Załącznik nr 1 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa sprzętu komputerowego i oprogramowania w ramach projektu Cyfrowa Gmina

RI.271.2.9.2022

Część 1 - Dostawa UTM wraz ze switch-em zarządzalnym

Minimalne parametry UTM

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.

System musi wspierać 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 – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum:
   - 10 portami Gigabit Ethernet RJ-45.
2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.

3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System musi być wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 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 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 Enterprise Traffic Mix - minimum 1.4 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps.

Funkcje Systemu Bezpieczeństwa:
W ramach dostarczonego 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 oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.
12. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system

Polityki Firewall

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać 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.
3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.

5. Element systemu realizujący funkcję Firewall musi integrować 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
   - Google Cloud Platform (GCP).
   - OpenStack.
   - VMware NSX.

Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
   - Obsługa protokołu Diffie-Hellman grup 19 i 20.
   - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
   - 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.
   - Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
   - Mechanizm „Split tunneling" dla połączeń Client-to-Site.
2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
   - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
   - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
   - Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

Routing i obsługa łączy WAN

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
   - Routingu statycznego.
   - Policy Based Routingu.
   - Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

Funkcje SD-WAN

1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.

Zarządzanie pasmem

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.

3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.

Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków powinna zawierać 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 musi zapewniać 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) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

1. Moduł kontroli WWW musi korzystać 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 musi dostarczać kategorii stron zabronionych prawem: Hazard.

4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
   - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
   - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
4. 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 powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

Logowanie

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W przypadku kiedy usługa logowania i raportowania realizowana jest w chmurze, Wykonawca musi dostarczyć stosowne licencje upoważniające do składowania logów przez okres co najmniej jednego roku.

3. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
4. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
5. Musi istnieć możliwość logowania do serwera SYSLOG.

Certyfikaty
Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

- ICSA lub EAL4 dla funkcji Firewall.

Serwisy i licencje
W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

1. Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesięcy.
2. Licencja na usługę realizowaną w chmurze na okres 12 miesięcy umożliwiająca logowanie i raportowanie z czasem retencji logów minimum 1 rok.

Gwarancja oraz wsparcie

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres min. 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Rozszerzone wsparcie serwisowe AHB/SOS

1. System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres gwarancji.
2. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Wykonawca winien przedłożyć dokumenty:
   - Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
   - Certyfikat ISO 9001 podmiotu serwisującego.

Opisy do wymagań ogólnych

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada

certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Wykonawca winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż Wykonawca posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

Minimalne parametry switch-a (przełącznika sieciowego)

W ramach postępowania wymaganym jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych.

Zamawiający jest w posiadaniu rozwiązania FortiGate model 60E. W ramach rozbudowy istniejącego systemu, której celem jest rozszerzenie mechanizmów bezpieczeństwa o warstwę dostępową, wymaganym jest dostarczenie przełącznika oraz innych elementów funkcjonalnych, współpracujących z istniejącym rozwiązaniem Fortigate, o następujących parametrach:

Parametry fizyczne platformy

- Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.
- Zasilanie AC 230V.
- Maksymalny pobór mocy: 60 W.
- Minimalny zakres temperatury pracy: 0-40°C.

Interfejsy sieciowe - wymagania minimalne

1. Wymaganym jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:
   - 48 porty GE RJ-45.
   - 4 porty 10 GE SFP+.

Zarządzanie

- Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).
- Wsparcie dla SNMP w wersjach 1-3
- Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.
- Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.
- Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.
- Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).
- Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.
- Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.
- Automatycznie wykonywane rewizje konfiguracji.

Parametry wydajnościowe

- Przepustowość urządzenia - min. 175 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 250 Mpps.
- Tablica adresów MAC o pojemności co najmniej 32k wpisów.

- Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.

