | TAK/NIE\* |
|  | Porty przełącznika: minimum 24x 10/100/1000Base-T RJ45 oraz minimum 4x 1/10GBase-X SFP+ |  | TAK/NIE\* |
|  | Port konsolowy: RJ45 (RS-232) |  | TAK/NIE\* |
|  | Port USB: minimum 1 port co najmniej w standardzie 2.0 |  | TAK/NIE\* |
|  | Szybkość przełączania: minimum 128Gb/s |  | TAK/NIE\* |
|  | Przepustowość: minimum 95Mp/s (dla pakietów 64Kb) |  | TAK/NIE\* |
|  | Bufor pakietów: minimum 1,5MB |  | TAK/NIE\* |
|  | Ramki Jumbo: minimum 10k |  | TAK/NIE\* |
|  | Tablica adresów MAC: minimum 16k |  | TAK/NIE\* |
|  | Adresy MAC – Multicast: minimum 4k |  | TAK/NIE\* |
|  | Tablica ACL: minimum 512 |  | TAK/NIE\* |
|  | Tablica VLAN: minimum 4k |  | TAK/NIE\* |
|  | Taktowanie procesora: minimum 800MHz |  | TAK/NIE\* |
|  | Pamięć Flash: minimum 32MB |  | TAK/NIE\* |
|  | Pamięć RAM: minimum 256MB |  | TAK/NIE\* |
|  | Temperatura pracy: zakres minimum 0°C - 50°C |  | TAK/NIE\* |
|  | Wilgotność względna: zakres minimum 10% - 90% (bez kondensacji) |  | TAK/NIE\* |
|  | Zasilanie: zabudowany zasilacz 230V AC |  | TAK/NIE\* |
|  | Pobór mocy: maksymalnie 21W |  | TAK/NIE\* |
|  | Zabezpieczenie przeciwprzepięciowe: minimum 6kV |  | TAK/NIE\* |
|  | Wymiary: maksymalna: szerokość 440 mm, wysokość 44mm , głębokość 170mm |  | TAK/NIE\* |
|  | Certyfikaty bezpieczeństwa: CE, RoHS |  | TAK/NIE\* |
|  | Algorytm: Store and Forward |  | TAK/NIE\* |
|  | VLAN: Voice VLAN, Port based VLAN, MAC based VLAN, Protocol based VLAN, Private VLAN, VLAN Translation, N:1 VLAN Translation, GVRP, IEEE 802.1Q, Normal QinQ, Flexible QinQ |  | TAK/NIE\* |
|  | DHCP: IPv4/IPv6 DHCP Client,IPv4/IPv6 DHCP Relay, Option 82, IPv4/IPv6 DHCP Snooping,IPv4/IPv6 DHCP Server |  | TAK/NIE\* |
|  | Spanning tree: IEEE802.1D (STP), IEEE802.1W (RSTP), IEEE802.1S (MSTP), Multi-Process MSTP, Root Guard, BPDU guard, BPDU forwarding |  | TAK/NIE\* |
|  | Protekcja ringowa: ITU-T G.8032 – recovery time < 50ms, Fast Link, Loopback Detection |  | TAK/NIE\* |
|  | Agregacja łączy: IEEE 802.3ad (LACP), 64 groups per device / 8 ports per group, load balance |  | TAK/NIE\* |
|  | Bezpieczeństwo: Storm Control based on packets, Port Security, MAC Limit based on VLAN and Port, Anti-ARP-Spoofing , Anti-ARP-Scan, ARP Binding, Gratuitous ARP, ARP Limit, Anti ARP/NDP Cheat, Anti ARP Scan, ND Snooping, DAI, IEEE 802.1x, Authentication, Authorization, Accounting, Radius IPv4/IPv6, TACACS+, MAB, Port and MAC based authentication, Accounting based on time length and traffic, Guest VLAN and auto VLAN, |  | TAK/NIE\* |
|  | Multicast: IGMP v1/v2/v3 snooping and L2 Query, IGMP Fast leave, MVR, MLD v1/v2 Snooping, IPv4/IPv6 DCSCM, IGMP authentication |  | TAK/NIE\* |
|  | QoS: 8 queques per port, Bandwidth Control, Flow Control: HOL, IEEE802.3x, Flow Redirect, Classification based on ACL, COS, TOS, DiffServ, DSCP, port number; Traffic Policing, PRI Mark/Remark, IEEE 802.1p, Queuing Method: Strict Priority, Weighted Deficit Round Robin, Strict priority in Weighted Deficit Round Robin; DNS Client, DNS Relay |  | TAK/NIE\* |
|  | Lista kontroli dostępu: IP Src/Dst ACL, MAC Src/Dst ACL, MAC-IP ACL, User-Defined ACL, Time Range ACL, port number TCP/UDP ACL, VLAN ACL, REDIRECT and Statistics based on ACL, Precedence, Vlan Tag/Untag, Rules can be configured to port and VLAN |  | TAK/NIE\* |
|  | Diagnostyka: sFlow, Traffic Analysis, RSPAN, VCT, Ping, Trace Route, Dying GASP |  | TAK/NIE\* |
|  | Zarządzanie: TFTP/FTP, CLI, Telnet, Console, Web/SSL (IPv4/IPv6), SSH (IPv4/IPv6), SNMP v1/v2c/v3, SNMP Trap, Public & Private MIB interface, RMON 1,2,3,9, Syslog (IPv4/IPv6), SNTP/NTP (IPv4/IPv6), Dual IMG, Multiple Configuration Files, Port Mirror, IEEE 802.3ah/802.1ag OAM, ULDP (like UDLD), LLDP/LLDP MED., VSF (4 devices in one stack) – hardware stacking |  | TAK/NIE\* |
|  | **Oprogramowanie oraz wsparcie techniczne:** oprogramowanie przełącznika (firmware) dostępne bez ograniczeń czasowych, przez cały okres cyklu życia urządzenia, poprzez Internet, wsparcie techniczne dystrybutora bez konieczności wykupu dodatkowych usług |  | TAK/NIE\* |
|  | Gwarancja producenta musi wynosić minimum gwarancji udzielonej przez Wykonawcę |  | TAK/NIE\* |
|  | **Urządzenie UTM:**  **Centrum Usług Społecznych w Skrzyszowie (1 szt.)**  **- fabrycznie nowe** | |  |
| **Cena jednostkowa:**  **brutto zł za sztukę** | |  |
|  | Marka/Model urządzenia UTM |  | TAK/NIE\* |
|  | Wymagania Ogólne  System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.  System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.  System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji.  Powinna istnieć możliwość dedykowania co najmniej 5 administratorów do poszczególnych instancji systemu.  System wspiera protokoły IPv4 oraz IPv6 w zakresie:   * + 1. Firewall.     2. Ochrony w warstwie aplikacji.     3. Protokołów routingu dynamicznego. |  | TAK/NIE\* |
|  | 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. |  | TAK/NIE\* |
|  | Interfejsy, Dysk, Zasilanie:   * + 1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:        1. 5 portami Gigabit Ethernet RJ-45.     2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB.     3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q.     4. System jest wyposażony w zasilanie AC. |  | TAK/NIE\* |
|  | Parametry wydajnościowe:   * + 1. W zakresie Firewall’a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę.     2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B.     3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps.     4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 4 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 1 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 500 Mbps.     7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps. |  | TAK/NIE\* |
|  | 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.     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. 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.     10. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.     11. Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system.     12. 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). |  | TAK/NIE\* |
|  | 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:        1. Translację jeden do jeden oraz jeden do wielu.        2. Dedykowany ALG (Application Level Gateway) dla protokołu SIP.     3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.     4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: adresy URL, adresy IP.     5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.     6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.     7. 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.        1. Amazon Web Services (AWS).        2. Microsoft Azure.        3. Cisco ACI.        4. Google Cloud Platform (GCP).        5. OpenStack.        6. VMware NSX.        7. Kubernetes. |  | TAK/NIE\* |
|  | Połączenia VPN   * + 1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:        1. Wsparcie dla IKE v1 oraz v2.        2. Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).        3. Obsługa protokołu Diffie-Hellman grup 19, 20.        4. Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.        5. Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.        6. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.        7. Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.        8. Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.        9. Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.        10. Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.        11. Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.        12. Mechanizm „Split tunneling” dla połączeń Client-to-Site.     2. Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji. |  | TAK/NIE\* |
|  | 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. |  | TAK/NIE\* |
|  | 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). |  | TAK/NIE\* |
|  | 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. |  | TAK/NIE\* |
|  | 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. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.     9. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu. |  | TAK/NIE\* |
|  | 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. 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. |  | TAK/NIE\* |
|  | 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). |  | TAK/NIE\* |
|  | 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. |  | TAK/NIE\* |
|  | Uwierzytelnianie użytkowników w ramach sesji:   * + 1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:        1. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.        2. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.        3. Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.     2. System daje możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego.     3. 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.     4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP. |  | TAK/NIE\* |
|  | 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. |  | TAK/NIE\* |
|  | 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. |  | TAK/NIE\* |
|  | Testy wydajnościowe oraz funkcjonalne:   * + 1. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta |  | TAK/NIE\* |
|  | Serwisy i licencje   * + 1. Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:        1. Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres minimum gwarancji udzielonej przez Wykonawcę |  | TAK/NIE\* |
|  | Gwarancja oraz wsparcie:  System jest objęty serwisem gwarancyjnym producenta przez okres minimum udzielonej gwarancji przez Wykonawcę, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania i wsparcie techniczne w trybie 24x7 przez dedykowany moduł internetowy oraz infolinię. |  | TAK/NIE\* |
|  | zestaw montażowy dla urządzenia przystosowany do montażu w szafie rack zamawiającego. |  | TAK/NIE\* |
