**Opis przedmiotu zamówienia – zał. nr 2**

|  |  |
| --- | --- |
| **UTM – 1 sztuka parametry techniczne minimum:** | |
| Wymagania ogólne | Oprogramowanie systemowe powinno realizować 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 powinien zapewnić pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.  System powinien umożliwiać budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, ss, IPS, Kontroli Aplikacji.  Powinna istnieć możliwość dedykowania co najmniej 5 administratorów do poszczególnych instancji systemu.  System wspiera protokoły IPv4 oraz IPv6 w zakresie:   * Firewall. * Ochrony w warstwie aplikacji. * Protokołów routingu dynamicznego. |
| Redundancja, monitoring i wykrywanie awarii | 1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – powinna istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewniający funkcję synchronizacji sesji. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System powinien umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Możliwość tworzenia interfejsów redundantnych. |
| Interfejsy, Dysk, Zasilanie | 1. System realizujący funkcję Firewall dysponujący co najmniej poniższą liczbą i rodzajem interfejsów:  * 10 portami Gigabit Ethernet RJ-45.  1. System Firewall powinien posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB. 2. System Firewall pozwalający skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q. 3. Urządzenie powinno być wyposażone w zasilanie AC. |
| Parametry wydajnościowe | 1. W zakresie Firewall’a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps. 4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 Gbps. 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions)- minimum 1.3 Gbps. 6. Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS,   Application Control, Antywirus - minimum 650 Mbps.   1. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 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:   1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN 4. Ochrona przed malware. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 10. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. 11. Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system. 12. Rozwiązanie musi posiadać wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa). |
| Polityki, Firewall | 1. Polityka Firewall uwzględniająca: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System realizujący translację adresów NAT: źródłowego i docelowego, translację PAT oraz:  * Translację jeden do jeden oraz jeden do wielu. * Dedykowany ALG (Application Level Gateway) dla protokołu SIP.  1. W ramach systemu powinna istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 2. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: adresy URL, adresy IP. 3. Polityka firewall umożliwiająca filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. 4. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. 5. Element systemu realizujący funkcję Firewall integrujący się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.  * Amazon Web Services (AWS). * Microsoft Azure. * Cisco ACI. * Google Cloud Platform (GCP). * OpenStack. * VMware NSX. * Kubernetes. |
| Połączenia VPN | 1. System umożliwiający konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:  * Wsparcie dla IKE v1 oraz v2. * Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). * Obsługa protokołu Diffie-Hellman grup 19, 20. * Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. * Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. * Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. * Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. * Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. * Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. * Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. * Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. * Mechanizm „Split tunneling” dla połączeń Client-to-Site.  1. Producent rozwiązania powinien posiadać w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie jako opcja i nie jest wymagane w implementacji. |
| Routing i obsługa łączy WAN | W zakresie routingu rozwiązanie powinno zapewniać obsługę:   1. Routingu statycznego. 2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego). 3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. 4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. 5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. 6. BFD (Bidirectional Forwarding Detection). 7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu. |
| Funkcje SD-WAN | 1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. SD-WAN wspierający zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec). |
| Zarządzanie pasmem | 1. System Firewall umożliwiający zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. System dający możliwość określania pasma dla poszczególnych aplikacji. 3. System pozwalający zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. 4. System winien zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL. |
| Ochrona przed malware | 1. Silnik antywirusowy umożliwiający skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. Silnik antywirusowy zapewniający skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. 3. W przypadku archiwów zagnieżdżonych powinna istnieć możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwiający konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum. 4. System umożliwiający blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. 5. System powinien dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 7. System współpracujący z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w usłudze chmurowej realizowanej na terenie Unii Europejskiej. 8. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. 9. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu. |
| Ochrona przed atakami | 1. Ochrona IPS opierająca się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System chroniący przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków zawierająca minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System zapewniający wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). 7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. 8. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie. |
| Kontrola aplikacji | 1. Funkcja Kontroli Aplikacji umożliwiający kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji zawierająca minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza sygnatur zawierająca kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. 6. Możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). 7. Możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80). |
| Kontrola WWW | 1. Moduł kontroli WWW korzystający z bazy zawierającej co najmniej 40 milionów adresów URL  pogrupowanych w kategorie tematyczne. 2. W ramach filtra WWW powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW dostarczający kategorii stron zabronionych prawem. 4. Administrator winien mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Filtr WWW umożliwiający statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwalający definiować strony z zastosowaniem wyrażeń regularnych (Regex). 6. Filtr WWW dający możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. 7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. 8. Administrator powinien mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. 9. System powinien pozwalać określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji. |
| Uwierzytelnianie użytkowników w ramach sesji | 1. System Firewall umożliwiający weryfikację tożsamości użytkowników za pomocą:  * Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. * Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. * Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.  1. Możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego. 2. System umożliwiający budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie. 3. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP. |
| Zarządzanie | 1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania powinna być  realizowana z wykorzystaniem szyfrowanych protokołów. 3. Możliwość włączenia mechanizmów uwierzytelniania wieloskładnikowego dla dostępu administracyjnego. 4. System współpracujący z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiający przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. 5. System dający możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję Firewall umożliwiający wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. 8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). 9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP. |
| Logowanie | 1. Elementy systemu bezpieczeństwa realizujące logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania element systemu pełniący funkcję Firewall zapewniający przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewniający możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie obejmujące zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. 4. Możliwość włączenia logowania per reguła w polityce firewall. 5. System zapewniający możliwość logowania do serwera SYSLOG. 6. Przesyłanie SYSLOG do zewnętrznych systemów winno być 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 lub w przypadku braku parametrów wydajnościowych w dokumentacji, wymagane jest dostarczenie wyników testów wydajnościowych (wykonanych przez producenta rozwiązania w czasie ostatnich 90 dni. |
| Wdrożenie | 1. Rejestracja urządzeń oraz licencji:   * Rejestracja urządzeń w systemie:   + Proces dodawania nowych urządzeń do systemu zarządzania.   + Konfiguracja parametrów urządzeń oraz weryfikacja poprawności rejestracji.   + Automatyczne wykrywanie urządzeń i integracja z istniejącymi zasobami. * Zarządzanie licencjami i subskrypcjami:   + Przegląd dostępnych licencji i subskrypcji.   + Procedury aktywacji i odnawiania licencji.   + Monitorowanie zużycia licencji oraz optymalizacja kosztów.   2. Aktualizacja oprogramowania i zmiana danych dostępowych:   * procedura aktualizacji oprogramowania:   + Przeprowadzanie aktualizacji firmware'u i oprogramowania urządzeń.   + Zasady bezpiecznego przeprowadzania aktualizacji (kopie zapasowe, testowanie).   + Automatyzacja procesu aktualizacji i harmonogramowanie. * Zmiana danych dostępowych (autoryzacja) do urządzeń:   + Procedury zmiany haseł i danych autoryzacyjnych.   + Implementacja polityk zmiany haseł i zarządzania dostępem.   + Audytowanie i zabezpieczanie danych dostępowych.   3. Konfiguracja metod dostępu i segmentacji sieci:   1. Konfiguracja metod dostępu do urządzeń:    * Konfiguracja \dDostępu SSH i HTTPS:      + Implementacja i konfiguracja bezpiecznego dostępu do urządzeń.      + Zarządzanie certyfikatami SSL/TLS.    * Wdrożenie dwuetapowej autoryzacji (2FA):      + Implementacja 2FA dla zwiększenia bezpieczeństwa dostępu.      + Konfiguracja aplikacji autoryzujących i tokenów sprzętowych. 2. Konfiguracja łącz dostępowych do internetu i redundancji:    * Ustawienie podstawowych łącz internetowych:      + Konfiguracja głównych połączeń internetowych.      + Monitorowanie i optymalizacja wydajności łączy.    * Konfiguracja łącz zapasowych i redundancji (WAN):      + Implementacja zapasowych łączy internetowych.      + Konfiguracja mechanizmów przełączania awaryjnego i load balancingu. 3. Segmentacja sieci LAN:    * Konfiguracja interfejsów sieciowych:      + Ustawienia interfejsów fizycznych i logicznych.      + Optymalizacja parametrów interfejsów dla różnych zastosowań.    * Konfiguracja VLAN i polityk dostępu do podsieci/VLAN:      + Tworzenie i zarządzanie VLANami.      + Implementacja polityk bezpieczeństwa dla poszczególnych VLANów.   4. Zarządzanie siecią i polityki bezpieczeństwa:   1. Uruchomienie serwerów DHCP:    * Konfiguracja serwerów DHCP na poszczególnych podsieciach/VLAN:      + Ustawienia serwerów DHCP dla dynamicznego przydzielania adresów IP.      + Zarządzanie pulami adresów i rezerwacjami. 2. Konfiguracja routingu i agregacji portów:    * ustawienia routingu statycznego i dynamicznego:      + Konfiguracja tras statycznych i protokołów routingu dynamicznego (OSPF, BGP).      + Optymalizacja trasowania i zarządzanie tablicami routingu.    * konfiguracja agregacji portów dla zwiększenia przepustowości:      + Implementacja agregacji portów (LACP).      + Balansowanie obciążenia i redundancja portów. 3. Polityki Bezpieczeństwa:    * filtrowanie i blokowanie treści oraz aplikacji internetowych:      + Konfiguracja filtrów treści i aplikacji.      + Zarządzanie czarnymi i białymi listami.    * konfiguracja antywirusa, filtrów DNS, IPS i DLP:      + Implementacja zabezpieczeń antywirusowych i systemów wykrywania intruzji (IPS).      + Konfiguracja filtrów DNS i polityk zapobiegania wyciekom danych (DLP).   5. Integracja i zarządzanie systemem:   1. Integracja z domena:    * Konfiguracja urządzeń do współpracy z domena:      + Procedury integracji z domeną Active Directory.      + Zarządzanie kontami i politykami bezpieczeństwa domeny. 2. Konfiguracja SNMP:    * Ustawienia SNMP do monitorowania sieci:      + Konfiguracja protokołu SNMP dla monitorowania i zarządzania urządzeniami sieciowymi.      + Implementacja pułapek SNMP i zbieranie danych z urządzeń.   6. Logowanie, kopie Zapasowe i VPN:   1. Konfiguracja procesu logowania:    * Konfiguracja zawartości logów i okresu przechowywania:      + Definiowanie typów logów, które mają być przechowywane.      + Ustalanie okresów retencji logów i zarządzanie przestrzenią dyskową. 2. Wykonanie kopii zapasowej ustawień urządzeń:    * procedury tworzenia kopii zapasowych i przywracania ustawień:      + Automatyzacja tworzenia kopii zapasowych ustawień urządzeń.      + Procedury przywracania ustawień z kopii zapasowych. 3. Konfiguracja tuneli VPN IPsec / SSL:    * Konfiguracja tuneli VPN typu IPsec i SSL:      + Tworzenie i zarządzanie tunelami VPN dla bezpiecznej komunikacji.      + Konfiguracja polityk bezpieczeństwa VPN i zarządzanie certyfikatami.   Wdrożenie musi być prowadzone przez jednego certyfikowanego inżyniera lub podmiot, (nie dopuszcza się łączenia certyfikatów przez dwóch lub więcej inżynierów ze względu na poziom bezpieczeństwa oferowanej usługi), posiadającego co najmniej 4 aktywne certyfikaty producenta oferowanego rozwiązania, w zakresie: Bezpieczeństwa Sieci (NS), Bezpieczeństwa Chmury Publicznej (PCS), Operacji Bezpieczeństwa (SO), Dostępu Zero Trust (ZTA). Dokumenty potwierdzające należy dostarczyć wraz z ofertą. |
| Serwisy i 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 na okres do **30 czerwca 2026 roku** |
| Gwarancja oraz wsparcie | System powinien być objęty serwisem gwarancyjnym producenta przez okres nie krótszy niż do **30 czerwca 2026 r.,** polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewni dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. |
| Rozszerzone wsparcie serwisowe AHB/SOS | System powinien być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w następnym dniu roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora do dnia **30 czerwca 2026 roku.** |
| Certyfikaty/Deklaracje | - ISO 9001 lub równoważny zapewniający zarządzanie jakością, podejście procesowe, ciągłe doskonalenie, zarządzanie ryzykiem oraz zgodność z przepisami.  - Deklaracja CE producenta sprzętu lub równoważny potwierdzający dopuszczenie sprzętu do obrotu w Europejskim Obszarze Gospodarczym. |
| Opisy do wymagań ogólnych | 1. Wykonawca winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta, iż produkt pochodzi z autoryzowanego kanału sprzedaży.  2. Wykonawca wraz z ofertą winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta, potwierdzające, że posiada autoryzację producenta do sprzedaży oferowanego produktu.  3. Wykonawca w ramach wdrożenia ma obowiązek przenieść wszystkie obecnie działające polityki bezpieczeństwa z istniejącego urządzenia UTM na nowo dostarczone urządzenie (Proces ten musi być wykonany w taki sposób, aby zapewnić ciągłość ochrony i minimalizować ryzyko wystąpienia luk w zabezpieczeniach podczas przejścia na nowe urządzenie). |