Wymagane funkcje

- Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.
- Obsługa Jumbo Frames.
- Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).
- Agregacja portów zgodna ze standardem 802.3ad.
- Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q.
- Obsługa routingu statycznego.
- Port-mirroring.
- Uwierzytelnianie 802.1x na poziomie portu.
- Uwierzytelnianie 802.1x w oparciu o adres MAC.
- W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN).
- W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.
- W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.
- Obsługa protokołu sFlow.

Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC

1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:
   - Centralne zarządzanie konfiguracją urządzenia
   - Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania
   - Centralne zarządzanie sieciami VLAN.
   - Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u
   - Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp..
   - Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.
   - Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego.
   - Automatyczna detekcja i rekomendacje konfiguracji.
   - Przesyłanie logów na zewnętrzny serwer syslog.
   - Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.
   - Obsługa białych i czarnych list adresów MAC.
   - Wykrywanie aplikacji komunikujących się w sieci.
2. Musi być możliwe redundantne połączenie z elementami zarządzającymi.
3. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.

Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa

- System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym.

- System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.

Gwarancja oraz wsparcie

1. System musi być objęty serwisem gwarancyjnym producenta przez okres min. 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Rozszerzone wsparcie serwisowe

1. System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres gwarancji.
2. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Wykonawca winien przedłożyć dokumenty:
   - Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
   - Certyfikat ISO 9001 podmiotu serwisującego.

Opisy do wymagań ogólnych

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Wykonawca winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż Wykonawca posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

Część 2 - Dostawa serwera NAS wraz z dyskami

Minimalna specyfikacja sprzętowa:

Procesor	Procesor 64 bit Intel x86 o takowaniu nie mniejszym niż 2.0 GHz
Procesor liczba rdzeni	Nie mniej niż 4
Pamięć RAM	Nie mniej niż 8GB DDR4
Pamięć RAM liczba slotów	Minimum 2 sloty
Pamięć RAM możliwość rozszerzenia	Nie mniej niż do 16GB
Pamięć Flash	Nie mniej niż 4GB

Liczba zatok na dyski twarde	Minimum 4
Obsługiwane dyski twarde	3.5" oraz 2.5" SATA oraz 2.5" SATA SSD
Pojemność dysków twardych	minimum do 18TB
Możliwość podłączenia modułu rozszerzającego	Tak, co najmniej 2
Porty LAN 2,5 GbE	Minimum 2
Diody LED	Minimum Status, LAN, HDD,
Porty USB 3.2 Gen 2	Minimum 2
Porty USB 2.0	Minimum 2
Port PCiE	Tak, minimum 1 Gen3
Przyciski	Reset, Zasilanie
Typ obudowy	RACK, 1U
Dopuszczalna temperatura pracy	od 0 do 40˚C
Wilgotność względna podczas pracy	5-95% R.H.
Zasilanie	Zasilacz redundatny max. 2 x 250 W, 100-240 V

Specyfikacja oprogramowania	
Agregacja łączy	Tak
Obsługiwane systemy plików	Dyski wewnętrzne: EXT4 Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+
Szyfrowanie wolumenów	Tak, min AES 256
Szyfrowanie dysków zewnętrznych	Tak
Zarządzanie dyskami	Pojedynczy Dysk, 0, 1, 5, 6, 10, JBOD, Obsługa Hot Spare per grupa RAID oraz global hot spare Rozszerzanie pojemności Online RAID Migracja poziomów Online RAID HDD S.M.A.R.T. Skanowanie uszkodzonych bloków (pliku) Przywracanie macierzy RAID Obsługa map bitowych Pula pamięci masowej Obsługa migawek Obsługa replikacji migawek
Wbudowana obsługa iSCSI	Multi-LUNs na Target Obsługa LUN Mapping & Masking Obsługa SPC-3 Persistent Reservation Obsługa MPIO & MC/S, Migawka / kopia zapasowa iSCSI LUN
Zarządzanie prawami dostępu	Ograniczenie dostępnej pojemności dysku dla użytkownika Importowanie listy użytkowników Zarządzanie kontami użytkowników Zarządzanie grupą użytkowników Zarządzanie współdzieleniem w sieci Tworzenie użytkowników za pomocą makr Obsługa zaawansowanych uprawnień dla podfolderów, Windows ACL