|  | **Serwer NAS/Macierz dyskowa wraz z 4 dyskami HDD:**  **Centrum Usług Wspólnych (1 szt.) - fabrycznie nowe**  **Cena jednostkowa:**  **brutto zł za sztukę** | | |
|  | Marka/Model Serwera NAS**/Macierzy dyskowej** oraz 4 dysków HDD |  | TAK/NIE\* |
|  | Typ urządzenia: Serwer NAS/Macierz Dyskowa |  | TAK/NIE\* |
|  | Obudowa: Rack 1U |  |  |
|  | Procesor: minimum czterordzeniowy procesor o taktowaniu 2,2 GHz. |  | TAK/NIE\* |
|  | Sprzętowy mechanizm szyfrowania: AES-NI |  | TAK/NIE\* |
|  | Pamięć RAM: min. 2 GB pamięci ECC SODIMM z możliwością rozszerzenia do min. 32 GB |  | TAK/NIE\* |
|  | 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. |  | TAK/NIE\* |
|  | * + 1. Porty zewnętrzne: minimum:        1. 2 porty USB 3.2.1        2. 1 port eSATA (jako gniazdo rozszerzenia) |  | TAK/NIE\* |
|  | * + 1. Porty sieciowe Minimum:        1. 4 porty 1GbE RJ45 (z obsługą funkcji Link Aggregation / przełączania awaryjnego) |  | TAK/NIE\* |
|  | Funkcja Wake on LAN/WAN |  | TAK/NIE\* |
|  | Gniazdo rozszerzeń PCIe 2.0: Min. 1x 4-liniowe gniazdo x8 gen. 3 |  | TAK/NIE\* |
|  | Wentylator obudowy: Min. 3 wentylatory (40 × 40 × 20 mm) |  | TAK/NIE\* |
|  | Obsługiwane protokoły sieciowe: Min. SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS Kerberized sessions, iSCSI, HTTP, HTTPs, FTP, SNMP, LDAP, CalDAV |  | TAK/NIE\* |
|  | * + 1. System plików: minimum:        1. Wewnętrzny: Btrfs, ext4        2. Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT |  | TAK/NIE\* |
|  | * + 1. Zarządzanie pamięcią masową:        1. Maksymalny rozmiar pojedynczego wolumenu: 108 TB        2. Minimalny liczba wewnętrznych wolumenów: 64        3. Minimalny liczba obiektów iSCSI Target: 128        4. Minimalny liczba jednostek iSCSI LUN: 256        5. Obsługa klonowania/migawek jednostek iSCSI LUN |  | TAK/NIE\* |
|  | Obsługiwane typy macierzy RAID: minimum: SHR, Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10 |  | TAK/NIE\* |
|  | * + 1. Konto i folder współdzielony:        1. Minimalna liczba kont użytkowników: 1 024        2. Minimalna liczba grup użytkowników: 256        3. Minimalna liczba folderów współdzielonych: 256        4. Minimalna liczba zadań synchronizacji folderów   współdzielonych: 8 |  | TAK/NIE\* |
|  | 1. Usługi plików:  a) Protokół plików: SMB, AFP, NFS, FTP, WebDAV, Rsync  b) Minimalna liczba połączeń SMB (oparta na FSCT): 130  c)Integracja z listą kontroli dostępu Windows (ACL)  d) Uwierzytelnianie Kerberos NFS |  | TAK/NIE\* |
|  | Wirtualizacja: Obsługa VMware vSphere with VAAI, Windows Server 2022, Citrix Ready, OpenStack |  | TAK/NIE\* |
|  | 1. Bezpieczeństwo:  a) Zapora, szyfrowanie folderów współdzielonych, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania, wsparcie Let's Encrypt, HTTPS (konfigurowalny zestaw szyfrów) |  | TAK/NIE\* |
|  | 1.Oprogramowanie:  a) 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 współdzielonych  b) Urządzenie musi wspierać funkcję WORM (Write Once, Read Many) oraz migawki niezmienne  c) 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   * + - 1. 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.       2. 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. |  | TAK/NIE\* |
|  | Dyski – 4 sztuki- będące na liście kompatybilności producenta serwera NAS  Typ dysku: HDD  Interfejs dysku: SATA III - 6 Gb/s  Prędkość obrotowa: 7200 obr/min  Pojemność dysku: 12 TB  Gwarancja na dyski: minimum gwarancji oferowane przez Wykonawcę/Oferenta |  | TAK/NIE\* |
|  | **Zasilacze awaryjne UPS do serwerowni –**  **Urząd Gminy Skrzyszów (1 szt.),**  **Centrum Usług Społecznych – (1 szt.)**  **fabrycznie nowe Urządzenia**  **Cena jednostkowa:**  **brutto zł za sztukę** | | |
|  | Marka/Model zasilacza awaryjnego UPS |  | TAK/NIE\* |
|  | Technologia wykonania UPS: Line-interactive |  | TAK/NIE\* |
|  | Zasilanie/UPS: Jednofazowy |  | TAK/NIE\* |
|  | Moc pozorna (VA): 2200 |  | TAK/NIE\* |
|  | Moc rzeczywista (W): min. oraz max. 2200W; ze względów na charakterystyczną specyfikę instalacji sieci elektrycznej zamawiającego w budynkach gdzie będą wykorzystywane UPS-y nie dopuszcza się zasilacza awaryjnego UPS o wyższej mocy. |  | TAK/NIE\* |
|  | Kształt fali na wyjściu(praca na baterii): Czysta fala sinusoidalna |  | TAK/NIE\* |
|  | Kompatybilność z zasilaczami z aktywnym PFC |  | TAK/NIE\* |
|  | Automatyczna regulacja napięcia (mechanizm AVR) |  | TAK/NIE\* |
|  | Podwyższanie napięcia(przy zaniżonym napięciu z sieci): Dwustopniowe |  | TAK/NIE\* |
|  | Obniżanie napięcia(przy zawyżonym napięciu z sieci): Jednostopniowe |  | TAK/NIE\* |
|  | Ochrona przed przeciążeniem: minimum bezpiecznik i wewnętrzny ogranicznik prądu |  | TAK/NIE\* |
|  | Filtr EMI/RFI |  | TAK/NIE\* |
|  | Ochrona dla urządzeń telekomunikacyjnych minimum 1 port RJ45 wejście/wyjście |  | TAK/NIE\* |
|  | Układ przeciwprzepięciowy (Dżule):  Charakterystyka wejścia/wyjścia: minimum 2430 |  | TAK/NIE\* |
|  | Nominalne napięcie wejściowe (V): 220 ; 230 ; 240 |  | TAK/NIE\* |
|  | Obsługiwany zakres napięcia wejściowego (V): 159 ~ 288 |  | TAK/NIE\* |
|  | Częstotliwość wejściowa(Hz): 50+/-3 ; 60+/-3 |  | TAK/NIE\* |
|  | Wykrywanie częstotliwości wejściowej: automatyczne |  | TAK/NIE\* |
|  | Napięcie przy pracy na baterii (V): 220+/-5% ; 230+/-5% ; 240+/-5% |  | TAK/NIE\* |
|  | Częstotliwość przy pracy baterii (Hz): 50+/-1% ; 60+/-1% |  | TAK/NIE\* |
|  | Charakterystyka gniazd:   * + 1. Rodzaj złącza wejściowego: IEC C20        1. Całkowita ilość gniazd: minimum 8        2. Gniazdka: IEC C13 x 6 / IEC C19 x 2        3. Rozróżnienie gniazd na krytyczne i nie krytyczne: minimum 4 gniazda krytyczne |  | TAK/NIE\* |
|  | * + 1. Charakterystyka baterii:        1. Typowy czas przełączenia na baterie (ms): nie więcej niż 4        2. Czas pracy na baterii przy połowie obciążenia: minimum 11.4min        3. Typowy czas ponownego ładowania baterii (h): 3        4. Możliwość wymiany baterii przez użytkownika |  | TAK/NIE\* |
|  | * + 1. Zarządzanie:        1. Sygnalizacja: Wymagane alarmy dźwiękowe oraz wyświetlacz LCD        2. Alarmy dźwiękowe: minimum Tryb baterii, Niski poziom baterii, Przeciążenie, Przeładowanie        3. Konfiguracja wybranych parametrów: Ustawienie trybu, Ustawienia alarmu, Wejście i wyjście, Ustawienia baterii, Komunikacja, Język        4. Port komunikacyjny USB        5. Port wyłącznika awaryjnego EPO        6. Dołączone oprogramowanie do zarządzania        7. Wymagane, obsługa platform Windows, Linux, Vmware        8. Zarządzanie przez sieć: Wymagana możliwość rozbudowy o zarządzanie HTTP/SNMP, np. poprzez doinstalowanie karty zarządzającej |  | TAK/NIE\* |
|  | * + 1. Cechy fizyczne:        1. Obudowa: Wymagana możliwość instalacji w szafie RACK lub ustawienia jako Tower        2. Konstrukcja obudowy: Metalowa        3. Wymagane Szyny/uchwyty rack        4. Rozmiary (szer. x wys. x gł.) (mm): Nie większe niż 433 x 86.5 x 412        5. Waga: maksimum 26 kg |  | TAK/NIE\* |
|  | * + 1. Dane środowiskowe:        1. Temperatura robocza (°C): 0 ~ 40        2. Względna wilgotność robocza (bez kondensacji) (%): 0 ~ 95 |  | TAK/NIE\* |
|  | * + 1. Certyfikaty:        1. wymagane certyfikaty: CE, FCC klasa B, UL, cUL, RCM, VCCI, UKCA, RoHS |  | TAK/NIE\* |
|  | Gwarancja producenta na urządzenie oraz baterie (znajdujące się w UPS-ie): minimum oferowane przez Wykonawcę/Oferenta |  | TAK/NIE\* |
|  | **Zasilacze awaryjne UPS stanowiskowe–**  **Urząd Gminy Skrzyszów (40 szt.),**  **Centrum Usług Społecznych – (12 szt.)**  **fabrycznie nowe Urządzenia**  **Cena jednostkowa:**  **brutto zł za sztukę** | | |
|  | Marka/Model zasilacza awaryjnego UPS |  | TAK/NIE\* |
|  | Technologia wykonania UPS: Line-interactive |  | TAK/NIE\* |
|  | Zasilanie/UPS: Jednofazowy |  | TAK/NIE\* |
|  | Moc pozorna (VA): 1050 |  | TAK/NIE\* |
|  | Moc rzeczywista (W): min. 600 |  | TAK/NIE\* |
|  | Kształt fali na wyjściu(praca na baterii): Symulowane napięcie sinusoidalne |  | TAK/NIE\* |
|  | Automatyczna regulacja napięcia (mechanizm AVR) |  | TAK/NIE\* |
|  | Ochrona przed przeciążeniem |  | TAK/NIE\* |
|  | Filtr EMI/RFI |  | TAK/NIE\* |
|  | Układ przeciwprzepięciowy (J): minimum 150 |  | TAK/NIE\* |
|  | * + 1. Charakterystyka wejścia/wyjścia:        1. Nominalne napięcie wejściowe (V): 230+/-10%        2. Obsługiwany zakres napięcia wejściowego (V): minimum 165 - 290        3. Częstotliwość wejściowa(Hz): 50+/-5 ; 60+/-5        4. Wykrywanie częstotliwości wejściowej: automatyczne        5. Napięcie przy pracy na baterii (V): 230+/-10%        6. Częstotliwość przy pracy baterii (Hz): 50+/-1% ; 60+/-1% |  | TAK/NIE\* |
|  | * + 1. Charakterystyka gniazd:        1. Rodzaj złącza wejściowego: UniSchuko (połączenie złącza FR i Schuko)        2. Rodzaj złącza wyjściowego: FR x 4 |  | TAK/NIE\* |
|  | * + 1. Charakterystyka baterii:        1. Typowy czas przełączenia na baterie (ms) 4 ms        2. Czas podtrzymania na baterii: czas pracy przy pełnym obciążeniu (600W) do 1 min, przy połowie obciążenia (300W) do 4 min        3. Ładowanie baterii: Typowy czas ładowania do 6 h |  | TAK/NIE\* |
|  | * + 1. Zarządzanie:        1. Sygnalizacja: wymagane alarmy dźwiękowe oraz diody LED        2. Diody LED - syngalizacja Zasilanie włączone, Tryb liniowy, Tryb baterii, Tryb obejścia, Niski poziom baterii, Przeciążenie, Usterka UPS        3. Alarmy dźwiękowe - sygnalizacja: Tryb baterii, Niski poziom baterii, Przeciążenie, Usterka UPS        4. Dołączone oprogramowanie do zarządzania: obsługą platform Windows 11 , Windows 10 , Windows 8 , Windows 7 , Windows Server 2019 , Windows Server 2016 , Windows Server 2012 R2 , Windows Server 2012 , Windows Server 2008 R2, macOS 12 , macOS 11 , macOS 10.15 , macOS 13.1 , macOS 13.2 |  | TAK/NIE\* |
|  | * + 1. Cechy fizyczne:        1. Obudowa Tower        2. Konstrukcja obudowy - Plastikowa        3. Rozmiary (szer. x wys. x gł.) (mm): Nie większe niż 95 x 220 x 307        4. Waga maksimum 7 kg (urządzenie bez opakowania i akcesoriów) |  | TAK/NIE\* |
