

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 | | |
| I. | PRZELĄCZNIKI SIECIOWE ZARZĄDZALNE – URZĄD GMINY W SKRZYSZOWIE (5 SZT.), CENTRUM USŁUG SPOŁECZNYCH W SKRZYSZOWIE (2 SZT.) FABRYCZNIE NOWE URZĄDZENIA/ CENA JEDNOSTKOWA: BRUTTO ZŁ ZA SZTUKĘ | | |
| a. | Marka/Model przełącznika | | TAK/NIE* |
| b. | Przełącznik dostępowy gigabitowy | | TAK/NIE* |
| c. | Porty przełącznika: minimum 24x 10/100/1000Base-T RJ45 oraz minimum 4x 1/10GBase-X SFP+ | | TAK/NIE* |
| d. | Port konsolowy: RJ45 (RS-232) | | TAK/NIE* |
| e. | Port USB: minimum 1 port co najmniej w standardzie 2.0 | | TAK/NIE* |
| f. | Szybkość przełączania: minimum 128Gb/s | | TAK/NIE* |
| g. | Przepustowość: minimum 95Mp/s (dla pakietów 64Kb) | | TAK/NIE* |
| h. | Bufor pakietów: minimum 1,5MB | | TAK/NIE* |
| i. | Ramki Jumbo: minimum 10k | | TAK/NIE* |
| j. | Tablica adresów MAC: minimum 16k | | TAK/NIE* |
| k. | Adresy MAC – Multicast: minimum 4k | | TAK/NIE* |

| | | | |
|-----|--|--|----------|
| l. | Tablica ACL: minimum 512 | | TAK/NIE* |
| m. | Tablica VLAN: minimum 4k | | TAK/NIE* |
| n. | Taktowanie procesora: minimum 800MHz | | TAK/NIE* |
| o. | Pamięć Flash: minimum 32MB | | TAK/NIE* |
| p. | Pamięć RAM: minimum 256MB | | TAK/NIE* |
| q. | Temperatura pracy: zakres minimum 0°C - 50°C | | TAK/NIE* |
| r. | Wilgotność względna: zakres minimum 10% - 90% (bez kondensacji) | | TAK/NIE* |
| s. | Zasilanie: zabudowany zasilacz 230V AC | | TAK/NIE* |
| t. | Pobór mocy: maksymalnie 21W | | TAK/NIE* |
| u. | Zabezpieczenie przeciwprzepięciowe: minimum 6kV | | TAK/NIE* |
| v. | Wymiary: maksymalna: szerokość 440 mm, wysokość 44mm , głębokość 170mm | | TAK/NIE* |
| w. | Certyfikaty bezpieczeństwa: CE, RoHS | | TAK/NIE* |
| x. | Algorytm: Store and Forward | | TAK/NIE* |
| y. | 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* |
| z. | DHCP: IPv4/IPv6 DHCP Client, IPv4/IPv6 DHCP Relay, Option 82, IPv4/IPv6 DHCP Snooping, IPv4/IPv6 DHCP Server | | TAK/NIE* |
| aa. | Spanning tree: IEEE802.1D (STP), IEEE802.1W (RSTP), IEEE802.1S (MSTP), Multi-Process MSTP, Root Guard, BPDU guard, BPDU forwarding | | TAK/NIE* |
| bb. | Protekcja ringowa: ITU-T G.8032 – recovery time < 50ms, Fast Link, Loopback Detection | | TAK/NIE* |
| cc. | Agregacja łączy: IEEE 802.3ad (LACP), 64 groups per device / 8 ports per group, load balance | | TAK/NIE* |
| dd. | 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* |
| ee. | Multicast: IGMP v1/v2/v3 snooping and L2 Query, IGMP Fast leave, MVR, MLD v1/v2 Snooping, IPv4/IPv6 DCSCM, IGMP authentication | | TAK/NIE* |
| ff. | QoS: 8 queues 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* |
| gg. | 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* |
| hh. | Diagnostyka: sFlow, Traffic Analysis, RSPAN, VCT, Ping, Trace Route, Dying GASP | | TAK/NIE* |
| ii. | Zarządzanie: TFTP/FTP, CLI, Telnet, Console, Web/SSL (IPv4/IPv6), SSH (IPv4/IPv6), SNMP v1/v2c/v3, SNMP Trap, Public & Private MIB | | TAK/NIE* |



| | | | |
|---|---|--|----------|
| | 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 | | |
| jj. | 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* |
| kk. | Gwarancja producenta musi wynosić minimum gwarancji udzielonej przez Wykonawcę | | TAK/NIE* |
| II. Urządzenie UTM: Centrum Usług Społecznych w Skrzyszowie (1 szt.) - FABRYCZNIE NOWE CENA JEDNOSTKOWA: BRUTTO ZŁ ZA SZTUKĘ | | | |
| a. | Marka/Model urządzenia UTM | | TAK/NIE* |
| b. | 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* |
| c. | 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* |
| d. | Interfejsy, Dysk, Zasilanie: 1.System realizujący funkcję Firewall dysponuje co | | TAK/NIE* |



| | | | |
|----|---|--|----------|
| | <p>najmniej poniższą liczbą i rodzajem interfejsów:</p> <p>a) 5 portami Gigabit Ethernet RJ-45.</p> <p>2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB.</p> <p>3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.</p> <p>4. System jest wyposażony w zasilanie AC.</p> | | |
| e. | <p>Parametry wydajnościowe:</p> <p>1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę.</p> <p>2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B.</p> <p>3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps.</p> <p>4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 4 Gbps.</p> <p>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.</p> <p>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.</p> <p>7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps.</p> | | TAK/NIE* |
| f. | <p>Funkcje Systemu Bezpieczeństwa:</p> <p>W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:</p> <p>1. Kontrola dostępu - zaporą ogniową klasy Stateful Inspection.</p> <p>2. Kontrola Aplikacji.</p> <p>3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN.</p> <p>4. Ochrona przed malware.</p> <p>5. Ochrona przed atakami - Intrusion Prevention System.</p> <p>6. Kontrola stron WWW.</p> <p>7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP.</p> <p>8. Zarządzanie pasmem (QoS, Traffic shaping).</p> <p>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.</p> <p>10. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP,</p> | | TAK/NIE* |



| | | | |
|----|---|--|----------|
| | <p>POP3.</p> <p>11.Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system.</p> <p>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).</p> | | |
| g. | <p>Polityki, Firewall:</p> <p>1.Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.</p> <p>2.System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:</p> <p>a)Translację jeden do jeden oraz jeden do wielu.</p> <p>b)Dedykowany ALG (Application Level Gateway) dla protokołu SIP.</p> <p>3.W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.</p> <p>4.Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: adresy URL, adresy IP.</p> <p>5.Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.</p> <p>6.Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.</p> <p>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.</p> <p>a)Amazon Web Services (AWS).</p> <p>b)Microsoft Azure.</p> <p>c)Cisco ACL.</p> <p>d)Google Cloud Platform (GCP).</p> <p>e)OpenStack.</p> <p>f)VMware NSX.</p> <p>g)Kubernetes.</p> | | TAK/NIE* |
| h. | <p>Połączenia VPN</p> <p>1.System umożliwia konfigurację połączeń typu IPsec VPN. W zakresie tej funkcji zapewnia:</p> <p>a)Wsparcie dla IKE v1 oraz v2.</p> <p>b)Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).</p> <p>c)Obsługa protokołu Diffie-Hellman grup 19, 20.</p> <p>d)Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.</p> <p>e)Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.</p> <p>f)Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.</p> <p>g)Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.</p> <p>h)Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.</p> | | TAK/NIE* |



| | | | |
|----|--|--|----------|
| | <p>i)Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.</p> <p>j)Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.</p> <p>k)Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.</p> <p>l)Mechanizm „Split tunneling” dla połączeń Client-to-Site.</p> <p>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.</p> | | |
| i. | <p>Routing i obsługa łączy WAN</p> <p>W zakresie routingu rozwiązanie zapewnia obsługę:</p> <p>1.Routingu statycznego.</p> <p>2.Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego).</p> <p>3.Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.</p> <p>4.Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.</p> <p>5.ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.</p> <p>6.BFD (Bidirectional Forwarding Detection).</p> <p>7.Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.</p> | | TAK/NIE* |
| j. | <p>Funkcje SD-WAN</p> <p>1.System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.</p> <p>2.SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).</p> | | TAK/NIE* |
| k. | <p>Zarządzanie pasmem:</p> <p>1.System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.</p> <p>2.System daje możliwość określania pasma dla poszczególnych aplikacji.</p> <p>3.System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.</p> <p>4.System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.</p> | | TAK/NIE* |
| l. | <p>Ochrona przed malware:</p> <p>1.Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).</p> <p>2.Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.</p> <p>3.W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu</p> | | TAK/NIE* |



| | | | |
|----|--|--|----------|
| | <p>przeskanowania zawartości lub umożliwia konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum.</p> <p>4.System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.</p> <p>5.System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).</p> <p>6.Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</p> <p>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.</p> <p>8.Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.</p> <p>9.Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.</p> | | |
| m. | <p>Ochrona przed atakami</p> <p>1.Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.</p> <p>2.System chroni przed atakami na aplikacje pracujące na niestandardowych portach.</p> <p>3.Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</p> <p>4.Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.</p> <p>5.System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.</p> <p>6.Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).</p> <p>7.Wykrywanie i blokowanie komunikacji C&C do sieci botnet.</p> <p>8.Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej.</p> <p>Mechanizmy ochrony IPS nie mogą działać globalnie.</p> | | TAK/NIE* |
| n. | <p>Kontrola aplikacji:</p> <p>1.Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.</p> <p>2.Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</p> <p>3.Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.</p> | | TAK/NIE* |