Obsługa Windows AD	Logowanie użytkowników poprzez CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web Funkcja serwera LDAP
Funkcje backup	Oprogramowanie do tworzenia kopii bezpieczeństwa producenta urządzenia dla systemów Windows, backup na zewnętrzne dyski twarde,
Współpraca z zewnętrznymi dostawcami usług chmury	Przynajmniej: Google Drive, Dropbox, Microsoft OneDrive, Microsoft OneDrive for Business i Box
Darmowe aplikacje na urządzenia mobilne	Monitoring / Zarządzanie / Współdzielenie plików / obsługa kamer / Odtwarzacz muzyki Dostępne na systemy iOS oraz Android
Minimum obsługiwane serwery	Serwer plików Serwer FTP Serwer WEB Serwer kopii zapasowych Serwer multimediów UPnP Serwer pobierania (Bittorrent / HTTP / FTP) Serwer Monitoringu
VPN	VPN client / VPN server. Obsługa PPTP, OpenVPN
Administracja systemu	Połączenia HTTP/HTTPS Powiadamianie przez e-mail (uwierzytelnianie SMTP) Powiadamianie przez SMS Ustawienia inteligentnego chłodzenia DDNS oraz zdalny dostęp w chmurze SNMP (v2 & v3) Obsługa UPS z zarządzaniem SNMP (USB) Obsługa sieciowej jednostki UPS Monitor zasobów Kosz sieciowy dla CIFS/SMB oraz AFP Monitor zasobów systemu w czasie rzeczywistym Rejestr zdarzeń System plików dziennika Całkowity rejestr systemowy (poziom pliku) Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line Aktualizacja oprogramowania Kopia zapasowa ustawień/przywracanie ustawień/resetowanie ustawień systemu
Wirtualizacja	Wbudowana aplikacja umożliwiająca tworzenie środowiska wirtualnego wraz z instalacją maszyn wirtualnych na systemach Windows, Linux i Android. Dostęp do konsoli maszyn za pośrednictwem przeglądarki z HTML5 Funkcjonalności importu, eksportu, klonowania i wykonywania migawek maszyn wirtualnych.
Konteneryzacja	Możliwość uruchomienia wirtualnych kontenerów dla LXC i Docker

Zabezpieczenia	Filtracja IP Ochrona dostępu do sieci z automatycznym blokowaniem Połączenie HTTPS FTP z SSL/TLS (Explicit) Obsługa SFTP Szyfrowanie AES 256-bit Szyfrowana zdalna replikacja (Rsync poprzez SSH) Import certyfikatu SSL Powiadomienia o zdarzeniach za pośrednictwem Email i SMS
Możliwość instalacji dodatkowego oprogramowania	Tak, sklep z aplikacjami; możliwość instalacji z paczek

Gwarancja	Min. 36 miesięcy, świadczona przez producenta rozwiązania
Dodatki	Szyny montażowe do szafy rack
Dyski (4 szt)	4 dyski o pojemności 8TB Dyski musza być klasy serwerowej (enterprise) Dyski SATA 6 Gbit/s Obroty minimalnie 7200 / min Dyski musza posiadać MTTF (MTBF) nie mniejszy niż 2 000 000h Pojemność pamięci cache minimum 256 MB Znamionowe roczne obciążenie pracą 550TB (rocznie) Parametr maksymalnej utrzymywanej prędkość przesyłu danych (deklarowana przez producenta dysków) : Dla technologii sektorowej 512e: 248 MiB/s dla pojemności 8TB Gwarancja musi zawierać opcje pozostawienie dysków w razie awarii przez cały okres trwania gwarancji. Należy dostarczyć z oferta oficjalne dokumenty producenta dysków, spełniających wszystkie powyższe wymagania.

