**Załącznik nr 1 do SWZ**

**ZP.15.11.2024**

|  |
| --- |
|  |
| Opis Przedmiotu Zamówienia |
| Oprogramowanie i infrastruktura sprzętowa  oraz realizacja szkoleń |

|  |
| --- |
|  |

Spis treści

[Wstęp 3](#_Toc181090827)

[I. WYMAGANIA OGÓLNE 4](#_Toc181090828)

[1. RÓWNOWAŻNOŚĆ OFEROWANYCH ROZWIĄZAŃ 4](#_Toc181090829)

[II. Obszar techniczny 6](#_Toc181090830)

[1. UTM Unified Threat Management 6](#_Toc181090831)

[2. Serwer 12](#_Toc181090832)

[3. Network Attached Storage NAS typ 1 19](#_Toc181090833)

[4. Network Attached Storage NAS typ 2 22](#_Toc181090834)

[5. UPS typ 1 24](#_Toc181090835)

[6. UPS typ 2 25](#_Toc181090836)

[7. UPS typ 3 26](#_Toc181090837)

[8. UPS typ 4 27](#_Toc181090838)

[9. UPS typ 5 27](#_Toc181090839)

[10. UPS typ 6 28](#_Toc181090840)

[11. Zarządzalne urządzenia sieciowe z obsługą VLAN, MACsec, standardu 802.1X typ 1 29](#_Toc181090841)

[12. Zarządzalne urządzenia sieciowe z obsługą VLAN, MACsec, standardu 802.1X typ 2 31](#_Toc181090842)

[13. Zarządzalne urządzenia sieciowe z obsługą VLAN, MACsec, standardu 802.1X typ 3 33](#_Toc181090843)

[14. Oprogramowanie antywirusowe 35](#_Toc181090844)

[15. Oprogramowanie do wykonywania kopii zapasowych typ 1 39](#_Toc181090845)

[16. Oprogramowanie do wykonywania kopii zapasowych typ 2 40](#_Toc181090846)

[17. Oprogramowanie przeciwdziałającemu wyciekowi danych DLP - Data Leak Prevention 41](#_Toc181090847)

[18. Oprogramowanie do monitorowania infrastruktury informatycznej 43](#_Toc181090848)

[III. Obszar kompetencyjny 46](#_Toc181090849)

[1. Szkolenia dla działu IT typ 1 46](#_Toc181090850)

[2. Szkolenia dla działu IT typ 2 47](#_Toc181090851)

[3. Szkolenia dla działu IT typ 3 47](#_Toc181090852)

[4. Szkolenia pracowników spoza działu IT typ 4 49](#_Toc181090853)

# Wstęp

Niniejszy załącznik określa minimalne wymagania dla dostawy/wdrożenia/uruchomienia oprogramowania oraz infrastruktury sprzętowej dla Gminy Krzęcin realizowanego w ramach „Cyberbezpieczny Samorząd” dofinansowanego w formie grantu z programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa.

Celem projektu jest zwiększenia poziomu bezpieczeństwa informacji jednostek samorządu terytorialnego.

# WYMAGANIA OGÓLNE

## RÓWNOWAŻNOŚĆ OFEROWANYCH ROZWIĄZAŃ

#### w zakresie Oprogramowania

W celu zachowania zasad neutralności technologicznej i konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych, przy czym za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności nie odbiega znacząco od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym, przy czym nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym. W związku z tym, Wykonawca może zaproponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób, za rozwiązanie równoważne nie można uznać rozwiązania identycznego (tożsamego), a jedynie takie, które w porównywanych cechach wykazuje dokładnie tą samą lub bardzo zbliżoną wartość użytkową. Przez bardzo zbliżoną wartość użytkową rozumie się podobne, z dopuszczeniem nieznacznych różnic nie wpływających w żadnym stopniu na całokształt systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, dla których to warunków rozwiązania te są dedykowane. Rozwiązanie równoważne musi zawierać dokumentację potwierdzającą, że spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów, czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wyspecyfikowanego. Dostarczenie przez Wykonawcę rozwiązania równoważnego musi być zrealizowane w taki sposób, aby wymiana oprogramowania na równoważne nie zakłóciła bieżącej pracy Zamawiającego. W tym celu Wykonawca musi do oprogramowania równoważnego przenieść wszystkie dane niezbędne do prawidłowego działania nowych systemów, przeszkolić użytkowników, skonfigurować oprogramowanie, zapewnić gwarancję i serwis, uwzględnić niezbędną asystę ze strony pracowników Wykonawcy w operacji uruchamiania oprogramowania w środowisku produkcyjnym itp.

Mając na uwadze powyższe, w przypadku jeżeli Wykonawcy nie mają możliwości uzyskania odpowiedniego do realizacji dostępu do oprogramowania firm trzecich, w celu zapewnienia zasady konkurencyjności, przejrzystości, jawności a także równego traktowania wykonawców w trakcie prowadzenia postępowania, Zamawiający dopuszcza każdorazowo wymianę Oprogramowania u Zamawiającego pod warunkiem, że:

* + - * 1. Rozwiązania zastępujące dotychczas funkcjonujące u Zamawiającego systemy Wykonawca dostarcza i wdraża na swój koszt, z zachowaniem warunków licencjonowania wskazanych w niniejszym dokumencie.
        2. Wykonawca przeprowadzi migrację danych w zakresie wskazanym przez Zamawiającego na swój koszt, w sposób opisany w niniejszym OPZ a migracja musi objąć pełny zakres danych bieżących i archiwalnych.
        3. Wykonawca przeprowadzi instruktaże stanowiskowe, zapewni gwarancje i serwis gwarancyjny a także help desk oraz będzie świadczył asystę techniczną w zakresie umożliwiającym pracownikom Zamawiającego płynną obsługę Oprogramowania.
        4. Wymiana Oprogramowania nie może zakłócić bieżącej pracy Zamawiającego oraz musi zapewnić ciągłość pracy wynikającą z obowiązujących terminów, przepisów prawa i stosowanych procedur.
        5. Wszelkie uzgodnienia i konsultacje w zakresie transmisji danych powinny być dokonane w siedzibie Zamawiającego na podstawie zatwierdzonego harmonogramu.
        6. Proces migracji musi objąć pełne dane zawarte we wcześniej użytkowanym systemie.
        7. Nowe rozwiązania muszą realizować wszystkie wymienione wymagania względem Oprogramowania.

#### w zakresie Infrastruktury sprzętowej

W przypadkach, kiedy w opisie przedmiotu zamówienia wskazane zostały znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę co prowadziłoby do uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów, oznacza to, że Zamawiający nie może opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń i jest to uzasadnione specyfiką przedmiotu zamówienia. W takich sytuacjach ewentualne wskazania na znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, należy odczytywać z wyrazami „lub równoważne”.

W sytuacjach, kiedy Zamawiający opisuje przedmiot zamówienia poprzez odniesienie się do norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 i ust. 3 ustawy Pzp, Zamawiający dopuszcza rozwiązania równoważne opisywanym, a wskazane powyżej odniesienia należy odczytywać z wyrazami „lub równoważne”.

Pod pojęciem rozwiązań równoważnych Zamawiający rozumie taki sprzęt, który posiada parametry techniczne i/lub funkcjonalne co najmniej równe do określonych w OPZ. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy lub usługi spełniają wymagania określone przez Zamawiającego.

O ile inaczej nie zaznaczono, wszelkie zapisy OPZ zawierające parametry techniczne należy odczytywać jako parametry minimalne, np. zapis: “ Zainstalowany jeden procesor minimum 8-rdzeniowy klasy x86 dedykowany do pracy z zaoferowanym serwerem minimum 2.6GHz, 16MB pamięci cache, 65W i musi osiągać w teście Passmark CPU Mark, w kategorii Average CPU Mark wynik co najmniej 17400 pkt. według wyników opublikowanych na stronie http://www.cpubenchmark.net/cpu\_list.php ” należy rozumieć jako:

“Zainstalowany co najmniej jeden procesor, posiadający co najmniej 8 rdzeni, klasy co najmniej x86, posiadający taktowanie co najmniej 2.6GHz, osiągający w teście Passmark CPU Mark, w kategorii Average CPU Mark wynik co najmniej 17400 pkt. według wyników opublikowanych na stronie http://www.cpubenchmark.net/cpu\_list.php”.