| | | | |
|----|---|--|----------|
| | <p>4.Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.</p> <p>5.Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.</p> <p>6.Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 21).</p> <p>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).</p> | | |
| o. | <p>Kontrola WWW:</p> <p>1.Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.</p> <p>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.</p> <p>3.Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.</p> <p>4.Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.</p> <p>5.Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).</p> <p>6.Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.</p> <p>7.Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.</p> <p>8.Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.</p> <p>9.System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.</p> | | TAK/NIE* |
| p. | <p>Uwierzytelnianie użytkowników w ramach sesji:</p> <p>1.System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:</p> <p>a)Hasł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.</p> <p>b)Hasł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.</p> <p>c)Hasł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.</p> <p>2.System daje możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego.</p> <p>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.</p> <p>4.Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących</p> | | TAK/NIE* |

| | | | |
|----|--|--|----------|
| | ruchu HTTP. | | |
| q. | <p>Zarządzanie:</p> <p>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.</p> <p>2.Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.</p> <p>3.Istnieje możliwość włączenia mechanizmów uwierzytelniania wieloskładnikowego dla dostępu administracyjnego.</p> <p>4.System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.</p> <p>5.System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.</p> <p>6.Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.</p> <p>7.Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.</p> <p>8.Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).</p> <p>9.Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.</p> | | TAK/NIE* |
| r. | <p>Logowanie</p> <p>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.</p> <p>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.</p> <p>3.Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.</p> <p>4.Możliwość włączenia logowania per reguła w polityce firewall.</p> <p>5.System zapewnia możliwość logowania do serwera SYSLOG.</p> <p>6.Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.</p> | | TAK/NIE* |
| s. | <p>Testy wydajnościowe oraz funkcjonalne:</p> <p>1.Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta</p> | | TAK/NIE* |
| t. | Serwisy i licencje | | TAK/NIE* |



| | | | |
|---|--|--|----------|
| | 1.Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje: a) 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 | | |
| u. | 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* |
| v. | zestaw montażowy dla urządzenia przystosowany do montażu w szafie rack zamawiającego. | | TAK/NIE* |
| III. Serwer NAS/Macierz dyskowa wraz z 4 dyskami HDD: Centrum Usług Wspólnych (1 szt.) - FABRYCZNIE NOWE CENA JEDNOSTKOWA: BRUTTO ZŁ ZA SZTUKĘ | | | |
| a. | Marka/Model Serwera NAS/Macierzy dyskowej oraz 4 dysków HDD | | TAK/NIE* |
| b. | Typ urządzenia: Serwer NAS/Macierz Dyskowa | | TAK/NIE* |
| c. | Obudowa: Rack 1U | | |
| d. | Procesor: minimum czterordzeniowy procesor o taktowaniu 2,2 GHz. | | TAK/NIE* |
| e. | Sprzętowy mechanizm szyfrowania: AES-NI | | TAK/NIE* |
| f. | Pamięć RAM: min. 2 GB pamięci ECC SODIMM z możliwością rozszerzenia do min. 32 GB | | TAK/NIE* |
| g. | 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* |
| h. | 1.Porty zewnętrzne: minimum: a)2 porty USB 3.2.1 b)1 port eSATA (jako gniazdo rozszerzenia) | | TAK/NIE* |
| i. | 1.Porty sieciowe Minimum: a)4 porty 1GbE RJ45 (z obsługą funkcji Link Aggregation / przełączania awaryjnego) | | TAK/NIE* |
| j. | Funkcja Wake on LAN/WAN | | TAK/NIE* |
| k. | Gniazdo rozszerzeń PCIe 2.0: Min. 1x 4-liniowe gniazdo x8 gen. 3 | | TAK/NIE* |
| l. | Wentylator obudowy: Min. 3 wentylatory (40 × 40 × 20 mm) | | TAK/NIE* |
| m. | Obsługiwane protokoły sieciowe: Min. SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS Kerberized sessions, iSCSI, HTTP, HTTPS, FTP, SNMP, LDAP, CalDAV | | TAK/NIE* |
| n. | 1.System plików: minimum: a)Wewnętrzny: Btrfs, ext4 b)Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT | | TAK/NIE* |
| o. | 1.Zarządzanie pamięcią masową: a)Maksymalny rozmiar pojedynczego wolumenu: 108 | | TAK/NIE* |

| | | | |
|----|---|--|----------|
| | <p>TB</p> <p>b)Minimalny liczba wewnętrznych wolumenów: 64</p> <p>c)Minimalny liczba obiektów iSCSI Target: 128</p> <p>d)Minimalny liczba jednostek iSCSI LUN: 256</p> <p>e)Obsługa klonowania/migawek jednostek iSCSI LUN</p> | | |
| p. | Obsługiwane typy macierzy RAID: minimum: SHR, Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10 | | TAK/NIE* |
| q. | <p>1.Konto i folder współdzielony:</p> <p>a)Minimalna liczba kont użytkowników: 1 024</p> <p>b)Minimalna liczba grup użytkowników: 256</p> <p>c)Minimalna liczba folderów współdzielonych: 256</p> <p>d)Minimalna liczba zadań synchronizacji folderów współdzielonych: 8</p> | | TAK/NIE* |
| r. | <p>1. Usługi plików:</p> <p>a) Protokół plików: SMB, AFP, NFS, FTP, WebDAV, Rsync</p> <p>b) Minimalna liczba połączeń SMB (oparta na FSCT): 130</p> <p>c)Integracja z listą kontroli dostępu Windows (ACL)</p> <p>d) Uwierzytelnianie Kerberos NFS</p> | | TAK/NIE* |
| s. | Wirtualizacja: Obsługa VMware vSphere with VAAI, Windows Server 2022, Citrix Ready, OpenStack | | TAK/NIE* |
| t. | <p>1. Bezpieczeństwo:</p> <p>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)</p> | | TAK/NIE* |
| u. | <p>1.Oprogramowanie:</p> <p>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.</p> <p>Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów współdzielonych</p> <p>b) Urządzenie musi wspierać funkcję WORM (Write Once, Read Many) oraz migawki niezmiennie</p> <p>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</p> <p>e)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</p> | | TAK/NIE* |



| | | | |
|------------|---|--|----------|
| | 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 wspierać wersjonowanie oraz edycję tworzonych plików office w czasie rzeczywistym. f) 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. | | |
| v. | 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* |
| IV. | Zasilacze awaryjne UPS do serwerowni – Urząd Gminy Skrzyszów (1 szt.), Centrum Usług Społecznych – (1 szt.) FABRYCZNIE NOWE URZĄDZENIA CENA JEDNOSTKOWA: BRUTTO ZŁ ZA SZTUKĘ | | |
| a. | Marka/Model zasilacza awaryjnego UPS | | TAK/NIE* |
| b. | Technologia wykonania UPS: Line-interactive | | TAK/NIE* |
| c. | Zasilanie/UPS: Jednofazowy | | TAK/NIE* |
| d. | Moc pozorna (VA): 2200 | | TAK/NIE* |
| e. | Moc rzeczywista (W): min. oraz max. 2200W; ze względu 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* |
| f. | Kształt fali na wyjściu(praca na baterii): Czysta fala sinusoidalna | | TAK/NIE* |
| g. | Kompatybilność z zasilaczami z aktywnym PFC | | TAK/NIE* |
| h. | Automatyczna regulacja napięcia (mechanizm AVR) | | TAK/NIE* |
| i. | Podwyższanie napięcia(przy zaniżonym napięciu z sieci): Dwustopniowe | | TAK/NIE* |
| j. | Obniżanie napięcia(przy zawyżonym napięciu z sieci): Jednostopniowe | | TAK/NIE* |
| k. | Ochrona przed przeciążeniem: minimum bezpiecznik i wewnętrzny ogranicznik prądu | | TAK/NIE* |
| l. | Filtr EMI/RFI | | TAK/NIE* |
| m. | Ochrona dla urządzeń telekomunikacyjnych minimum 1 port RJ45 wejście/wyjście | | TAK/NIE* |
| n. | Układ przeciwprzepięciowy (Dżule): Charakterystyka wejścia/wyjścia: minimum 2430 | | TAK/NIE* |
| o. | Nominalne napięcie wejściowe (V): 220 ; 230 ; 240 | | TAK/NIE* |