|  |  |
| --- | --- |
| **Serwerowy system operacyjny – 1 sztuka parametry techniczne minimum:** | |
| System operacyjny | System operacyjny – fabrycznie nowy, nieużywany, nie pochodzący z recyklingu, z licencją na czas nieoznaczony, nie naruszający praw osób trzecich. Zamawiający nie dopuszcza zaoferowania systemu operacyjnego, programów i planów licencyjnych opartych o rozwiązania chmurowe oraz rozwiązań wymagających wnoszenia przez Zamawiającego jakichkolwiek dodatkowych opłat związanych z użytkowaniem zakupionego systemu operacyjnego.  MS Windows Server 2025 Standard 16-Core wersja polskojęzyczna z nieujawnianym wcześniej, nieaktywowanym wcześniej kluczem licencyjnym, pochodzący z oficjalnej sieci dystrybucji firmy Microsoft® lub równoważny.  Warunki równoważności:  1. System operacyjny musi być przeznaczony do zastosowań serwerowych w środowiskach fizycznych lub o minimalnej wirtualizacji. 2. System operacyjny musi być najnowszą wersją rodziny systemów operacyjnych danego producenta.  3. Licencja na system operacyjny musi uwzględniać prawo do bezpłatnej instalacji udostępnianych przez producenta poprawek krytycznych i opcjonalnych do zakupionej wersji oprogramowania co najmniej przez 5 lat.  4. Licencja na system operacyjny musi umożliwiać uruchomienie kontrolera domeny będącego w pełni zgodnym z domeną wdrożoną u Zamawiającego domeną Active Directory pracującą w oparciu o system Windows Server 2012 musi także być dostarczona możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie Microsoft Windows Server  5. Licencja na system operacyjny musi być licencją stałą, bez ograniczeń czasowych.  6. Licencja na system operacyjny musi uprawniać do uruchamiania systemu operacyjnego w środowisku fizycznym i min. 2 środowiskach wirtualnych za pomocą wbudowanych mechanizmów wirtualizacji, bez konieczności zakupu dodatkowych licencji.  7. Zaimplementowanie w systemie operacyjnym środowiska wirtualizacyjnego musi umożliwiać dodawanie i usuwanie pamięci wirtualnej oraz wirtualnych kart sieciowych podczas pracy maszyny wirtualnej.  8. System operacyjny musi posiadać graficzny interfejs użytkownika.  9. System operacyjny musi być w pełni kompatybilny z usługą Active Directory w zakresie: a) zarządzania użytkownikami, b) zarządzania certyfikatami dla użytkowników wraz ze wsparciem możliwości logowania do domeny kartą mikroprocesorową, c) możliwości przydzielania praw dostępu do zasobów sieciowych, d) instalacji zdalnej oprogramowania z pakietów msi, e) definiowania polityk bezpieczeństwa dla użytkowników, grup oraz stacji roboczych z systemami MS Windows: 7,8,8.1, 10. 11.  10. System operacyjny musi wspierać pracę domenową wraz z automatyczną synchronizacją dla dodatkowych serwerów.  11. System operacyjny musi wspierać zarządzanie przez dostępne narzędzia administracji serwera dla systemu Windows 10 (RSAT) oraz Windows Admin Centre.  12. System operacyjny musi posiadać obsługę zdalnego pulpitu poprzez protokół RDP  13. System operacyjny musi umożliwiać ustawianie relacji zaufania pomiędzy domenami.  14. Wszystkie narzędzia i usługi systemu operacyjnego powinny być rozwiązaniem jednego producenta.  15. System operacyjny musi posiadać obsługę pamięci USB jako monitora klastra.  16. System operacyjny musi pozwalać na stopniowe uaktualnienia systemu operacyjnego klastra.  17. System operacyjny musi posiadać obsługę deduplikacji na potrzeby systemu plików ReFS.  18. System operacyjny musi posiadać obsługę optymalizacji transportu w tle pod kątem opóźnień.  19. System operacyjny musi posiadać wbudowaną zaporę internetową (firewall) dla ochrony połączeń internetowych; zapora musi być zintegrowana z systemem konsoli do zarządzania ustawieniami zapory i regułami ip v4 i v6;  20. System operacyjny musi posiadać możliwość uruchomienia serwera DNS z możliwością integracji z kontrolerem domeny;  21. System operacyjny musi posiadać możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu;  22. System operacyjny musi posiadać domyślną obsługę PowerShell 5.1 ;  23. System operacyjny musi posiadać obsługę certyfikatów w Active Directory.  24. Wszystkie wymienione powyżej parametry, role, funkcje, itp. systemu operacyjnego objęte musza być dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).  Wymagania dla równoważnych licencji dostępowych dla urządzenia: - Licencja dostępowa dla urządzenia umożliwiająca podłączenie i wykorzystywanie wszystkich dostępnych funkcjonalności serwera Microsoft Windows Server 2025 typu Device Cal z wdrożoną rolą Active Directory. - Każda z licencji musi pozwalać na dostęp wielu użytkowników z jednego, licencjonowanego urządzenia do zasobów serwera. W przypadku zaproponowania przez Dostawcę oprogramowania równoważnego zobowiązuje się on do: − wdrożenia oprogramowania oraz przeprowadzenia certyfikowanych szkoleń dla użytkowników oferowanego rozwiązania w wymiarze co najmniej 40 godzin. − pokrycia wszelkich możliwych kosztów, wymaganych w czasie wdrożenia oferowanego rozwiązania, w szczególności związanych z dostosowaniem infrastruktury informatycznej, oprogramowania nią zarządzającego, systemowego i narzędziowego (licencje, wdrożenie), serwisu gwarancyjnego oraz kosztów certyfikowanych szkoleń dla administratorów i użytkowników oferowanego rozwiązania |

|  |  |
| --- | --- |
| **Licencje dostępowe systemu operacyjnego – 16 licencji parametry techniczne minimum:** | |
| Nazwa licencji | Licencje dostępowe do serwerowego systemu operacyjnego opisanego powyżej. |

|  |  |
| --- | --- |
| **Oprogramowanie DLP – 1 sztuka parametry techniczne minimum:** | |
| Rozwiązanie musi obejmować 18 licencji bezterminowych dla Urzędu Gminy oraz osobno 8 licencji bezterminowych dla Gminnego Ośrodka Pomocy Społecznej. Wsparcie do 30 czerwca 2026 r. | |
| Wymagania ogólne | 1. Pomoc i dokumentacja programu dostępne w języku angielskim.  2. Konsola administracyjna i komunikaty klienta muszą być w języku polskim.  3. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta.  4. Serwer administracyjny musi umożliwiać instalację/dezinstalację zdalnego klienta na stacjach roboczych.  5. Reguły DLP muszą być egzekwowane nawet przy braku połączenia między klientem a serwerem zarządzającym.  6. Brak połączenia klienta z serwerem zarządzającym musi umożliwiać lokalne przechowywanie informacji i zebranych danych do czasu ponownego połączenia.  7. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsoli.  8. System musi mieć możliwość konfiguracji automatycznej konserwacji dla bazy danych, usuwając najstarsze informacje, gdy rozmiar bazy osiągnie skonfigurowany limit.  9. Serwer administracyjny musi automatycznie pobierać aktualizacje definicji kategoryzowania stron internetowych, aplikacji i rozszerzeń plików, z opcją wyłączenia automatycznego pobierania.  10. Administrator musi mieć możliwość aby tworzyć, usuwać i konta administratorów w konsoli programu.  11. Administrator musi mieć możliwość przypisywania i odbierania uprawnień do wybranych modułów programu, podzielonych na ustawienia (konfiguracja modułu) i logi (wyświetlanie logów modułu).  12. Serwer musi synchronizować użytkowników i stacje robocze z domeną Active Directory.  13. Administrator musi móc wymusić synchronizację ustawień i logów między stacją roboczą a serwerem w czasie rzeczywistym.  14. 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.  15. 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.  16. Administrator musi mieć możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji i typów plików.  17. Administrator musi mieć możliwość filtrowania i sortowania zebranych danych.  18. Serwer musi posiadać możliwość wysyłania alertów, przynajmniej za pośrednictwem wiadomości email.  19. Dashboardy muszą być generowane na podstawie wskazanych stacji roboczych, użytkowników lub grup w określonym przedziale czasu.  20. Serwer administracyjny musi posiadać wbudowany serwer SMTP dostarczony przez producenta oprogramowania.  21. 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.  22. Serwer administracyjny musi mieć możliwość kategoryzacji plików wrażliwych na podstawie aplikacji, lokalizacji, adresu URL, formatu pliku i zawartości pliku.  23. 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.  24. 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.  25. Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym.  26. Serwer administracyjny musi pozwalać na eksport logów do rozwiązania SIEM.  27. Konsola musi umożliwiać konfigurację/zmianę domyślnego serwera SMTP.  28. Konsola webowa musi pozwalać na weryfikację wersji zainstalowanego oprogramowania klienta, a także umożliwia aktualizację do nowej wersji lub dezaktywację tego oprogramowania.  29. System musi ochraniać pocztę e-mail Microsoft 365, sprawdzając każdą wiadomość e-mail wysyłaną przez użytkowników Microsoft 365.  30. System musi ochraniać pliki w Microsoft 365, kontrolując aktywność plików w Microsoft SharePoint, Microsoft OneDrive dla Firm i Microsoft Teams.  31. System musi wykorzystywać mechanizm OCR (optical character recognition), aby wykrywać poufne treści w obrazach, zdjęciach i zeskanowanych dokumentach  32. System musi posiadać możliwość integracji z systemami do analizy danych (PowerBI, Tableau, etc.)  33. System musi zapewniać możliwość zarządzanie szyfrowaniem dysków twardych oraz urządzeń wymiennych. |
| System operacyjny | * Windows 10 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi * Windows 11 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi * MacOS 12 lub nowszy. |
| Serwer administracyjny musi obsługiwać instalację na systemach | Windows Server 2016 (64-bit) i nowszych |
| Serwer administracyjny musi obsługiwać bazy danych | * MS SQL Server 2016 lub nowsze, * MS SQL Express, * AzureSQL S3 lub nowsze. |

|  |  |
| --- | --- |
| **Oprogramowanie do kopii zapasowych – 1 sztuka parametry techniczne minimum:** | |
| Dostawa 22 licencji dla Urzędu Gminy (w tym 16 dla stacji roboczych, 1 dla serwera fizycznego,  5 dla hosta wirtualnego) oraz osobno 13 licencji dla Gminnego Ośrodka Pomocy Społecznej (w tym 10 dla stacji roboczych, 1 dla serwera fizycznego, 1 dla hosta wirtualnego) | |
| Opis technologii | * Możliwość backupu X komputerów, Y serwerów, Z hostów wirtualizacji (np.: 100 stacji, 10 serwerów, 2 hosty), edycja (Std, Pro, lub Ent) * Oprogramowanie działające w architekturze klient-serwer w oparciu o protokół TCP/IP, z centralnym modułem sterowania wykonywaniem kopii zapasowych z dysków komputerów klienckich * Program serwerowy kompatybilny z systemami: Microsoft Windows XP, Vista, Windows 7, Windows 8, Windows 10; Windows 11; Microsoft Windows Server 2003, 2008, 2012, 2016, 2019, 2022, 2025 Linux, BSD, Mac OS X, QNAP, Synology * Program kliencki kompatybilny z systemami: Microsoft Windows 2000, XP, Vista, Windows 7, Windows 8, Windows 10; Windows 11; Microsoft Windows Server 2000, 2003, 2008, 2012, 2016, 2019, 2022, 2025 Linux, BSD, Mac OS X, QNAP, Synology * 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) * Backup i odzyskiwanie maszyn wirtualnych Microsoft Hyper-V oraz VMWare ESX/ESXi * 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, * 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 * Bezterminowa licencja - licencja nie może być ograniczona czasowo * Interfejs, instrukcja i pomoc techniczna w języku polskim * Edycja Pro: Replikcacja na napęd optyczny: CD, DVD, Blu-Ray, HD-DVD i napęd taśmowy: DDS, DLT, LTO, AIT (tylko Windows) * Edycja Pro: Możliwość instalacji klienta przez GPO * Edycja Pro: Współpraca z systemami Systemami Zarządzania Informacją i Zdarzeniami Bezpieczeństwa (SIEM - Security Information and Event Management) * Edycja Pro: Możliwość zastosowania własnych certyfikatów SSL |
| Dokumenty | Oświadczenie producenta lub autoryzowanego dystrybutora producenta, iż produkt pochodzi z autoryzowanego kanału sprzedaży. |
| Licencja bezterminowa | Tak |