|  | * + 1. Dane środowiskowe:        1. Temperatura robocza (°C): 0 - 40        2. Względna wilgotność robocza (bez kondensacji) (%) 0 - 90        3. Rozproszenie ciepła (BTU/hr): Nie więcej niż 27 BTU/hr |  | TAK/NIE\* |
|  | Certyfikaty: CE |  | TAK/NIE\* |
|  | Gwarancja producenta na urządzenie i baterie: minimum oferowane przez Wykonawcę/Oferenta |  | TAK/NIE\* |
|  | **Oprogramowanie do tworzenia kopii zapasowych – Centrum Usług Wspólnych(1 szt.) - fabrycznie nowe**  **Cena jednostkowa:**  **brutto zł za sztukę** | | |
|  | Nazwa Oprogramowania do tworzenia kopii zapasowych |  | TAK/NIE\* |
|  | Zarządzanie i magazyny:   * + 1. Produkt dostępny w polskiej wersji językowej.     2. Konsola zarządzająca dostępna z poziomu przeglądarki internetowej     3. System musi umożliwiać tworzenie kopii zapasowych na poziomie dysków     4. System musi umożliwiać tworzenie kopii zapasowych na poziomie plików i folderów     5. System musi umożliwiać replikację kopii zapasowych do wielu lokalizacji docelowych     6. System musi umożliwiać tworzenie kopii zapasowych i przywracanie systemów wykorzystujących UEFI/GPT     7. System musi umożliwiać współpracę z usługą kopiowania woluminów w tle (VSS) firmy Microsoft     8. Możliwość zdefiniowania limitu przepustowości sieciowej z jakiej ma korzystać oprogramowanie backupowe     9. System zarządzania nie może być oparty o relacyjne bazy danych.     10. Rozwiązanie działa w architekturze wykluczającej pojedynczy punkt awarii (awaria jednego z komponentów nie spowoduje przestoju w procesie tworzenia kopii zapasowej).     11. Rozwiązanie zapewnia zoptymalizowaną trasę transmisji danych poprzez możliwość wybrania dowolnego workera (urządzenia, które odpowiadać będzie za pobieranie danych z konkretnych usług) oraz browsera (urządzenia, które będzie wykorzystywane do przeszukiwania m.in. magazynów).     12. Aplikacje klienckie powinny wysyłać dane z kopii zapasowej bezpośrednio na wskazany magazyn – serwer backupu/usługa zarządzania, ani żaden inny element Systemu, nie powinien brać udziału w przesyłaniu danych.     13. Rozwiązanie musi być systemem multi-storage-owym i umożliwia tworzenie wielu repozytoriów danych jednocześnie również na innych środowiskach jako przestrzeń do replikacji danych.     14. System musi oferować mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykle.     15. Rozwiązanie w warstwie sprzętowej powinno bazować na standardowych komponentach architektury x86, bez powiązania i poleganiu na komponentach wyłącznie jednego dostawy (tzw. "no propietary vendor lock").     16. System pozwala administratorowi na ustawienie dowolnego harmonogramu replikacji danych pomiędzy dowolnymi wspieranymi magazynami.     17. System musi umożliwiać wykonywanie kopii obrazu dysku, kopii plików i katalogów oraz kopii maszyn wirtualnych bez ich zatrzymywania z zachowaniem stuprocentowej integralności i spójności danych wewnątrz wykonanej kopii zapasowej.     18. Rozwiązanie musi realizować funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie.     19. Rozwiązanie zapewnia backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia.     20. System musi umożliwiać automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku wystąpienia błędu.     21. Rozwiązanie powinno umożliwiać klonowanie planów kopii zapasowych, planów replikacji oraz planów testowego odtwarzania maszyn wirtualnych     22. Rozwiązanie powinno umożliwiać uruchamianie przy zadaniach backupu dowolnych skryptów PRE/POST oraz po wykonaniu migawki VSS.     23. System powinien umożliwiać definiowanie tzw. okna backupowego dla każdego z zadań w celu umożliwienia zarządzania obciążeniem sieci i uwzględnienia okien serwisowych występujących u Zamawiającego.     24. System musi automatycznie dodawać do polityki i harmonogramu tworzenia backupów nowe źródła / maszyny wirtualnych, dodane do bieżącego środowiska (automatyzacja oparta na polityce tworzenia kopii).     25. Rozwiązanie musi udostępniać możliwość podglądu postępu działania dowolnego zadania, w tym zadania wykonywania kopii zapasowych, odtwarzania danych, testowego odtwarzania danych, usuwania danych oraz zadania odświeżania zajętości magazynu na dane.     26. Rozwiązanie musi posiadać system powiadamiania poprzez e-mail oraz Slack o zdarzeniach w następujących przypadkach: zadanie zostało zakończone pomyślnie, zadanie zostało zakończone z ostrzeżeniami, zadanie zostało zakończone z błędem, zadanie zostało anulowane, zadanie nie zostało uruchomione.     27. System powinien umożliwiać wysyłanie powiadomień o statusie wykonanych zadań na dowolne adresy webhook, podawane przez użytkownika,     28. Oferowane rozwiązanie musi być dobrane pod względem wydajności w oparciu o najlepsze praktyki producenta.     29. Rozwiązanie musi być wyskalowane, dobrane pod względem wymaganej funkcjonalności i wydajności stosownie do ilości zabezpieczanych danych i obiektów z uwzględnieniem przyrostu danych (serwery, maszyny wirtualne, bazy danych itp.) zgodnie z opisem w zapytaniu ofertowym.     30. Wydajność oferowanej konfiguracji musi być taka, aby wszystkie funkcje systemu były dostępne w chwili wdrożenia (np. deduplikacja, kompresja, instancja workerów i browserów, replikacja, testowe odtwarzanie maszyn wirtualnych).     31. System pozwala na zmniejszenie rozmiaru przechowywanych i przesyłanych danych poprzez usuwanie zduplikowanych bloków danych ze źródła kopii pomiędzy wszystkimi źródłami w obrębie wszystkich kopii na magazynie danych.     32. Proces deduplikacji musi być możliwy dla każdego z typów obsługiwanych magazynów.     33. Proces deduplikacji nie może wymagać instalacji żadnych dodatkowych komponentów, które będą pośredniczyły w zapisie danych z deduplikowanych     34. Proces deduplikacji nie może posiadać pojedynczego punktu awarii, tym samym musi być dostępny jednocześnie na każdym wspieranym magazynie na dane - również replikacyjnych. Awaria jednego z magazynów na dane nie może wpłynąć na integralność deduplikatów, jak i tablicy deduplikatów na innym magazynie.     35. Proces deduplikacji realizowany jest blokiem o stałej wielkości, którego wielkość może zostać ustalona na etapie wdrożenia rozwiązania zgodnie z najlepszymi praktykami producenta.     36. Proces szyfrowania kopii zapasowych nie może ograniczać procesu deduplikacji w ramach tego samego klucza szyfrującego.     37. Kompresja kopii zapasowych musi obsługiwać jeden z wymienionych algorytmów: LZ4, ZStandard. Dodatkowo, musi umożliwiać określenie szczegółowego poziomu kompresji, w tym: niski, średni, wysoki.     38. Instalacja, modyfikacja ustawień, polityki tworzenia kopii zapasowej systemu nie może wymagać przerwania pracy lub restartu systemu.     39. System musi pozwalać na automatyczne aktualizacje oprogramowania.     40. System musi być w stanie kompresować i szyfrować zabezpieczone dane w systemach NAS.     41. System musi pozwalać na uruchomienie kontenerów Docker w dowolnych urządzeniach NAS w celu ich zabezpieczenia.     42. System tworzenia kopii zapasowej musi przechowywać dane w sposób zapewniający ich niezmienność (tzw. "resilience"), dzięki czemu kopie zapasowe nie będą mogły zostać nadpisane lub zmodyfikowane przez cały okres ich przechowywania, retencji.     43. System zarówno będzie przechowywać dane w kopii zapasowej w postaci zaszyfrowanej jak też ruch wewnątrz systemu również musi być szyfrowany.     44. Archiwum długoterminowych kopii zapasowych musi być szyfrowane, a odzyskiwanie z archiwum obsługiwane z tego samego interfejsu użytkownika, co inne przywracanie dane.     45. System musi mieć mechanizmy chroniące przejęcie konta administratora oraz umożliwiać definiowanie dodatkowych uprawnień dla każdej z predefiniowanych ról użytkowników.     46. System musi pozwalać na gradację uprawnień administratorów - umożliwia tworzenie wielu kont administracyjnych z dedykowanymi rolami oraz uprawnieniami, jak m. in.: system operator, backup operator, restore operator, viewer. Dla każdej z tych ról system musi umożliwiać przypisywanie dodatkowych uprawnień, w tym możliwość zablokowania usuwania danych.     47. Rozwiązanie musi posiadać możliwość nieodwracalnego usuwania danych z magazynu na dane w momencie spełnienia dodatkowych wymogów.     48. W sytuacji, gdyby podstawowe urządzenie tworzenia kopii zapasowej było niedostępne, system musi posiadać możliwość przywrócenia z archiwum za pomocą innej instancji systemu dostarczonej przez tego samego producenta. tzn. archiwum musi zawierać wszystkie informacje konieczne do odzyskania.     49. Rozwiązanie musi umożliwiać uruchomienie konsoli w chmurze producenta zlokalizowanej na terenie Unii Europejskiej, w celu umożliwienia dostępu do środowiska zarządzania kopiami zapasowymi w przypadku czasowej niedostępności środowiska lokalnego.     50. System kopii zapasowej musi umożliwiać dostęp do konsoli administracyjnej z wielu stacji roboczych.     51. System kopii zapasowej musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.     52. System powinien posiadać predefiniowane schemat tworzenia kopii zapasowych: Custom, Basic, G-F-S, Forever incremental,     53. Rozwiązanie musi obsługiwać kontrolę dostępu opartą na rolach (RBAC).     54. Możliwość składowania utworzonych kopii zapasowych na magazynach chmurowych Amazon AWS, Azure, Wasabi, Google Cloud Storage, Backblaze B2, magazyny zgodne z S3.     55. Możliwość składowania utworzonych kopii zapasowych na udziałach sieciowych po protokole smb, nfs, iscsi, katalog lokalny     56. Zarządzanie i odzyskiwanie danych z kopii musi odbywać się z tego samego interfejsu użytkownika (konsoli), niezależnie od tego, gdzie znajduje się kopia zapasowa (w chmurze AWS, Azure, GCP, w Data Center czy w usłudze typu SaaS).     57. Czas przechowywania kopii zapasowej (retention time) systemu backupu nie może być zmieniony np. poprzez manipulowanie wskazaniami zegara serwera NTP w celu szybszego ich wyekspirowania - tzn. czasy przechowywania kopii zapasowych nie będą zależne od wskazań zegara czasu serwera NTP, ale będą wykorzystywać technologię, która mierzy upływ czasu.     58. Możliwość generowania raportów dobowych w oparciu o harmonogram     59. Produkt musi posiadać możliwość zapisu kopii zapasowych do magazynu chmurowego dostarczanego bezpośrednio przez producenta oprogramowania (datacenter musi być zlokalizowane na terenie Unii Europejskiej)     60. Produkt musi posiadać możliwość zdefiniowania maksymalnej liczby równocześnie backupowanych urządzeń w ramach jednego planu backupowego, niezależnie od typu urządzenia (np. stacja robocza, serwer, maszyna wirtualna)     61. Możliwość wyświetlenia szczegółowych informacji o chronionym urządzeniu takich jak: CPU, RAM, System operacyjny, Adres IP.     62. Produkt musi posiadać możliwość zdefiniowania poziomu obciążenia magazynu, po osiągnięciu którego zostanie wysłane powiadomienia e-mail. (poziom definiowany indywidualnie dla każdego magazynu) |  | TAK/NIE\* |