| | | | |
|-----------|--|--|----------|
| p. | Obsługiwany zakres napięcia wejściowego (V): 159 ~ 288 | | TAK/NIE* |
| q. | Częstotliwość wejściowa(Hz): 50+/-3 ; 60+/-3 | | TAK/NIE* |
| r. | Wykrywanie częstotliwości wejściowej: automatyczne | | TAK/NIE* |
| s. | Napięcie przy pracy na baterii (V): 220+/-5% ; 230+/-5% ; 240+/-5% | | TAK/NIE* |
| t. | Częstotliwość przy pracy baterii (Hz): 50+/-1% ; 60+/-1% | | TAK/NIE* |
| u. | Charakterystyka gniazd: 1.Rodzaj złącza wejściowego: IEC C20 a)Całkowita ilość gniazd: minimum 8 b)Gniazdko: IEC C13 x 6 / IEC C19 x 2 c)Rozróżnienie gniazd na krytyczne i nie krytyczne: minimum 4 gniazda krytyczne | | TAK/NIE* |
| v. | 1.Charakterystyka baterii: a)Typowy czas przełączenia na baterie (ms): nie więcej niż 4 b)Czas pracy na baterii przy połowie obciążenia: minimum 11.4min c)Typowy czas ponownego ładowania baterii (h): 3 d)Możliwość wymiany baterii przez użytkownika | | TAK/NIE* |
| w. | 1.Zarządzanie: a)Sygnalizacja: Wymagane alarmy dźwiękowe oraz wyświetlacz LCD b)Alarmy dźwiękowe: minimum Tryb baterii, Niski poziom baterii, Przeciążenie, Przeładowanie c)Konfiguracja wybranych parametrów: Ustawienie trybu, Ustawienia alarmu, Wejście i wyjście, Ustawienia baterii, Komunikacja, Język d)Port komunikacyjny USB e)Port wyłącznika awaryjnego EPO f)Dołączone oprogramowanie do zarządzania g)Wymagane, obsługa platform Windows, Linux, Vmware h)Zarządzanie przez sieć: Wymagana możliwość rozbudowy o zarządzanie HTTP/SNMP, np. poprzez doinstalowanie karty zarządzającej | | TAK/NIE* |
| x. | 1.Cechy fizyczne: a)Obudowa: Wymagana możliwość instalacji w szafie RACK lub ustawienia jako Tower b)Konstrukcja obudowy: Metalowa c)Wymagane Szyny/uchwyty rack d)Rozmiary (szer. x wys. x gł.) (mm): Nie większe niż 433 x 86.5 x 412 e)Waga: maksimum 26 kg | | TAK/NIE* |
| y. | 1.Dane środowiskowe: a)Temperatura robocza (°C): 0 ~ 40 b)Względna wilgotność robocza (bez kondensacji) (%): 0 ~ 95 | | TAK/NIE* |
| z. | 1.Certyfikaty: a)wymagane certyfikaty: CE, FCC klasa B, UL, cUL, RCM, VCCI, UKCA, RoHS | | TAK/NIE* |
| aa. | Gwarancja producenta na urządzenie oraz baterie (znajdujące się w UPS-ie): minimum oferowane przez Wykonawcę/Oferenta | | TAK/NIE* |
| V. | Zasilacze awaryjne UPS stanowiskowe – Urząd Gminy Skrzyszów (40 szt.), Centrum Usług Społecznych – (12 szt.) | | |

| FABRYCZNIE NOWE URZĄDZENIA CENA JEDNOSTKOWA: BRUTTO ZŁ ZA SZTUKĘ | | | |
|---|--|--|----------|
| a) | Marka/Model zasilacza awaryjnego UPS | | TAK/NIE* |
| b) | Technologia wykonania UPS: Line-interactive | | TAK/NIE* |
| c) | Zasilanie/UPS: Jednofazowy | | TAK/NIE* |
| d) | Moc pozorna (VA): 1050 | | TAK/NIE* |
| e) | Moc rzeczywista (W): min. 600 | | TAK/NIE* |
| f) | Kształt fali na wyjściu(praca na baterii): Symulowane napięcie sinusoidalne | | TAK/NIE* |
| g) | Automatyczna regulacja napięcia (mechanizm AVR) | | TAK/NIE* |
| h) | Ochrona przed przeciążeniem | | TAK/NIE* |
| i) | Filtr EMI/RFI | | TAK/NIE* |
| j) | Układ przeciwprzepięciowy (J): minimum 150 | | TAK/NIE* |
| k) | 1.Charakterystyka wejścia/wyjścia: a)Nominalne napięcie wejściowe (V): 230+/-10% b)Obsługiwany zakres napięcia wejściowego (V): minimum 165 - 290 c)Częstotliwość wejściowa(Hz): 50+/-5 ; 60+/-5 d)Wykrywanie częstotliwości wejściowej: automatyczne e)Napięcie przy pracy na baterii (V): 230+/-10% f)Częstotliwość przy pracy baterii (Hz): 50+/-1% ; 60+/-1% | | TAK/NIE* |
| l) | 1.Charakterystyka gniazd: a)Rodzaj złącza wejściowego: UniSchuko (połączenie złącza FR i Schuko) b)Rodzaj złącza wyjściowego: FR x 4 | | TAK/NIE* |
| m) | 1.Charakterystyka baterii: a)Typowy czas przełączenia na baterie (ms) 4 ms b)Czas podtrzymania na baterii: czas pracy przy pełnym obciążeniu (600W) do 1 min, przy połowie obciążenia (300W) do 4 min c)Ładowanie baterii: Typowy czas ładowania do 6 h | | TAK/NIE* |
| n) | 1.Zarządzanie: a)Sygnalizacja: wymagane alarmy dźwiękowe oraz diody LED b)Diody LED - sygnalizacjaZasilanie włączone, Tryb liniowy, Tryb baterii, Tryb obejścia, Niski poziom baterii, Przeciążenie, Usterka UPS c)Alarmy dźwiękowe - sygnalizacja: Tryb baterii, Niski poziom baterii, Przeciążenie, Usterka UPS d)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* |
| o) | 1.Cechy fizyczne: a)Obudowa Tower b)Konstrukcja obudowy - Plastikowa c)Rozmiary (szer. x wys. x gł.) (mm): Nie większe niż 95 x 220 x 307 d)Waga maksimum 7 kg (urządzenie bez opakowania i akcesoriów) | | TAK/NIE* |
| p) | 1.Dane środowiskowe: a)Temperatura robocza (°C): 0 - 40 b)Względna wilgotność robocza (bez kondensacji) (%) 0 - 90 | | TAK/NIE* |



| | | | |
|------------|---|--|----------|
| | c) Rozproszenie ciepła (BTU/hr): Nie więcej niż 27 BTU/hr | | |
| q) | Certyfikaty: CE | | TAK/NIE* |
| r) | Gwarancja producenta na urządzenie i baterie: minimum oferowane przez Wykonawcę/Oferenta | | TAK/NIE* |
| VI. | Oprogramowanie do tworzenia kopii zapasowych – Centrum Usług Wspólnych(1 szt.) - FABRYCZNIE NOWE CENA JEDNOSTKOWA: BRUTTO ZŁ ZA SZTUKĘ | | |
| a. | Nazwa Oprogramowania do tworzenia kopii zapasowych | | TAK/NIE* |
| 1. | <p>Zarządzanie i magazyny:</p> <p>1.Produkt dostępny w polskiej wersji językowej.</p> <p>2.Konsola zarządzająca dostępna z poziomu przeglądarki internetowej</p> <p>3.System musi umożliwiać tworzenie kopii zapasowych na poziomie dysków</p> <p>4.System musi umożliwiać tworzenie kopii zapasowych na poziomie plików i folderów</p> <p>5.System musi umożliwiać replikację kopii zapasowych do wielu lokalizacji docelowych</p> <p>6.System musi umożliwiać tworzenie kopii zapasowych i przywracanie systemów wykorzystujących UEFI/GPT</p> <p>7.System musi umożliwiać współpracę z usługą kopiowania woluminów w tle (VSS) firmy Microsoft</p> <p>8.Możliwość zdefiniowania limitu przepustowości sieciowej z jakiej ma korzystać oprogramowanie backupowe</p> <p>9.System zarządzania nie może być oparty o relacyjne bazy danych.</p> <p>10.Rozwiązanie działa w architekturze wykluczającej pojedynczy punkt awarii (awaria jednego z komponentów nie spowoduje przestoju w procesie tworzenia kopii zapasowej).</p> <p>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).</p> <p>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.</p> <p>13.Rozwiązanie musi być systemem multi-storage-owym i umożliwia tworzenie wielu repozytoriów danych jednocześnie również na innych środowiskach jako przestrzeń do replikacji danych.</p> <p>14.System musi oferować mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykle.</p> <p>15.Rozwiązanie w warstwie sprzętowej powinno bazować na standardowych komponentach architektury x86, bez powiązania i poleganiu na komponentach wyłącznie jednego dostawcy (tzw. "no proprietary vendor lock").</p> <p>16.System pozwala administratorowi na ustawienie dowolnego harmonogramu replikacji danych pomiędzy dowolnymi wspieranymi magazynami.</p> <p>17.System musi umożliwiać wykonywanie kopii</p> | | TAK/NIE* |



| | | |
|--|--|--|
| <p>obrazu dysku, kopii plików i katalogów oraz kopii maszyn wirtualnych bez ich zatrzymywania z zachowaniem stuprocentowej integralności i spójności danych wewnątrz wykonanej kopii zapasowej.</p> <p>18.Rozwiązanie musi realizować funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie.</p> <p>19.Rozwiązanie zapewnia backup jednorazowy - nawet w przypadku wymagania granularnego odtworzenia.</p> <p>20.System musi umożliwiać automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku wystąpienia błędu.</p> <p>21.Rozwiązanie powinno umożliwiać klonowanie planów kopii zapasowych, planów replikacji oraz planów testowego odtwarzania maszyn wirtualnych</p> <p>22.Rozwiązanie powinno umożliwiać uruchamianie przy zadaniach backupu dowolnych skryptów PRE/POST oraz po wykonaniu migawki VSS.</p> <p>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.</p> <p>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).</p> <p>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.</p> <p>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.</p> <p>27.System powinien umożliwiać wysyłanie powiadomień o statusie wykonanych zadań na dowolne adresy webhook, podawane przez użytkownika,</p> <p>28.Oferowane rozwiązanie musi być dobrane pod względem wydajności w oparciu o najlepsze praktyki producenta.</p> <p>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.</p> <p>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).</p> <p>31.System pozwala na zmniejszenie rozmiaru</p> | | |
|--|--|--|