# II. Obszar techniczny

## 1. UTM Unified Threat Management

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla sprzętu** |
| **Typ** | Urządzenie klasy UTM (Unified Threat Management) dla Środowiskowego Domu Samopomocy |
| **Wymagania ogólne** | W ramach przedmiotu zamówienia wymagana jest dostawa systemu bezpieczeństwa, który 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 musi umożliwiać 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 7 administratorów do poszczególnych instancji systemu.  System musi wspierać protokoły IPv4 oraz IPv6 w zakresie:   * Firewall. * Ochrony w warstwie aplikacji. * Protokołów routingu dynamicznego. |
| **Redundancja, monitoring i wykrywanie awarii** | W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.  Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.  Monitoring stanu realizowanych połączeń VPN.  System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych. |
| **Interfejsy, Dysk, Zasilanie** | System realizujący funkcję Firewall musi dysponować co najmniej poniższą liczbą i rodzajem interfejsów:   * 5 portami Gigabit Ethernet RJ-45. * System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. * System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q. * System jest wyposażony w zasilanie AC. |
| **Parametry wydajnościowe** | W zakresie Firewall’a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę.  Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B.  Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps.  Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 4 Gbps.  Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1 Gbps.  Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 500 Mbps.  Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps. |
| **Funkcje Systemu Bezpieczeństwa** | W ramach systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:   * Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. * Kontrola Aplikacji. * Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. * Ochrona przed malware. * Ochrona przed atakami - Intrusion Prevention System. * Kontrola stron WWW. * Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. * Zarządzanie pasmem (QoS, Traffic shaping). * Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). * 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. * Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. * Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. * Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa). |
| **Polityki, Firewall** | Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.  System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:   * Translację jeden do jeden oraz jeden do wielu. * Dedykowany ALG (Application Level Gateway) dla protokołu SIP.   W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.  Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.  Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.  Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.  Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.   * Amazon Web Services (AWS). * Microsoft Azure. * Cisco ACI. * Google Cloud Platform (GCP). * OpenStack. * VMware NSX. * Kubernetes. |
| **Połączenia VPN** | System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:   * Wsparcie dla IKE v1 oraz v2. * Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). * Obsługa protokołu Diffie-Hellman grup 19, 20. * Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. * Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. * Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. * Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. * Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. * Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. * Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. * Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. * Mechanizm „Split tunneling” dla połączeń Client-to-Site.   System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:   * Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0. * Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. |
| **Routing i obsługa łączy WAN** | W zakresie routingu rozwiązanie musi zapewniać obsługę:   * Routingu statycznego. * Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP). * Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. * Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. * ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. * BFD (Bidirectional Forwarding Detection). * Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu. |
| **Funkcje SD-WAN** | System musi umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.  SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec). |
| **Zarządzanie pasmem** | System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.  System musi dawać możliwość określania pasma dla poszczególnych aplikacji.  System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.  System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL. |
| **Ochrona przed malware** | Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).  Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.  System musi umożliwiać skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.  System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.  System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).  Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.  System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.  System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.  Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.  Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu. |
| **Ochrona przed atakami** | Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.  System musi chronić przed atakami na aplikacje pracujące na niestandardowych portach.  Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.  Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.  System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.  Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).  Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.  Wykrywanie i blokowanie komunikacji C&C do sieci botnet.  Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie. |
| **Kontrola aplikacji** | Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.  Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.  Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.  Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.  Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.  Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).  System musi dawać możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80). |
| **Kontrola WWW** | Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.  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.  Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.  Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.  Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).  Filtr WWW musi dawać możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.  Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.  Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.  System musi pozwalać określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji. |
| **Uwierzytelnianie użytkowników w ramach sesji** | System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:  Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.  Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.  Haseł dynamicznych (RADIUS) w oparciu o zewnętrzne bazy danych.  System musi dawać możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.  System musi umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.  Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP. |
| **Zarządzanie** | 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.  Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.  Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.  System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.  System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.  Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.  Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.  Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).  Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP. |
| **Logowanie** | Elementy systemu bezpieczeństwa muszą realizować 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.  W przypadku, kiedy usługa logowania i raportowania realizowana jest w chmurze, wymagane są stosowne licencje upoważniające do składowania logów przez okres co najmniej jednego roku.  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.  Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.  Możliwość włączenia logowania per reguła w polityce firewall.  System zapewnia możliwość logowania do serwera SYSLOG.  Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS. |
| **Testy wydajnościowe oraz funkcjonalne** | Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy. |
| **Serwisy i licencje** | Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:  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 do daty minimum 06.05.2026r. |
| **Gwarancja oraz wsparcie** | System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora do dnia minimum 02.05.2026r.  Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 lub równoważny w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Czas reakcji winien być nie dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym. |
| **Ilość** | 1 szt. |

## 

## 2. Serwer

|  |  |
| --- | --- |
| **Nazwa** | **Wymagania minimalne dla sprzętu** |
| **Typ** | Serwer sprzęt serwerowy wraz z systemem operacyjnym dla Urzędu Gminy w Krzęcinie |
| **Obudowa** | Obudowa typu Tower z możliwością instalacji do 4 dysków twardych 3,5”. |
| **Płyta główna** | Płyta główna z możliwością zainstalowania jednego fizycznego procesora, posiadająca minimum 4 sloty na pamięć RAM UDIMM z możliwością zainstalowania do minimum 128GB pamięci RAM,  możliwe zabezpieczenia pamięci: ECC.  Płyta główna musi być zaprojektowana przez producenta serwera. |
| **Procesor** | Zainstalowany minimum jeden procesor minimum 8-rdzeniowy klasy x86 dedykowany do pracy z zaoferowanym serwerem minimum 2.6GHz, 16MB pamięci cache, 65W i musi osiągać w teście Passmark CPU Mark, w kategorii Average CPU Mark wynik co najmniej 17400 pkt. według wyników opublikowanych na stronie <http://www.cpubenchmark.net/cpu_list.php> Wydruk z testu należy dołączyć do oferty. Zamawiający dopuszcza wydruk w języku angielskim. |
| **RAM** | Minimum 2x16 GB pamięci RAM UDIMM o częstotliwości taktowania minimum 3200MHz |
| **SAS HBA** | Możliwe konfiguracje poziomów RAID: No RAID Pass-Thru |
| **Interfejsy sieciowe/FC/SAS** | Minimum 2 interfejsy sieciowe 1Gb/s Ethernet nie zajmujące żadnego z dostępnych slotów PCI Express. |
| **Dyski twarde** | Zainstalowane minimum:   * 2x dysk SSD SATA MU o pojemności minimum 480GB * 2x dysk SAS o pojemności min. 2.4TB   Możliwość instalacji dwóch dysków M.2 SATA o pojemności min. 480GB oraz możliwość konfiguracji w RAID1. |
| **Wbudowane porty** | Minimum 8 portów USB z czego minimum 2 w technologii 3.0  Minimum 1x RS-232  Minimum 1x VGA |
| **Video** | Zintegrowana karta graficzna umożliwiająca wyświetlenie obrazu w rozdzielczości minimum 1280x1024 pikseli |
| **System operacyjny/ dodatkowe oprogramowanie** | Zakres Przedmiotu Zamówienia obejmuje dostarczenie Oprogramowania Systemowego zwanego dalej SSO.  Licencja musi uprawniać do uruchamiania SSO w środowisku fizycznym i dwóch środowisk SSO za pomocą wbudowanych mechanizmów wirtualizacji.  SSO musi posiadać następujące, wbudowane cechy:  a) możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym,  b) możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny,  c) możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych,  d) 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,  e) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy, f) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy,  g) automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego, możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading),  i) wbudowane wsparcie instalacji i pracy na wolumenach, które:  I. pozwalają na zmianę rozmiaru w czasie pracy systemu,  II. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,  III. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,  IV. umożliwiają zdefiniowanie list kontroli dostępu (ACL),  j) wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość,  k) wbudowane szyfrowanie dysków  l) możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET,  m) możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów,  n) wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych,  o) graficzny interfejs użytkownika,  p) zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,  r) wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play),  s) możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu,  t) dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa,  u) możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:  I. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,  II. 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:  1) podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,  2) ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,  3) odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,  III. zdalna dystrybucja oprogramowania na stacje robocze,  IV. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej,  V. centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:  1) dystrybucję certyfikatów poprzez http,  2) konsolidację CA dla wielu lasów domeny,  3) automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,  VI. szyfrowanie plików i folderów,  VII. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),  VIII.możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów,  IX. serwis udostępniania stron WWW,  X. wsparcie dla protokołu IP w wersji 6 (IPv6),  XI. 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:  1) dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,  2) obsługi ramek typu jumbo frames dla maszyn wirtualnych,  3) obsługi 4-KB sektorów dysków,  4) nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,  5) możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API,  6) możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model),  v) 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,  w) wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath),  x) możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego,  y) mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty,  z) możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.  W ramach dostawy SSO mają zostać dostarczone także licencje dostępowe do serwera dla 2 użytkowników i 35 urządzeń. |
| **Bezpieczeństwo** | Możliwość wyłączenia w BIOS funkcji przycisku zasilania.  BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła  Moduł TPM 2.0 V3  Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem  Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155 lub równoważnymi. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust). |
| **Karta Zarządzania** | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:   * zdalny dostęp do graficznego interfejsu Web karty zarządzającej; * zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); * szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; * możliwość podmontowania zdalnych wirtualnych napędów; * wirtualną konsolę z dostępem do myszy, klawiatury; * wsparcie dla IPv6; * wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; * możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; * możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; * integracja z usługą katalogową; * możliwość obsługi przez dwóch administratorów jednocześnie; * wsparcie dla dynamic DNS; * wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. * możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera * możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera oraz z możliwością rozszerzenia funkcjonalności o: * Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej * Przesyłanie danych telemetrycznych w czasie rzeczywistym * Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze * Automatyczna rejestracja certyfikatów (ACE) |
| **Oprogramowanie do zarządzania** | Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniające poniższe wymagania:   * Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych * integracja z usługą katalogową * Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta * Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish * Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram * Szczegółowy opis wykrytych systemów oraz ich komponentów * Możliwość eksportu raportu do CSV, HTML, XLS, PDF * Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. * Grupowanie urządzeń w oparciu o kryteria użytkownika * Tworzenie automatycznie grup urządzeń w opraciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji * Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach * Szybki podgląd stanu środowiska * Podsumowanie stanu dla każdego urządzenia * Szczegółowy status urządzenia/elementu/komponentu * Generowanie alertów przy zmianie stanu urządzenia. * Filtry raportów umożliwiające podgląd najważniejszych zdarzeń * Integracja z service desk producenta dostarczonej platformy sprzętowej * Możliwość przejęcia zdalnego pulpit * Możliwość podmontowania wirtualnego napędu * Kreator umożliwiający dostosowanie akcji dla wybranych alertów * Możliwość importu plików MIB * Przesyłanie alertów „as-is” do innych konsol firm trzecich * Możliwość definiowania ról administratorów * Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów * Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) * Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta * Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów * Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. * Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstwie weryfikacji środowiska w celu wykrycia rozbieżności. * Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile * Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. * Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. * Zdalne uruchamianie diagnostyki serwera. * Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarzadzającym. * Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V. |
| **Certyfikaty** | Serwer aplikacji musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001 lub normami równoważnymi  Serwer aplikacji musi posiadać deklarację CE lub równoważną |
| **Warunki gwarancji** | * Gwarancja producenta na minimum 36 miesięcy świadczona przez podmiot posiadający ISO 9001:2015 (lub równoważną) oraz ISO-27001 (lub równoważną) na świadczenie usług serwisowych. Na potwierdzenie wymogu wymagane jest dołączenie do oferty Poświadczenia producenta, że serwis oferowanego serwera będzie:   - realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta;  - firma serwisująca posiada autoryzacje producenta oferowanego serwera;  - firma serwisująca posiada ISO 9001:2015 (lub równoważną) oraz ISO-27001 (lub równoważną) na świadczenie usług serwisowych.   * Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. * Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. * Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych. * Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania. * Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. * Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera. * Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii. * Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. * Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:   + Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego.   + Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy.   + Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową.   + Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu.   + Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. * Zamawiający w ramach gwarancji wymaga dodatkowo usługi, w ramach której, w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Na potwierdzenie, że oferowany serwer będzie posiadał odpowiednią gwarancję, wymagane jest dołączenie do oferty oświadczenia producenta oferowanego sprzętu. |
| **Ilość** | 1 szt. |