|  |  |
| --- | --- |
| **Oprogramowanie do zarządzania infrastrukturą IT – 1 sztuka parametry techniczne minimum:** | |
| Wymagania ogólne dla systemu zarządzania | * Oprogramowanie musi posiadać polski oraz angielski interfejs językowy. * Oprogramowanie musi posiadać architekturę trójwarstwową składającą się z Bazy Danych, Serwera Aplikacji, Agenta/Konsoli zarządzającej. * Oprogramowanie musi umożliwiać obsługę dedykowanych kluczy szyfrujących podczas komunikacji pomiędzy agentami, serwer aplikacji i konsolą zarządzającą. * Odczyt informacji dotyczących parametrów sprzętowych komputera musi odbywać się za pośrednictwem agenta systemu instalowanego na komputerach użytkowników. * Agent systemu nie może nasłuchiwać na żadnym porcie sieciowym po stronie stanowiska komputerowego użytkownika. * Oprogramowanie musi umożliwiać wybór instalacji agenta w trybie standardowym oraz bezpiecznym tj. braku wkompilowanych funkcji takich jak zdalne zarządzanie, transfer plików, zdalny pulpit. * Oprogramowanie musi posiadać procedurę uwierzytelnienia i autoryzacji kont operatorów w konsoli zarządzającej poprzez fizyczne zabezpieczenie sprzętowe (lokalne lub sieciowe) wraz z hasłem, który umożliwia jednoczesną prace wielu administratorom. Logowanie użytkowników konsoli zarządzającej musi umożliwiać integrację z kontami Active Directory. Wymagane zabezpieczenie sprzętowe musi posiadać mechanizm szyfrowania danych AES w obrębie przechowywania danych wrażliwych. * Oprogramowanie musi posiadać dodatkową autoryzację użytkownika konsoli zarządzającej za pomocą usługi Google Authenticator oraz Microsoft Authenticator. * Oprogramowanie musi posiadać moduł zarządzania uprawnieniami do poszczególnych funkcjonalności systemu dla operatorów konsoli zarządzającej zgodny z modelem RBAC (Role Based Access Control). * Oprogramowanie musi umożliwiać nadawanie oraz odbieranie uprawnień w czasie rzeczywistym (brak konieczności przelogowania użytkownika konsoli systemu). * Oprogramowanie musi umożliwiać blokadę wybranych uprawnień konkretnego użytkownika niezależnie od uprawnień wynikających z przypisanych ról. * Oprogramowanie musi współpracować z serwerem MSSQL Server 2008R2-2019 * Oprogramowanie, w zakresie wszystkich warstw, nie może wymagać do prawidłowej pracy komponentów Java. * Oprogramowanie serwera aplikacji musi posiadać funkcjonalność centralnego wysyłania wybranych powiadomień mailowych . * Oprogramowanie musi posiadać moduł zarządzania uprawnieniami do danych w zakresie wybranych jednostek organizacyjnych oraz typów zasobów poszczególnych użytkowników konsoli. Wszelkie raporty, zestawienia oraz funkcje obejmują wtedy tylko wynikowe obiekty. * Oprogramowanie musi być podpisane cyfrowo przez Producenta ważnym certyfikatem, z prawidłową ścieżką certyfikacji, w której główny urząd certyfikacji (Root CA) jest uczestnikiem programu certyfikatów głównych systemu Windows. Podpis cyfrowy dotyczy składników Producenta systemu w zakresie plików wykonywalnych (\*.exe), plików bibliotek współdzielonych (\*.dll), plików sterowników (\*.sys) oraz pakietów instalacyjnych oprogramowania (\*.msi). * Oprogramowanie agentów musi posiadać obsługę sesji terminalowych Windows. * Oprogramowanie musi zapewniać dowolną konfigurację pracy wszystkich agentów, jednostek organizacyjnych, pojedynczego agenta, poprzez dziedziczenie definiowanych przez administratora parametrów. Zmiany konfiguracji agentów następują w trybie natychmiastowym (online). * Oprogramowanie musi posiadać raport przedstawiający różnice w konfiguracji poszczególnych agentów w stosunku do konfiguracji globalnej. * Oprogramowanie musi posiadać mechanizm logowania zmian w konfiguracji agentów przez użytkowników konsoli (data, czas, login, poprzednia i nowa wartość). * Oprogramowanie musi posiadać mechanizm analizy czasu pracy komputera, informujący użytkownika (alert oraz wymuszone działanie – restart) o przekroczeniu zadanego czasu pracy bez restartu systemu operacyjnego. * Oprogramowanie musi zapewniać automatyczny import drzewiastej struktury organizacyjnej zamawiającego (bez ograniczeń ilości zagnieżdżeń z kontenera Active Directory/OpenLDAP), kont użytkowników i komputerów z zachowaniem ich oryginalnego położenia wg. OU. * Oprogramowanie musi zapewniać w obrębie synchronizacji z Active Directory/OpenLDAP tworzenie listy filtrów zawężających węzły danych wraz z możliwością wskazania docelowej gałęzi struktury organizacyjnej lub lokalizacyjnej Zamawiającego. * Oprogramowanie musi posiadać kreator powiązań (mapowanie atrybutów) dowolnych atrybutów obiektów z usługi katalogowej do wskazanych atrybutów zasobów systemowych. * Oprogramowanie musi umożliwiać współpracę z nieograniczoną ilością kontrolerów domen z zachowaniem podległej struktury drzewiastej. * Oprogramowanie musi umożliwiać automatyczny import informacji dotyczących przynależności użytkowników oraz stanowisk komputerowych do grup struktury katalogowej. * Oprogramowanie musi posiadać raport przedstawiający informacje nt. grup struktury katalogowej wraz przynależącymi do nich użytkownikami. * Oprogramowanie musi umożliwiać tworzenie dynamicznych grup stanowisk w oparciu o kreator zawierający filtry (AND, OR) w zakresie min. wersja OS, nazwa oraz wersja wybranej aplikacji, RAM, CPU, HDD, jednostka organizacyjna, jednostka lokalizacyjna, architektura (x32, x64), zainstalowane oprogramowanie, wersja oprogramowania, lista usług systemowych, producent oraz model komputera, poziom uprawnień użytkownika, zainstalowana usługa systemowa, ostatnie uruchomienie systemu, obecność pliku EXE na dysku, predefiniowane atrybuty komputera (np. dostawca, numer faktury, data zakupu). * Oprogramowanie musi umożliwiać prezentację widoku zarządzanych stanowisk komputerowych w postaci listy stanowisk, drzewiastej struktury wg jednostek organizacyjnych, jednostek lokalizacyjnych, struktury Active Directory, struktury sieciowej (pule IP) oraz grup dynamicznych. * Oprogramowanie musi umożliwiać dynamiczne zawężanie wyników wyszukiwania ww. widoków na podstawie prezentowanych w nich atrybutów. * Oprogramowanie musi umożliwiać graficzną prezentację aktualnego stanu aktywności agenta (online/offline) z dokładnością do 1 minuty. * Oprogramowanie musi umożliwiać zapisywanie w bazie danych informacji o uruchomieniu i wyłączeniu komputera oraz zalogowaniu i wylogowaniu użytkownika. |
| Inwentaryzacja konfiguracji komputerów | * Oprogramowanie musi umożliwiać wydruk kartoteki sprzętowej stanowiska komputerowego. * Oprogramowanie musi umożliwiać samodzielną edycję wyglądu kartoteki sprzętowej, protokołów przekazania oraz zwrotu zasobów za pomocą graficznego kreatora wyglądu. * Oprogramowanie musi umożliwiać zapisywanie edytowanych szablonów (min. kartoteka sprzętowa, protokoły przekazania/zwrotu zasobów) w kontekście zalogowanego operatora konsoli zarządzającej. * Oprogramowanie musi umożliwiać projektowanie, generowanie oraz wydruk etykiet inwentaryzacyjnych w zakresie: model, nr inwentaryzacyjny, data zakupu, jednostka, wraz z obsługą kodów kreskowych w standardzie EAN128 oraz PDF417 * Oprogramowanie musi umożliwiać okresową automatyczną inwentaryzację parametrów sprzętowych stanowiska: HDD, RAM, CPU, karta sieciowa, system operacyjny, karta graficzna itp. * Oprogramowanie Agenta musi umożliwiać audyt off-line, poprzez uruchomienie skanera (z GUI) bez konieczności instalacji, oraz zapis wyników do pliku w postaci zaszyfrowanej. * Oprogramowanie musi umożliwiać analizę sprzętową:   - płyty głównej w zakresie model, producent, nr. seryjny,  - CPU w zakresie nazwy, modelu, producenta, częstotliwości,  - HDD w zakresie numeru seryjnego dysku, numeru seryjnego partycji, rozmiaru pamięci,  - RAM w zakresie wielkości pamięci,  - karty sieciowej w zakresie model, adres IP, adres MAC,  - karty graficznej w zakresie model.   * Oprogramowanie musi umożliwiać odczyt informacji dotyczących systemu operacyjnego w zakresie nazwy, wersji, daty instalacji, zainstalowanych poprawek, dostępnych kluczy licencyjnych, produkt ID. * Oprogramowanie musi umożliwiać odczyt informacji sieciowych w zakresie adresu IO, adresu MAC, nazwy sieciowej. * Oprogramowanie musi umożliwiać odczyt informacji sprzętowych z BIOS w zakresie nazwy BIOS, daty, producenta. * Oprogramowanie musi umożliwiać przegląd historii zmian parametrów sprzętowych komputerowych. * Oprogramowanie musi umożliwiać globalny przegląd stanowisk komputerowych pod względem parametrów sprzętowo-systemowych. * Oprogramowanie musi zawierać raport stanowisk komputerowych posiadających co najmniej jedno konto z uprawnieniami administratora. * Oprogramowanie musi umożliwiać odczyt urządzeń podłączonych do stanowiska komputerowego przez interfejs USB, z możliwością odczytania nazwy urządzenia, producenta, modelu oraz numeru seryjnego (o ile urządzenie dostarcza ww. informacji) * Oprogramowanie musi umożliwiać globalną analizę urządzeń podłączonych do stanowisk komputerowych przez interfejs USB * Oprogramowanie musi umożliwiać integrację z zewnętrzną usługą Dell API w celu automatycznego odczytania informacji na temat okresu gwarancji stanowiska komputerowego na podstawie odczytanego przez agenta identyfikatora (ServiceTag) * Oprogramowanie musi umożliwiać okresowe próbkowanie obciążenia procesora oraz zajętości pamięci RAM z możliwością zapisu odczytanych wyników do bazy w celu późniejszej analizy (historia obciążenia komputera). |
| Inwentaryzacja oprogramowania | * Oprogramowanie musi umożliwiać automatyczną inwentaryzację zainstalowanego na komputerach oprogramowania. * Oprogramowanie musi umożliwiać globalny przegląd wszystkich programów zainstalowanych na komputerach. * Oprogramowanie musi umożliwiać tworzenie zestawień zainstalowanych typów programów (freeware, shareware itp.). * Oprogramowanie musi umożliwiać tworzenie wykazów z zainstalowanym, dowolnie wybranym programem. * Oprogramowanie musi umożliwiać tworzenie zestawień zainstalowanych systemów operacyjnych na komputerach. * Oprogramowanie musi umożliwiać tworzenie wykazów stanowisk z brakiem zainstalowanego, dowolnie wybranego, programu. * Oprogramowanie musi posiadać wbudowany mechanizm umożliwiający, poprzez GUI konsoli, zdalną grupową dezinstalację oprogramowania np. pakietów MS Office. * Oprogramowanie musi umożliwiać oznaczanie kolorem aplikacji zabronionych oraz zgodnych ze standardem wraz z możliwością raportowania wg w/w klasyfikacji. * Oprogramowanie musi umożliwiać zablokowanie na stacji roboczej wybranych procesów celem uniemożliwienia ich uruchomienia przez użytkownika. * Oprogramowanie musi posiadać globalne zestawienie pozwalające na zdalne usunięcie nielegalnych danych np. plików AVI, MP3, MP4 bez konieczności fizycznej obecności użytkownika przy stacji. |
| Zarządzanie licencjami, audyt oprogramowania | * Oprogramowanie musi posiadać wbudowaną bazę sygnatur aplikacji (produktów) wraz z możliwością automatycznej aktualizacji wzorców ze strony Producenta oprogramowania * Oprogramowanie musi umożliwiać zdefiniowanie własnych sygnatur aplikacji (produktów) wykorzystywanych * w procesie automatycznego audytu licencji (rozliczenie ilościowe). * Oprogramowanie musi umożliwiać wykonanie audytu licencji tj. systemowego porównania zidentyfikowanego na stanowiskach komputerowych oprogramowania (produktów) z zakupionymi licencjami wprowadzonymi do systemu jako odpowiednie obiekty. Mechanizm audytu musi umożliwiać rozliczenie licencji z wykorzystaniem mechanizmów downgrade, upgrade. * Oprogramowanie musi umożliwiać zapis historii wykonywanych audytów licencji. * Oprogramowanie musi umożliwiać tworzenie bazy licencji systemowo/programowych i przypisywanie ich do stanowisk komputerowych oraz użytkowników. |
| CMDB | * Oprogramowanie musi umożliwiać tworzenie własnych typów elementów konfiguracji (CI) * Oprogramowanie musi umożliwiać dodawanie dowolnych atrybutów dla typów CI w szczególności: wartości logiczne, data/czas, numeryczne, tekstowe, słownikowe * Oprogramowanie musi umożliwiać tworzenie podrzędnych i nadrzędnych typów CI * Oprogramowanie musi umożliwiać dziedziczenie atrybutów przez elementy konfiguracji posiadające typ nadrzędny * Oprogramowanie musi umożliwiać tworzenie dowolnych typów relacji do obsługi połączeń pomiędzy różnymi typami CI * Oprogramowanie musi umożliwiać tworzenie atrybutów dla relacji * Oprogramowanie musi umożliwiać prezentowanie powiązań pomiędzy elementami konfiguracji w formie struktury płaskiej oraz graficznej * Oprogramowanie musi umożliwiać zbiorczy podgląd relacji pomiędzy poszczególnymi elementami konfiguracji * Oprogramowanie musi umożliwiać modelowanie struktury relacji pomiędzy usługami, sprzętem, organizacją oraz pracownikami * Oprogramowanie musi umożliwiać nadzór nad wpływem zmian na poszczególne elementy konfiguracji * Oprogramowanie musi umożliwiać import elementów konfiguracji ze źródeł takich jak usługa katalogowa, skaner sieci, zewnętrzne pliki płaskie (CSV) * Oprogramowanie musi umożliwiać tworzenie oraz edycję własnych list elementów konfiguracji * Oprogramowanie musi umożliwiać wyszukiwanie i analizę elementów konfiguracji wg posiadanych atrybutów * Oprogramowanie musi umożliwiać tworzenie własnych typów relacji z określaniem nazwy relacji podstawowe i odwrotnej * Oprogramowanie musi umożliwiać tworzenie własnych formularzy dla wszystkich elementów konfiguracji |
| Zarządzanie zasobami oraz użytkownikami | * Oprogramowanie musi umożliwiać tworzenie własnych szablonów widoków zasobów z określeniem analizowanych typów zasobów, widocznych atrybutów oraz informacji nt. powiązań pomiędzy zasobami. * Oprogramowanie musi umożliwiać tworzenie własnych atrybutów o typach co najmniej: tekst, liczba, bit, data, wartość słownikowa dla wybranego typu zasobu. * Oprogramowanie musi umożliwiać zapis oraz przegląd historii zmian dowolnego atrybutu zasobu w zakresie: operator, data, czas, poprzednia oraz nowa wartość. * Oprogramowanie musi umożliwiać zdefiniowanie dowolnych relacji pomiędzy zasobami (np. powiązania stanowiska z pracownikiem, licencją, innym zasobem) wraz z zapisem historii relacji zasobów. * Oprogramowanie musi umożliwiać przypisywanie do każdego z zarządzanych w systemie zasobów dokumentów typu: faktura zakupu, gwarancja, umowa serwisowa. Bazą dokumentów musi być centralne repozytorium umożliwiające powiazania dokumentów z zasobami w relacji 1:N wraz z podglądem przypisanych zasobów oraz wydrukiem. * Oprogramowanie musi umożliwiać zdefiniowanie dowolnego zasobu inwentaryzacyjnego (np. telefon, drukarka, nawigacja) w strukturze drzewiastej wraz z kreatorem widocznych/wymaganych atrybutów edycyjnych. * Oprogramowanie musi posiadać dedykowaną (zintegrowaną z systemem) aplikację na platformę Android umożliwiającą spis z natury zinwentaryzowanych zasobów. * Oprogramowanie musi umożliwiać import danych z zewnętrznego pliku CSV zawierającego informacje inwentaryzacyjne z nowo zakupionych urządzeń w zakresie: numer faktury, numer seryjny, model, nazwa, data zakupu. * Oprogramowanie musi umożliwiać zaprojektowanie własnego schematu importu danych z zewnętrznego pliku CSV. * Oprogramowanie musi umożliwiać automatyczne tworzenie relacji pracownik-komputer na podstawie atrybutów obiektu w usłudze katalogowej. * Oprogramowanie musi zawierać wbudowany kreator wydruków w zakresie protokołów przekazania, zwrotu, likwidacji wraz z możliwością utworzenia dowolnego typu dokumentu * Oprogramowanie musi umożliwiać export ww. protokołów w formacie PDF * Oprogramowanie musi umożliwiać obsługę kodów kreskowych oraz QR w obrębie ww. kreatora wydruków * Oprogramowanie musi umożliwiać użycie w kreatorze wydruków własnego logotypu organizacji * Oprogramowanie musi umożliwiać użycie w kreatorze wydruków dowolnego atrybutu zasobu * Oprogramowanie musi umożliwiać przypisanie dowolnej firmy serwisowej z bazy organizacji do zasobu * Oprogramowanie musi umożliwiać przypisanie załącznika do zasobu * Oprogramowanie musi umożliwiać pogląd wszystkich zgłoszeń serwisowych dotyczących danego zasobu * Oprogramowanie musi umożliwiać podgląd zasobów (przypisanych do danego pracownika) z poziomu jego portalu użytkownika końcowego * Oprogramowanie musi umożliwiać zarządzanie cyklem życia zasobu * Oprogramowanie musi umożliwiać tworzenie niestandardowych reguł biznesowych dla zarządzania zasobami * Oprogramowanie musi umożliwiać seryjne dodawanie zasobów * Oprogramowanie musi umożliwiać automatyczne nadawanie numerów inwentaryzacyjnych dla zasobów * Oprogramowanie musi udostępniać kreator raportów dla zasobów * Oprogramowanie musi udostępniać możliwość kopiowania widoku dla określonego typu(ów) zasobu z innego typ zasobu * Oprogramowanie musi udostępniać możliwość kopiowania formularz dla określonego typu(ów) zasobu z innego typ zasobu * Oprogramowanie musi umożliwiać ewidencję magazynów * Oprogramowanie musi umożliwiać ewidencję lokalizacji magazynowych * Oprogramowanie musi umożliwiać ewidencję produktów magazynowych * Oprogramowanie musi udostępniać informację o stanie magazynowym(ilościowo) * Oprogramowanie musi umożliwiać generowanie dokumentów PZ/PW/RW/MM * Oprogramowanie musi umożliwiać przyjęcie zasobów ewidencjonowanych i eksploatacyjnych na magazyn * Oprogramowanie musi umożliwiać wydawanie zasobów ewidencjonowanych i eksploatacyjnych z magazynu * Oprogramowanie musi umożliwiać zwrot zasobów na magazyn * Oprogramowanie musi umożliwiać zmianę szablonów dokumentów PZ/PW/RW/MM * Oprogramowanie musi umożliwiać wyszukiwanie dokumentów po dowolnym atrybucie * Oprogramowanie musi umożliwiać zarządzanie organizacjami/typami organizacji (np. klient, podwykonawca) * Oprogramowanie musi umożliwiać dowolne przypisanie osoby do organizacji * Oprogramowanie musi umożliwiać tworzenia dynamicznych grup użytkowników * Oprogramowanie musi umożliwiać zarządzanie kontaktami osób/organizacji * Oprogramowanie musi umożliwiać zarządzanie nieobecnościami użytkowników * Oprogramowanie musi umożliwiać zarzadzanie uprawnieniami i poziomami dostępu do danych w zakresie zarządzania zasobami * Oprogramowanie musi umożliwiać automatyczne pobieranie danych rejestrowych kontrahentów z bazy GUS |
| Zdalny pulpit, zdalne zarządzanie komputerem | * Oprogramowanie musi umożliwiać interakcję administratora z użytkownikiem, polegającą na podłączeniu do stanowiska (przejęcie pulpitu) administratora bez konieczności uprzedniego wylogowania użytkownika. Funkcjonalność zdalnego pulpit nie może wymagać instalacji aplikacji firm trzecich, wymagane jest obsłużenie przejęcia zdalnego pulpitu przez mechanizm wbudowany w agencie (ten sam proces systemowy). * Oprogramowanie musi umożliwiać wybór monitora, którego ekran ma zostać przejęty podczas połączenia zdalnego. Podczas aktywnego połączenia zdalnego, użytkownik jest informowany o trwaniu sesji zdalnej poprzez wyświetlanie na aktywnym monitorze kontrastowego obramowania ekranu. * Oprogramowanie musi umożliwiać zdalne zarządzanie (bez użycia RDP/VNC itp.) lokalnymi kontami użytkowników w zakresie (tworzenie, usuwanie, edycja, zmiana hasła oraz typ konta). * Oprogramowanie musi umożliwiać wysyłanie polecenia Wake-on LAN. * Oprogramowanie musi umożliwiać zdalną dwukierunkową linię poleceń. * Oprogramowanie musi umożliwiać przesyłanie plików/katalogów od zdalnego użytkownika do administratora i/lub od administratora do zdalnego użytkownika bez względu na lokalizację sieciową komputera (LAN, WAN, Internet). * Oprogramowanie musi umożliwiać konfigurację przez administratora parametrów połączenia z użytkownikiem w zakresie: ilość kolorów, ilość klatek/sekundę, skalowanie okna użytkownika, jeżeli jest ono większe niż rozdzielczość stacji administratora. * Oprogramowanie musi umożliwiać wybór aktywnych sesji terminalowych, do których chcemy się podłączyć. * Oprogramowanie musi umożliwiać zbiorczy podgląd zdalnych pulpitów stacji. * Oprogramowanie musi posiadać zarządzanie technologią iAMT, vPro w zakresie uwzględniającym min.: Serial Over Lan (SOL), IDE Redirection (IDER), Hardware KVM, Assets. * Oprogramowanie musi zapewniać zdalną konfigurację technologii iAMT w trybie Client Control Configuration Mode. * Oprogramowanie musi umożliwiać zarządzanie stacjami komputerowymi poza siecią LAN/WAN, wymagane jest tylko dowolne połączenie internetowe * Oprogramowanie musi umożliwiać zdalne wykonywanie zapytań WQL * Oprogramowanie musi umożliwiać zdalny odczyt oraz modyfikację rejestru Windows * Oprogramowanie musi umożliwiać pełne wykorzystanie funkcji zawartych w sekcji zdalne zarządzanie dla stacji posiadających dowolne połączenie do sieci INTERNET bez konieczności zestawiania połączenia VPN * Oprogramowanie musi umożliwiać przejęcie pulpitu zdalnego z poziomu konsoli zarządzającej znajdującej się poza siecią LAN organizacji poprzez połącznie konsoli ze wskazanym serwerem aplikacji. * Oprogramowanie musi umożliwiać prowadzenie w czasie rzeczywistym dwukierunkowej komunikacji tekstowej (chat) pomiędzy użytkownikiem a administratorem. |
| Automatyzacja | * Oprogramowanie musi umożliwiać zdalną instalację pakietów \*.msi, plików \*.cmd, \*.bat, \*.reg, \*.ps1 poprzez utworzenie zadań dystrybucji aplikacji oraz wskazanie docelowych komputerów lub grup komputerów za pomocą dedykowanego GUI użytkownika. Zadanie dystrybucji musi umożliwiać określenie okresu aktywności, godziny rozpoczęcia oraz przedstawiać status instalacji na wybranych stanowiskach. * Oprogramowanie musi umożliwiać tworzenie zadań dystrybucji polegające na jednorazowym uruchomieniu wybranego szablonu akcji na wybranych stanowiskach komputerowych. * Oprogramowanie musi umożliwiać tworzenie polis uruchamianych cyklicznie na wybranych stanowiskach komputerowych wg aktualnej przynależności do struktury organizacyjnej, lokalizacyjnej lub wybranych grup dynamicznych. * Oprogramowanie musi umożliwiać tworzenie dystrybucji zadań oraz polis dla wybranych stanowisk komputerowych poprzez interaktywny kreator (krok po kroku). Wybór odbiorców musi uwzględniać listę stanowisk, strukturę organizacyjną, strukturę lokalizacyjną oraz dynamiczne grupy stanowisk. * Oprogramowanie musi umożliwiać globalną dystrybucję plików oraz folderów do wskazanych lokalizacji do wybranych stanowisk komputerowych wg przynależności do struktury organizacyjnej, lokalizacyjnej lub grupy dynamicznej wraz z automatycznym (polisa) odtworzeniem brakujących danych w przypadku wykrycia niespójności. * Oprogramowanie musi umożliwiać szyfrowanie plików źródłowych dla zadań instalacji. * Oprogramowanie musi umożliwiać globalny przegląd postępu wykonania wybranych zadań oraz polis wraz z odczytem standardowego wyjścia (stdout) oraz standardowego wyjścia błędów (stderr). * Oprogramowanie musi umożliwiać tworzenie własnych szablonów akcji zawierających zdefiniowaną listę akcji pozwalających na warunkowe uruchamianie akcji zależnych (oczekiwanie na zakończenie akcji, praca w tle). * Oprogramowanie musi umożliwiać konfigurację typów akcji co najmniej w zakresie: dystrybucja i uruchomienie plików wsadowego BAT, dystrybucja plików rejestru REG, dystrybucja i instalacja pakietu MSI, dystrybucja i instalacja poprawki MSP, dystrybucja i uruchomienie aplikacji EXE, dystrybucja i uruchomienie skryptu PowerShell, dystrybucja plików i folderów, uruchomienie/wyłączenie/restart usługi systemowej, zakończenie procesu systemowego, wywołanie polecenia CMD. * Oprogramowanie musi umożliwiać konfigurowanie dedykowanych parametrów dla każdej z ww. akcji. * Oprogramowanie musi umożliwiać uruchomienie na prawach administracyjnych pliku instalacyjnego EXE (z GUI) w sesji użytkownika z ograniczonymi uprawnieniami do instalacji aplikacji. Proces instalacji jest manualnie kontynuowany przez użytkownika. * Oprogramowanie musi umożliwiać ograniczenie zakresu działania zadania, polisy oraz zawężenie wszelkich raportów systemowych do stanowisk spełniających kryteria wybranej dynamicznej grupy stanowisk. * Oprogramowanie w zakresie automatyzacji musi realizować m.in. następujące przypadki użycia z wykorzystaniem mechanizmu grup dynamicznych dla zadań oraz polis: * Automatyczną instalacji aplikacji na komputerach spełniających warunki: stanowiska z Windows 10 z pamięcią RAM>4GB i zainstalowaną wybraną aplikacją w wersji mniejszej (np. 7.0) * Automatyczne odinstalowanie aplikacji na komputerach spełniających warunki: stanowiska z Windows 7 gdzie producentem komputera jest np. Dell i zainstalowaną wybraną aplikacją w wersji większej niż (np. 8.0) * Dystrybucję plików oraz folderów (ze wskazaną zawartością np. dokumenty, skróty do aplikacji) na pulpity stanowisk komputerowych spełniających warunki: stanowiska z Windows 10 z brakiem zainstalowanej wybranej aplikacji oraz nie posiadające konta użytkownika z prawami administracyjnymi * Uruchomienia wybranego skryptu PowerShell dla komputerów spełniających warunki: stanowiska z Windows 10 w architekturze 32 bitowej, zainstalowaną aplikacją X w wersji większej niż (np. 6.0) i brakiem zainstalowanej aplikacji Y. * Uruchomienia wybranych szablonów akcji w przypadku wykrycia zmiany jednostki organizacyjnej stanowiska komputerowego. * W przypadku wcześniej zdefiniowanych polis wymagane jest, aby zostały one automatycznie uruchomione dla nowych stanowisk komputerowych po spełnieniu warunków przynależności do określonych grup dynamicznych. * Oprogramowanie musi umożliwić instalację oprogramowania z plików exe, które nie posiadają instalacji w trybie cichym poprzez automatyzację procesu manualnej instalacji (nagrywanie makr w zakresie wyborów typu zaznaczenie checkbox, wybór pozycji z listy, kliknięcie przycisku, wpisanie parametru/ścieżki itp.) * Oprogramowanie musi posiadać repozytorium szablonów makr automatyzacji do późniejszego wykorzystania podczas procesów instalacji * Oprogramowanie musi zawierać funkcję testowania nagranych makr z poziomu interfejsu użytkownika * Oprogramowanie musi wznawiać instalację, w przypadku przerwania procesu instalacji (np. z powodu wyłączenia komputera) * Nagrywanie makr musi być realizowane przez wybranie/wskazanie elementu okna, na którym ma zostać wykonana akcja (np. kliknięcie, wprowadzenie tekstu, zaznaczenie) * Oprogramowanie musi umożliwiać wysyłanie komunikatów (Windows Notification) do wskazanych stanowisk komputerowych (wybór manualny, wg struktury organizacyjnej, lokalizacyjnej lub grupy dynamicznej) * Oprogramowanie musi umożliwiać wysyłanie komunikatów przed każdą zdefiniowaną akcją automatyzacji (np.: przed rozpoczęciem instalacji pakietu MSI, przed dystrybucją plików, przed uruchomieniem skryptu PowerShell) * Oprogramowanie musi umożliwiać automatyzację procesu konfiguracji dowolnej aplikacji Windows w celu odtworzenia zapamiętanych akcji (makr) dla wskazanych stanowisk komputerowych. |