| | | |
|--|--|--|
| <p>przechowywanych i przesyłanych danych poprzez usuwanie zduplikowanych bloków danych ze źródła kopii pomiędzy wszystkimi źródłami w obrębie wszystkich kopii na magazynie danych.</p> <p>32.Proces deduplikacji musi być możliwy dla każdego z typów obsługiwanych magazynów.</p> <p>33.Proces deduplikacji nie może wymagać instalacji żadnych dodatkowych komponentów, które będą pośredniczyły w zapisie danych z deduplikowanych</p> <p>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.</p> <p>35.Proces deduplikacji realizowany jest blokiem o stałej wielkości, którego wielkość może zostać ustalona na etapie wdrożenia rozwiązania zgodnie z najlepszymi praktykami producenta.</p> <p>36.Proces szyfrowania kopii zapasowych nie może ograniczać procesu deduplikacji w ramach tego samego klucza szyfrującego.</p> <p>37.Kompresja kopii zapasowych musi obsługiwać jeden z wymienionych algorytmów: LZ4, ZStandard. Dodatkowo, musi umożliwiać określenie szczegółowego poziomu kompresji, w tym: niski, średni, wysoki.</p> <p>38.Instalacja, modyfikacja ustawień, polityki tworzenia kopii zapasowej systemu nie może wymagać przerwania pracy lub restartu systemu.</p> <p>39.System musi pozwalać na automatyczne aktualizacje oprogramowania.</p> <p>40.System musi być w stanie kompresować i szyfrować zabezpieczone dane w systemach NAS.</p> <p>41.System musi pozwalać na uruchomienie kontenerów Docker w dowolnych urządzeniach NAS w celu ich zabezpieczenia.</p> <p>42.System tworzenia kopii zapasowej musi przechowywać dane w sposób zapewniający ich niezmienną (tzw. "resilience"), dzięki czemu kopie zapasowe nie będą mogły zostać nadpisane lub zmodyfikowane przez cały okres ich przechowywania, retencji.</p> <p>43.System zarówno będzie przechowywać dane w kopii zapasowej w postaci zaszyfrowanej jak też ruch wewnątrz systemu również musi być szyfrowany.</p> <p>44.Archiwum długoterminowych kopii zapasowych musi być szyfrowane, a odzyskiwanie z archiwum obsługiwane z tego samego interfejsu użytkownika, co inne przywracanie dane.</p> <p>45.System musi mieć mechanizmy chroniące przejęcie konta administratora oraz umożliwiać definiowanie dodatkowych uprawnień dla każdej z predefiniowanych ról użytkowników.</p> <p>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</p> | | |
|--|--|--|



| | | |
|--|--|--|
| <p>uprawnień, w tym możliwość zablokowania usuwania danych.</p> <p>47.Rozwiązanie musi posiadać możliwość nieodwracalnego usuwania danych z magazynu na dane w momencie spełnienia dodatkowych wymogów.</p> <p>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.</p> <p>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.</p> <p>50.System kopii zapasowej musi umożliwiać dostęp do konsoli administracyjnej z wielu stacji roboczych.</p> <p>51.System kopii zapasowej musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.</p> <p>52.System powinien posiadać predefiniowane schemat tworzenia kopii zapasowych: Custom, Basic, G-F-S, Forever incremental,</p> <p>53.Rozwiązanie musi obsługiwać kontrolę dostępu opartą na rolach (RBAC).</p> <p>54.Możliwość składowania utworzonych kopii zapasowych na magazynach chmurowych Amazon AWS, Azure, Wasabi, Google Cloud Storage, Backblaze B2, magazyny zgodne z S3.</p> <p>55.Możliwość składowania utworzonych kopii zapasowych na udziałach sieciowych po protokole smb, nfs, iscsi, katalog lokalny</p> <p>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).</p> <p>57.Czas przechowywania kopii zapasowej (retention time) systemu backupu nie może być zmieniony np. poprzez manipulowanie wskazaniem 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.</p> <p>58.Możliwość generowania raportów dobowych w oparciu o harmonogram</p> <p>59.Produkt musi posiadać możliwość zapisu kopii zapasowych do magazynu chmurowego dostarczanego bezpośrednio przez producenta oprogramowania (datacenter musi być zlokalizowane na terenie Unii Europejskiej)</p> <p>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)</p> <p>61.Możliwość wyświetlenia szczegółowych informacji o chronionym urządzeniu takich jak: CPU, RAM,</p> | | |
|--|--|--|

| | | | |
|----|--|--|----------|
| | 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) | | |
| b. | <p>Wspierane systemy: Możliwość instalacji oraz uruchomienia agenta backupowego na hostach fizycznych, maszynach wirtualnych czy też kontenerach docker opartych o systemy oraz wszystkie nowsze:</p> <p>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+,</p> <p>Środowisk wirtualnych: Hyper-V 2016+, VMware: 6.7+.</p> <p>Możliwość instalacji oraz uruchomienia serwera zarządzania na hostach fizycznych, maszynach wirtualnych czy też kontenerach docker opartych o systemy:</p> <p>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+,</p> | | TAK/NIE* |
| c. | <p>Środowiska fizyczne i bazy danych:</p> <p>1.Rozwiązanie powinno umożliwiać tworzenie grup urządzeń w celu automatyzacji procesów podczas pracy z urządzeniami.</p> <p>2.Produkt musi posiadać możliwość tworzenia zadań dla grupy urządzeń oraz dla wybranych urządzeń.</p> <p>3.Rozwiązanie musi pozwalać na automatyczne wyłączenie stacji roboczej po wykonaniu kopii zapasowej.</p> <p>4.Rozwiązanie backupowe musi pozwalać na zabezpieczanie zaszyfrowanych partycji min. BitLocker, Veracrypt, TrueCrypt, Eset Endpoint Encryption.</p> <p>5.System jest niezależny od wersji Microsoft SQL i musi umożliwiać przywracanie danych SQL dla tej samej lub nowszej wersji.</p> <p>6.System musi obsługiwać również narzędzia RMAN firmy Oracle do tworzenia kopii zapasowych i odzyskiwania. Dodatkowo system musi obsługiwać funkcję przyrostowego skalania danych.</p> <p>7.System kopii zapasowej musi wspierać odtwarzanie pojedynczych plików z systemów Windows oraz Linux.</p> | | TAK/NIE* |



| | | | |
|----|---|--|----------|
| | <p>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.</p> <p>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.</p> <p>10. Rozwiązanie powinno umożliwiać uruchamianie procesu Bare Metal Restore z dowolnego bootowalnego nośnika danych.</p> <p>11.Rozwiązanie powinno wspierać odtwarzanie danych w scenariuszach P2P, P2V, V2P, V2V.</p> <p>12.Rozwiązanie umożliwia odtwarzanie kopii obrazu dysku w wybranym formacie (RAW, VHD, VHDX, VMDK).</p> <p>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.</p> <p>14.Rozwiązanie musi umożliwiać przywracanie plików pomiędzy różnymi systemami operacyjnymi i systemami plików (np. odtwarzanie danych plikowych Linux na systemie Windows).</p> | | |
| d. | <p>Środowiska wirtualne:</p> <p>1.System musi wspierać kopię w trybie application-aware dla wszystkich wspieranych wirtualizatorów.</p> <p>2.System musi umożliwiać wykonywanie kopii maszyn wirtualnych z zastosowaniem zaawansowanych metod transportu (HotAdd, SAN, LAN), w tym metodami LAN-Free, tj. takimi, które podczas wykonywania backupu nie obciążają interfejsów sieciowych maszyn wirtualnych.</p> <p>3.System kopii zapasowej musi wykorzystywać mechanizmy Change Block Tracking oraz Replica Change Tracking dla wspieranych przez producenta platformach wirtualizacyjnych.</p> <p>4.Rozwiązanie producenta musi być certyfikowane przez dostawcę platformy wirtualizacyjnej, tj. producent musi uczestniczyć w programie Technology Alliance Partner.</p> <p>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.</p> | | TAK/NIE* |