## 

## 3. Network Attached Storage NAS typ 1

|  |  |
| --- | --- |
| **Nazwa** | **Wymagania minimalne dla sprzętu** |
| **Typ** | Network Attached Storage NAS typ 1 dla Urzędu Gminy w Krzęcinie |
| **Obudowa** | Tower |
| **Procesor** | Procesor minimum 4 rdzeniowym 64 bit x86 o takowaniu nie mniejszym niż 2.0 GHz |
| **RAM** | Minimum 8GB |
| **Pamięć Flash** | Minimum 4GB |
| **Liczba zatok na dyski** | Minimum 4 zatoki 3,5" |
| **Obsługiwane dyski** | 3.5" HDD SATA oraz 2.5" HDD SATA oraz 2.5" SATA SSD |
| **Wbudowane w urządzenie interfejsy na dyski M2** | Minimum 2 x M2 PCIe Gen3x2 |
| **Moduł rozszerzający** | Możliwość podłączenia co najmniej 2 modułów rozszerzających |
| **Porty** | Minimum:  2x Porty USB 3.2 Gen2  2x Port HDMI  2x RJ-45 2,5 GbE |
| **Diody LED** | Minimum:  Status, LAN, HDD |
| **Normy środowiskowe** | Dopuszczalna temaperatura pracy: 0-40 ˚C |
| **Zasilacz** | Maksymalnie 90 W |
| **Agregacja łączy** | Wymagana agregacja łączy |
| **Obsługiwane systemy plików** | Dyski wewnętrzne: EXT4  Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+, exFAT |
| **Szyfrowanie udziałów** | Minimum AES 256 |
| **Szyfrowanie dysków zewnętrznych** | Zamawiający wymaga szyfrowania dysków zewnętrznych |
| **Zarządzanie dyskami** | Pojedynczy Dysk, 0, 1, 5, 6, 10, JBOD,  Obsługa Hot Spare per grupa RAID oraz global hot spare  Rozszerzanie pojemności Online RAID  Migracja poziomów Online RAID  HDD S.M.A.R.T.  Skanowanie uszkodzonych bloków  Przywracanie macierzy RAID  Obsługa map bitowych  Pula pamięci masowej  Obsługa migawek  Obsługa replikacji migawek |
| **Wbudowana obsługa iSCSI** | Multi-LUNs na Target  Obsługa LUN Mapping & Masking  Obsługa MPIO  Migawka / kopia zapasowa iSCSI LUN |
| **Zarządzanie prawami dostępu** | Ograniczenie dostępnej pojemności dysku dla użytkownika  Importowanie listy użytkowników  Zarządzanie kontami użytkowników  Zarządzanie grupą użytkowników  Zarządzanie współdzieleniem w sieci  Tworzenie użytkowników za pomocą makr  Obsługa zaawansowanych uprawnień dla podfolderów |
| **Funkcje backup** | Oprogramowanie do tworzenia kopii bezpieczeństwa plików producenta urządzenia dla systemów Windows, backup na zewnętrzne dyski twarde |
| **Obsługiwane serwery** | Serwer plików  Serwer FTP  Serwer WEB  Serwer kopii zapasowych  Serwer multimediów UPnP  Serwer pobierania (Bittorrent / HTTP / FTP)  Serwer Monitoringu |
| **VPN** | VPN client / VPN server  Obsługa PPTP, OpenVPN |
| **Administracja systemu** | Połączenia HTTP/HTTPS  Powiadamianie przez e-mail (uwierzytelnianie SMTP)  Powiadamianie przez SMS  Ustawienia inteligentnego chłodzenia  DDNS oraz zdalny dostęp w chmurze  SNMP (v2 & v3)  Obsługa UPS z zarządzaniem SNMP (USB)  Obsługa sieciowej jednostki UPS  Monitor zasobów  Kosz sieciowy dla CIFS/SMB oraz AFP  Monitor zasobów systemu w czasie rzeczywistym  Rejestr zdarzeń  System plików dziennika  Całkowity rejestr systemowy (poziom pliku)  Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line  Aktualizacja oprogramowania automatyczna  Możliwość aktualizacji oprogramowania ręcznie  Ustawienia systemu: Kopia, Przywracanie, Resetowanie |
| **Wirtualizacja** | Wbudowana aplikacja umożliwiająca tworzenie środowiska wirtualnego wraz z instalacją maszyn wirtualnych na systemach Windows, Linux i Android.  Dostęp do konsoli maszyn za pośrednictwem przeglądarki z HTML5  Funkcjonalności importu, eksportu, klonowania i wykonywania migawek maszyn wirtualnych. |
| **Konteneryzacja** | Możliwość uruchomienia wirtualnych kontenerów dla LXD i Docker |
| **Zabezpieczenia** | Filtracja IP  Ochrona dostępu do sieci z automatycznym blokowaniem  Połączenie HTTPS  FTP z SSL/TLS (Explicit)  Obsługa SFTP (tylko admin)  Szyfrowanie AES 256-bit  Szyfrowana zdalna replikacja (Rsync poprzez SSH)  Import certyfikatu SSL  Powiadomienia o zdarzeniach za pośrednictwem Email i SMS |
| **Zainstalowane dyski** | Ilość: minimum 4 szt.  Pojemność: minimum 2TB  Obudowa: 3.5”  Interfejs: minimum SATA 6Gb/s  Prędkość obrotowa: minimum 5400 rpm |
| **Gwarancja** | Minimum 36 miesięcy gwarancji producenta na sprzęt i dyski |
| **Ilość** | 1 szt. |

## 

## 4. Network Attached Storage NAS typ 2

|  |  |
| --- | --- |
| **Nazwa** | **Wymagania minimalne dla sprzętu** |
| **Typ** | Network Attached Storage NAS typ 2 dla Urzędu Gminy w w Krzęcinie |
| **Obudowa** | Tower |
| **Procesor** | Procesor minimum 4 rdzeniowym 64 bit x86 o takowaniu nie mniejszym niż 2.0 GHz |
| **RAM** | Minimum 8GB |
| **Pamięć Flash** | Minimum 4GB |
| **Liczba zatok na dyski** | Minimum 4 zatoki 3,5" |
| **Obsługiwane dyski** | 3.5" HDD SATA oraz 2.5" HDD SATA oraz 2.5" SATA SSD |
| **Wbudowane w urządzenie interfejsy na dyski M2** | Minimum 2 x M2 PCIe Gen3x2 |
| **Moduł rozszerzający** | Możliwość podłączenia co najmniej 2 modułów rozszerzających |
| **Porty** | Minimum:  2x Porty USB 3.2 Gen2  2x Port HDMI  2x RJ-45 2,5 GbE |
| **Diody LED** | Minimum:  Status, LAN, HDD |
| **Normy środowiskowe** | Dopuszczalna temaperatura pracy: 0-40 ˚C |
| **Zasilacz** | Maksymalnie 90 W |
| **Agregacja łączy** | Wymagana agregacja łączy |
| **Obsługiwane systemy plików** | Dyski wewnętrzne: EXT4  Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+, exFAT |
| **Szyfrowanie udziałów** | Minimum AES 256 |
| **Szyfrowanie dysków zewnętrznych** | Zamawiający wymaga szyfrowania dysków zewnętrznych |
| **Zarządzanie dyskami** | Pojedynczy Dysk, 0, 1, 5, 6, 10, JBOD,  Obsługa Hot Spare per grupa RAID oraz global hot spare  Rozszerzanie pojemności Online RAID  Migracja poziomów Online RAID  HDD S.M.A.R.T.  Skanowanie uszkodzonych bloków  Przywracanie macierzy RAID  Obsługa map bitowych  Pula pamięci masowej  Obsługa migawek  Obsługa replikacji migawek |
| **Wbudowana obsługa iSCSI** | Multi-LUNs na Target  Obsługa LUN Mapping & Masking  Obsługa MPIO  Migawka / kopia zapasowa iSCSI LUN |
| **Zarządzanie prawami dostępu** | Ograniczenie dostępnej pojemności dysku dla użytkownika  Importowanie listy użytkowników  Zarządzanie kontami użytkowników  Zarządzanie grupą użytkowników  Zarządzanie współdzieleniem w sieci  Tworzenie użytkowników za pomocą makr  Obsługa zaawansowanych uprawnień dla podfolderów |
| **Funkcje backup** | Oprogramowanie do tworzenia kopii bezpieczeństwa plików producenta urządzenia dla systemów Windows, backup na zewnętrzne dyski twarde |
| **Obsługiwane serwery** | Serwer plików  Serwer FTP  Serwer WEB  Serwer kopii zapasowych  Serwer multimediów UPnP  Serwer pobierania (Bittorrent / HTTP / FTP)  Serwer Monitoringu |
| **VPN** | VPN client / VPN server  Obsługa PPTP, OpenVPN |
| **Administracja systemu** | Połączenia HTTP/HTTPS  Powiadamianie przez e-mail (uwierzytelnianie SMTP)  Powiadamianie przez SMS  Ustawienia inteligentnego chłodzenia  DDNS oraz zdalny dostęp w chmurze  SNMP (v2 & v3)  Obsługa UPS z zarządzaniem SNMP (USB)  Obsługa sieciowej jednostki UPS  Monitor zasobów  Kosz sieciowy dla CIFS/SMB oraz AFP  Monitor zasobów systemu w czasie rzeczywistym  Rejestr zdarzeń  System plików dziennika  Całkowity rejestr systemowy (poziom pliku)  Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line  Aktualizacja oprogramowania automatyczna  Możliwość aktualizacji oprogramowania ręcznie  Ustawienia systemu: Kopia, Przywracanie, Resetowanie |
| **Wirtualizacja** | Wbudowana aplikacja umożliwiająca tworzenie środowiska wirtualnego wraz z instalacją maszyn wirtualnych na systemach Windows, Linux i Android.  Dostęp do konsoli maszyn za pośrednictwem przeglądarki z HTML5  Funkcjonalności importu, eksportu, klonowania i wykonywania migawek maszyn wirtualnych. |
| **Konteneryzacja** | Możliwość uruchomienia wirtualnych kontenerów dla LXD i Docker |
| **Zabezpieczenia** | Filtracja IP  Ochrona dostępu do sieci z automatycznym blokowaniem  Połączenie HTTPS  FTP z SSL/TLS (Explicit)  Obsługa SFTP (tylko admin)  Szyfrowanie AES 256-bit  Szyfrowana zdalna replikacja (Rsync poprzez SSH)  Import certyfikatu SSL  Powiadomienia o zdarzeniach za pośrednictwem Email i SMS |
| **Zainstalowane dyski** | Ilość: minimum 4 szt.  Pojemność: minimum 2TB  Obudowa: 3.5”  Interfejs: minimum SATA 6Gb/s  Prędkość obrotowa: minimum 5400 rpm |
| **Gwarancja** | Minimum 36 miesięcy gwarancji producenta na sprzęt i dyski |
| **Ilość** | 1 szt. |