|  | Wspierane systemy:  Możliwość instalacji oraz uruchomienia agenta backupowego na hostach fizycznych, maszynach wirtualnych czy też kontenerach docker opartych o systemy oraz **wszystkie nowsze**:  Alpine 3.10+,  Debian: 9+,  Ubuntu: 16.04+,  Fedora: 29+,  centOS: 7+,  RHEL: 6+,  openSUSE: 15+,  SUSE Enterprise Linux(SLES): 12 SP2+,  macOS: 10.13+,  Windows: 7, 8.1, 10(1607+),  Windows Server: 2008 R2+,  Środowisk wirtualnych:  Hyper-V 2016+,  VMware: 6.7+.  Możliwość instalacji oraz uruchomienia serwera zarządzania na hostach fizycznych, maszynach wirtualnych czy też kontenerach docker opartych o systemy:  Debian: 9+  Ubuntu: 16.04+  Fedora: 29+  centOS: 7+  RHEL: 6+  openSUSE: 15+  SUSE Enterprise Linux (SLES): 12 SP2+  Windows Client: 7, 8.1, 10 (1607+)  Windows Server: 2012 R2+, |  | TAK/NIE\* |
|  | Środowiska fizyczne i bazy danych:   * + 1. Rozwiązanie powinno umożliwiać tworzenie grup urządzeń w celu automatyzacji procesów podczas pracy z urządzeniami.     2. Produkt musi posiadać możliwość tworzenia zadań dla grupy urządzeń oraz dla wybranych urządzeń.     3. Rozwiązanie musi pozwalać na automatyczne wyłączenie stacji roboczej po wykonaniu kopii zapasowej.     4. Rozwiązanie backupowe musi pozwalać na zabezpieczanie zaszyfrowanych partycji min. BitLocker, Veracrypt, TrueCrypt, Eset Endpoint Encryption.     5. System jest niezależny od wersji Microsoft SQL i musi umożliwiać przywracanie danych SQL dla tej samej lub nowszej wersji.     6. System musi obsługiwać również narzędzia RMAN firmy Oracle do tworzenia kopii zapasowych i odzyskiwania. Dodatkowo system musi obsługiwać funkcję przyrostowego scalania danych.     7. System kopii zapasowej musi wspierać odtwarzanie pojedynczych plików z systemów Windows oraz Linux.     8. W przypadku niedostępności źródła danych, system musi oczekiwać na powrót dostępności źródła danych przez określony przez administratora okres. W przypadku braku powrotu dostępności źródła, system musi podjąć ustaloną przez administratora liczbę prób kontynuacji kopii. W przypadku powrotu źródła danych system musi kontynuować zadanie backupu od momentu, w którym wystąpiła niedostępność źródła - system nie może rozpoczynać zadania od punktu początkowego i rozpoczynać przesyłania kopii od zera. W przypadku braku powrotu źródła danych system powinien zakończyć zadanie błędem.     9. Odtwarzanie Bare Metal Restore w Systemie może odbywać się na takim samym sprzęcie, jak ten który był backupowany, jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników oraz z możliwością dodania sterowników przez użytkownika.     10. Rozwiązanie powinno umożliwiać uruchamianie procesu Bare Metal Restore z dowolnego bootowalnego nośnika danych.     11. Rozwiązanie powinno wspierać odtwarzanie danych w scenariuszach P2P, P2V, V2P, V2V.     12. Rozwiązanie umożliwia odtwarzanie kopii obrazu dysku w wybranym formacie (RAW, VHD, VHDX, VMDK).     13. Rozwiązanie musi umożliwiać odtwarzanie zasobów plikowych bez praw dostępu (tzw. ACL) oraz z prawami dostępu. Funkcjonalność ta musi być możliwa do skonfigurowania przez administratora na etapie konfiguracji procesu przywracania danych.     14. Rozwiązanie musi umożliwiać przywracanie plików pomiędzy różnymi systemami operacyjnymi i systemami plików (np. odtwarzanie danych plikowych Linux na systemie Windows). |  | TAK/NIE\* |
|  | Środowiska wirtualne:   * + 1. System musi wspierać kopię w trybie application-aware dla wszystkich wspieranych wirtualizatorów.     2. System musi umożliwiać wykonywanie kopii maszyn wirtualnych z zastosowanie zaawansowanych metod transportu (HotAdd, SAN, LAN), w tym metodami LAN-Free, tj. takimi, które podczas wykonywania backupu nie obciążają interfejsów sieciowych maszyn wirtualnych.     3. System kopii zapasowej musi wykorzystywać mechanizmy Change Block Tracking oraz Replica Change Tracking dla wspieranych przez producenta platformach wirtualizacyjnych.     4. Rozwiązanie producenta musi być certyfikowane przez dostawcę platformy wirtualizacyjnej, tj. producent musi uczestniczyć w programie Technology Alliance Partner.     5. System kopii zapasowej musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage-u użytego do przechowywania kopii zapasowych.     6. Dla środowiska vSphere i Hyper-V rozwiązanie powinno umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).     7. System kopii zapasowej musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSphere.     8. System kopii zapasowej musi umożliwiać weryfikację odtwarzalności wirtualnych maszyn według własnego harmonogramu w dowolnym środowisku. |  | TAK/NIE\* |
|  | Aplikacje SaaS   * + 1. Ochrona z tej samej konsoli dla Microsoft 365 minimum na poziomie, skrzynek pocztowych, onedrive, kontaktów, kalendarza.     2. Rozwiązanie musi umożliwiać przywracanie danych Microsoft 365: do wskazanej, dowolnej lokalizacji, na wybranym urządzeniu w formie pliku .pst oraz do istniejącego konta w usłudze Microsoft 365 (tego samego lub innego, w tym w innej organizacji)     3. System musi umożliwiać granularne odtwarzanie danych, tj. pojedynczych plików z kopii obrazu dysku oraz pojedynczych wiadomości z kopii skrzynki pocztowej Microsoft 365.     4. System musi umożliwiać zabezpieczanie środowisk Git, w tym GitHub, GitLab oraz Bitbucket wraz z metadanymi     5. System musi umożliwiać odtworzenie dowolnego środowiska Git w dowolnym innym środowisku Git, tzw. odtwarzanie crossowe.     6. System musi umożliwiać zabezpieczenie metadanych zebranych wokół repozytorium w ramach zabezpieczanego środowiska Git.     7. System musi umożliwiać odtwarzanie metadanych repozytorium Git do dowolnego innego środowiska Git w przypadku chęci odtworzenia repozytorium.     8. System musi umożliwiać zabezpieczenie środowisk Jira     9. System musi umożliwiać odtworzenie środowiska Jira do chmury lub środowiska lokalnego.     10. System musi umożliwiać zabezpieczenie środowisk Jira |  | TAK/NIE\* |
|  | Licencjonowanie i wsparcie techniczne   * + 1. Wszystkie linie supportu muszą być obsługiwane w języku polskim.     2. Wsparcie techniczne musi być świadczone bezpośrednio przez główną siedzibę producenta.     3. Możliwość zgłaszania ticketów supportowych bezpośrednio z poziomu interfejsu zarządzania w formie czatu.     4. Producent wraz z rozwiązaniem musi udostępnić materiały samopomocowe w j. polskim (minimum dostęp do bazy wiedzy, materiałów wideo oraz kart produktów)     5. Wsparcie techniczne musi umożliwiać korzystanie z połączeń zdalnych, systemu ticketowego oraz wsparcia telefonicznego.     6. Licencje w ramach rozwiązania powinny pozwalać na zabezpieczenie określonej przez Zamawiającego ilości hostów w obrębie wspieranych przez System środowisk.     7. Licencje powinny być dostępne w opcji wieczystej .     8. Dostęp do wsparcia technicznego producenta powinno obowiązywać przez okres min. 24 miesięcy     9. Sposób licencjonowania opiera się na:        1. ilości serwerów/endpointów - dla fizycznych urządzeń,        2. ilości socketów w hostach - dla środowisk wirtualnych lub ilości maszyn wirtualnych,        3. ilość repozytoriów - dla GIT.     10. Licencje powinny umożliwiać zabezpieczenie w wersji wieczystej:         1. 12 stacji roboczych,         2. 2 serwery wirtualne, |  | TAK/NIE\* |
|  | Anty-ransomware i bezpieczeństwo:   * + 1. System plików rozwiązania musi być odporny na ataki Ransomware (zapewnić ochronę przed szyfrowaniem end-to-end, kopie zapasowe nie mogą być nadpisywane - "niezmienny system plików").     2. System powinien umożliwiać wykorzystanie wbudowanego menedżera haseł do przechowywania wszelkich sekretów (haseł, danych dostępowych, kluczy szyfrujących) wykorzystywanych przez System     3. System powinien umożliwiać przywrócenie hasła głównego administratora w przypadku jego utraty.     4. W ramach systemu, komunikacja pomiędzy hostem źródłowym, a magazynem powinna odbywać się tylko i wyłącznie bezpośrednio pomiędzy agentem backupu, a magazynem. Komunikacja nie może przechodzić przez serwer backupu, ani żaden inny komponent, którego awaria sparaliżowały by działanie Systemu. System nie może posiadać pojedynczego punktu awarii.   System musi działać w zgodzie z regułą Zero-knowledge Encryption. Oznacza to, że wszelkie sekrety muszą być przechowywane w centralnym Managerze Haseł w postaci zaszyfrowanej algorytmem AES i być udostępniane agentowi dopiero w momencie rozpoczęcia wykonywania kopii zapasowej. Sekrety nie mogą być przechowywane w konfiguracji agenta na zabezpieczonym urządzeniu. |  | TAK/NIE\* |
|  | **Serwer z oprogramowaniem systemowym i licencjami dostępowymi oraz systemem do wirtualizacji:**  **Urząd Gminy w Skrzyszowie (1 szt.)**  **- fabrycznie nowe urządzenie**  **Cena jednostkowa:**  **brutto zł za sztukę** | | |
|  | Marka/Model Serwera |  | TAK/NIE\* |
|  | Obudowa Rack o wysokości max 2U z możliwością instalacji min. 16 dysków 2.5” wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.. |  | TAK/NIE\* |
|  | Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera.  Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać min. 1TB pamięci RAM. |  | TAK/NIE\* |