| | | | |
|----|---|--|----------|
| | <p>6.Dla środowiska vSphere i Hyper-V rozwiązanie powinno umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).</p> <p>7.System kopii zapasowej musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSphere.</p> <p>8.System kopii zapasowej musi umożliwiać weryfikację odtwarzalności wirtualnych maszyn według własnego harmonogramu w dowolnym środowisku.</p> | | |
| e. | <p>Aplikacje SaaS</p> <p>1.Ochrona z tej samej konsoli dla Microsoft 365 minimum na poziomie, skrzynek pocztowych, onedrive, kontaktów, kalendarza.</p> <p>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)</p> <p>3.System musi umożliwiać granularne odtwarzanie danych, tj. pojedynczych plików z kopii obrazu dysku oraz pojedynczych wiadomości z kopii skrzynki pocztowej Microsoft 365.</p> <p>4.System musi umożliwiać zabezpieczanie środowisk Git, w tym GitHub, GitLab oraz Bitbucket wraz z metadanymi</p> <p>5.System musi umożliwiać odtworzenie dowolnego środowiska Git w dowolnym innym środowisku Git, tzw. odtwarzanie crossowe.</p> <p>6.System musi umożliwiać zabezpieczenie metadanych zebranych wokół repozytorium w ramach zabezpieczanego środowiska Git.</p> <p>7.System musi umożliwiać odtwarzanie metadanych repozytorium Git do dowolnego innego środowiska Git w przypadku chęci odtworzenia repozytorium.</p> <p>8.System musi umożliwiać zabezpieczenie środowisk Jira</p> <p>9.System musi umożliwiać odtworzenie środowiska Jira do chmury lub środowiska lokalnego.</p> <p>10.System musi umożliwiać zabezpieczenie środowisk Jira</p> | | TAK/NIE* |
| f. | <p>Licencjonowanie i wsparcie techniczne</p> <p>1.Wszystkie linie supportu muszą być obsługiwane w języku polskim.</p> <p>2.Wsparcie techniczne musi być świadczone bezpośrednio przez główną siedzibę producenta.</p> <p>3.Możliwość zgłaszania ticketów supportowych bezpośrednio z poziomu interfejsu zarządzania w formie czatu.</p> <p>4.Producent wraz z rozwiązaniem musi udostępnić materiały samopomocowe w j. polskim (minimum dostęp do bazy wiedzy, materiałów wideo oraz kart produktów)</p> <p>5.Wsparcie techniczne musi umożliwiać korzystanie z połączeń zdalnych, systemu ticketowego oraz wsparcia telefonicznego.</p> <p>6.Licencje w ramach rozwiązania powinny pozwalać na zabezpieczenie określonej przez Zamawiającego</p> | | TAK/NIE* |



| | | | |
|-------------|--|--|----------|
| | <p>ilości hostów w obrębie wspieranych przez System środowisk.</p> <p>7.Licencje powinny być dostępne w opcji wieczystej .</p> <p>8.Dostęp do wsparcia technicznego producenta powinno obowiązywać przez okres min. 24 miesiące</p> <p>9.Sposób licencjonowania opiera się na:</p> <p>a)ilości serwerów/endpointów - dla fizycznych urządzeń,</p> <p>b)ilości socketów w hostach - dla środowisk wirtualnych lub ilości maszyn wirtualnych,</p> <p>c)ilość repozytoriów - dla GIT.</p> <p>10.Licencje powinny umożliwiać zabezpieczenie w wersji wieczystej:</p> <p>a)12 stacji roboczych,</p> <p>b)2 serwery wirtualne,</p> | | |
| g. | <p>Anty-ransomware i bezpieczeństwo:</p> <p>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").</p> <p>2.System powinien umożliwiać wykorzystanie wbudowanego menedżera haseł do przechowywania wszelkich sekretów (haseł, danych dostępowych, kluczy szyfrujących) wykorzystywanych przez System</p> <p>3.System powinien umożliwiać przywrócenie hasła głównego administratora w przypadku jego utraty.</p> <p>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 sparaliżowałaby działanie Systemu. System nie może posiadać pojedynczego punktu awarii.</p> <p>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.</p> | | TAK/NIE* |
| VII. | <p>Serwer z oprogramowaniem systemowym i licencjami dostępowymi oraz systemem do wirtualizacji:</p> <p>Urząd Gminy w Skrzyszowie (1 szt.)</p> <p>- FABRYCZNIE NOWE URZĄDZENIE</p> <p>CENA JEDNOSTKOWA: BRUTTO ZŁ ZA SZTUKĘ</p> | | |
| a. | Marka/Model Serwera | | TAK/NIE* |
| b. | 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* |
| c. | <p>Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera.</p> <p>Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać min. 1TB pamięci RAM.</p> | | TAK/NIE* |
| d. | 1.Zainstalowane dwa procesory min. 8-rdzeniowe, min. 2.6GHz z częstotliwości nominalnej, klasy x86, | | TAK/NIE* |



| | | | |
|----|---|--|----------|
| | osiągające minimalne wyniki testów w konfiguracji dwuprocesorowej: a)SPECrate2017_int_base wynik min. 169pkt b)SPECrate2017_int_peak wynik min. 174pkt c)SPECrate2017_fp_base wynik min. 246pkt d)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. | | |
| e. | RAM: 64GB (w układzie 2x32GB) | | TAK/NIE* |
| f. | Funkcjonalność pamięci RAM: Demand Scrubbing, Patrol Scrubbing, Permanent Fault Detection (PFD) | | TAK/NIE* |
| g. | Gniazda PCI: Minimum 5 slotów PCIe x16 generacji 4 | | TAK/NIE* |
| h. | 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* |
| i. | 1.Kontroler RAID: Sprzętowy kontroler dyskowy, posiadający a)Min. 8GB nieulotnej pamięci cache, b)Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60. c)Wsparcie dla dysków samoszyfrujących | | TAK/NIE* |
| j. | 1.Dyski twarde Zainstalowane: a)2x dyski SAS 10k rpm o pojemności min. 600GB, Hot-Plug skonfigurowane w Raid1 pod virtualizator b)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* |
| k. | 1.Wbudowane porty: a)3xUSB z czego nie mniej niż 1x USB 3.0, b)2xVGA z czego jeden na panelu przednim. | | TAK/NIE* |
| l. | Video: Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1900x1200 | | TAK/NIE* |
| m. | Zasilacze: Redundantne, Hot-Plug max 700W każdy. Klasy Titanium | | TAK/NIE* |
| n. | 1.Bezpieczeństwo a)Zatrask górnej pokrywy oraz blokada na ramce panela frontowego zamykane na klucz w celu do ochrony nieautoryzowanego dostępu do dysków twardej i wewnętrznych elementów serwera. b)Możliwość wyłączenia w BIOS funkcji przycisku zasilania. c)BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła d)Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. e)Moduł TPM 2.0 f)Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu | | |



| | | | |
|----|---|--|----------|
| | serwera. g)Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem. | | |
| o. | 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* |
| p. | 1.Karta Zarządzania: Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: a)zdalny dostęp do graficznego interfejsu Web karty zarządzającej; b)zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); c)szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika; d)wsparcie dla IPv6; e)wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; f)możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; g)integracja z Active Directory; h)wsparcie dla dynamic DNS; i)wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. j)możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera k)możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera | | TAK/NIE* |
| q. | 1.Certyfikaty: a)Serwer musi być wyprodukowany zgodnie z normą ISO-9001, ISO-14001, ISO-50001 lub równoważną - dołączyć do oferty jako przedmiotowy środek dowodowy. b)Serwer musi posiadać deklarację CE - dołączyć do oferty jako przedmiotowy środek dowodowy. | | TAK/NIE* |
| r. | 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, | | TAK/NIE* |



| | | |
|--|--|--|
| <p>3.możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania min. 8000 maszyn wirtualnych,</p> <p>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,</p> <p>5.wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy,</p> <p>6.wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy,</p> <p>7.automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego,</p> <p>8.możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading),</p> <p>9.wbudowane wsparcie instalacji i pracy na wolumenach, które:</p> <p>a)pozwalają na zmianę rozmiaru w czasie pracy systemu,</p> <p>b)umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,</p> <p>c)umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,</p> <p>d)umożliwiają zdefiniowanie list kontroli dostępu (ACL),</p> <p>1. wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość,</p> <p>2.wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających min. certyfikat FIPS 140-2</p> <p>3.możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET,</p> <p>4.możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów,</p> <p>5.wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych,</p> <p>6.graficzny interfejs użytkownika,</p> <p>7.zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,</p> <p>8.qwsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play),</p> <p>9.możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu,</p> <p>10.dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa,</p> | | |
|--|--|--|



| | | |
|---|--|--|
| <p>11.możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:</p> <p>a)podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,</p> <p>b)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:</p> <ul style="list-style-type: none">– 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, <p>c)zdalna dystrybucja oprogramowania na stacje robocze,</p> <p>d)praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej,</p> <p>e)centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:</p> <ul style="list-style-type: none">– dystrybucję certyfikatów poprzez http,– konsolidację CA dla wielu lasów domeny,– automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, <p>f)szyfrowanie plików i folderów,</p> <p>g)szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),</p> <p>h)możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów,</p> <p>i)serwis udostępniania stron WWW,</p> <p>j)wsparcie dla protokołu IP w wersji 6 (IPv6),</p> <p>k)wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 1000 aktywnych środowisk wirtualnych systemów operacyjnych.</p> <p>12.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:</p> <p>a)dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,</p> <p>b)obsługi ramek typu jumbo frames dla maszyn wirtualnych,</p> <p>c)obsługi 4-KB sektorów dysków,</p> <p>d)nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,</p> <p>e)możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API,</p> <p>f)możliwości kierowania ruchu sieciowego z wielu</p> | | |
|---|--|--|



| | | | |
|----|---|--|----------|
| | <p>sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model),</p> <p>g) 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,</p> <p>h) wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath),</p> <p>i) możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego,</p> <p>j) mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty,</p> <p>k) możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.</p> <p><u>Zamawiający wymaga dostarczenia nośnika downgrade 1 wersji wcześniejszej oferowanego Systemu operacyjnego wraz z kluczem aktywacyjnym jeśli jest wymagany do poprawnej pracy systemu.</u></p> | | |
| s. | Licencje dostępowe: należy dostarczyć dodatkowo 45 licencji dostępowych do serwera dla użytkowników | | TAK/NIE* |
| t. | <p>Warunki gwarancji</p> <p>1.Gwarancja producenta musi wynosić minimum gwarancji udzielonej przez Wykonawcę/Oferenta z czasem reakcji do 48 godzin od przyjęcia zgłoszenia</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>5.Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta.</p> <p>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.</p> <p>7.Zamawiający oczekuje możliwości samodzielnego</p> | | TAK/NIE* |