## 

## 5. UPS typ 1

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla sprzętu** |
| **Typ** | UPS typ 1 dla Urzędu Gminy Krzęcin |
| **Wymagania minimalne** | Moc kVA: minimum 30 kVA  Moc kW: minimum 30 kW  Współczynnik mocy: 1.0  Podtrzymanie obciążenia na poziomie 6kW przez minimum 157 minut  Zainstalowane akumulatory 12V40Ah minimum: 40 szt. |
| **Wejście** | Fazy: minimum 3  Napięcie nominalne: 380V/400V/415V  Zakres napięcia przy 100% obciążenia: 304-478Vac  Zakres napięcia przy 50% obciążenia: 208-478Vac  Częstotliwość nominalna: 50/60 Hz  Zakres częstotliwości dla pracy on-line: ± 10%  Wejściowe THD: 3%  Współczynnik mocy wejściowej: 0.99 |
| **Wyjście** | Fazy: minimum 3  Napięcie nominalne: 380V/400V/415V  Zmiana napięcia: ±1%  Kształt napięcia: czysta sinusoida  Współczynnik szczytu: 3:1  Częstotliwość: 50Hz lub 60Hz  Stabilność częstotliwości: ± 0,2%  Przeciążenie: 125% przez 10 minut; 150% przez 1 minutę |
| **Komunikacja** | Interfejs: USB, RS 232  Interfejs przekaźnikowy bezpotencjałowy: Dostępne informacje:   * brak zasilania, * niskie napięcie akumulatorów (LB), * bypass załączony, * uszkodzenie ups-a.   Inne: EPO |
| **Filtr przeciwzakłóceniowy** | Zamawiający wymaga filtra przeciwzakłóceniowego EMI/RFI |
| **Warunki środowiskowe** | Temperatura przechowywania: -25 stopni Celcjusza do +55 stopni Celcjusza  Temperatura pracy: 0 stopni Celcjusza do +40 stopni Celcjusza |
| **Parametry techniczne** | Waga bez baterii (kg): Maksymalnie 75 kg |
| **Certyfikaty i normy** | Normy minimum: EN 62040-1-1, EN 62040-2 lub równoważne  Certyfikat minimum: CE lub równoważne |
| **Opcje** | Wewnętrzny lub zewnętrzny SNMP, bloki akumulatorowe. |
| **Wymagania dodatkowe** | Zamawiający wymaga adaptera SNMP umożlwiającego bieżącą kontrolę pracy urządzenia oraz różnych jego parametrów z dowolnego miejsca poprzez sieć.  Zamawiający wymaga montażu dodatkowego bypassu zewnętrznego.  Zamawiający wymaga montażu UPS wraz ze szkoleniem w zakresie obsługi urządzenia Zamawiającego.  Zamawiający wymaga dostarczenia UPS wraz z zamkniętą szafą. |
| **Gwarancja** | Minimum 24 miesięcy gwarancji producenta |
| **Ilość** | 1 szt. |

## 6. UPS typ 2

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla sprzętu** |
| **Typ** | UPS typ 2 dla Środowiskowego Domu Samopomocy |
| **Wymagania minimalne** | Typ obudowy: Tower  Rodzaj akumulatora: kwasowo- ołowiowy  Moc znamionowa w W: minimum 540 W  Moc znamionowa w VA: minimum 900 VA  Czas pracy przy mocy 100 W: minimum 42 minuty |
| **Wejście** | Główne napięcie wejściowe: minimum 230 V  Częstotliwość wejściowa: 50/60 Hz +/- 3Hz automatyczne wykrywanie  Maksymalny prąd wejściowy: 10 A |
| **Wyjście** | Maksymalna możliwa do konfiguracji moc (W): 540 W  Częstotliwość na wyjściu: 50/60 Hz +/- 1 Hz synchronicznie z siecią  Maksymalna możliwa do konfiguracji moc (VA): 900 VA  Topologia: Line interactive  Czas przełączenia zasilania: maksymalnie 12 ms |
| **Akumulatory i czasy podtrzymania** | Typowy czas pełnego ładowania akumulatora: maksymalnie 12 godzin  Napięcie akumulatora: 11V  Pojemność baterii: minimum 9.4 A.h. |
| **Gniazdo wejściowe** | Minimum: IEC 60320 C13 |
| **Gniazdo wyjściowe** | Minimum: 6x IEC 60320 C13 |
| **Porty** | Minimum:  1 x USB (Type B)  2 x RJ-11  2 x RJ-45 LAN |
| **Certyfikaty i normy** | Minimum: A-Tick, C-Tick, CE, EAC, RCM, TISI  Minimum: EN/IEC 62040-1:2019/A11:2021, EN/IEC 62040-2:2006/AC:2006, EN/IEC 62040-2:2018 |
| **Parametry środowiskowe** | Temperatura otoczenia dla pracy urządzenia: 0-40 °C  Temperatura otoczenia dla przechowywania: -15-40 °C |
| **Zarządzanie** | Wielofunkcyjna konsola sterownicza i informacyjna LCD |
| **Gwarancja** | Minimum 36 miesięcy gwarancji producenta |
| **Ilość** | 1 szt. |

## 

## 7. UPS typ 3

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla sprzętu** |
| **Typ** | UPS typ 3 dla Urzędu Gminy w Krzęcinie |
| **Wymagania minimalne** | Rodzaj akumulatora: kwasowo- ołowiowy  Moc znamionowa w W: minimum 520 W  Moc znamionowa w VA: minimum 850 VA  Montaż: podłogowo/ścienny |
| **Wejście** | Częstotliwość sieciowa: 47- 63 Hz  Maksymalny prąd wejściowy: 6 A |
| **Wyjście** | Maksymalna możliwa do konfiguracji moc (W): 540 W  Częstotliwość na wyjściu: 47- 63 Hz synchronicznie z siecią  50/60 Hz +/- 1 Hz niezsynchronizowana z siecią zasilającą  Maksymalna możliwa do konfiguracji moc (VA): 850 VA  Czas przełączenia zasilania: maksymalnie 10 ms |
| **Akumulatory i czasy podtrzymania** | Typowy czas pełnego ładowania akumulatora: maksymalnie 16 godzin  Napięcie akumulatora: 12 V  Pojemność baterii: minimum 9.0 A.h. |
| **Gniazdo wyjściowe** | Minimum: 8x typ, francuskie/belgijskie |
| **Porty** | Minimum:  1 x USB (Type C)  1 x USB 2.0 |
| **Certyfikaty i normy** | Minimum: CE, EAC  Minimum: EN/IEC 62040-1:2019/A11:2021 EN/IEC 62040-2:2006/AC:2006 EN/IEC 62040-2:2018 |
| **Parametry środowiskowe** | Temperatura otoczenia dla pracy urządzenia: 0-40 °C  Temperatura otoczenia dla przechowywania: -15-40 °C |
| **Zarządzanie** | Wielofunkcyjna konsola sterownicza i informacyjna LCD |
| **Gwarancja** | Minimum 36 miesięcy gwarancji producenta |
| **Ilość** | 3 szt. |

## 

## 8. UPS typ 4

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla sprzętu** |
| **Typ** | UPS typ 4 dla Środowiskowego Domu Samopomocy |
| **Wymagania minimalne** | Rodzaj akumulatora: kwasowo- ołowiowy  Moc znamionowa w W: minimum 520 W  Moc znamionowa w VA: minimum 850 VA  Montaż: podłogowo/ścienny |
| **Wejście** | Częstotliwość sieciowa: 47- 63 Hz  Maksymalny prąd wejściowy: 6 A |
| **Wyjście** | Maksymalna możliwa do konfiguracji moc (W): 540 W  Częstotliwość na wyjściu: 47- 63 Hz synchronicznie z siecią  50/60 Hz +/- 1 Hz niezsynchronizowana z siecią zasilającą  Maksymalna możliwa do konfiguracji moc (VA): 850 VA  Czas przełączenia zasilania: maksymalnie 10 ms |
| **Akumulatory i czasy podtrzymania** | Typowy czas pełnego ładowania akumulatora: maksymalnie 16 godzin  Napięcie akumulatora: 12 V  Pojemność baterii: minimum 9.0 A.h. |
| **Gniazdo wyjściowe** | Minimum: 8x typ, francuskie/belgijskie |
| **Porty** | Minimum:  1 x USB (Type C)  1 x USB 2.0 |
| **Certyfikaty i normy** | Minimum: CE, EAC  Minimum: EN/IEC 62040-1:2019/A11:2021 EN/IEC 62040-2:2006/AC:2006 EN/IEC 62040-2:2018 |
| **Parametry środowiskowe** | Temperatura otoczenia dla pracy urządzenia: 0-40 °C  Temperatura otoczenia dla przechowywania: -15-40 °C |
| **Zarządzanie** | Wielofunkcyjna konsola sterownicza i informacyjna LCD |
| **Gwarancja** | Minimum 36 miesięcy gwarancji producenta |
| **Ilość** | 9 szt. |