|  | * + 1. Zainstalowane dwa procesory min. 8-rdzeniowe, min. 2.6GHz z częstotliwości nominalnej, klasy x86, osiągające minimalne wyniki testów w konfiguracji dwuprocesorowej:        1. SPECrate2017\_int\_base wynik min. 169pkt        2. SPECrate2017\_int\_peak wynik min. 174pkt        3. SPECrate2017\_fp\_base wynik min. 246pkt        4. SPECrate2017\_fp\_peak wynik min. 252pkt   Maksymalny TDP dla procesora 125W  Wynik testu musi być opublikowany na stronie https://www.spec.org/cpu2017/results/ w dniu złożenia oferty.  Do oferty należy załączyć wyniki testów - dołączyć do oferty jako przedmiotowy środek dowodowy. |  | TAK/NIE\* |
|  | RAM: 64GB (w układzie 2x32GB) |  | TAK/NIE\* |
|  | Funkcjonalność pamięci RAM:  Demand Scrubbing,  Patrol Scrubbing,  Permanent Fault Detection (PFD) |  | TAK/NIE\* |
|  | Gniazda PCI: Minimum 5 slotów PCIe x16 generacji 4 |  | TAK/NIE\* |
|  | Interfejsy sieciowe: Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 10/25Gb SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) |  | TAK/NIE\* |
|  | * + 1. Kontroler RAID: Sprzętowy kontroler dyskowy, posiadający        1. Min. 8GB nieulotnej pamięci cache,        2. Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60.        3. Wsparcie dla dysków samoszyfrujących |  | TAK/NIE\* |
|  | * + 1. Dyski twarde   Zainstalowane:   * + - 1. 2x dyski SAS 10k rpm o pojemności min. 600GB, Hot-Plug skonfigurowane w Raid1 pod virtualizator       2. 6x dysków SAS 10k rpm o pojemności min. 2,4TB, Hot-Plug skonfigurowane w Raid6   Możliwość zainstalowania dwóch dysków M.2 NVME o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1. |  | TAK/NIE\* |
|  | * + 1. Wbudowane porty:        1. 3xUSB z czego nie mniej niż 1x USB 3.0,        2. 2xVGA z czego jeden na panelu przednim. |  | TAK/NIE\* |
|  | Video: Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1900x1200 |  | TAK/NIE\* |
|  | Zasilacze: Redundantne, Hot-Plug max 700W każdy. Klasy Titanium |  | TAK/NIE\* |
|  | * + 1. Bezpieczeństwo        1. Zatrzask górnej pokrywy oraz blokada na ramce panela frontowego zamykane na klucz w celu do ochrony nieautoryzowanego dostępu do dysków twardych i wewnętrznych elementów serwera.        2. Możliwość wyłączenia w BIOS funkcji przycisku zasilania.        3. BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła        4. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.        5. Moduł TPM 2.0        6. Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera.        7. Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem. |  |  |
|  | Diagnostyka:  Serwer musi być wyposażony w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze. |  | TAK/NIE\* |
|  | * + 1. Karta Zarządzania:   Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:   * + - 1. zdalny dostęp do graficznego interfejsu Web karty zarządzającej;       2. zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);       3. szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;       4. wsparcie dla IPv6;       5. wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;       6. możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;       7. integracja z Active Directory;       8. wsparcie dla dynamic DNS;       9. wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.       10. możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera       11. możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera |  | TAK/NIE\* |
|  | * + 1. Certyfikaty:        1. Serwer musi być wyprodukowany zgodnie z normą ISO-9001, ISO-14001, ISO-50001 lub równoważną - dołączyć do oferty jako przedmiotowy środek dowodowy.        2. Serwer musi posiadać deklarację CE - dołączyć do oferty jako przedmiotowy środek dowodowy. |  | TAK/NIE\* |
|  | System operacyjny:  Zamawiający wymaga dostarczenia oprogramowania systemowego w najnowszej aktualnej wersji, nieograniczonej czasowo. Licencja musi uprawniać do uruchamiania oprogramowania systemowego (dalej: SSO) w postaci 2 wirtualnych środowisk SSO za pomocą wbudowanych mechanizmów wirtualizacji.  Dostarczona licencja musi być kompatybilna z dostarczonym serwerem oraz musi być zgodna z prawami licencyjnymi producenta.  SSO musi posiadać następujące, wbudowane cechy:   * + 1. możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym,     2. możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny,     3. możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania min. 8000 maszyn wirtualnych,     4. możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci,     5. wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy,     6. wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy,     7. automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego,     8. możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading),     9. wbudowane wsparcie instalacji i pracy na wolumenach, które:        1. pozwalają na zmianę rozmiaru w czasie pracy systemu,        2. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,        3. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,        4. umożliwiają zdefiniowanie list kontroli dostępu (ACL),     10. wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość,     11. wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających min. certyfikat FIPS 140-2     12. możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET,     13. możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów,     14. wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych,     15. graficzny interfejs użytkownika,     16. zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,     17. qwsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play),     18. możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu,     19. dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa,     20. możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:         1. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,         2. usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:            - podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,            - ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,            - odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,         3. zdalna dystrybucja oprogramowania na stacje robocze,         4. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej,         5. centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:            - dystrybucję certyfikatów poprzez http,            - konsolidację CA dla wielu lasów domeny,            - automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,         6. szyfrowanie plików i folderów,         7. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),         8. możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów,         9. serwis udostępniania stron WWW,         10. wsparcie dla protokołu IP w wersji 6 (IPv6),         11. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 1000 aktywnych środowisk wirtualnych systemów operacyjnych.     21. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:         1. dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,         2. obsługi ramek typu jumbo frames dla maszyn wirtualnych,         3. obsługi 4-KB sektorów dysków,         4. nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,         5. możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API,         6. możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model),         7. możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet,         8. wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath),         9. możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego,         10. mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty,         11. możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.   **Zamawiający wymaga dostarczenia nośnika downgreade 1 wersje wcześniejszej oferowanego Systemu operacyjnego wraz z kluczem aktywacyjnym jeśli jest wymagany do poprawnej pracy systemu.** |  | TAK/NIE\* |
|  | Licencje dostępowe: należy dostarczyć dodatkowo 45 licencji dostępowych do serwera dla użytkowników |  | TAK/NIE\* |
|  | Warunki gwarancji   * + 1. Gwarancja producenta musi wynosić minimum gwarancji udzielonej przez Wykonawcę/Oferenta z czasem reakcji do 48 godzin od przyjęcia zgłoszenia     2. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.     3. Wymagane dołączenie do oferty oświadczenia Wykonawcy potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta – dołączyć dokumenty do oferty jako przedmiotowy środek dowodowy.     4. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej tj. realizacji gwarancji, serwisu w terminach określonych w umowie. Certyfikowany Technik wykonawcy / producenta/ autoryzowanego partnera serwisowego producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego z zachowaniem terminów określonych w umowie od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.     5. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta.     6. 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.     7. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.     8. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji urządzenia.     9. Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. |  | TAK/NIE\* |
|  | System do wirtualizacji:   * + 1. Wymagania funkcjonalne        1. Obsługa maszyn wirtualnych (KVM) i kontenerów LXC        2. Możliwość tworzenia i zarządzania snapshot’ami        3. Możliwość migracji L2/L3 (live migration)        4. Integracja z Ceph, ZFS, NFS, iSCSI, GlusterFS (opcjonalnie)   2. Zarządzanie   * + - 1. Interfejs webowy do zarządzania środowiskiem wirtualizacji       2. Monitorowanie wykorzystania zasobów (CPU, RAM, dyski, sieć)       3. Możliwość tworzenia VLAN-ów i mostków sieciowych     1. Bezpieczeństwo        1. Integrowany firewall (Proxmox Firewall)        2. Możliwość integracji z LDAP/AD        3. Brak wpływu na bezpieczeństwo infrastruktury fizycznej     2. Skalowalność        1. Możliwość rozbudowy do klastra wieloserwerowego        2. Wsparcie dla rozproszonego magazynu danych     3. Roczyny dostęp do repozytorium oraz do stabilnych aktualizacji oprogramowania |  | TAK/NIE\* |