Część 3 - Dostawa serwera wraz z oprogramowaniem

Minimalna specyfikacja: Pamięć ram minimum 16GB DDR4 ze wsparciem ECC, taktowanie pamięci nie mniejsze niż 3200 Mhz, możliwość zainstalowanie łącznie do 128GB pamięci, płyta powinna posiadać minimum 4 sloty na pamięć RAM

- Zainstalowany dwa dyski SSD klasy enterpise o pojemności minimum 960GB oraz dwa dyski SATA3 o pojemności nie mniejszej niż 2TB każdy
- Wszystkie dyski muszą pracować w kieszeniach hot swap, z możliwością wyjęcia w trakcie pracy
- Zainstalowany dedykowany kontroler do obsługi RAID, wymagane poziomy RAID to minimum: 0,1,5,6,10,50,60, kontroler musi posiadać wsparcie dla minimum 8 dysków SATA/SAS/NVME, cache minimum 4GB

- Zainstalowany procesor, posiadający minimum 6 rdzeni / 12 wątków, o taktowaniu minimum 3.5 GHz, osiągający w teście passmark minimum 20000 pkt.
- Zasilacze o mocy minimum 700W przeznaczony do pracy ciągłej 24/7 i pozwalający na utrzymanie wszystkich podzespołów serwera,
- Obudowa RACK o wysokości maksymalnej 2U, do zestawu dołączone szyny montażowe
- Obudowa musi posiadać minimum 8 slotów hot swap dla dysków twardych 3.5 cala
- Serwer musi posiadać wszelkie kable lub adaptery– musi być gotowy do pracy w momencie dostawy
- Serwer wyposażony w moduł zdalnego zarządzania pozwalający na dostęp do serwera z innych lokalizacji niż fizyczne położenie serwera
- Płyta główna powinna być przygotowana do obsługi minimum 1 procesora
- Wbudowany napęd dvd slim
- Wymagane złącze karty graficznej: VGA
- Serwer musi posiadać min. 36 miesięcy gwarancji onsite z czasem reakcji 24h, realizowaną w siedzibie Zamawiającego z opcją pozostawienia uszkodzonego dysku twardego u Zamawiającego
- Serwis musi być realizowany przez producenta lub autoryzowanego serwis partnera producenta
- Serwer musi posiadać w BIOSIe wpisane informacje na temat numeru seryjnego, producenta oraz modelu sprzętu
- Wymagane certyfikaty dla producenta serwera: ISO 9001, ISO 14001, CE
- Możliwość sprawdzenia na stronie producenta po podaniu numeru seryjnego: Okresu gwarancji, konfiguracji sprzętu oraz pobrania sterowników
- Karta sieciowa posiadająca 2 porty 1gb ethernet, złącza wyjściowe 2x RJ45
- Zainstalowany moduł TPM dedykowany do płyty
- Dołączony system Windows Server 2022 w wersji standard obsługujący wymaganą ilość rdzeni
- Dołączone licencje CAL na użytkownika w wersji Windows Server 2022, wymagana ilość licencji: 30

Część 4 - Dostawa zestawów komputerowych i laptopów z oprogramowaniem

Zestawy komputerowe minimalna specyfikacja – ilość 15 zestawów:

Procesor:	6 rdzeni, 12 wątków, taktowanie bazowe 2,6GHz, w trybie turbo 4,4GHz, 12MB cache, TDP – 65W, ze zintegrowaną kartą graficzną, osiągający wynik minimum 17100 punktów w teście PassMark – CPU Benchmarks opublikowany na stronie https://www.cpubenchmark.net/cpu_list.php
Chłodzenie procesora	Dostosowane do obsługi procesorów z TDP 95W
Pamięć RAM	Minimum 8 GB (DIMM DDR4, 3200MHz)
Płyta główna	2 sloty pamięci, obsługa do 64GB RAM, wbudowana karta sieciowa 1Gbit z obsługą WOL/PXE, 1x PCI Express 4.0 x16, 2x PCI Express x1, złącza na tylnym panelu: 2x PS, 1x DVI-D, 1x HDMI, 1x DP, 1x VGA, 6x USB z czego min. 2x USB 3.2 Gen1
BIOS	Zapisana trwale w BIOS informacja dotycząca nazwy producenta, numeru seryjnego i modelu.
Dysk	SSD PCIe NVMe, minimum 500GB, prędkość odczytu min. 3500MB/s, zapisu min. 2300MB/s
Napęd ODD	brak
Karta graficzna	Zintegrowana
Multimedia	Wbudowana karta dźwiękowa 8-kanałowa zgodna z High Definition,