## 9. UPS typ 5

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla sprzętu** |
| **Typ** | UPS typ 5 dla Urzędu Gminy Krzęcin |
| **Wymagania minimalne** | Typ obudowy: Tower  Rodzaj akumulatora: kwasowo- ołowiowy  Moc znamionowa w W: minimum 540 W  Moc znamionowa w VA: minimum 900 VA  Czas pracy przy mocy 100 W: minimum 42 minuty |
| **Wejście** | Główne napięcie wejściowe: minimum 230 V  Częstotliwość wejściowa: 50/60 Hz +/- 3Hz automatyczne wykrywanie  Maksymalny prąd wejściowy: 10 A |
| **Wyjście** | Maksymalna możliwa do konfiguracji moc (W): 540 W  Częstotliwość na wyjściu: 50/60 Hz +/- 1 Hz synchronicznie z siecią  Maksymalna możliwa do konfiguracji moc (VA): 900 VA  Topologia: Line interactive  Czas przełączenia zasilania: maksymalnie 12 ms |
| **Akumulatory i czasy podtrzymania** | Typowy czas pełnego ładowania akumulatora: maksymalnie 12 godzin  Napięcie akumulatora: 11V  Pojemność baterii: minimum 9.4 A.h. |
| **Gniazdo wejściowe** | Minimum: IEC 60320 C13 |
| **Gniazdo wyjściowe** | Minimum: 6x IEC 60320 C13 |
| **Porty** | Minimum:  1 x USB (Type B)  2 x RJ-11  2 x RJ-45 LAN |
| **Certyfikaty i normy** | Minimum: A-Tick, C-Tick, CE, EAC, RCM, TISI  Minimum: EN/IEC 62040-1:2019/A11:2021 EN/IEC 62040-2:2006/AC:2006 EN/IEC 62040-2:2018 |
| **Parametry środowiskowe** | Temperatura otoczenia dla pracy urządzenia: 0-40 °C  Temperatura otoczenia dla przechowywania: -15-40 °C |
| **Zarządzanie** | Wielofunkcyjna konsola sterownicza i informacyjna LCD |
| **Gwarancja** | Minimum 36 miesięcy gwarancji producenta |
| **Ilość** | 1 szt. |

## 

## 10. UPS typ 6

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla sprzętu** |
| **Typ** | UPS typ 6 dla Ośrodka Pomocy Społecznej w Krzęcinie |
| **Wymagania minimalne** | Rodzaj akumulatora: kwasowo- ołowiowy  Moc znamionowa w W: minimum 520 W  Moc znamionowa w VA: minimum 850 VA  Montaż: podłogowo/ścienny |
| **Wejście** | Częstotliwość sieciowa: 47- 63 Hz  Maksymalny prąd wejściowy: 6 A |
| **Wyjście** | Maksymalna możliwa do konfiguracji moc (W): 540 W  Częstotliwość na wyjściu: 47- 63 Hz synchronicznie z siecią  50/60 Hz +/- 1 Hz niezsynchronizowana z siecią zasilającą  Maksymalna możliwa do konfiguracji moc (VA): 850 VA  Czas przełączenia zasilania: maksymalnie 10 ms |
| **Akumulatory i czasy podtrzymania** | Typowy czas pełnego ładowania akumulatora: maksymalnie 16 godzin  Napięcie akumulatora: 12 V  Pojemność baterii: minimum 9.0 A.h. |
| **Gniazdo wyjściowe** | Minimum: 8x typ, francuskie/belgijskie |
| **Porty** | Minimum:  1 x USB (Type C)  1 x USB 2.0 |
| **Certyfikaty i normy** | Minimum: CE, EAC  Minimum: EN/IEC 62040-1:2019/A11:2021 EN/IEC 62040-2:2006/AC:2006 EN/IEC 62040-2:2018 |
| **Parametry środowiskowe** | Temperatura otoczenia dla pracy urządzenia: 0-40 °C  Temperatura otoczenia dla przechowywania: -15-40 °C |
| **Zarządzanie** | Wielofunkcyjna konsola sterownicza i informacyjna LCD |
| **Gwarancja** | Minimum 36 miesięcy gwarancji producenta |
| **Ilość** | 5 szt. |

## 11. Zarządzalne urządzenia sieciowe z obsługą VLAN, MACsec, standardu 802.1X typ 1

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla sprzętu** |
| **Typ** | Zarządzalne urządzenia sieciowe z obsługą VLAN, MACsec, standardu 802.1X typ 1 dla Urzędu Gminy w Krzęcinie |
| **Przełącznik sieciowy** | W ramach postępowania wymaganym jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych. |
| **Parametry fizyczne platformy** | Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.  Zasilanie AC 230V.  Maksymalny pobór mocy: 20 W.  Minimalny zakres temperatury pracy: 0-40ᵒC. |
| **Interfejsy sieciowe** | Wymaganym jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości minimum:   * 24 porty GE RJ-45. * 4 porty GE, SFP. |
| **Zarządzanie** | * Wbudowany minimum 1 port konsoli szeregowej do pełnego zarządzania. * Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS). * Wsparcie dla SNMP w wersjach 1-3 * Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami. * Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI. * Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline. * Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP). * Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+. * Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji. * Automatycznie wykonywane rewizje konfiguracji. |
| **Parametry wydajnościowe** | * Przepustowość urządzenia minimum 56 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz minimum 80 Mpps. * Tablica adresów MAC o pojemności co najmniej 8 k wpisów. * Opóźnienie wprowadzane przez przełącznik - poniżej 5 mikrosekund. |
| **Wymagane funkcje** | * Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń. * Obsługa Jumbo Frames. * Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree). * Agregacja portów zgodna ze standardem 802.3ad. * Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q. * Obsługa routingu statycznego. * Port-mirroring. * Uwierzytelnianie 802.1x na poziomie portu. * Uwierzytelnianie 802.1x w oparciu o adres MAC. * W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN). * W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia. * W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN. |
| **Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC** | 1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:   * Centralne zarządzanie konfiguracją urządzenia * Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania * Centralne zarządzanie sieciami VLAN. * Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u * Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki. * Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej. * Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego. * Automatyczna detekcja i rekomendacje konfiguracji. * Przesyłanie logów na zewnętrzny serwer syslog. * Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników. * Obsługa białych i czarnych list adresów MAC. * Wykrywanie aplikacji komunikujących się w sieci.   2. Musi być możliwe redundantne połączenie z elementami zarządzającymi.  3. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC. |
| **Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa** | * System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym. * System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing. |
| **Gwarancja oraz wsparcie** | System musi być objęty serwisem gwarancyjnym producenta na okres 24 miesięcy polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. |
| **Ilość** | 1 szt. |

## 12. Zarządzalne urządzenia sieciowe z obsługą VLAN, MACsec, standardu 802.1X typ 2

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla sprzętu** |
| **Typ** | Zarządzalne urządzenia sieciowe z obsługą VLAN, MACsec, standardu 802.1X typ 2 dla Urzędy Gminy w Krzęcinie |
| **Przełącznik sieciowy** | W ramach postępowania wymaganym jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych. |
| **Parametry fizyczne platformy** | Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.  Zasilanie AC 230V.  Wbudowany redundantny zasilacz.  Maksymalny pobór mocy: 20 W.  Minimalny zakres temperatury pracy: 0-50ᵒC. |
| **Interfejsy sieciowe** | Wymaganym jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości minimum:   * 24 porty GE RJ-45. * 4 porty GE, SFP. |
| **Zarządzanie** | * Dedykowany minimum 1 interfejs Ethernet RJ-45 do zarządzania. * Wbudowany minimum 1 port konsoli szeregowej do pełnego zarządzania. * Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS). * Wsparcie dla SNMP w wersjach 1-3 * Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami. * Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI. * Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline. * Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP). * Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+. * Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji. * Automatycznie wykonywane rewizje konfiguracji. |
| **Parametry wydajnościowe** | * Przepustowość urządzenia minimum 56 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz minimum 82 Mpps. * Tablica adresów MAC o pojemności co najmniej 16 k wpisów. * Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund. |
| **Wymagane funkcje** | * Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń. * Obsługa Jumbo Frames. * Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree). * Agregacja portów zgodna ze standardem 802.3ad. * Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q. * Wsparcie dla Private VLAN. * Obsługa routingu statycznego. * Obsługa Quality of Service, w tym zakresie: 802.1p oraz DSCP. * Port-mirroring. * Uwierzytelnianie 802.1x na poziomie portu. * Uwierzytelnianie 802.1x w oparciu o adres MAC. * W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN). * W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia. * W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN. * Obsługa protokołu sFlow. |
| **Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC** | 1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:   * Centralne zarządzanie konfiguracją urządzenia * Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania * Centralne zarządzanie sieciami VLAN. * Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u * Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki. * Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej. * Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego. * Automatyczna detekcja i rekomendacje konfiguracji. * Przesyłanie logów na zewnętrzny serwer syslog. * Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników. * Obsługa białych i czarnych list adresów MAC. * Wykrywanie aplikacji komunikujących się w sieci.   2. Musi być możliwe redundantne połączenie z elementami zarządzającymi.  3. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC. |
| **Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa** | * System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym. * System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing. |
| **Gwarancja oraz wsparcie** | System musi być objęty serwisem gwarancyjnym producenta na okres 24 miesięcy polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. |
| **Ilość** | 2 szt. |