|  | **Serwer z systemem do wirtualizacji:**  **Urząd Gminy w Skrzyszowie (1 szt.)**  **Cena jednostkowa:**  **brutto zł za sztukę** | | |
|  | Marka/Model Serwera |  | TAK/NIE\* |
|  | Obudowa Rack o wysokości max 2U z możliwością instalacji min. 16 dysków 2.5” wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.. |  | TAK/NIE\* |
|  | Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera.  Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać min. 1TB pamięci RAM. |  | TAK/NIE\* |
|  | * + 1. Zainstalowane dwa procesory min. 8-rdzeniowe, min. 2.6GHz z częstotliwości nominalnej, klasy x86, osiągające minimalne wyniki testów w konfiguracji dwuprocesorowej:        1. SPECrate2017\_int\_base wynik min. 169pkt        2. SPECrate2017\_int\_peak wynik min. 174pkt        3. SPECrate2017\_fp\_base wynik min. 246pkt        4. SPECrate2017\_fp\_peak wynik min. 252pkt   Maksymalny TDP dla procesora 125W  Wynik testu musi być opublikowany na stronie https://www.spec.org/cpu2017/results/ w dniu złożenia oferty.  Do oferty należy załączyć wyniki testów - dołączyć do oferty jako przedmiotowy środek dowodowy. |  | TAK/NIE\* |
|  | RAM: 64GB (w układzie 2x32GB) |  | TAK/NIE\* |
|  | Funkcjonalność pamięci RAM:  Demand Scrubbing,  Patrol Scrubbing,  Permanent Fault Detection (PFD) |  | TAK/NIE\* |
|  | Gniazda PCI: Minimum 5 slotów PCIe x16 generacji 4 |  | TAK/NIE\* |
|  | Interfejsy sieciowe: Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 10/25Gb SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) |  | TAK/NIE\* |
|  | * + 1. Kontroler RAID: Sprzętowy kontroler dyskowy, posiadający        1. Min. 8GB nieulotnej pamięci cache,        2. Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60.        3. Wsparcie dla dysków samoszyfrujących |  | TAK/NIE\* |
|  | * + 1. Dyski twarde   Zainstalowane:   * + - 1. 2x dyski SAS 10k rpm o pojemności min. 600GB, Hot-Plug skonfigurowane w Raid1 pod virtualizator       2. 6x dysków SAS 10k rpm o pojemności min. 2,4TB, Hot-Plug skonfigurowane w Raid6   Możliwość zainstalowania dwóch dysków M.2 NVME o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1. |  | TAK/NIE\* |
|  | * + 1. Wbudowane porty:        1. 3 x USB z czego nie mniej niż 1x USB 3.0,        2. 2xVGA z czego jeden na panelu przednim. |  | TAK/NIE\* |
|  | Video: Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1900x1200 |  | TAK/NIE\* |
|  | Zasilacze: Redundantne, Hot-Plug max 700W każdy. Klasy Titanium |  | TAK/NIE\* |
|  | * + 1. Bezpieczeństwo        1. Zatrzask górnej pokrywy oraz blokada na ramce panela frontowego zamykane na klucz w celu do ochrony nieautoryzowanego dostępu do dysków twardych i wewnętrznych elementów serwera.        2. Możliwość wyłączenia w BIOS funkcji przycisku zasilania.        3. BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła        4. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.        5. Moduł TPM 2.0        6. Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera.        7. Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem. |  | TAK/NIE\* |
|  | Diagnostyka:  Serwer musi być wyposażony w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze. |  | TAK/NIE\* |
|  | Karta Zarządzania   * + 1. Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:        1. zdalny dostęp do graficznego interfejsu Web karty zarządzającej;        2. zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);        3. szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;        4. wsparcie dla IPv6;        5. wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;        6. możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;        7. integracja z Active Directory;        8. wsparcie dla dynamic DNS;        9. wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.        10. możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera        11. możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera |  | TAK/NIE\* |
|  | * + 1. Certyfikaty:        1. Serwer musi być wyprodukowany zgodnie z normą ISO-9001, ISO-14001, ISO-50001 lub równoważną - dołączyć do oferty jako przedmiotowy środek dowodowy.        2. Serwer musi posiadać deklarację CE - dołączyć do oferty jako przedmiotowy środek dowodowy. |  | TAK/NIE\* |
|  | Warunki gwarancji   * + 1. Gwarancja producenta musi wynosić minimum gwarancji udzielonej przez wykonawcę/oferenta z czasem reakcji do 48 godzin od przyjęcia zgłoszenia     2. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego     3. Wymagane dołączenie do oferty oświadczenia Wykonawcy potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta – dołączyć dokumenty do oferty jako przedmiotowy środek dowodowy.     4. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej tj. realizacji gwarancji, serwisu w terminach określonych w umowie. Certyfikowany Technik wykonawcy / producenta/ autoryzowanego partnera serwisowego producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego z zachowaniem terminów określonych w umowie od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.     5. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta.     6. 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.     7. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.     8. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji urządzenia.     9. Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. |  | TAK/NIE\* |
|  | System do wirtualizacji:   * + 1. Wymagania funkcjonalne        1. Obsługa maszyn wirtualnych (KVM) i kontenerów LXC        2. Możliwość tworzenia i zarządzania snapshot’ami        3. Możliwość migracji L2/L3 (live migration)        4. Integracja z Ceph, ZFS, NFS, iSCSI, GlusterFS (opcjonalnie)     2. Zarządzanie        1. Interfejs webowy do zarządzania środowiskiem wirtualizacji        2. Monitorowanie wykorzystania zasobów (CPU, RAM, dyski, sieć)        3. Możliwość tworzenia VLAN-ów i mostków sieciowych     3. Bezpieczeństwo        1. Integrowany firewall (Proxmox Firewall)        2. Możliwość integracji z LDAP/AD        3. Brak wpływu na bezpieczeństwo infrastruktury fizycznej     4. Skalowalność        1. Możliwość rozbudowy do klastra wieloserwerowego        2. Wsparcie dla rozproszonego magazynu danych     5. Roczyny dostęp do repozytorium oraz do stabilnych aktualizacji oprogramowania |  | TAK/NIE\* |
|  | **Serwer z systemem do wirtualizacji:**  **Urząd Gminy w Skrzyszowie (1 szt.)**  **Cena jednostkowa:**  **brutto zł za sztukę** | | |
|  | Marka/Model Serwera |  | TAK/NIE\* |
|  | Obudowa Rack o wysokości max 2U z możliwością instalacji min. 16 dysków 2.5” wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.. |  | TAK/NIE\* |
|  | Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera.  Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać min. 1TB pamięci RAM. |  | TAK/NIE\* |
|  | * + 1. Zainstalowane dwa procesory min. 8-rdzeniowe, min. 2.6GHz z częstotliwości nominalnej, klasy x86, osiągające minimalne wyniki testów w konfiguracji dwuprocesorowej:        1. SPECrate2017\_int\_base wynik min. 169pkt        2. SPECrate2017\_int\_peak wynik min. 174pkt        3. SPECrate2017\_fp\_base wynik min. 246pkt        4. SPECrate2017\_fp\_peak wynik min. 252pkt   Maksymalny TDP dla procesora 125W  Wynik testu musi być opublikowany na stronie https://www.spec.org/cpu2017/results/ w dniu złożenia oferty.  Do oferty należy załączyć wyniki testów - dołączyć do oferty jako przedmiotowy środek dowodowy. |  | TAK/NIE\* |
|  | RAM: 64GB (w układzie 2x32GB) |  | TAK/NIE\* |
|  | Funkcjonalność pamięci RAM:  Demand Scrubbing,  Patrol Scrubbing,  Permanent Fault Detection (PFD) |  | TAK/NIE\* |
|  | Gniazda PCI: Minimum 5 slotów PCIe x16 generacji 4 |  | TAK/NIE\* |
|  | Interfejsy sieciowe: Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 10/25Gb SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) |  | TAK/NIE\* |
|  | * + 1. Kontroler RAID: Sprzętowy kontroler dyskowy, posiadający        1. Min. 8GB nieulotnej pamięci cache,        2. Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60.        3. Wsparcie dla dysków samoszyfrujących |  | TAK/NIE\* |
|  | Dyski twarde   * + 1. Zainstalowane:        1. 2x dyski SAS 10k rpm o pojemności min. 600GB, Hot-Plug skonfigurowane w Raid1 pod virtualizator        2. 8x dysków SAS 10k rpm o pojemności min. 2,4TB, Hot-Plug skonfigurowane w Raid6   Możliwość zainstalowania dwóch dysków M.2 NVME o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1. |  | TAK/NIE\* |
|  | * + 1. Wbudowane porty:        1. 3 x USB z czego nie mniej niż 1x USB 3.0,        2. 2xVGA z czego jeden na panelu przednim. |  | TAK/NIE\* |
|  | Video: Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1900x1200 |  | TAK/NIE\* |
|  | Zasilacze: Redundantne, Hot-Plug max 700W każdy. Klasy Titanium |  | TAK/NIE\* |
|  | * + 1. Bezpieczeństwo        1. Zatrzask górnej pokrywy oraz blokada na ramce panela frontowego zamykane na klucz w celu do ochrony nieautoryzowanego dostępu do dysków twardych i wewnętrznych elementów serwera.        2. Możliwość wyłączenia w BIOS funkcji przycisku zasilania.        3. BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła        4. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.        5. Moduł TPM 2.0        6. Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera.        7. Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem. |  | TAK/NIE\* |
|  | Diagnostyka:  Serwer musi być wyposażony w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze. |  | TAK/NIE\* |
|  | Karta Zarządzania:   * + 1. Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:        1. zdalny dostęp do graficznego interfejsu Web karty zarządzającej;        2. zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);        3. szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;        4. wsparcie dla IPv6;        5. wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;        6. możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;        7. integracja z Active Directory;        8. wsparcie dla dynamic DNS;        9. wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.        10. możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera        11. możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera |  | TAK/NIE\* |