Łączność	LAN 10/100/1000 Mbps z obsługą WOL/PXE
Obudowa	MiniTower (obsługa kart o pełnym profilu), zaprojektowana i wyprodukowana na zlecenie producenta komputera, suma wymiarów nie większa niż 945mm, 2x USB 3.2 Gen1, Mic-In, Phone-out, możliwość instalacji wewnątrz napędów 2x 3,5” + 1x 2,5”
Zasilacz	O mocy minimum 350W, spełnia wymagania normy 80 Plus Bronze, aktywne PFC. Głośność pracy (przy obciążeniu 20%/50%/100%): 21,6dB(A) / 21,8dB(A) / 30,4dB(A)
Klawiatura, mysz	Myszka USB 1000dpi, klawiatura USB – obie oznaczone trwałym logo producenta komputera
Właściwości specjalne	Możliwość zabezpieczenia linką, TPM 2.0, Windows AutoPilot ready
System operacyjny	W pełni będzie integrował się z istniejącą usługą Active Directory, w tym GPO (m.in. automatyzacja procesów instalacji oprogramowania). Wykonawca ma obowiązek dostarczyć sprzęt z systemem operacyjnym Windows 10 Pro PL (wersja 64 – bitowa). Klucz systemu musi być zapisany trwale w BIOS i umożliwiać instalację systemu operacyjnego z nośnika lub napędu lub zdalnie bez potrzeby ręcznego wpisywania klucza licencyjnego.
Certyfikaty	CE, ISO 9001, ISO 14001 Zgodność: SMBios (DMI), EN62368-1, EN55032, EN55035, EN61000-3-2/3, EN62623, 89/336/ECC
Gwarancja	Min. 12 miesięcy. Gwarancja musi być realizowana przez producenta lub autoryzowanego serwis-partnera producenta. Możliwość sprawdzenia konfiguracji oraz okresu gwarancji na stronie producenta po podaniu numeru seryjnego sprzętu.
Wymagania dodatkowe:	Sprzęt fabrycznie nowy, oryginalnie zapakowany, bez śladów użytkowania, trwale oznaczony logo producenta. Możliwość pobrania sterowników oraz obrazu systemu ze strony producenta po podaniu numeru seryjnego. Sprzęt wyprodukowany w Europie, nie wcześniej niż w 2022 roku. Na sprzęcie powinien być umieszczony symbol legalności systemu operacyjnego w formie naklejki/hologramu potwierdzający jego autentyczność
Monitor	23,8”, matryca IPS, Full-HD, czas reakcji 5ms, kontrast dynamiczny – 30 000 000:1 (DCR), plamka 0,2745mm Złącza VGA, HDMI Wbudowane głośniki Możliwość pochylenia ekranu w zakresie -5 ° - 20 ° Funkcja Flicker-Free oraz Anti-Blue-Light VESA 100x100 Zużycie energii - <0,3W (wyłączony), <0,5W (standby) Opatrzony logiem producenta komputera Kabel HDMI i Audio w komplecie. Gwarancja min. 12 miesięcy – w przypadku usterki zawsze wymiana monitora na nowy na miejscu u klienta. Gwarancja musi być realizowana przez producenta lub autoryzowanego serwis-partnera producenta. Możliwość sprawdzenia okresu gwarancji na stronie producenta po podaniu numeru seryjnego sprzętu.