| Backup danych użytkownika | * Oprogramowanie musi umożliwiać tworzenie dowolnej ilości automatycznych zadań w zakresie archiwizacji danych – globalnie z poziomu głównej konsoli zarządzającej. * Oprogramowanie musi umożliwiać globalną zmianę parametrów zadań archiwizacji (ilość archiwów, kompresja, okres, zakres). * Oprogramowanie musi umożliwiać definiowanie rozszerzeń plików, które mają być pomijane podczas procesu archiwizacji oraz rozszerzeń plików np. \*.doc, które mają być archiwizowane. * Oprogramowanie Agenta musi umożliwiać kopię całościową danych oraz przesyłanie plików z archiwizacji na wskazany serwer FTP. * Mechanizm archiwizacji danych musi być realizowany przez Agenta systemu bez udziału zdalnych sesji (typu zdalny pulpit, wywoływanie skryptów) * Oprogramowanie musi umożliwiać definiowanie cyklu archiwizacji. * Oprogramowanie musi umożliwiać automatyczne usuwanie starszych plików kopii całościowej, definiowanie globalnego zadania archiwizacji |
| Zarządzanie urządzeniami USB Storage | * Oprogramowanie musi umożliwiać zapisywanie w bazie danych informacji o kopiowaniu z/do urządzeń zewnętrznych typu: Pendrive USB, dysk zewnętrzny. * Oprogramowanie musi posiadać raport w zakresie rejestracji informacji na temat użytkownika, który kopiował i/lub uruchamiał napęd, kiedy miało miejsce zdarzenie i jakie dokumenty zostały skopiowane. * Oprogramowanie musi umożliwiać blokadę oraz autoryzację wybranych urządzeń USB w obrębie klasy USBStorage. * Oprogramowanie musi umożliwiać włączenie trybu ReadOnly dla klasy USBStorage * Oprogramowanie musi umożliwiać całkowitą blokadę klasy FDD/CD/DVD |
| Monitoring stanowisk komputerowych | * Oprogramowanie musi umożliwiać zestawienie najpopularniejszych adresów (jakie stanowiska je wywoływały, kiedy) z możliwością zapisu całego adresu lub tylko głównej strony. * Oprogramowanie umożliwia zestawienie najaktywniejszych stanowisk (pod kątem WWW), jakie adresy odwiedzały, kiedy, wszystkie zestawienia do poziomu: jednostka organizacyjna, stanowisko, zalogowany użytkownik. * Oprogramowanie musi umożliwiać analizę uruchamianych aplikacji (aktywność stanowisk wg aplikacji oraz wykorzystanie zainstalowanych aplikacji wg stanowisk). * Oprogramowanie musi umożliwiać analizę efektywności pracy użytkowników na poszczególnych aplikacjach * Oprogramowanie musi umożliwiać blokadę stron www (biała i czarna lista adresów, blokada pełna lub selektywna) z możliwością automatycznego zamykania przeglądarki lub konkretnej karty przeglądarki (w przypadku wykrycia adresu zabronionego). * Oprogramowanie musi umożliwiać tworzenie statystyk aktywności stron WWW oraz aktywności stanowisk. * Oprogramowanie musi umożliwiać podział stron na dozwolone i zabronione. * Oprogramowanie musi umożliwiać wydruki tabelaryczne oraz graficzne (wykresy aktywności). * Oprogramowanie musi umożliwiać okresowe tworzenie zrzutu ekranu użytkownika z możliwością przesłania go na serwer. * Oprogramowanie musi umożliwiać rozróżnienie stanów monitorowanego komputera w szczególności stan aktywności (focus okna), hibernacji, uśpienia oraz wylogowania * Oprogramowanie musi umożliwiać odczyt aktywności użytkownika w czasie rzeczywistym w zakresie min. tytuł okna, adres www przeglądanej strony z dokładnością do 1 sekundy. * Oprogramowanie musi umożliwiać analizę aktywności myszy oraz klawiatury dla poszczególnych monitorowanych aplikacji oraz stron internetowych (ilość kliknięć). * Oprogramowanie musi umożliwiać monitorowanie wszystkich prac drukowania generowanych na urządzeniach sieciowych udostępnionych przez centralny serwer wydruków i udostępnionych lokalnie przez port TCP/IP * Oprogramowanie musi umożliwiać monitorowanie wszystkich prac drukowania generowanych na urządzeniach lokalnych udostępnionych przez port LPT, USB. Monitorowanie tych wydruków musi odbywać się poprzez agenta aplikacji zainstalowanego na stacji roboczej będącej serwerem wydruków dla drukarki lokalnej. * Oprogramowanie po zainstalowaniu musi przesyłać do serwera aplikacji następujące informacje: nazwa stacji roboczej, nazwa zainstalowanego sterownika drukarki, nazwa portu z jakiego dany sterownik korzysta, opis sterownika drukarki, format drukowanych stron oraz nazwę drukowanego dokumentu. * Oprogramowanie musi posiadać możliwość definicji kosztów wydruku dla poszczególnych urządzeń drukujących (podział kosztu na mono/kolor). |
| ServiceDesk – Zarządzanie zgłoszeniami | * Oprogramowanie w części HelpDesk musi być oparte na zasadach ITIL w szczególności: * Zarządzanie problemem * Zarządzanie incydentem * Obsługa procesów poprzez WorkFlow (wnioski o usługi, uprawnienia, zakupy) * Zarządzanie umowami serwisowymi * Definicje poziomów SLA (reakcja, naprawa, reklamacja) * Oprogramowanie musi umożliwiać zgłaszania przez użytkowników z poziomu przeglądarki WWW (dedykowany portal) awarii sprzętu, usług, oprogramowania i innych typów awarii zdefiniowanych przez administratora. * Portal ServiceDesk musi mieć możliwość obsługi przez wiodące przeglądarki WWW na urządzeniach mobilnych poprzez responsywny interfejs użytkownika. * Portal ServiceDesk musi umożliwiać wybór wersji językowej interfejsu (co najmniej polski i angielski). * Obsługa listy zgłoszeń serwisowych (incydentów i problemów) musi być realizowana przez portal ServiceDesk z zachowaniem nadanego poziomu uprawnień. * Oprogramowanie musi umożliwiać kontrolę obciążenia działu IT, optymalizację podziału pracy pomiędzy pracowników działu IT oraz przegląd awaryjności sprzętu. * Oprogramowanie musi umożliwiać uwierzytelnianie użytkowników wykorzystując bazę Active Directory poprzez protokół LDAP. * Oprogramowanie musi umożliwiać automatyczne autoryzowanie określonych stanowisk i użytkowników (z wykorzystaniem mechanizmy SSO), aby uniknąć każdorazowego uwierzytelniania przed korzystaniem z systemu zgłoszeń. * Oprogramowanie musi umożliwiać sortowanie listy zgłoszeń awarii, wg daty zgłoszenia, priorytetu, statusu. * Oprogramowanie musi umożliwiać filtrację zgłoszeń wg priorytetu oraz statusów zgłoszeń, stanowisk oraz inżynierów obsługujących zgłoszenia. * Oprogramowanie musi umożliwiać tworzenie dedykowanych list zgłoszeń z różnymi danymi, domyślnym filtrowaniem i sortowaniem. * Oprogramowanie musi umożliwiać określenie widoczności poszczególnych list zgłoszeń w zależności od zalogowanego użytkownika. * Oprogramowanie musi umożliwiać określenie widoczności zgłoszeń w zależności od kategorii i lokalizacji zgłoszeń przypisanych do zalogowanego użytkownika. * Oprogramowanie musi umożliwiać dostęp do zgłoszeń swoich podwładnych przez przełożonego. * Oprogramowanie musi umożliwiać dodawanie przez administratora nowych wpisów (komentarzy) w zgłoszeniu, jak i umożliwiać zmianę statusu sprawy. Użytkownik także ma możliwość dodawania nowych wpisów do zgłoszonego problemu wraz ze zmianą statusu. * Oprogramowanie musi umożliwiać tworzenie zadań w ramach konkretnego zgłoszenia z możliwością przekazania do realizacji przez innych użytkowników. * Oprogramowanie musi umożliwiać tworzenie globalnych zadań do realizacji przez zalogowanego użytkownika. * Oprogramowanie musi umożliwiać tworzenie szablonów zadań. * Oprogramowanie musi umożliwiać rejestrację czasu pracy poświęconego na realizację zgłoszenia przez opiekuna. * Oprogramowanie musi umożliwiać przesyłanie użytkownikom powiadomień pocztą elektroniczną o nowych wpisach i zmianach w zgłoszeniu. * Oprogramowanie musi umożliwiać edycję szablonów powiadomień email. * Oprogramowanie musi umożliwiać tworzenie wielopoziomowych list kategorii zawierających nazwę i opis kategorii. * Oprogramowanie musi umożliwiać określenie widoczności poszczególnych kategorii w zależności od zalogowanego użytkownika. * Oprogramowanie musi umożliwiać tworzenie pól dodatkowych na formularzu rejestracji zgłoszenia. * Oprogramowanie musi umożliwiać określenie widoczności poszczególnych pól dodatkowych w zależności od zalogowanego użytkownika. * Rozwiązania w bazie wiedzy muszą posiadać znacznik określający czy są dostępne dla użytkowników, czy są wewnętrznymi uwagami działu IT. Panel www użytkownika musi zawierać wyszukiwarkę tematów wg słów kluczowych oraz wewnętrznej treści. * Oprogramowanie musi umożliwiać edycję bazy wiedzy z poziomu przeglądarki WWW wraz z możliwością formatowania tekstu (wraz z grafiką) oraz wstawiania załączników. * Oprogramowanie musi umożliwiać administratorowi wprowadzenie do systemu zgłoszenia użytkownika, który nie ma dostępu do PC (np. telefoniczna informacja o awarii komputera). * Oprogramowanie musi umożliwiać delegowanie zgłoszenia innemu administratorowi (technikowi), jak również przejęcie innego zgłoszenia (np. w przypadku nieplanowanej nieobecności pracownika). * Oprogramowanie musi umożliwiać obsługę tzw. Linii wsparcia poprzez samodzielne tworzenie nowych linii wraz z przypisywaniem do nich dowolnej ilości kont operatorów HelpDesk. Zgłoszenie serwisowe musi mieć możliwość przekazania do dowolnej linii wsparcia lub dedykowanego operatora HelpDesk. Linia wsparcia musi mieć możliwość przypisania powiązanych z nią kategorii zgłoszeń. * Oprogramowanie musi umożliwiać informowanie pracowników o planowanych działaniach, awariach za pomocą komunikatów wprowadzanych na stronę główną panelu zgłaszania usterki, bądź do poszczególnych kategorii. * Oprogramowanie musi umożliwiać określenie widoczności komunikatów o planowanych działaniach, awariach w zależności od zalogowanego użytkownika. * Oprogramowanie musi umożliwiać tworzenia baz umów serwisowych powiązanych z bazami firm serwisowych (dostawców sprzętu, oprogramowania, lokalnych serwisów). lub z zakupionym sprzętem. * Oprogramowanie w oparciu o bazę firm/umów serwisowych musi umożliwiać zapis przekazania zgłoszenia do serwisu zewnętrznego. * Oprogramowanie musi umożliwiać przesyłanie powiadomień do firm serwisowych powiązanych ze zgłoszeniem. * Oprogramowanie musi posiadać możliwość rejestracji w historii zgłoszenia (w komentarzach) korespondencji * mailowej między opiekunami zgłoszenia a firmami serwisowymi powiązanymi ze zgłoszeniem. * Oprogramowanie musi posiadać dedykowane panele WWW w zależności od aktywnie zalogowanego użytkownika końcowego (panel dla użytkownika tj. zgłaszanie incydentów, panel dla operatora serwisowego – obsługa zgłoszeń, panel dla managera HelpDesk – analiza graficzna oraz tabelaryczna pracy operatorów HelpDesk). * Oprogramowanie musi umożliwiać wyświetlenie w panelu WWW użytkownika informacji nt. powiązanych z użytkownikiem zasobów (przypisane stanowiska PC, przydzielone licencje aplikacji, wydane urządzenia). * Oprogramowanie musi umożliwiać wybranie zasobu w określonej kategorii powiązanego z użytkownikiem podczas rejestracji zgłoszenia. * Oprogramowanie musi umożliwiać tworzenie zgłoszeń cyklicznych z możliwością definiowania częstości występowania oraz typu okresu (codziennie, co tydzień, co miesiąc) * Oprogramowanie musi umożliwiać tworzenie reguł w celu automatyzacji obsługi zgłoszeń. Reguły muszą uruchamiać się w odpowiedzi na określone zdarzenia w systemie i wykonywać akcje w zależności od spełnionych warunków. W zakresie reguł ServiceDesk musi realizować m.in. następujące przypadki użycia: * Zmiana statusu po przejęciu zgłoszenia przez opiekuna. * Przejmowanie zadań po przejęciu zgłoszenia przez opiekuna. * Dodawanie zadań w zgłoszeniu w zależności od parametrów zgłoszenia. * Wznawianie zgłoszenia po odpowiedzi przez zgłaszającego użytkownika. * Zamykanie zgłoszenia po upływie czasu bez odpowiedzi użytkownika. * Zamykanie zgłoszenia po upływie czasu reklamacji. * Dodawanie wpisów (komentarzy) w zgłoszeniu na podstawie szablonów. * Zmiana parametrów zgłoszenia po znalezieniu wybranej frazy w treści komentarza. * Walidacja zamkniętych zadań w zamykanym zgłoszeniu. * Systemowe potwierdzanie realizacji zgłoszenia. * Wysyłanie dodatkowych powiadomień cyklicznych ze zgłoszeniami, np. zgłoszenia wymagające reakcji, zgłoszenia do realizacji lub zgłoszenia wstrzymane/wznowione. * Oprogramowanie musi umożliwiać tworzenie szablonów komentarzy wykorzystywanych przez opiekunów zgłoszeń. * Oprogramowanie musi posiadać możliwość rejestracji zgłoszeń i komentarzy drogą mailową, zarówno przez zarejestrowanych użytkowników systemu jak i niezarejestrowanych użytkowników. * Oprogramowanie musi umożliwiać obsługę dowolnej ilości kont pocztowych do wysyłania powiadomień i generowania zgłoszeń/komentarzy przez email. * Oprogramowanie musi posiadać wbudowane raporty prezentujące m.in. realizację obsługi zgłoszeń w zakładanym SLA (statystyka miesięczna, kwartalna, roczna). * Oprogramowanie musi umożliwiać definiowanie własnych widoków oraz zestawień dla każdego zalogowanego użytkownika * Oprogramowanie musi umożliwiać zdefiniowanie własne macierzy priorytetów na podstawie pilności oraz wpływu zgłoszenia * Oprogramowanie musi umożliwiać zamodelowanie trzy zmianowego trybu pracy inżynierów (opiekunów zgłoszeń) * Oprogramowanie musi umożliwiać informowanie użytkowników o nowych zdarzeniach systemowych za pomocą notyfikacji (dymku) podczas pracy z systemem * Oprogramowanie musi umożliwiać tworzenie obiegu procesu decyzyjnego dla wniosków o uprawnienia lub elementy konfiguracji w oparciu o bazę CMDB * Oprogramowanie musi umożliwiać zaprojektowanie dowolnego formularza do wprowadzania danych z wykorzystaniem własnych atrybutów (wraz ze zmianą układu/położenia atrybutów w projektowanym widoku) * Oprogramowanie musi umożliwiać definicję czasów SLA w oparciu o matrycę priorytetów, statusy, kategorie lub dowolne warunki i atrybuty zgłoszenia * Oprogramowanie musi umożliwiać dodanie Akceptacji do już istniejącego zgłoszenia * Oprogramowanie musi umożliwiać definiowanie własnych reguł zarządzania w oparciu o warunki i akcje dla Prawdy i Fałszu (zdarzenie -> warunek -> akcja) * Oprogramowanie musi umożliwiać tworzenie wielu zgłoszeń poprzez wybór kilku użytkowników w zgłoszeniu * Oprogramowanie musi umożliwiać tworzenie słowników wartości dla atrybutów w oparciu o strukturę płaską lub drzewiastą * Oprogramowanie musi umożliwiać tworzenie atrybutów zależnych poprzez określone warunki widoczności * Oprogramowanie musi umożliwiać definiowanie formularzy zamykających zgłoszenie oraz zatwierdzające zmiany w zgłoszeniu * Oprogramowanie musi umożliwiać definiowanie reguł biznesowych za pomocą graficznego/blokowego kreatora. * Oprogramowanie musi umożliwiać definiowanie obiegów za pomocą graficznego/blokowego kreatora. * Oprogramowanie musi umożliwiać tworzenie niestandardowych raportów za pomocą kreatora. * Oprogramowanie musi umożliwiać definiowanie poziomu dostępu do zgłoszeń dla dynamicznych grup użytkowników. * Oprogramowanie musi umożliwiać definiowanie formularzy dla zgłoszeń w danej kategorii za pomocą kreatora Drag&Drop z możliwością określenia układu kolumn. * Oprogramowanie musi umożliwiać tworzenie dowolnej liczby Dashboard-ów dla użytkownika za pomocą kreatora Drag&Drop. * Oprogramowanie musi umożliwiać zmianę układu szczegółów zgłoszenia za pomocą kreatora Drag&Drop. * Oprogramowanie musi umożliwiać udostępniania ogłoszeń w formie Widget-u oraz okienka modalnego z wymaganym potwierdzeniem dla użytkownika. * Oprogramowanie musi umożliwiać zaprojektowanie dowolnego szablonu protokołu zgłoszenia. * Oprogramowanie musi udostępniać matrycę(wpływ/pilność) dla obliczania priorytetu zgłoszeń. * Oprogramowanie musi umożliwiać zmianę koloru dla statusu/priorytetu/wpływu/pilności zgłoszenia prezentowanego na liście zgłoszeń. * Oprogramowanie musi umożliwiać definiowanie dowolnych kolejek zgłoszeń. * Oprogramowanie musi umożliwiać rejestrację nieobecności administratorów z możliwością wybrania zastępstwa. |
| ServiceDesk – Zarządzanie wnioskami | * Oprogramowanie musi zapewnić obsługę Workflow w zgłoszeniach serwisowych poprzez zdefiniowanie logicznych ścieżek (zbiór węzłów logicznych). * Oprogramowanie musi umożliwiać wybór wielu zasobów na jednym formularzu wniosku. Przykładowo dla wniosku o nadanie uprawnień musi istnieć możliwość wskazania wielu systemów/zbiorów danych z podziałem na moduły lub poziomy uprawnień użytkownika. * Na poziomie każdego węzła logicznego w workflow musi być możliwość edycji/modyfikacji zawartości danych w szczególności statusu, uwag, załączników (o dowolnym typie pliku) wraz z utworzeniem wpisu w historii przetwarzanego obiegu. |
| ServiceDesk – Zarządzanie uprawnieniami | * Oprogramowanie musi umożliwiać inwentaryzację Systemów Informatycznych oraz Zbiorów danych * Oprogramowanie musi umożliwiać określanie powiązań pomiędzy pracownikami z Systemami Informatycznymi oraz Zbiorami danych * Oprogramowanie musi umożliwiać budowanie powiązanych zestawów atrybutów dla Systemów Informatycznych oraz Zbiorów danych (np. termin ważności dostępu, poziom dostępu, przetwarzanie danych wrażliwych) * Oprogramowanie musi umożliwiać tworzenie ścieżek decyzyjnych dla dowolnych wniosków o uprawnienia do Systemów Informatycznych oraz Zbiorów danych * Oprogramowanie musi umożliwiać akceptację poszczególnych etapów przez dedykowane osoby decyzyjne zdefiniowane w konfiguracji ścieżek * Oprogramowanie musi umożliwiać akceptację etapów ścieżki przez automatyczny wybór powiązanych opiekunów merytorycznych oraz technicznych * Oprogramowanie musi umożliwiać definiowanie dowolnych akcji dla poszczególnych kroków (np. zmiana opiekuna, statusu) * Oprogramowanie musi umożliwiać automatyczne tworzenie powiązań pracownika z Systemem informatycznym lub Zbiorem danych po akceptacji wniosku * Oprogramowanie musi umożliwiać obsługę procesu (wniosku) o odebranie uprawnień (koniec terminu dostępu, zwolnienie pracownika) * Oprogramowanie musi umożliwiać raportowanie uprawnień wg Systemów Informatycznych oraz Zbiorów danych dla poszczególnych osób * Oprogramowanie musi umożliwiać raportowanie uprawnień w pracowników do Systemów Informatycznych oraz Zbiorów danych * Oprogramowanie musi umożliwiać generowanie edytowalnej Karty Uprawnień Pracownika |
| ServiceDesk – Zarządzanie rezerwacjami | * Oprogramowanie musi umożliwiać rezerwację dowolnego aktywnego zasobu w systemie. * Oprogramowanie musi umożliwiać kategoryzowanie rejestrowanych rezerwacji. * Oprogramowanie musi umożliwiać określenie widoczności poszczególnych kategorii rezerwacji w zależności od zalogowanego użytkownika. * Oprogramowanie musi informować o możliwych konfliktach podczas tworzenia/edycji rezerwacji z zasobem. * Oprogramowanie musi prezentować informacje o rezerwacjach w formie graficznej – kalendarza. * Oprogramowanie musi umożliwiać akceptację, odrzucenie lub anulowanie rezerwacji przez upoważnionych użytkowników. |
| Monitoring sieci LAN | * Oprogramowanie musi umożliwiać okresowe skanowanie sieci LAN (wg. zadanych kryteriów, na wybranych serwerach lokalnych) z wykorzystaniem protokołu SNMP, celem prezentacji aktywnych urządzeń IP w zakresie co najmniej komputery, drukarki, routery, smartphony * Oprogramowanie musi umożliwiać monitorowanie poprzez wykorzystanie protokołu SNMP stanu drukarek tj. poziomy tonerów, liczba wydrukowanych stron oraz informować błędach takich jak brak papieru, zacięcie papieru. * Oprogramowanie musi umożliwiać wizualizację ruchu sieciowego na poszczególnych portach urządzeń sieciowych wraz z wizualizacją w postaci mapy sieci dla wskazanego urządzenia typu switch, router. * Oprogramowanie musi umożliwiać z zdalną instalację agenta systemu z poziomu wykrytej struktury sieciowej z wykorzystaniem poświadczeń administracyjnych, w tym również stanowisk poza usługą katalogową. * Oprogramowanie musi umożliwiać monitorowanie stanu dowolnej usługi sieciowej TCP. * Oprogramowanie musi umożliwiać monitorowanie dowolnego licznika SNMP(v1/2/3) urządzenia. * Oprogramowanie musi umożliwiać monitorowanie stanu dowolnego urządzenia sieciowego poprzez odpytywanie typu PING. * Oprogramowanie musi umożliwiać tworzenie konfigurowalnych zdarzeń sieciowych powodujących wysyłanie komunikatów informacyjnych i/lub ostrzegawczych poprzez SMS i/lub Email. |
| Zarządzanie dokumentami | * Oprogramowanie musi umożliwiać centralną ewidencję dokumentów * Oprogramowanie musi umożliwiać zawierać dedykowany formularz dodawania nowego dokumentu z możliwością edycji widocznych oraz wymaganych atrybutów dokumentu * Oprogramowanie musi umożliwiać dołączenie skanu dokumentu (m.in.: skany faktur, umów) * Oprogramowanie musi umożliwiać stworzenie dedykowanego zbioru ról i uprawnień w zakresie obsługi rejestru dokumentów * Oprogramowanie musi umożliwiać utworzenie pomocniczych rejestrów oraz słowników * Oprogramowanie musi umożliwiać przeszukiwanie bazy dokumentów oraz kontrahentów po dowolnie wskazanym atrybucie opisującym * Oprogramowanie musi umożliwiać utworzenie rejestru osób reprezentujących * Oprogramowanie musi umożliwiać analizę zmian wartości dowolnych atrybutów opisujących dokument w zakresie daty zmiany, aktualnej/poprzedniej wartości oraz osoby dokonującej zmiany |
| System wewnętrznego komunikatora dla użytkowników | * Oprogramowanie musi zawierać wewnętrzny komunikator pracujący w sieci LAN, integrujący się z usługą katalogową w zakresie kont użytkowników (dane osobowe, avatar), jednostek organizacyjnych. * Oprogramowanie w zakresie modułu komunikatora dla użytkowników musi współpracować z serwerem MSSQL Server 2008R2-2019 lub PostrgeSQL * Oprogramowanie komunikatora musi umożliwiać automatyczne logowanie użytkowników pochodzących z usługi katalogowej. * Oprogramowanie komunikatora musi umożliwiać konwersację grupową oraz prywatną pomiędzy użytkownikami * Oprogramowanie komunikatora musi umożliwiać wysyłanie wiadomości powitalnych; komunikatów grupowych z raportowaniem doręczenia oraz odczytania. * Oprogramowanie komunikatora musi umożliwiać generowanie raportów doręczenia/odczytania wiadomości wymagających potwierdzenia. * Oprogramowanie komunikatora musi umożliwiać określenie maksymalnego rozmiaru transferowanego pliku (przez administratora). * Oprogramowanie komunikatora musi umożliwiać wysyłanie powiadomień e-mail o utworzeniu/modyfikacji użytkowników, którzy nie pochodzą z usługi katalogowej. * Oprogramowanie komunikatora musi umożliwiać automatyczną aktualizację wg. zadanej konfiguracji danych synchronizowanych (ze szczególnym uwzględnieniem danych o użytkownikach, jednostkach organizacyjnych z usługi katalogowej). * Oprogramowanie komunikatora musi umożliwiać archiwizację starych rozmów między użytkownikami. * Oprogramowanie komunikatora musi umożliwiać administratorowi wyłączenie globalnie możliwości zamknięcia/wylogowanie/zapisywanie poświadczeń dla klientów końcowych. * Oprogramowanie komunikatora musi umożliwiać administratorowi bezpieczeństwa wgląd do rozmów pracowników, wyłączenie wybranych funkcjonalności dla klienta końcowego (np. transferu plików, konferencji audio-video). * Oprogramowanie komunikatora musi umożliwiać wymianę plików pomiędzy zalogowanymi użytkownikami * Oprogramowanie komunikatora musi umożliwiać nawiązanie sesji audio oraz wideo pomiędzy zalogowanymi użytkownikami wraz z obsługą konferencji grupowych. |
| Wymagania formalne: | * Dostarczone licencje na oprogramowanie muszą być bezterminowe. * Dostarczone licencje na oprogramowanie muszą być dostarczone z supportem producenta do dnia **30 czerwca 2026** **r.**, liczonym od daty zakończenia wdrożenia. * Obsługa serwisowa w zakresie obsługi błędów realizowana ma być z czasem reakcji 16 godzin roboczych oraz czasem naprawy 80 godzin roboczych. W ramach supportu wymagany jest dostęp do nowych wersji systemu oraz wsparcia technicznego producenta. * Dostarczone licencje na oprogramowanie muszą objąć co najmniej 35 stanowisk komputerowych ( w tym 22 licencje dla Urzędu Gminy oraz osobno 13 licencji rok dla Gminnego Ośrodka Pomocy Społecznej) z systemem klasy Microsoft Windows. Licencje nie mogą mieć ograniczeń ilościowych dotyczących liczby obsługiwanych innych zasobów (np. drukarki, skanery, monitory itp). Ponadto musi posiadać co najmniej 2 licencje dostępowych do konsoli zarządzającej. * W przypadku wątpliwości zamawiający zastrzega sobie prawo (w przeciągu do 7 dni od terminu otwarcia ofert) do wezwania wykonawcy do prezentacji zaoferowanego rozwiązania celem weryfikacji zgodności z wymaganiami stawianymi przez zamawiającego w niniejszym postępowaniu. * Zamawiający wymaga, aby Wykonawca dołączył do oferty oświadczenie producenta lub autoryzowanego dystrybutora producenta, iż produkt pochodzi z autoryzowanego kanału sprzedaży. |