## 

## 13. Zarządzalne urządzenia sieciowe z obsługą VLAN, MACsec, standardu 802.1X typ 3

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla sprzętu** |
| **Typ** | Zarządzalne urządzenia sieciowe z obsługą VLAN, MACsec, standardu 802.1X typ 3 dla Urzędu Gminy w Krzęcinie |
| **Obudowa** | Obudowa urządzenia musi umożliwiać montaż na suficie lub ścianie wewnątrz budynku i zapewniać prawidłową pracę urządzenia w następujących warunkach klimatycznych:   * Temperatura -20 – 45°C, * Wilgotność 5–90%.   Urządzenie musi być dostarczone z elementami mocującymi. Obudowa musi być fabrycznie przystosowana do zastosowania linki zabezpieczającej przed kradzieżą i być wyposażona w złącze typu Kensington. |
| **Parametry minimalne** | Urządzenie musi być wyposażone w dwa niezależne moduły radiowe pracujące w podanych poniżej pasmach i obsługiwać następujące standardy:   * 2.4 GHz 802.11b/g/n, * 5 GHz 802.11a/n/ac.   Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 16 SSID.  Urządzenie musi być wyposażone w moduł BLE.  Urządzenie musi być wyposażone w minimum jeden interfejs 10/100/1000 Base-TX.  Urządzenie powinno być zasilane poprzez interfejs ETH w standardzie 802.3af lub zewnętrzny zasilacz.  Punkt dostępowy musi umożliwiać następujące tryby przesyłania danych:   * Tunnel, * Bridge, * Mesh.   Wsparcie dla QoS: 802.11e, konfigurowalne polityki QoS per użytkownik/aplikacja.  Wsparcie dla poniższych metod uwierzytelnienia: WEP, WPA-PSK, WPA-TKIP, WPA2-AES, WPA3, Web Captive Portal, MAC blacklist & whitelist, 802.1X (EAP-TLS, EAP-TTLS/MSCHAPv2, PEAP, EAP-FAST, EAP-SIM, EAP-AKA).  Interfejs radiowy urządzenia powinien wspierać następujące funkcje:   * MIMO – 2x2, * Maksymalna przepustowość dla poszczególnych modułów radiowych: * 400 Mbps; * 867 Mbps;   Wymagana moc nadawania:   * Minimum 23 dBm dla pasma 2.4GHz z możliwością zmiany co 1dBm; * Minimum 24 dBm dla pasma 5GHz z możliwością zmiany co 1dBm;   Wsparcie dla 802.11n 20/40Mhz HT,  Wsparcie dla kanałów 80MHz,  Anteny – minimum 4 zewnętrzne dla nadajników standardu 802.11 o zysku minimum 4dBi dla pasma 2.4GHz, 5dBi dla pasma 5GHz.  Nieużywany moduł radiowy może zostać wyłączony programowo w celu obniżenia poboru mocy,  Maksymalna deklarowana liczba klientów per moduł radiowy:   * 512, * 512. |
| **Gwarancja oraz wsparcie** | Urządzenie musi mieć zapewnioną dożywotnią ograniczoną gwarancję producenta, tj. Do 60 miesięcy od zaprzestania produkcji oraz być objęte serwisem gwarancyjnym producenta przez okres minimum 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. |
| **Ilość** | 3 szt. |

## 

## 14. Oprogramowanie antywirusowe

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla oprogramowania** |
| **Typ** | Oprogramowanie antywirusowe dla Urzędu Gminy Krzęcin |
| **Administracja zdalna w chmurze** | 1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego.  2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.  3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL.  4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.  5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.  7. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.  8. Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.  9. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.  10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.  11. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.  12. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej. |
| **Ochrona stacji roboczych** | 1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).  2. Rozwiązanie musi wspierać architekturę 32 i 64-bitową systemu Windows.  3. Rozwiązanie musi wspierać architekturę ARM64.  3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.  4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.  5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.  6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.  7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.  8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.  9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.  10. Rozwiązanie musi integrować się z Intel Threat Detection Technology.  11. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).  12. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.  13. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.  14. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.  15. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.  16. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:  • tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,  • tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,  • tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,  • tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,  • tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.  17. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.  18. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.  19. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.  20. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).  21. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.  22. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.  23. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:  • tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,  • tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,  • tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,  • tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.  24. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.  25. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.  26. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.  27. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.  28. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.  29. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.  30. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum. |
| **Ochrona serwera** | 1. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 7,8 i 9, CentOS 7, Ubuntu  Server 18.04 LTS i nowsze, Debian 10, Debian 11 i Debian 12, SUSE Linux Enterprise  Server (SLES) 15, Oracle Linux 8 oraz Amazon Linux.  2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.  3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.  4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.  5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.  6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.  7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.  8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.  Dodatkowe wymagania dla ochrony serwerów Windows:  9. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.  10. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).  11. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.  12. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.  13. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.  14. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.  15. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.  16. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.  17. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.  Dodatkowe wymagania dla ochrony serwerów Linux:  18. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.  19. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.  20. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu. |
| **Licencje** | Zamawiający wymaga dostarczenia licencji na minimum 50 użytkowników. Licencje muszą obowiązywać do dnia minimum 02.05.2026r. |
| **Ilość** | 1 szt. |

## 15. Oprogramowanie do wykonywania kopii zapasowych typ 1

|  |  |
| --- | --- |
| **Nazwa** | **Wymagania minimalne dla oprogramowania** |
| **Typ** | Oprogramowanie do wykonywania kopii zapasowych typ 1 dla Urzędu Gminy w Krzęcinie |
| **Wymagania**  **funkcjonalne** | • Oprogramowanie działające w architekturze klient-serwer w oparciu o protokół TCP/IP, z centralnym modułem sterowania wykonywaniem kopii zapasowych z dysków komputerów klienckich  • Możliwość archiwizacji pełnej, przyrostowej/różnicowej i delta (różnica na poziomie fragmentów plików)  • Możliwość archiwizacji otwartych i zablokowanych plików bez korzystania z usługi Volume Shadow Copy Service (VSS)  • Automatyczny backup przy wyłączaniu komputera  • Możliwość wybrania do archiwizacji lub wykluczenia z archiwizacji określonych woluminów, katalogów, plików za pomocą symboli wieloznacznych \* i ?  • Backup całego systemu operacyjnego i zainstalowanych programów (tylko Windows)  • Backup baz danych i plików poczty w trybie online i offline  • Kopie rotacyjne (wersjonowanie)  • Zapis archiwów w otwartym formacie (ZIP 64-bit)  • Odzyskiwanie systemu operacyjnego na czystym dysku twardym bez konieczności ponownej instalacji (bare metal restore)  • Bezpośrednie odzyskiwanie plików do lokalizacji oryginalnej  • Odzyskiwanie z kopii różnicowych i delta tak jak z kopii pełnych  • Szyfrowanie archiwów i transferu zapewniających bezpieczeństwo sieci i informacji wymaganych przez RODO  • Kompresja po stronie stacji roboczej  • Replikacja archiwów na dodatkowy dysk twardy, NAS, serwer FTP,  • Replikacja na napęd optyczny: CD, DVD, Blu-Ray, HD-DVD i napęd taśmowy: DDS, DLT, LTO, AIT (tylko Windows)  • Centralne sterowanie całym Systemem z jednego miejsca  • Transparentna archiwizacja wykonywana w tle, która nie jest odczuwalna przez pracowników  • Możliwość równoległej archiwizacji wszystkich komputerów podłączonych do sieci LAN/WAN  • Wysyłanie Alertów administracyjnych na e-mail  • Możliwość uruchamiania zewnętrznych programów, skryptów i plików wsadowych na serwerze backupu i na komputerach zdalnych  • Raporty podsumowujące przebieg archiwizacji, zawierające informacje na temat zaległych zadań archiwizacji oraz statystyki  • Automatyczna aktualizacja oprogramowania na komputerach zdalnych |
| **Licencja** | Zamawiający wymaga dostarczenia licencji bezterminowych dla minimum 30 stanowisk klienckich i minimum 1 serwera. |
| **Ilość** | 1 szt. |

## 

## 16. Oprogramowanie do wykonywania kopii zapasowych typ 2

|  |  |
| --- | --- |
| **Nazwa** | **Wymagania minimalne dla oprogramowania** |
| **Typ** | Oprogramowanie do wykonywania kopii zapasowych typ 2 dla Środowiskowego Domu Kultury w Krzęcinie |
| **Wymagania**  **funkcjonalne** | • Oprogramowanie działające w architekturze klient-serwer w oparciu o protokół TCP/IP, z centralnym modułem sterowania wykonywaniem kopii zapasowych z dysków komputerów klienckich  • Możliwość archiwizacji pełnej, przyrostowej/różnicowej i delta (różnica na poziomie fragmentów plików)  • Możliwość archiwizacji otwartych i zablokowanych plików bez korzystania z usługi Volume Shadow Copy Service (VSS)  • Automatyczny backup przy wyłączaniu komputera  • Możliwość wybrania do archiwizacji lub wykluczenia z archiwizacji określonych woluminów, katalogów, plików za pomocą symboli wieloznacznych \* i ?  • Backup całego systemu operacyjnego i zainstalowanych programów (tylko Windows)  • Backup baz danych i plików poczty w trybie online i offline  • Kopie rotacyjne (wersjonowanie)  • Zapis archiwów w otwartym formacie (ZIP 64-bit)  • Odzyskiwanie systemu operacyjnego na czystym dysku twardym bez konieczności ponownej instalacji (bare metal restore)  • Bezpośrednie odzyskiwanie plików do lokalizacji oryginalnej  • Odzyskiwanie z kopii różnicowych i delta tak jak z kopii pełnych  • Szyfrowanie archiwów i transferu zapewniających bezpieczeństwo sieci i informacji wymaganych przez RODO  • Kompresja po stronie stacji roboczej  • Replikacja archiwów na dodatkowy dysk twardy, NAS, serwer FTP,  • Replikacja na napęd optyczny: CD, DVD, Blu-Ray, HD-DVD  • Centralne sterowanie całym Systemem z jednego miejsca  • Transparentna archiwizacja wykonywana w tle, która nie jest odczuwalna przez pracowników  • Możliwość równoległej archiwizacji wszystkich komputerów podłączonych do sieci LAN/WAN  • Wysyłanie Alertów administracyjnych na e-mail  • Możliwość uruchamiania zewnętrznych programów, skryptów i plików wsadowych na serwerze backupu i na komputerach zdalnych  • Raporty podsumowujące przebieg archiwizacji, zawierające informacje na temat zaległych zadań archiwizacji oraz statystyki  • Automatyczna aktualizacja oprogramowania na komputerach zdalnych |
| **Licencja** | Zamawiający wymaga dostarczenia licencji bezterminowych dla minimum 10 stanowisk klienckich i minimum 1 serwera. |
| **Ilość** | 1 szt. |