|  | * + 1. Certyfikaty:        1. Serwer musi być wyprodukowany zgodnie z normą ISO-9001, ISO-14001, ISO-50001 lub równoważną - dołączyć do oferty jako przedmiotowy środek dowodowy.        2. Serwer musi posiadać deklarację CE - dołączyć do oferty jako przedmiotowy środek dowodowy. |  | TAK/NIE\* |
|  | Warunki gwarancji   * + 1. Gwarancja producenta musi wynosić minimum gwarancji udzielonej przez Wykonawcę z czasem reakcji do 48 godzin od przyjęcia zgłoszenia.     2. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.     3. Wymagane dołączenie do oferty oświadczenia Wykonawcy potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta – dołączyć dokumenty do oferty jako przedmiotowy środek dowodowy.     4. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej tj. realizacji gwarancji, serwisu w terminach określonych w umowie. Certyfikowany Technik wykonawcy / producenta/ autoryzowanego partnera serwisowego producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego z zachowaniem terminów określonych w umowie od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.     5. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta.     6. 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.     7. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.     8. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji urządzenia.     9. Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. |  | TAK/NIE\* |
|  | System do wirtualizacji:   * + 1. Wymagania funkcjonalne        1. Obsługa maszyn wirtualnych (KVM) i kontenerów LXC        2. Możliwość tworzenia i zarządzania snapshot’ami        3. Możliwość migracji L2/L3 (live migration)        4. Integracja z Ceph, ZFS, NFS, iSCSI, GlusterFS (opcjonalnie)     2. Zarządzanie        1. Interfejs webowy do zarządzania środowiskiem wirtualizacji        2. Monitorowanie wykorzystania zasobów (CPU, RAM, dyski, sieć)        3. Możliwość tworzenia VLAN-ów i mostków sieciowych     3. Bezpieczeństwo        1. Integrowany firewall (Proxmox Firewall)        2. Możliwość integracji z LDAP/AD        3. Brak wpływu na bezpieczeństwo infrastruktury fizycznej     4. Skalowalność        1. Możliwość rozbudowy do klastra wieloserwerowego        2. Wsparcie dla rozproszonego magazynu danych     5. Roczyny dostęp do repozytorium oraz do stabilnych aktualizacji oprogramowania |  | TAK/NIE\* |
|  | **Serwer z oprogramowaniem systemowym i licencjami dostępowymi oraz systemem do wirtualizacji:**  **Centrum Usług Społecznych w Skrzyszowie (1 szt.)**  **Cena jednostkowa:**  **brutto zł za sztukę** | | |
|  | Marka/Model serwera |  | TAK/NIE\* |
|  | Obudowa Rack o wysokości max 1U z możliwością instalacji 8 dysków 2.5”  Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych |  | TAK/NIE\* |
|  | Chipset: Dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych |  | TAK/NIE\* |
|  | Procesor   * + 1. Zainstalowany jeden procesor minimum 8-rdzeniowy, min. 2.8GHz częstotliwości nominalnej, osiągający minimalne wyniki testów w konfiguracji jednoprocesorowej:        1. SPECrate2017\_int\_base wynik min. 89pkt        2. SPECrate2017\_int\_peak wynik min. 93pkt        3. SPECrate2017\_fp\_base wynik min. 105pkt        4. SPECrate2017\_fp\_peak wynik min. 106pkt   Maksymalny TDP dla procesora 80W  Wynik testu musi być opublikowany na stronie https://www.spec.org/cpu2017/results/ w dniu złożenia oferty.  Do oferty należy załączyć wyniki testów - dołączyć do oferty jako przedmiotowy środek dowodowy.. |  | TAK/NIE\* |
|  | Pamięć RAM: Min. 32GB pamięci RAM DDR5 UDIMM |  | TAK/NIE\* |
|  | Karta graficzna: Zintegrowana karta graficzna, umożliwiająca wyświetlanie obrazu w rozdzielczości minimum 1280x1024 pikseli |  | TAK/NIE\* |
|  | Gniazda PCI: Minimum 2 sloty PCIe Gen4 z czego jeden wolny po obsadzeniu wymaganymi kartami sieciowymi pod przyszłą rozbudowę |  | TAK/NIE\* |
|  | Interfejsy sieciowe: 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 10/25Gb SFP28 |  | TAK/NIE\* |
|  | Kontroler RAID:  Sprzętowy kontroler dyskowy, posiadający:   * + Min. 8GB nieulotnej pamięci cache,   + Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60.   + Wsparcie dla dysków samoszyfrujących |  | TAK/NIE\* |
|  | Dyski twarde   * + 1. Zainstalowane:        1. 2x dyski SAS 10k rpm o pojemności min. 600GB, Hot-Plug skonfigurowane w Raid1 pod virtualizator        2. 6x dysków SAS 10k rpm o pojemności min. 2,4TB, Hot-Plug skonfigurowane w Raid6   Możliwość zainstalowania dwóch dysków M.2 NVME o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1. |  | TAK/NIE\* |
|  | Karta graficzna:  Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200 |  | TAK/NIE\* |
|  | Wbudowane porty: Min. 4 porty USB w tym 1 port USB 3.0 z tyłu obudowy, 1 port VGA na tylnym panelu |  | TAK/NIE\* |
|  | Bezpieczeństwo: Zintegrowany z płytą główną moduł TPM 2.0 |  | TAK/NIE\* |
|  | Diagnostyka: Obudowa wyposażona w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze. |  | TAK/NIE\* |
|  | Karta Zarządzania   * + 1. Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:        1. zdalny dostęp do graficznego interfejsu Web karty zarządzającej;        2. zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);        3. szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;        4. możliwość podmontowania zdalnych wirtualnych napędów;        5. wirtualną konsolę z dostępem do myszy, klawiatury;        6. wsparcie dla IPv6;        7. wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;        8. możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;        9. możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;        10. integracja z Active Directory;        11. możliwość obsługi przez dwóch administratorów jednocześnie;        12. wsparcie dla dynamic DNS;        13. wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.        14. możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera        15. możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera oraz z możliwością rozszerzenia funkcjonalności o:            - Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej            - Przesyłanie danych telemetrycznych w czasie rzeczywistym            - Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze            - Automatyczna rejestracja certyfikatów (ACE) |  | TAK/NIE\* |
|  | * + 1. Certyfikaty:        1. Serwer musi być wyprodukowany zgodnie z normą ISO-9001, ISO-14001, ISO-50001 lub równoważną - dołączyć do oferty jako przedmiotowy środek dowodowy.        2. Serwer musi posiadać deklarację CE - dołączyć do oferty jako przedmiotowy środek dowodowy. |  | TAK/NIE\* |
|  | System operacyjny:  Zamawiający wymaga dostarczenia oprogramowania systemowego w najnowszej aktualnej wersji, nieograniczonej czasowo. Licencja musi uprawniać do uruchamiania oprogramowania systemowego (dalej: SSO) w postaci 2 wirtualnych środowisk SSO za pomocą wbudowanych mechanizmów wirtualizacji.  Dostarczona licencja musi być kompatybilna z dostarczonym serwerem oraz musi być zgodna z prawami licencyjnymi producenta.  SSO musi posiadać następujące, wbudowane cechy:   * + 1. możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym,     2. możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny,     3. możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania min. 8000 maszyn wirtualnych,     4. możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci,     5. wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy,     6. wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy,     7. automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego,     8. możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading),     9. wbudowane wsparcie instalacji i pracy na wolumenach, które:        1. pozwalają na zmianę rozmiaru w czasie pracy systemu,        2. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,        3. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,        4. umożliwiają zdefiniowanie list kontroli dostępu (ACL),     10. wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość,     11. wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających min. certyfikat FIPS 140-2     12. możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET,     13. możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów,     14. wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych,     15. graficzny interfejs użytkownika,     16. zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,     17. wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play),     18. możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu,     19. dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa,     20. możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:         1. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,         2. usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:            - podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,            - ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,            - odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,         3. zdalna dystrybucja oprogramowania na stacje robocze,         4. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej,         5. centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:            - dystrybucję certyfikatów poprzez http,            - konsolidację CA dla wielu lasów domeny,            - automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,         6. szyfrowanie plików i folderów,         7. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),         8. możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów,         9. serwis udostępniania stron WWW,         10. wsparcie dla protokołu IP w wersji 6 (IPv6),         11. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:             - dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,             - obsługi ramek typu jumbo frames dla maszyn wirtualnych,             - obsługi 4-KB sektorów dysków,             - nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,             - możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API,             - możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model),         12. możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet,         13. wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath),         14. możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego,         15. mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty,         16. możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.   **Zamawiający wymaga dostarczenia nośnika downgreade 1 wersje wcześniejszej oferowanego Systemu operacyjnego wraz z kluczem aktywacyjnym jeśli jest wymagany do poprawnej pracy systemu.** |  | TAK/NIE\* |