|  |  |
| --- | --- |
| **UPS do stacji roboczych – 10 sztuk parametry techniczne minimum:** | |
| moc pozorna | min. 850VA |
| moc rzeczywista | min. 480W |
| Technologia | VI (line interactive) |
| Typ obudowy | wolnostojąca |
| Napięcie wejściowe | 170 ÷ 280 V AC ± 7 % |
| Częstotliwość napięcia wejściowego | 45 ÷ 55 Hz ± 1 Hz |
| Zakres napięcia wyjściowego | 230 V AC ± 10 % |
| Progi przełączania sieć – UPS | 170 ÷ 280 V AC ± 7 % |
| Czas przełączania sieć – UPS | <6ms |
| Napięcie wyjściowe | ~230V ± 10% |
| Częstotliwość napięcia wyjściowego | 50Hz ± 1Hz |
| Kształt napięcia wyjściowego na pracy bateryjnej | Schodkowa aproksymacja sinusoidy |
| Zabezpieczenie wyjściowe przeciwzwarciowe | elektroniczne |
| Zabezpieczenie wyjściowe przeciążeniowe | elektroniczne |
| Czas podtrzymania (P 0,8max/P 0,5max) | minimum 2/6 min |
| akumulatory wewnętrzne | minimum 12V9Ah; szczelne, bezobsługowe |
| Ilość i typ gniazd wyjściowych | minimum 2 gniazda z podtrzymaniem bateryjnym w tym minimum 2 gniazda PN-E-93201 |
| Filtr telekomunikacyjny/teleinformatyczny | Filtr telekomunikacyjny – RJ11 |
| Sygnalizacja | Akustyczno-optyczna, w tym minimum wyświetlacz LCD sygnalizujący napięcie wejściowe i wyjściowe, poziom obciążenia, stan naładowania baterii oraz aktywność systemu AVR |
| Zimny Start | tak |
| Interfejs komunikacyjny | USB (kabel w komplecie) |
| Waga UPS | do 5,5kg |
| gwarancja | min 24 miesięcy na elektronikę i 12 miesięcy na akumulatory |
| serwis | autoryzowany serwis producenta. |
| serwis realizowany w systemie door-to-door |
| oprogramowanie | Tego samego producenta co UPS, bezpłatne bez ograniczeń funkcjonalności oraz ilości podłączonych stanowisk komputerowych; pod Windows 10, Windows 11, Windows Server 2019, 2022, 2025, Linux - możliwość pobierania ze strony producenta i dokonywania aktualizacji przez użytkownika bez dodatkowych kosztów (potwierdzone oświadczeniem producenta oprogramowania załączonym wraz z ofertą) |
| możliwość edycji nazw urządzeń na liście monitorowanych UPSów |
| wymagane wsparcie producenta (telefoniczne oraz mailowe) w języku polskim odnośnie konfiguracji i rozwiązywania problemów |
| wsparcie dla systemów Linux, Windows oraz wirtualizacji Hyper-V, Vmware, XenServer |
| certyfikaty producenta (załączyć do oferty) | ISO 9001 lub równoważny zapewniający zarządzanie jakością, podejście procesowe, ciągłe doskonalenie, zarządzanie ryzykiem oraz zgodność z przepisami |
| deklaracja CE producenta sprzętu lub równoważny potwierdzający dopuszczenie sprzętu do obrotu w Europejskim Obszarze Gospodarczym |