## 17. Oprogramowanie przeciwdziałającemu wyciekowi danych DLP - Data Leak Prevention

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla oprogramowania** |
| **Typ** | Oprogramowanie przeciwdziałającemu wyciekowi danych DLP - Data Leak Prevention dla Urzędu Gminy w Krzęcinie |
| **Wymagania ogólne** | Zamawiający wymaga dostarczenia licencji o minimalnych wymaganiach:  System musi być wspierany przez:   * 1. Windows 10 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi   2. Windows 11 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi   Serwer administracyjny musi obsługiwać instalację na systemach: a. Windows Server 2016 (64-bit) i nowszych.  Serwer administracyjny musi obsługiwać bazy danych:   1. MS SQL Server 2016 lub nowsze, 2. MS SQL Express,   Pomoc i dokumentacja programu dostępne w języku polskim lub angielskim.  Konsola administracyjna i komunikaty klienta muszą być w języku polskim.  Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta.  Serwer administracyjny musi umożliwiać instalację/dezinstalację zdalnego klienta na stacjach roboczych.  Reguły DLP muszą być egzekwowane nawet przy braku połączenia między klientem a serwerem zarządzającym.  Brak połączenia klienta z serwerem zarządzającym musi umożliwiać lokalne przechowywanie informacji i zebranych danych do czasu ponownego połączenia.  Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsoli.  Administrator musi mieć możliwość konfiguracji automatycznej konserwacji dla bazy danych, usuwając najstarsze informacje, gdy rozmiar bazy osiągnie skonfigurowany limit.  Serwer administracyjny musi automatycznie pobierać aktualizacje definicji kategoryzowania stron internetowych, aplikacji i rozszerzeń plików, z opcją wyłączenia automatycznego pobierania.  Administrator musi mieć możliwość, aby tworzyć, usuwać i konta administratorów w konsoli programu.  Administrator musi mieć możliwość przypisywania i odbierania uprawnień do wybranych modułów programu, podzielonych na ustawienia (konfiguracja modułu) i logi (wyświetlanie logów modułu).  Serwer musi synchronizować użytkowników i stacje robocze z domeną Active Directory.  System musi rejestrować zdarzenia aktywności stacji roboczej, takie jak logowanie, wylogowanie, włączenie, wyłączenie, blokada, odblokowanie i przejście w stan bezczynności.  Administrator musi móc wymusić synchronizację ustawień i logów między stacją roboczą a serwerem w czasie rzeczywistym. Serwer administracyjny musi umożliwiać ustawienie powiadomień dla użytkownika końcowego w przypadku złamania reguł związanych z ochroną DLP, z możliwością dostosowania grafiki, adresu e-mail i odnośnika do polityki bezpieczeństwa.  Administrator musi mieć możliwość wykonać audyt stacji roboczych/użytkowników w oparciu o różne czynności, takie jak uruchomione aplikacje, podłączone urządzenia, odwiedzane strony internetowe, wydrukowane dokumenty, wysyłane i odebrane wiadomości email oraz czynności na plikach.  Administrator musi mieć możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji i typów plików.  Administrator musi mieć możliwość filtrowania i sortowania zebranych danych.  Serwer musi posiadać możliwość wysyłania alertów, przynajmniej za pośrednictwem wiadomości email.  Dashboardy muszą być generowane na podstawie wskazanych stacji roboczych, użytkowników lub grup w określonym przedziale czasu.  Serwer administracyjny musi posiadać wbudowany serwer SMTP dostarczony przez producenta oprogramowania.  Serwer administracyjny musi umożliwiać wykonywanie zadań kategoryzacji plików, zarówno istniejących na stacjach roboczych i zasobach sieciowych, jak i nowo powstałych na bazie już skategoryzowanych plików.  Serwer administracyjny musi mieć możliwość kategoryzacji plików wrażliwych na podstawie aplikacji, lokalizacji, adresu URL, formatu pliku i zawartości pliku.  Administrator musi mieć możliwość wyszukiwania danych osobowych na zasobach zarówno lokalnych, jak i sieciowych.  Dla plików skategoryzowanych, wymagana jest możliwość tworzenia reguł dotyczących blokowania i zezwalania na różne operacje, takie jak zapisywanie, przenoszenie, drukowanie, wysyłanie pocztą, wysyłanie do chmury, przesyłanie komunikatorami itp.  Serwer administracyjny musi umożliwiać wyszukiwanie i ochronę plików w oparciu o różne kryteria, takie jak numery kart kredytowych, numer PESEL, numer dowodu osobistego, numer paszportu, wyrażenia regularne, określone ciągi znaków i numer IBAN.  Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym.  Serwer administracyjny musi pozwalać na eksport logów do rozwiązania SIEM.  Konsola musi umożliwiać konfigurację/zmianę domyślnego serwera SMTP.  Konsola webowa musi pozwalać na weryfikację wersji zainstalowanego oprogramowania klienta, a także umożliwia aktualizację do nowej wersji lub dezaktywację tego oprogramowania.  System musi wykorzystywać mechanizm OCR (optical character recognition), aby wykrywać poufne treści w obrazach, zdjęciach i zeskanowanych dokumentach. |
| **Licencja** | Zamawiający wymaga w ramach dostawy do dostarczenia licencji bezterminowych oprogramowania klasy DLP dla minimum 30 użytkowników wraz ze wsparciem obowiązującym do dnia minimum 02.05.2026r. |
| **Wdrożenie** | Zamawiający wymaga wdrożenia rozwiązania w zakresie minimum:  Instalacja oprogramowania DLP  Instalacja konsoli zarządzającej  Przeprowadzenie logowania do konsoli zarządzającej  Konfiguracja SMTP  Podłączenie do infrastruktury posiadanej przez Zamawiającego (Active Directory)  Wygenerowanie agenta rozwiązania DLP oraz przeprowadzenie instalacji na środowiskach testowych wybranych przed wdrożeniem  Przypisanie licencji  Konfiguracja raportowania i monitorowania  Utworzenie stref bezpiecznych i niebezpiecznych  Instalacja klienta na stacjach z zainstalowanym agentem  Utworzenie reguł DLP wcześniej skonsultowanych z Zamawiającym  Wykonanie testów |
| **Ilość** | 1 szt. |

## 

## 18. Oprogramowanie do monitorowania infrastruktury informatycznej

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla oprogramowania** |
| **Typ** | Oprogramowanie do monitorowania infrastruktury informatycznej dla Urzędu Gminy w Krzęcinie |
| **Monitorowanie infrastruktury** | Dostarczone oprogramowanie powinno spełniać minimalne wymagania:  Wykrywanie urządzeń w sieci poprzez skanowanie ping (oraz arp-ping).  Wizualizacja stanu urządzeń w postaci ikon urządzeń na mapach sieci.  Wizualizacja połączeń pomiędzy urządzeniami a przełącznikami i informacji, do którego portu przełącznika podłączone jest dane urządzenie.  Serwisy TCP/IP, HTTP, POP3, SMTP, FTP i inne wraz z możliwością definiowania własnych serwisów. Program powinien monitorować czas ich odpowiedzi i procent utraconych pakietów.  Serwerów pocztowych:  program powinien monitorować zarówno serwis odbierający, jak i wysyłający pocztę,  program powinien mieć możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie,  program powinien mieć możliwość wykonywania operacji testowych,  program powinien mieć możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa.  Monitorowanie serwerów WWW i adresów URL.  Obsługa szyfrowania SSL/TLS w powiadomieniach e-mail.  Obsługa urządzeń SNMP wspierających SNMP v1/2/3 (przełączniki, routery, drukarki sieciowe, urządzenia VoIP).  Obsługa komunikatów syslog i pułapek SNMP.  Monitoring routerów i przełączników wg:  zmian stanu interfejsów sieciowych,  ruchu sieciowego,  podłączonych stacji roboczych,  ruchu generowanego przez podłączone stacje robocze.  Wydajności systemów z rodziny Windows posiadanych przez Zamawiającego:  obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy. |
| **Inwentaryzacja sprzętu i oprogramowania** | Dostarczone oprogramowanie powinno spełniać minimalne wymagania:  Prezentacja szczegółów dotyczących sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart  Zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade.  Informacja o zainstalowanych aplikacjach oraz aktualizacjach co bezpośrednio umożliwia audytowanie i weryfikację użytkowania licencji w organizacji.  Zbieranie informacji w zakresie zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP  Posiadanie możliwości wysyłania powiadomienia e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera.  Możliwość odczytania numeru seryjnego (klucze licencyjne).  Możliwość automatycznego zarządzania instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych.  Możliwość przeglądu informacji o konfiguracji systemu, tj. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań. |
| **Zdalna pomoc** | Dostarczone oprogramowanie powinno spełniać minimalne wymagania:  W ramach kontroli stacji użytkownika dostępny powinien być podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli. Podczas dostępu zdalnego, zarówno użytkownik jak i administrator powinni widzieć ten sam ekran. Administrator w trakcie zdalnego dostępu powinien mieć możliwość zablokowania działania myszy oraz klawiatury dla użytkownika.  Pobieranie listy użytkowników z usługi katalogowej,  Przypisywanie pracowników helpdesk do kategorii zgłoszeń.  Procesowanie zgłoszeń użytkowników z wiadomości e-mail.  Dołączanie załączników do zgłoszeń.  Zrzuty ekranowe (podgląd pulpitu).  Dystrybucję oprogramowania przez Agentów.  Dystrybucję oraz uruchamianie plików za pomocą Agentów.  Zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecania operacji następuje kolejkowanie zadania dystrybucji pliku.  Możliwość skonfigurowania automatyzacji procesowania zgłoszeń.  Planowanie nieobecności pracowników helpdesk.  Obsługę umów o gwarantowanym poziomie świadczenia usług (SLA).  Generowanie raportów obsługi helpdesk.  Zdalne wykonywanie poleceń poprzez Agentów (utworzenie / edycja konta lokalnego użytkownika systemu).  Możliwość użytkownikom monitorowania procesu rozwiązywania zgłoszonych przez nich problemów i ich aktualnych statusów, jak również możliwość wymiany informacji z administratorem poprzez komentarze, które są wpisywane i widoczne dla obu stron.  Oprogramowanie powinno posiadać komunikator.  Oprogramowanie powinno posiadać bazę zgłoszeń umożliwiającą użytkownikom zgłaszanie problemów technicznych, które z kolei są przetwarzane i przyporządkowywane odpowiednim administratorom, otrzymującym automatycznie powiadomienie o przypisanym im problemie. |
| **Monitorowanie aktywności użytkowników** | Dostarczone oprogramowanie powinno spełniać minimalne wymagania:  Monitorowanie procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika) wraz informacją o uruchomieniu na podwyższonych uprawnieniach.  Monitorowanie rzeczywistego użytkowania programów (procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność.  Monitorowanie listy odwiedzanych stron WWW (liczba odwiedzin stron z nagłówkami, liczbą i czasem wizyt).  Monitorowania transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika).  Blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla stacji roboczej, na której zalogowany jest użytkownik, z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen. Reguły w postaci listy domen tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami.  Przygotowania zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu.  Definiowania godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone.  Mechanizm blokowania uruchamiania aplikacji wg maski nazwy oraz lokalizacji pliku. Reguły w postaci listy blokowanych plików lub lokalizacji tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami. |
| **Ochrona przed wyciekiem danych** | Oprogramowanie powinno umożliwiać ochronę danych przed wyciekiem oraz posiadać min. Funkcjonalności:  Zarządzanie prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny.  Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek.  Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych.  Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików. Autoryzowanie urządzeń firmowych: pendrive’ów, dysków zewnętrznych - urządzenia nieautoryzowane.  Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci.  Monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika.  Możliwość usuwania z listy znanych urządzeń tych nośników. |
| **Licencja** | Licencja musi pozwalać na użytkowanie oprogramowania na minimum 30 stacjach roboczych, wsparcie musi obowiązywać do daty minimum 02.05.2026r. |
| **Ilość** | 1 szt. |