| | | | |
|--------------|---|--|----------|
| | <p>kwalifikowania poziomu ważności naprawy.</p> <p>8.Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikro kodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji urządzenia.</p> <p>9.Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych.</p> | | |
| u. | <p>System do wirtualizacji:</p> <p>1.Wymagania funkcjonalne</p> <p>a)Obsługa maszyn wirtualnych (KVM) i kontenerów LXC</p> <p>b)Możliwość tworzenia i zarządzania snapshot'ami</p> <p>c)Możliwość migracji L2/L3 (live migration)</p> <p>d)Integracja z Ceph, ZFS, NFS, iSCSI, GlusterFS (opcjonalnie)</p> <p>2. Zarządzanie</p> <p>a)Interfejs webowy do zarządzania środowiskiem wirtualizacji</p> <p>b)Monitorowanie wykorzystania zasobów (CPU, RAM, dyski, sieć)</p> <p>a)Możliwość tworzenia VLAN-ów i mostków sieciowych</p> <p>3.Bezpieczeństwo</p> <p>a)Integrowany firewall (Proxmox Firewall)</p> <p>b)Możliwość integracji z LDAP/AD</p> <p>c) Brak wpływu na bezpieczeństwo infrastruktury fizycznej</p> <p>4.Skalowalność</p> <p>a)Możliwość rozbudowy do klastra wieloserwerowego</p> <p>b)Wsparcie dla rozproszonego magazynu danych</p> <p>5.Rozczyń dostęp do repozytorium oraz do stabilnych aktualizacji oprogramowania</p> | | TAK/NIE* |
| VIII. | <p>Serwer z systemem do wirtualizacji:</p> <p>Urząd Gminy w Skrzyszowie (1 szt.)</p> <p>CENA JEDNOSTKOWA: BRUTTO ZŁ ZA SZTUKĘ</p> | | |
| a. | Marka/Model Serwera | | TAK/NIE* |
| b. | 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* |
| c. | <p>Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera.</p> <p>Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać min. 1TB pamięci RAM.</p> | | TAK/NIE* |
| d. | <p>1.Zainstalowane dwa procesory min. 8-rdzeniowe, min. 2.6GHz z częstotliwości nominalnej, klasy x86, osiągające minimalne wyniki testów w konfiguracji dwuprocesorowej:</p> <p>a)SPECrate2017_int_base wynik min. 169pkt</p> <p>b)SPECrate2017_int_peak wynik min. 174pkt</p> <p>c)SPECrate2017_fp_base wynik min. 246pkt</p> <p>d)SPECrate2017_fp_peak wynik min. 252pkt</p> <p>Maksymalny TDP dla procesora 125W</p> <p>Wynik testu musi być opublikowany na stronie https://www.spec.org/cpu2017/results/ w dniu złożenia oferty.</p> | | TAK/NIE* |

| | | | |
|----|---|--|----------|
| | Do oferty należy załączyć wyniki testów - dołączyć do oferty jako przedmiotowy środek dowodowy. | | |
| e. | RAM: 64GB (w układzie 2x32GB) | | TAK/NIE* |
| f. | Funkcjonalność pamięci RAM: Demand Scrubbing, Patrol Scrubbing, Permanent Fault Detection (PFD) | | TAK/NIE* |
| g. | Gniazda PCI: Minimum 5 slotów PCIe x16 generacji 4 | | TAK/NIE* |
| h. | 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* |
| i. | 1.Kontroler RAID: Sprzętowy kontroler dyskowy, posiadający a)Min. 8GB nieulotnej pamięci cache, b)Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60. c)Wsparcie dla dysków samoszyfrujących | | TAK/NIE* |
| j. | 1.Dyski twarde Zainstalowane: a)2x dyski SAS 10k rpm o pojemności min. 600GB, Hot-Plug skonfigurowane w Raid1 pod virtualizator b)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* |
| k. | 1.Wbudowane porty: a)3 x USB z czego nie mniej niż 1x USB 3.0, b)2xVGA z czego jeden na panelu przednim. | | TAK/NIE* |
| l. | Video: Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1900x1200 | | TAK/NIE* |
| m. | Zasilacze: Redundantne, Hot-Plug max 700W każdy. Klasy Titanium | | TAK/NIE* |
| n. | 1.Bezpieczeństwo a)Zatrzaszk górnej pokrywy oraz blokada na ramce panela frontowego zamykane na klucz w celu do ochrony nieautoryzowanego dostępu do dysków twardych i wewnętrznych elementów serwera. b)Możliwość wyłączenia w BIOS funkcji przycisku zasilania. c)BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła d)Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. e)Moduł TPM 2.0 f)Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera. g)Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem. | | TAK/NIE* |
| o. | 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* |

| | | | |
|----|--|--|----------|
| p. | <p>Karta Zarządzania</p> <p>1.Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiającą:</p> <p>a)zdalny dostęp do graficznego interfejsu Web karty zarządzającej;</p> <p>b)zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);</p> <p>c)szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika;</p> <p>d)wsparcie dla IPv6;</p> <p>e)wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;</p> <p>f)możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;</p> <p>g)integracja z Active Directory;</p> <p>h)wsparcie dla dynamic DNS;</p> <p>i)wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.</p> <p>j)możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera</p> <p>k)możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera</p> | | TAK/NIE* |
| q. | <p>1.Certyfikaty:</p> <p>a)Serwer musi być wyprodukowany zgodnie z normą ISO-9001, ISO-14001, ISO-50001 lub równoważną - dołączyć do oferty jako przedmiotowy środek dowodowy.</p> <p>b)Serwer musi posiadać deklarację CE - dołączyć do oferty jako przedmiotowy środek dowodowy.</p> | | TAK/NIE* |
| r. | <p>Warunki gwarancji</p> <p>1.Gwarancja producenta musi wynosić minimum gwarancji udzielonej przez wykonawcę/oferenta z czasem reakcji do 48 godzin od przyjęcia zgłoszenia</p> <p>2.Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego</p> <p>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.</p> <p>4.Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej tj. realizacji gwarancji, serwisu w terminach określonych w umowie.</p> <p>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.</p> | | TAK/NIE* |



| | | | |
|------------|--|--|----------|
| | <p>5.Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta.</p> <p>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.</p> <p>7.Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.</p> <p>8.Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikro kodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji urządzenia.</p> <p>9.Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych.</p> | | |
| s. | <p>System do wirtualizacji:</p> <p>1.Wymagania funkcjonalne</p> <p>a) Obsługa maszyn wirtualnych (KVM) i kontenerów LXC</p> <p>b) Możliwość tworzenia i zarządzania snapshot'ami</p> <p>c) Możliwość migracji L2/L3 (live migration)</p> <p>d) Integracja z Ceph, ZFS, NFS, iSCSI, GlusterFS (opcjonalnie)</p> <p>2.Zarządzanie</p> <p>a) Interfejs webowy do zarządzania środowiskiem wirtualizacji</p> <p>b) Monitorowanie wykorzystania zasobów (CPU, RAM, dyski, sieć)</p> <p>c) Możliwość tworzenia VLAN-ów i mostków sieciowych</p> <p>3.Bezpieczeństwo</p> <p>a)Integrowany firewall (Proxmox Firewall)</p> <p>b)Możliwość integracji z LDAP/AD</p> <p>c)Brak wpływu na bezpieczeństwo infrastruktury fizycznej</p> <p>4.Skalowalność</p> <p>a)Możliwość rozbudowy do klastra wieloserwerowego</p> <p>b)Wsparcie dla rozproszonego magazynu danych</p> <p>5.Rozczyń dostęp do repozytorium oraz do stabilnych aktualizacji oprogramowania</p> | | TAK/NIE* |
| IX. | <p>Serwer z systemem do wirtualizacji: Urząd Gminy w Skrzyszowie (1 szt.) CENA JEDNOSTKOWA: BRUTTO ZŁ ZA SZTUKĘ</p> | | |
| a. | Marka/Model Serwera | | TAK/NIE* |
| b. | Obudowa Rack o wysokości max 2U z możliwością instalacji min. 16 dysków 2.5" wraz z kompletem wysuwanych szyn umożliwiającym montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.. | | TAK/NIE* |
| c. | <p>Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera.</p> <p>Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać min. 1TB pamięci RAM.</p> | | TAK/NIE* |
| d. | 1.Zainstalowane dwa procesory min. 8-rdzeniowe, min. 2.6GHz z częstotliwości nominalnej, klasy x86, osiągające minimalne wyniki testów w konfiguracji dwuprocesorowej: | | TAK/NIE* |