|  |  |
| --- | --- |
| **UPS do serwera Typ A – 2 sztuki parametry techniczne minimum:** | |
| Moc wyjściowa (pozorna / czynna) | minimum 1650 VA |
| minimum 1650 W |
| Topologia | VI (line interactive) |
| Typ obudowy | Rack / Tower |
| Chłodzenie | Wymuszone, wewnętrzne wentylatory |
| Napięcie znamionowe (wartość skuteczna) | 230 V AC |
| Zakres napięcia wejściowego (wartości skuteczne) i tolerancja | 178 ÷ 281 V AC ± 2 % |
| Częstotliwość znamionowa napięcia wejściowego | 50 Hz |
| Zakres częstotliwości i tolerancja | 45 ÷ 55 Hz ± 1 Hz |
| Progi przełączania: sieć – UPS | 178 ÷ 281 V AC ± 2 % |
| Napięcie znamionowe (wartość skuteczna) | 230 V AC |
| Zakres napięcia wyjściowego (wartości skuteczne) i tolerancja – praca sieciowa | 195 ÷ 253 V AC ± 2 % |
| Zakres napięcia wyjściowego (wartości skuteczne) i tolerancja – praca rezerwowa | 230 V AC ± 5 % |
| Automatyczna regulacja napięcia (AVR) | ± 10 % |
| Kształt napięcia wyjściowego (przy pracy rezerwowej / sieciowej) | Sinusoidalny |
| Częstotliwość znamionowa napięcia wyjściowego | 50 Hz |
| Progi przełączania: UPS – sieć | 183 ÷ 276 V AC ± 2 % |
| Czas przełączenia na pracę rezerwową | < 3 ms |
| Czas powrotu na pracę sieciową | 0 ms |
| Przeciążalność | > 105% - 15 s (wyłączenie UPS) |
| Akumulatory wewnętrzne | minimum 12 V / 7 Ah VRLA |
| możliwość podpięcia modułów bateryjnych | wymagane minimum 1szt |
| Czas podtrzymania z baterii wewnętrznych (100 %/ 80 % / 50 % Pmax) | minimum 3 / 4 / 6 min |
| Maksymalny czas ładowania baterii wewnętrznych UPS do 90% pojemności baterii - po uprzednim rozładowaniu obciążeniem równym 80% Pmax (do wyłączenia się zasilacza). | do 4 h |
| Masa zasilacza | nie większa niż 26 kg |
| Zabezpieczenie wejściowe | Przeciwzwarciowe – Bezpiecznik automatyczny |
| 16 A / 250 V AC |
| Przeciwprzepięciowe |
| Zabezpieczenie wyjściowe | Elektroniczne – przeciwzwarciowe i przeciążeniowe |
| Zabezpieczenia wejścia DC (akumulatory wewnętrzne) | Zabezpieczenie nadprądowe |
| Zabezpieczenia DC (zewnętrzny moduł bateryjny) | Zabezpieczenie nadprądowe |
| Przyłącza wyjściowe (liczba i typ gniazd) | minimum 9 gniazd z podtrzymaniem bateryjnym (w tym minimum 2 gniazda w standardzie PL z bolcem uziemiającym) |
|
|
| Sygnalizacja | Akustyczno – optyczna; graficzny wyświetlacz LCD |
| Interfejsy komunikacyjne | USB HID, SNMP/HTTP |
| Wsporniki do montażu w szafie RACK | wymagane |
| Oprogramowanie monitorująco-zarządzające | Tego samego producenta co UPS, bezpłatne bez ograniczeń funkcjonalności oraz ilości podłączonych stanowisk komputerowych - możliwość zamykania systemu na min. 75 stanowiskach komputerowych w sieci; pod Windows 10, Windows 11, Windows Server 2019, 2022, 2025, Linux - możliwość pobierania ze strony producenta i dokonywania aktualizacji przez użytkownika bez dodatkowych kosztów (potwierdzone oświadczeniem producenta oprogramowania) |
| możliwość zdalnego włączenia / wyłączenia UPSa (poprzez SNMP) |
| możliwość zdalnego wyłączenia zarządzanej sekcji gniazd |
| możliwość edycji nazw urządzeń na liście monitorowanych UPSów |
| wymagane wsparcie producenta (telefoniczne oraz mailowe) w języku polskim odnośnie konfiguracji i rozwiązywania problemów. |
| wsparcie dla systemów Linux, Windows oraz wirtualizacji Hyper-V, Vmware, XenServer |
| Możliwość ustawienie minimalnego stopnia naładowania akumulatorów, przy którym zasilacz uruchomi się po rozładowaniu akumulatorów i powrocie napięcia sieciowego | wymagane |
| Możliwość aktualizacji oprogramowania firmware przez użytkownika | wymagane |
| Deklaracje | CE lub równoważny potwierdzający dopuszczenie sprzętu do obrotu w Europejskim Obszarze Gospodarczym |
| Gwarancja | min 36 miesięcy na elektronikę i 24 miesiące na akumulatory; |
| Serwis | autoryzowany serwis producenta. |
| serwis realizowany w systemie door to door |
| certyfikaty producenta (załączyć do oferty) | ISO 9001 lub równoważny zapewniający zarządzanie jakością, podejście procesowe, ciągłe doskonalenie, zarządzanie ryzykiem oraz zgodność z przepisami |
| Dodatkowe oświadczenia / dokumenty składane wraz z ofertą | Oświadczenie producenta lub autoryzowanego dystrybutora producenta, iż produkt pochodzi z autoryzowanego kanału sprzedaży |
| Jeżeli oferowana jest niestandardowa, rozszerzona gwarancja to wymagane jest by realizowana była wyłącznie przez serwis producenta - należy przedstawić odpowiednie oświadczenie producenta |