# III. Obszar kompetencyjny

## 1. Szkolenia dla działu IT typ 1

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla szkolenia** |
| **Typ** | Szkolenia dla działu IT typ 1 |
| **Wymagania podstawowe** | Wykonawca zapewni certyfikowane szkolenie (minimum 1 dzień) dla administratora Zamawiającego (1 osoba) z dostarczonego w pkt. II. 1. Rozwiązania klasy UTM.  Szkolenie w formie online.  Szkolenie musi być zrealizowane w formie vouchera z możliwością zrealizowania w wybranym przez Administratora terminie w przeciągu 12 miesięcy od daty wystawienia. |
| **Wymagania szczegółowe** | Program szkolenia będzie obejmować w zakresie minimum:   * Omówienie wstępnej konfiguracji urządzenia   - Tryby pracy  - Konfiguracja sieci i routingu  - System Dashboard i moduły systemu   * Konfiguracje routingu * Polityki zapory sieciowej   - Koncepcja firewall  - Tworzenie obiektów dla reguł firewall  - Translacja adresów NAT i Virtual IP   * Konfiguracje funkcji ochronnych (profile bezpieczeństwa)   - Ochrona antywirusowa  - Filtrowanie antyspamowe  - System IPS  - Kontrola ruchu WWW / blokowanie URL  - Kontrola aplikacji  - Data Leak Prevention (DLP)  - Wirtualne sieci prywatne – VPN IPSec   * Bieżącą obsługę systemu   - Tworzenie kopii zapasowej konfiguracji i jej odtwarzanie  - Aktualizacja firmware   * Filtry logów * Zewnętrzne mechanizmy logowania |
| **Ilość** | 1. szt. |

## 2. Szkolenia dla działu IT typ 2

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla szkolenia** |
| **Typ** | Szkolenia dla działu IT typ 2 |
| **Wymagania podstawowe** | Wykonawca zapewni szkolenie dla administratora Zamawiającego (1 osoba) z dostarczonego w pkt II. 14 rozwiązania antywirusowego.  Szkolenie w formie online. |
| **Wymagania szczegółowe** | Program szkolenia będzie obejmować w zakresie minimum:   * Architektura produktu * Wdrożenie i konfiguracja agentów * Omówienie funkcji * Reguły i automatyzacja * Raportowanie, powiadomienia i zarządzanie uprawnieniami, * Management Agent - zdalna instalacja i omówienie możliwości * Grupy statyczne i dynamiczne, * Zadania klienta, serwera oraz wyzwalacze, * Zdalna instalacja klienta, * Omówienie funkcji podstawowych i zaawansowanych klienta, * Ochrona antywirusowa, * Zarządzanie aktualizacją, * Polityki i dziedziczenie * Zapora osobista * Moduł antyspamowy, * Powiadomienia, * Raportowanie, * Kontrola dostępu do stron internetowych, * Kontrola dostępu do urządzeń |
| **Ilość** | 1. szt. |

## 3. Szkolenia dla działu IT typ 3

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla szkolenia** |
| **Typ** | Szkolenia dla działu IT typ 1 |
| **Wymagania podstawowe** | Wykonawca zapewni certyfikowane szkolenie (minimum 5 dni) dla administratora Zamawiającego (1 osoba) z bezpieczeństwa systemów serwerowych.  Szkolenie w formie online.  Szkolenie powinno zostać dostarczone w formie vouchera, z możliwością zrealizowania w wybranym przez Administratora terminie w okresie do minimum 02.05.2026r. |
| **Wymagania szczegółowe** | Program szkolenia będzie obejmować w zakresie minimum:  1. Wprowadzenie do administracji systemu Windows Server   * Wprowadzenie do systemu Windows Server * Wprowadzenie do systemu Windows Server Core * Wprowadzenie do zasad i narzędzi administracyjnych systemu Windows Server   Ćwiczenie: Wdrażanie i konfiguracja systemu Windows Server  2. Usługi zarządzania tożsamością w systemie Windows Server   * Wdrażanie kontrolerów domeny Windows Server * Wdrażanie zasad grupy * Wprowadzenie do usług certyfikatów usługi katalogowej   Ćwiczenie: Wdrażanie usług zarządzania tożsamością i zasad grupy  3. Usługi infrastruktury sieciowej w systemie Windows Server   * Wdrażanie i zarządzanie protokołem DHCP * Wdrażanie i zarządzanie systemem DNS * Wdrażanie i zarządzanie systemem IPAM * Usługi dostępu zdalnego w systemie Windows Server   Ćwiczenie: Wdrażanie i konfiguracja usług infrastruktury sieciowej w systemie Windows Server  4. Serwery plików i zarządzanie pamięcią masową w systemie Windows Server   * Woluminy i systemy plików w systemie Windows Server * Wdrażanie udostępniania w systemie Windows Server * Wdrażanie deduplikacji danych * Wdrażanie interfejsu iSCSI * Wdrażanie rozproszonego systemu plików   Ćwiczenie: Wdrażanie rozwiązań pamięci masowej w systemie Windows Server  5. Wirtualizacja Hyper-V i kontenery w systemie Windows Server   * Hyper-V w systemie Windows Server * Konfiguracja maszyn wirtualnych * Zabezpieczanie wirtualizacji w systemie Windows Server * Kontenery w systemie Windows Server * Wprowadzenie do platformy Kubernetes   Ćwiczenie: Wdrażanie i konfiguracja wirtualizacji w systemie Windows Server  6. Wysoka dostępność w systemie Windows Server   * Planowanie wdrożenia klastra pracy awaryjnej * Tworzenie i konfiguracja klastra pracy awaryjnej * Wprowadzenie do rozciągniętych klastrów * Planowanie rozwiązań w zakresie wysokiej dostępności i odzyskiwania danych po awarii z wykorzystaniem maszyn wirtualnych funkcji Hyper-V   Ćwiczenie: Wdrażanie klastra pracy awaryjnej  7. Odzyskiwanie danych po awarii w systemie Windows Server   * Funkcja Hyper-V Replica * Tworzenie kopii zapasowych i przywracanie infrastruktury w systemie Windows Server   Ćwiczenie: Wdrażanie funkcji Hyper-V Replica i Windows Server Backup  8. Bezpieczeństwo systemu Windows Server   * Ochrona danych uwierzytelniających i dostępu uprzywilejowanego * Zabezpieczanie i analiza ruchu w SMB * Zarządzanie aktualizacjami w systemie Windows Server   Ćwiczenie: Konfiguracja zabezpieczeń w systemie Windows Server  9. RDS (usługi pulpitu zdalnego) w systemie Windows Server   * Wprowadzenie do RDS * Konfiguracja wdrażania pulpitu opartego na sesji * Wprowadzenie do osobistych i połączonych pulpitów wirtualnych   Ćwiczenie: Wdrażanie RDS w systemie Windows Server  10. Dostęp zdalny i usługi internetowe w systemie Windows Server   * Wdrażanie sieci VPN * Wdrażanie systemu NPS * Wdrażanie serwera WWW w systemie Windows Server   Ćwiczenie: Wdrażanie obciążeń sieciowych  11. Monitorowanie serwera i wydajności w systemie Windows Server   * Wprowadzenie do narzędzi do monitorowania systemu Windows Server * Korzystanie z monitora wydajności * Monitorowanie dzienników zdarzeń w celu rozwiązywania problemów   Ćwiczenie: Monitorowanie i rozwiązywanie problemów z systemem Windows Server  12. Aktualizacja i migracja w systemie Windows Server   * Migracja AD DS * Usługa migracji pamięci masowej * Narzędzia do migracji systemu Windows Server   Ćwiczenie: Migracja obciążeń serwera |
| **Ilość** | 1 szt. |

## 4. Szkolenia pracowników spoza działu IT typ 4

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla szkolenia** |
| **Typ** | Szkolenia dla pracowników spoza działu IT typ 4 dla Urzędu Gminy w Krzęcinie, Środowiskowego Domu Samopomocy w Krzęcinie i Ośrodka Pomocy Społecznej w Krzęcinie |
| **Szkolenie cyberbezpieczeństwa** | Szkolenie musi zostać przeprowadzone w minimum 2 grupach 30 osobowych.  Szkolenie musi trwać minimum 1 h.  Szkolenie musi obejmować w zakresie minimum:  Wycieki informacji – mechanizmy i skutki.  Zarządzanie hasłami – dobre praktyki i narzędzia pomocnicze.  Psychomanipulacja w sieci – zasady i zastosowania.  Sfałszowane komunikaty i strony – identyfikacja zagrożeń.  Ataki głosowe i podszywanie się pod identyfikator dzwoniącego (vishing)  Archiwizacja internetowa – cyfrowy ślad nie znika.  Mechanizmy śledzenia w sieci – rola i funkcja cookies.  Niebezpieczeństwa ze strony nieautoryzowanego sprzętu.  Ataki siłowe na hasła – jak nie dać się złamać.  Wyłudzenie informacji przez celowane ataki phishingowe (spear phishing).  Świadomość pracowników – kultura bezpieczeństwa w organizacji. |
| **Ilość** | 1 szt. |