| | | | |
|----|---|--|----------|
| | <p>a)SPECrate2017_int_base wynik min. 169pkt b)SPECrate2017_int_peak wynik min. 174pkt c)SPECrate2017_fp_base wynik min. 246pkt d)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.</p> | | |
| e. | RAM: 64GB (w układzie 2x32GB) | | TAK/NIE* |
| f. | Funkcjonalność pamięci RAM: Demand Scrubbing, Patrol Scrubbing, Permanent Fault Detection (PFD) | | TAK/NIE* |
| g. | Gniazda PCI: Minimum 5 slotów PCIe x16 generacji 4 | | TAK/NIE* |
| h. | 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* |
| i. | 1.Kontroler RAID: Sprzętowy kontroler dyskowy, posiadający a)Min. 8GB nieulotnej pamięci cache, b)Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60. c)Wsparcie dla dysków samoszyfrujących | | TAK/NIE* |
| j. | Dyski twarde 1.Zainstalowane: a)2x dyski SAS 10k rpm o pojemności min. 600GB, Hot-Plug skonfigurowane w Raid1 pod virtualizator b)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* |
| k. | 1.Wbudowane porty: a)3 x USB z czego nie mniej niż 1x USB 3.0, b)2xVGA z czego jeden na panelu przednim. | | TAK/NIE* |
| l. | Video: Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1900x1200 | | TAK/NIE* |
| m. | Zasilacze: Redundantne, Hot-Plug max 700W każdy. Klasy Titanium | | TAK/NIE* |
| n. | 1.Bezpieczeństwo a)Zatrask górnej pokrywy oraz blokada na ramce panela frontowego zamykane na klucz w celu do ochrony nieautoryzowanego dostępu do dysków twardych i wewnętrznych elementów serwera. b)Możliwość wyłączenia w BIOS funkcji przycisku zasilania. c)BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła d)Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. e)Moduł TPM 2.0 f)Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera. g)Możliwość wymazania danych ze znajdujących się | | TAK/NIE* |



| | | | |
|----|---|--|----------|
| | dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem. | | |
| o. | 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* |
| p. | Karta Zarządzania: 1.Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: a)zdalny dostęp do graficznego interfejsu Web karty zarządzającej; b)zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); c)szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika; d)wsparcie dla IPv6; e)wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; f)możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; g)integracja z Active Directory; h)wsparcie dla dynamic DNS; i)wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. j)możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera k)możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera | | TAK/NIE* |
| q. | 1.Certyfikaty: a)Serwer musi być wyprodukowany zgodnie z normą ISO-9001, ISO-14001, ISO-50001 lub równoważną - dołączyć do oferty jako przedmiotowy środek dowodowy. b)Serwer musi posiadać deklarację CE - dołączyć do oferty jako przedmiotowy środek dowodowy. | | TAK/NIE* |
| r. | 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 wsparciem 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 | | TAK/NIE* |



| | | | |
|-----------|---|--|----------|
| | <p>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.</p> <p>5.Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta.</p> <p>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.</p> <p>7.Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.</p> <p>8.Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikro kodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji urządzenia.</p> <p>9.Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych.</p> | | |
| s. | <p>System do wirtualizacji:</p> <p>1.Wymagania funkcjonalne</p> <p>a)Obsługa maszyn wirtualnych (KVM) i kontenerów LXC</p> <p>b)Możliwość tworzenia i zarządzania snapshot'ami</p> <p>c)Możliwość migracji L2/L3 (live migration)</p> <p>d)Integracja z Ceph, ZFS, NFS, iSCSI, GlusterFS (opcjonalnie)</p> <p>2.Zarządzanie</p> <p>a)Interfejs webowy do zarządzania środowiskiem wirtualizacji</p> <p>b)Monitorowanie wykorzystania zasobów (CPU, RAM, dyski, sieć)</p> <p>c)Możliwość tworzenia VLAN-ów i mostków sieciowych</p> <p>3.Bezpieczeństwo</p> <p>a)Integrowany firewall (Proxmox Firewall)</p> <p>b)Możliwość integracji z LDAP/AD</p> <p>c)Brak wpływu na bezpieczeństwo infrastruktury fizycznej</p> <p>4.Skalowalność</p> <p>a)Możliwość rozbudowy do klastra wieloserwerowego</p> <p>b)Wsparcie dla rozproszonego magazynu danych</p> <p>5.Rozszerzony dostęp do repozytorium oraz do stabilnych aktualizacji oprogramowania</p> | | TAK/NIE* |
| X. | <p>Serwer z oprogramowaniem systemowym i licencjami dostępowymi oraz systemem do wirtualizacji:</p> <p>Centrum Usług Społecznych w Skrzyszowie (1 szt.)</p> <p>CENA JEDNOSTKOWA: BRUTTO ZŁ ZA SZTUKĘ</p> | | |
| a. | Marka/Model serwera | | TAK/NIE* |
| b. | <p>Obudowa Rack o wysokości max 1U z możliwością instalacji 8 dysków 2.5"</p> <p>Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych</p> | | TAK/NIE* |

| | | | |
|----|--|--|----------|
| c. | Chipset: Dedykowany przez producenta procesora do pracy w serwerach jednoprocessorowych | | TAK/NIE* |
| d. | Procesor 1.Zainstalowany jeden procesor minimum 8-rdzeniowy, min. 2.8GHz częstotliwości nominalnej, osiągający minimalne wyniki testów w konfiguracji jednoprocessorowej: a)SPECrate2017_int_base wynik min. 89pkt b)SPECrate2017_int_peak wynik min. 93pkt c)SPECrate2017_fp_base wynik min. 105pkt d)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* |
| e. | Pamięć RAM: Min. 32GB pamięci RAM DDR5 UDIMM | | TAK/NIE* |
| f. | Karta graficzna: Zintegrowana karta graficzna, umożliwiająca wyświetlanie obrazu w rozdzielczości minimum 1280x1024 pikseli | | TAK/NIE* |
| g. | Gniazda PCI: Minimum 2 sloty PCIe Gen4 z czego jeden wolny po obsadzeniu wymaganymi kartami sieciowymi pod przyszłą rozbudowę | | TAK/NIE* |
| h. | Interfejsy sieciowe: 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 10/25Gb SFP28 | | TAK/NIE* |
| i. | Kontroler RAID: Sprzętowy kontroler dyskowy, posiadający: <ul style="list-style-type: none"> Min. 8GB nieulotnej pamięci cache, Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących | | TAK/NIE* |
| j. | Dyski twarde 1.Zainstalowane: a)2x dyski SAS 10k rpm o pojemności min. 600GB, Hot-Plug skonfigurowane w Raid1 pod virtualizator b)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* |
| k. | Karta graficzna: Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200 | | TAK/NIE* |
| l. | Wbudowane porty: Min. 4 porty USB w tym 1 port USB 3.0 z tyłu obudowy, 1 port VGA na tylnym panelu | | TAK/NIE* |
| m. | Bezpieczeństwo: Zintegrowany z płytą główną moduł TPM 2.0 | | TAK/NIE* |
| n. | 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* |
| o. | Karta Zarządzania 1.Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: a)zdalny dostęp do graficznego interfejsu Web karty | | TAK/NIE* |



| | | | |
|----|--|--|----------|
| | zarządzającej; b)zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); c)szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; d)możliwość podmontowania zdalnych wirtualnych napędów; e)wirtualną konsolę z dostępem do myszy, klawiatury; f)wsparcie dla IPv6; g)wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; h)możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; i)możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; j)integracja z Active Directory; k)możliwość obsługi przez dwóch administratorów jednocześnie; l)wsparcie dla dynamic DNS; m)wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. n)możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera o)możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera oraz z możliwością rozszerzenia funkcjonalności o: <ul style="list-style-type: none"> – 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) | | |
| p. | 1.Certyfikaty: a)Serwer musi być wyprodukowany zgodnie z normą ISO-9001, ISO-14001, ISO-50001 lub równoważną - dołączyć do oferty jako przedmiotowy środek dowodowy. b)Serwer musi posiadać deklarację CE - dołączyć do oferty jako przedmiotowy środek dowodowy. | | TAK/NIE* |
| q. | 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, | | TAK/NIE* |



| | | |
|---|--|--|
| <p>3.możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania min. 8000 maszyn wirtualnych,</p> <p>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,</p> <p>5.wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy,</p> <p>6.wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy,</p> <p>7.automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego,</p> <p>8.możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading),</p> <p>9.wbudowane wsparcie instalacji i pracy na wolumenach, które:</p> <p>a)pozwalają na zmianę rozmiaru w czasie pracy systemu,</p> <p>b)umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,</p> <p>c)umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,</p> <p>d)umożliwiają zdefiniowanie list kontroli dostępu (ACL),</p> <p>10.wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość,</p> <p>11.wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających min. certyfikat FIPS 140-2</p> <p>12.możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET,</p> <p>13.możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów,</p> <p>14.wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych,</p> <p>15.graficzny interfejs użytkownika,</p> <p>16.zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,</p> <p>17.wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play),</p> <p>18.możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu,</p> <p>19.dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa,</p> | | |
|---|--|--|



| | | |
|--|--|--|
| <p>20.możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:</p> <p>a)podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,</p> <p>b)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:</p> <ul style="list-style-type: none">– 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, <p>c)zdalna dystrybucja oprogramowania na stacje robocze,</p> <p>d)praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej,</p> <p>e)centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:</p> <ul style="list-style-type: none">– dystrybucję certyfikatów poprzez http,– konsolidację CA dla wielu lasów domeny,– automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, <p>f)szyfrowanie plików i folderów,</p> <p>g)szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),</p> <p>h)możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów,</p> <p>i)serwis udostępniania stron WWW,</p> <p>j)wsparcie dla protokołu IP w wersji 6 (IPv6),</p> <p>k)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:</p> <ul style="list-style-type: none">– 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, | | |
|--|--|--|