|  |  |
| --- | --- |
| **UPS do serwera Typ B – 1 sztuka parametry techniczne minimum:** | |
| Moc rzeczywista | min. 2000 W |
| Pojemność akumulatora | min. 2000 Wh |
| Typ wbudowanego akumulatora | LiFePO4 |
| Porty wyjścia | Min. 2× AC 230V, 4× USB-C (w tym min. 1× 100 W), 2× USB-A, 2× DC5521 12V/3A |
| Napięcie wyjściowe | 200 - 230 V AC |
| Częstotliwość napięcia wyjściowego | 50 Hz |
| Kształt napięcia wyjściowego na pracy bateryjnej | sinusoidalny |
| Waga | Max. 25 kg |
| Serwis | autoryzowany serwis producenta |
| Certyfikaty producenta/ dokumenty | deklaracja zgodności CE lub równoważne potwierdzający dopuszczenie sprzętu do obrotu w Europejskim Obszarze Gospodarczym, karta produktowa oferowanego sprzętu |
| Gwarancja | Min. 2 lata |

|  |  |
| --- | --- |
| **Dyski do serwera zapasowego – 2 sztuki parametry techniczne minimum:** | |
| Wymagania ogólne | Kompatybilny z posiadanym przez Zamawiającego serwerem DELL R330 |
| Stan produktu | Nowy |
| Pojemność | Min. 1.2TB |
| RPM | Min. 10000 |
| Cache | Min. 128MB |
| Gwarancja | Min. 3 lata |