|  | Licencje dostępowe: Należy dostarczyć dodatkowo 12 licencji dostępowych do serwera dla użytkowników |  | TAK/NIE\* |
|  | Warunki gwarancji   * + 1. Gwarancja producenta musi wynosić minimum gwarancji udzielonej przez wykonawcę/oferenta z czasem reakcji do 48 godzin od przyjęcia zgłoszenia.     2. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.     3. Wymagane dołączenie do oferty oświadczenia Wykonawcy potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta – dokumenty potwierdzające należy załączyć do oferty jako przedmiotowy środek dowodowy.     4. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej tj. realizacji gwarancji, serwisu w terminach określonych w umowie. Certyfikowany Technik wykonawcy / producenta/ autoryzowanego partnera serwisowego producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego z zachowaniem terminów określonych w umowie od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.     5. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta.     6. 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.     7. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.     8. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji urządzenia.     9. Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. |  | TAK/NIE\* |
|  | System do wirtualizacji   * + 1. Wymagania funkcjonalne        1. Obsługa maszyn wirtualnych (KVM) i kontenerów LXC        2. Możliwość tworzenia i zarządzania snapshot’ami        3. Możliwość migracji L2/L3 (live migration)        4. Integracja z Ceph, ZFS, NFS, iSCSI, GlusterFS (opcjonalnie)     2. Zarządzanie        1. Interfejs webowy do zarządzania środowiskiem wirtualizacji        2. Monitorowanie wykorzystania zasobów (CPU, RAM, dyski, sieć)        3. Możliwość tworzenia VLAN-ów i mostków sieciowych     3. Bezpieczeństwo        1. Integrowany firewall (Proxmox Firewall)        2. Możliwość integracji z LDAP/AD        3. Brak wpływu na bezpieczeństwo infrastruktury fizycznej     4. Skalowalność        1. Możliwość rozbudowy do klastra wieloserwerowego        2. Wsparcie dla rozproszonego magazynu danych     5. Roczyny dostęp do repozytorium oraz do stabilnych aktualizacji oprogramowania |  | TAK/NIE\* |
|  | **Serwer z systemem do wirtualizacji:**  **Centrum Usług Społecznych w Skrzyszowie (1 szt.)**  **Cena jednostkowa: brutto zł za sztukę** | | |
|  | Marka/Model serwera |  | TAK/NIE\* |
|  | Obudowa Rack o wysokości max 1U z możliwością instalacji 8 dysków 2.5”  Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych |  | TAK/NIE\* |
|  | Chipset: Dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych |  | TAK/NIE\* |
|  | Procesor   * + 1. Zainstalowany jeden procesor minimum 8-rdzeniowy, min. 2.8GHz częstotliwości nominalnej, osiągający minimalne wyniki testów w konfiguracji jednoprocesorowej:        1. SPECrate2017\_int\_base wynik min. 89pkt        2. SPECrate2017\_int\_peak wynik min. 93pkt        3. SPECrate2017\_fp\_base wynik min. 105pkt        4. SPECrate2017\_fp\_peak wynik min. 106pkt   Maksymalny TDP dla procesora 80W  Wynik testu musi być opublikowany na stronie https://www.spec.org/cpu2017/results/ w dniu złożenia oferty.  Do oferty należy załączyć wyniki testów - dołączyć do oferty jako przedmiotowy środek dowodowy.. |  | TAK/NIE\* |
|  | Pamięć RAM: Min. 32GB pamięci RAM DDR5 UDIMM |  | TAK/NIE\* |
|  | Karta graficzna: Zintegrowana karta graficzna, umożliwiająca wyświetlanie obrazu w rozdzielczości minimum 1280x1024 pikseli |  | TAK/NIE\* |
|  | Gniazda PCI: Minimum 2 sloty PCIe Gen4 z czego jeden wolny po obsadzeniu wymaganymi kartami sieciowymi pod przyszłą rozbudowę |  | TAK/NIE\* |
|  | Interfejsy sieciowe: 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 10/25Gb SFP28 |  | TAK/NIE\* |
|  | Kontroler RAID   * + 1. Sprzętowy kontroler dyskowy, posiadający:        1. Min. 8GB nieulotnej pamięci cache,        2. Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60.        3. Wsparcie dla dysków samoszyfrujących |  | TAK/NIE\* |
|  | Dyski twarde   * + 1. Zainstalowane:        1. 2x dyski SAS 10k rpm o pojemności min. 600GB, Hot-Plug skonfigurowane w Raid1 pod virtualizator        2. 6x dysków SAS 10k rpm o pojemności min. 2,4TB, Hot-Plug skonfigurowane w Raid6   Możliwość zainstalowania dwóch dysków M.2 NVME o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1. |  | TAK/NIE\* |
|  | Karta graficzna:  Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200 |  | TAK/NIE\* |
|  | Wbudowane porty: Min. 4 porty USB w tym 1 port USB 3.0 z tyłu obudowy, 1 port VGA na tylnym panelu |  | TAK/NIE\* |
|  | Bezpieczeństwo: Zintegrowany z płytą główną moduł TPM 2.0 |  | TAK/NIE\* |
|  | Diagnostyka: Obudowa wyposażona w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze. |  | TAK/NIE\* |
|  | Karta Zarządzania   * + 1. Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:        1. zdalny dostęp do graficznego interfejsu Web karty zarządzającej;        2. zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);        3. szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;        4. możliwość podmontowania zdalnych wirtualnych napędów;        5. wirtualną konsolę z dostępem do myszy, klawiatury;        6. wsparcie dla IPv6;        7. wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;        8. możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;        9. możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;        10. integracja z Active Directory;        11. możliwość obsługi przez dwóch administratorów jednocześnie;        12. wsparcie dla dynamic DNS;        13. wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.        14. możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera        15. możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera oraz z możliwością rozszerzenia funkcjonalności o:            - Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej            - Przesyłanie danych telemetrycznych w czasie rzeczywistym            - Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze            - Automatyczna rejestracja certyfikatów (ACE) |  | TAK/NIE\* |
|  | * + 1. Certyfikaty:        1. Serwer musi być wyprodukowany zgodnie z normą ISO-9001, ISO-14001, ISO-50001 lub równoważną - dołączyć do oferty jako przedmiotowy środek dowodowy.        2. Serwer musi posiadać deklarację CE - dołączyć do oferty jako przedmiotowy środek dowodowy. |  | TAK/NIE\* |
|  | Warunki gwarancji   * + 1. Gwarancja producenta musi wynosić minimum gwarancji udzielonej przez wykonawcę/oferenta z czasem reakcji do 48 godzin od przyjęcia zgłoszenia     2. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego     3. Wymagane dołączenie do oferty oświadczenia Wykonawcy potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta – dokumenty potwierdzające należy załączyć do oferty jako przedmiotowy środek dowodowy.     4. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej tj. realizacji gwarancji, serwisu w terminach określonych w umowie. Certyfikowany Technik wykonawcy / producenta/ autoryzowanego partnera serwisowego producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego z zachowaniem terminów określonych w umowie od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.     5. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta.     6. 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.     7. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.     8. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji urządzenia.     9. Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. |  | TAK/NIE\* |
|  | System do wirtualizacji   * + 1. Wymagania funkcjonalne        1. Obsługa maszyn wirtualnych (KVM) i kontenerów LXC        2. Możliwość tworzenia i zarządzania snapshot’ami        3. Możliwość migracji L2/L3 (live migration)        4. Integracja z Ceph, ZFS, NFS, iSCSI, GlusterFS (opcjonalnie)     2. Zarządzanie        1. Interfejs webowy do zarządzania środowiskiem wirtualizacji        2. Monitorowanie wykorzystania zasobów (CPU, RAM, dyski, sieć)        3. Możliwość tworzenia VLAN-ów i mostków sieciowych     3. Bezpieczeństwo        1. Integrowany firewall (Proxmox Firewall)        2. Możliwość integracji z LDAP/AD        3. Brak wpływu na bezpieczeństwo infrastruktury fizycznej     4. Skalowalność        1. Możliwość rozbudowy do klastra wieloserwerowego        2. Wsparcie dla rozproszonego magazynu danych     5. Roczyny dostęp do repozytorium oraz do stabilnych aktualizacji oprogramowania |  | TAK/NIE\* |
|  | **Dyski Zewnętrzne:**  **Urząd Gminy w Skrzyszowie (30 szt.)**  **Centrum Usług Społecznych (10 szt.)**  **- fabrycznie nowe**  **Cena jednostkowa:**  **brutto zł za sztukę** | | |
|  | Marka/Model dysku |  | TAK/NIE\* |
|  | Typ dysku: zewnętrzny |  | TAK/NIE\* |
|  | Interfejs: USB |  | TAK/NIE\* |
|  | Rodzaj dysku: SSD |  | TAK/NIE\* |
|  | Pojemność: min 500GB |  | TAK/NIE\* |