| | | | |
|----|--|--|----------|
| | <p>– możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model),</p> <p>l)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,</p> <p>m)wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath),</p> <p>n)możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego,</p> <p>o)mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty,</p> <p>p)możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.</p> <p><u>Zamawiający wymaga dostarczenia nośnika downgrade 1 wersji wcześniejszej oferowanego Systemu operacyjnego wraz z kluczem aktywacyjnym jeśli jest wymagany do poprawnej pracy systemu.</u></p> | | |
| r. | Licencje dostępowe: Należy dostarczyć dodatkowo 12 licencji dostępowych do serwera dla użytkowników | | TAK/NIE* |
| s. | <p>Warunki gwarancji</p> <p>1.Gwarancja producenta musi wynosić minimum gwarancji udzielonej przez wykonawcę/oferenta z czasem reakcji do 48 godzin od przyjęcia zgłoszenia.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>5.Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta.</p> <p>6.Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie</p> | | TAK/NIE* |



| | | | |
|------------|---|--|----------|
| | <p>realizacji naprawy i po jej zakończeniu.</p> <p>7.Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.</p> <p>8.Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikro kodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji urządzenia.</p> <p>9.Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych.</p> | | |
| t. | <p>System do wirtualizacji</p> <p>1.Wymagania funkcjonalne</p> <p>a)Obsługa maszyn wirtualnych (KVM) i kontenerów LXC</p> <p>b)Możliwość tworzenia i zarządzania snapshot'ami</p> <p>c)Możliwość migracji L2/L3 (live migration)</p> <p>d)Integracja z Ceph, ZFS, NFS, iSCSI, GlusterFS (opcjonalnie)</p> <p>2.Zarządzanie</p> <p>a)Interfejs webowy do zarządzania środowiskiem wirtualizacji</p> <p>b)Monitorowanie wykorzystania zasobów (CPU, RAM, dyski, sieć)</p> <p>c)Możliwość tworzenia VLAN-ów i mostków sieciowych</p> <p>3.Bezpieczeństwo</p> <p>a)Integrowany firewall (Proxmox Firewall)</p> <p>b)Możliwość integracji z LDAP/AD</p> <p>c)Brak wpływu na bezpieczeństwo infrastruktury fizycznej</p> <p>4.Skalowalność</p> <p>a)Możliwość rozbudowy do klastra wieloserwerowego</p> <p>b)Wsparcie dla rozproszonego magazynu danych</p> <p>5.Rozczyny dostęp do repozytorium oraz do stabilnych aktualizacji oprogramowania</p> | | TAK/NIE* |
| XI. | <p>Serwer z systemem do wirtualizacji:</p> <p>Centrum Usług Społecznych w Skrzyszowie (1 szt.)</p> <p>Cena jednostkowa: brutto zł za sztukę</p> | | |
| a. | Marka/Model serwera | | TAK/NIE* |
| b. | <p>Obudowa Rack o wysokości max 1U z możliwością instalacji 8 dysków 2.5"</p> <p>Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych</p> | | TAK/NIE* |
| c. | Chipset: Dedykowany przez producenta procesora do pracy w serwerach jednoprocessorowych | | TAK/NIE* |
| d. | <p>Procesor</p> <p>1.Zainstalowany jeden procesor minimum 8-rdzeniowy, min. 2.8GHz częstotliwości nominalnej, osiągający minimalne wyniki testów w konfiguracji jednoprocessorowej:</p> <p>a)SPECrate2017_int_base wynik min. 89pkt</p> <p>b)SPECrate2017_int_peak wynik min. 93pkt</p> <p>c)SPECrate2017_fp_base wynik min. 105pkt</p> <p>d)SPECrate2017_fp_peak wynik min. 106pkt</p> <p>Maksymalny TDP dla procesora 80W</p> <p>Wynik testu musi być opublikowany na stronie https://www.spec.org/cpu2017/results/ w dniu złożenia oferty.</p> | | TAK/NIE* |



| | | | |
|----|---|--|----------|
| | Do oferty należy załączyć wyniki testów - dołączyć do oferty jako przedmiotowy środek dowodowy.. | | |
| e. | Pamięć RAM: Min. 32GB pamięci RAM DDR5 UDIMM | | TAK/NIE* |
| f. | Karta graficzna: Zintegrowana karta graficzna, umożliwiająca wyświetlanie obrazu w rozdzielczości minimum 1280x1024 pikseli | | TAK/NIE* |
| g. | Gniazda PCI: Minimum 2 sloty PCIe Gen4 z czego jeden wolny po obsadzeniu wymaganymi kartami sieciowymi pod przyszłą rozbudowę | | TAK/NIE* |
| h. | Interfejsy sieciowe: 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 10/25Gb SFP28 | | TAK/NIE* |
| i. | Kontroler RAID 1.Sprzętowy kontroler dyskowy, posiadający: a)Min. 8GB nieulotnej pamięci cache, b)Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60. c)Wsparcie dla dysków samoszyfrujących | | TAK/NIE* |
| j. | Dyski twarde 1.Zainstalowane: a)2x dyski SAS 10k rpm o pojemności min. 600GB, Hot-Plug skonfigurowane w Raid1 pod virtualizator b)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* |
| k. | Karta graficzna: Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200 | | TAK/NIE* |
| l. | Wbudowane porty: Min. 4 porty USB w tym 1 port USB 3.0 z tyłu obudowy, 1 port VGA na tylnym panelu | | TAK/NIE* |
| m. | Bezpieczeństwo: Zintegrowany z płytą główną moduł TPM 2.0 | | TAK/NIE* |
| n. | 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* |
| o. | Karta Zarządzania 1.Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: a)zdalny dostęp do graficznego interfejsu Web karty zarządzającej; b)zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); c)szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika; d)możliwość podmontowania zdalnych wirtualnych napędów; e)wirtualną konsolę z dostępem do myszy, klawiatury; f)wsparcie dla IPv6; g)wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; h)możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; i)możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; | | TAK/NIE* |



| | | | |
|----|---|--|----------|
| | <p>j)integracja z Active Directory;</p> <p>k)możliwość obsługi przez dwóch administratorów jednocześnie;</p> <p>l)wsparcie dla dynamic DNS;</p> <p>m)wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.</p> <p>n)możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera</p> <p>o)możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera oraz z możliwością rozszerzenia funkcjonalności o:</p> <ul style="list-style-type: none"> – 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) | | |
| p. | <p>1.Certyfikaty:</p> <p>a)Serwer musi być wyprodukowany zgodnie z normą ISO-9001, ISO-14001, ISO-50001 lub równoważną - dołączyć do oferty jako przedmiotowy środek dowodowy.</p> <p>b)Serwer musi posiadać deklarację CE - dołączyć do oferty jako przedmiotowy środek dowodowy.</p> | | TAK/NIE* |
| q. | <p>Warunki gwarancji</p> <p>1.Gwarancja producenta musi wynosić minimum gwarancji udzielonej przez wykonawcę/oferenta z czasem reakcji do 48 godzin od przyjęcia zgłoszenia</p> <p>2.Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego</p> <p>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.</p> <p>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.</p> <p>5.Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta.</p> <p>6.Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia</p> | | TAK/NIE* |



| | | | |
|-------------|---|--|----------|
| | <p>pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.</p> <p>7.Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.</p> <p>8.Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikro kodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji urządzenia.</p> <p>9.Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych.</p> | | |
| r. | <p>System do wirtualizacji</p> <p>1.Wymagania funkcjonalne</p> <p>a)Obsługa maszyn wirtualnych (KVM) i kontenerów LXC</p> <p>b)Możliwość tworzenia i zarządzania snapshot'ami</p> <p>c)Możliwość migracji L2/L3 (live migration)</p> <p>d)Integracja z Ceph, ZFS, NFS, iSCSI, GlusterFS (opcjonalnie)</p> <p>2.Zarządzanie</p> <p>a)Interfejs webowy do zarządzania środowiskiem wirtualizacji</p> <p>b)Monitorowanie wykorzystania zasobów (CPU, RAM, dyski, sieć)</p> <p>c)Możliwość tworzenia VLAN-ów i mostków sieciowych</p> <p>3.Bezpieczeństwo</p> <p>a)Integrowany firewall (Proxmox Firewall)</p> <p>b)Możliwość integracji z LDAP/AD</p> <p>c)Brak wpływu na bezpieczeństwo infrastruktury fizycznej</p> <p>4.Skalowalność</p> <p>a)Możliwość rozbudowy do klastra wieloserwerowego</p> <p>b)Wsparcie dla rozproszonego magazynu danych</p> <p>5.Roczny dostęp do repozytorium oraz do stabilnych aktualizacji oprogramowania</p> | | TAK/NIE* |
| XII. | <p>Dyski Zewnętrzne:</p> <p>Urząd Gminy w Skrzyszowie (30 szt.)</p> <p>Centrum Usług Społecznych (10 szt.)</p> <p>- FABRYCZNIE NOWE</p> <p>CENA JEDNOSTKOWA: BRUTTO ZŁ ZA SZTUKĘ</p> | | |
| a. | Marka/Model dysku | | TAK/NIE* |
| b. | Typ dysku: zewnętrzny | | TAK/NIE* |
| c. | Interfejs: USB | | TAK/NIE* |
| d. | Rodzaj dysku: SSD | | TAK/NIE* |
| e. | Pojemność: min 500GB | | TAK/NIE* |