Dostawa infrastruktury cybernetycznej dla Urzędu Gminy w Budrach i Gminnego Ośrodka Pomocy Społecznej w Budrach w celu stworzenia bezpiecznego, zintegrowanego i wydajnego środowiska informatycznego, które zapewni ciągłość działania, ochronę danych oraz szybki i bezpieczny dostęp do kluczowych zasobów informacyjnych. Główne aspekty środowiska obejmą zabezpieczenie sieci przed zagrożeniami, monitorowanie incydentów, zarządzanie dostępem do zasobów oraz ochronę przed wyciekiem danych, co umożliwi skuteczne funkcjonowanie oraz zapewni ochronę przed cyberatakami, jak również umożliwi monitorowanie i zarządzanie infrastrukturą w czasie rzeczywistym oraz zagwarantuje bezpieczeństwo krytycznych danych obywateli, urzędu i jednostki organizacyjnej GOPS.

**Zamówienie realizowane w ramach projektu pn. „Podniesienie poziomu cyberbezpieczeństwa w Gminie Budry” współfinansowanego z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa”**

Zakres dostawy obejmuje zakup i wdrożenie tj. instalację i konfigurację, implementacje oprogramowania, uruchomienie, testowanie i optymalizacje urządzeń i oprogramowania stanowiących infrastrukturę cybernetyczną zwiększającą odporność na cyberataki.

**Miejsce dostawy: Urząd Gminy w Budrach, Aleja Wojska Polskiego 27, 11-606 Budry.**

**Termin dostawy: do 30 dni od dnia podpisania umowy.**

Jeżeli w opisie przedmiotu zamówienia wskazano jakikolwiek znak towarowy, patent lub pochodzenie, źródło lub szczególny proces, które wskazują lub mogłyby wskazywać na konkretnego producenta/dostawcę – nie stanowi to preferowania konkretnego wyrobu lub producenta/dostawcy, lecz ma na celu jedynie wskazanie cech – parametrów technicznych, użytkowych i jakościowych nie gorszych od podanych w opisie. Należy to więc traktować jedynie jako pomoc w opisie przedmiotu zamówienia. Podane w opisie nazwy własne mają na celu poinformowanie Wykonawców o zasobach, którymi dysponuje Zamawiający, aby zapewnić pełną kompatybilność oferowanych rozwiązań z istniejącą infrastrukturą. Zamawiający oczekuje, że dostarczone produkty i usługi nie będą generować dodatkowych kosztów związanych z koniecznością zakupu dodatkowego oprogramowania, sprzętu czy modyfikacji istniejących systemów.

Jeżeli Wykonawca stwierdzi, że użyte w opisie parametry lub normy krajowe lub przenoszące na normy europejskie lub normy międzynarodowe mogą wskazywać na producentów produktów lub źródła ich pochodzenia to oznacza, że mają takie znaczenie, że parametry techniczne tak wskazanych produktów określają wymagane przez Zamawiającego minimalne oczekiwania co do jakości produktów, które mają być użyte do wykonania przedmiotu umowy. Wykonawca jest uprawniony do stosowania produktów równoważnych, przez które rozumie się takie, które posiadają parametry techniczne nie gorsze od tych wskazanych w opisie, również dopuszcza się wykazanie normami równoważnymi w stosunku do tych wskazanych w zapytaniu ofertowym. Na Wykonawcy spoczywa ciężar wykazania "równoważności”.

Wykonawca musi zaoferować spełniające min. takie wymagania i parametry techniczne, jak w opisie przedmiotu zamówienia. Wykonawca może zaoferować produkty o lepszych parametrach. Dostarczone przedmioty zamówienia powinny być fabrycznie nowe, wykonane zgodnie z wymaganiami i normami mającymi zastosowanie do danego wyrobu, wolne od wad, odpowiadać normom jakościowym, określonym we właściwych aktach prawnych, posiadać aktualne aprobaty techniczne, gwarancje producenta oraz winny spełniać wszelkie wymogi przewidziane obowiązującymi przepisami dla tego typu wyrobów.

Poniższa specyfikacja obejmuje parametry techniczne minimum, jakie ma spełnić dostarczona infrastruktura.