Pakiet biurowy	Microsoft Office 2021 Licencja komercyjna, wieczysta

Komputery przenośne – laptopy – ilość 3 szt.:

Typ:	Komputer przenośny
Zastosowanie:	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, dostępu do Internetu oraz poczty elektronicznej.
Ekran:	15,6" o rozdzielczości FHD (min. 1920x1080 przy 60Hz) z powłoką przeciwodblaskową
Procesor:	4 rdzenie, 8 wątków, ze zintegrowaną grafiką, taktowanie bazowe 1,6GHz, w trybie turbo 4,2GHz, 6MB cache, osiągający w teście PassMark CPU Mark wynik min. 6350 punktów (należy dołączyć wydruk ze strony https://www.cpubenchmark.net z wynikiem testu dla oferowanego procesora). Pobór mocy TDP nie większy niż 15W.
Pamięć operacyjna:	min. 8GB, 1 slot wolny, możliwość rozbudowy pamięci do 32GB
Parametry pamięci masowej:	Dysk SSD PCIe/NVMe o pojemności min. 500GB, prędkość odczytu/zapisu: 3500/2300 MB/s
Karta graficzna:	Zintegrowana z procesorem z dynamicznie przydzielaną pamięcią współdzieloną.
Wyposażenie multimedialne:	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, wbudowane głośniki
Płyta główna:	Wyposażona przez producenta w dedykowany chipset dla oferowanego procesora.
Napęd:	Wbudowany napęd DVD±RW
Komunikacja:	Wbudowana karta sieci bezprzewodowej 802.11 a/b/g/n/ac, moduł Bluetooth w wersji min. 5.0, karta sieciowa 10/100/1000 ze złączem RJ-45, możliwość instalacji modemu LTE wewnątrz obudowy (nie dopuszcza się modemu podłączanego do portu USB)
Klawiatura:	Układ klawiszy US, możliwość 4 stopniowej regulacji podświetlenia oraz zmiany koloru podświetlenia, wydzielony blok klawiszy numerycznych
Bateria i zasilanie:	Komputer wyposażony w baterię o pojemności min. 41Wh umożliwiającą pracę przez min. 360 minut (wg. danych producenta) oraz zasilacz. Możliwość wyjęcia i wymiany baterii bez otwierania laptopa.
Gwarancja:	Min. 12 miesięcy door-to-door. Gwarancja musi być realizowana przez producenta lub autoryzowanego serwis-partnera producenta. Możliwość sprawdzenia konfiguracji oraz okresu gwarancji na stronie producenta po podaniu numeru seryjnego sprzętu.
Certyfikaty:	Certyfikat CE, ISO14001, ISO9001 lub równoważne
System operacyjny:	W pełni będzie integrował się z istniejącą usługą Active Directory, w tym GPO (m.in. automatyzacja procesów instalacji oprogramowania). Wykonawca ma obowiązek dostarczyć sprzęt z systemem operacyjnym Windows 11 Pro PL (wersja 64 – bitowa). Klucz systemu musi być zapisany trwale w BIOS i umożliwiać instalację systemu operacyjnego z nośnika lub napędu lub zdalnie bez potrzeby ręcznego wpisywania klucza licencyjnego.

Wymagania dodatkowe:	Wbudowana kamera internetowa trwale zainstalowana w obudowie matrycy, wejście audio, wbudowany mikrofon, wbudowane głośniki, czytnik kart pamięci, złącza USB – min. 4 szt. w tym 1x USB 3.1 Type-C i 1x USB 3.1 Type-A, wyjście HDMI, wyjście VGA, Touchpad, TPM 2.0, gniazdo Kensington Lock, waga max 2,2 kg, sprzęt fabrycznie nowy, oryginalnie zapakowany, bez śladów użytkowania. Możliwość pobrania sterowników oraz obrazu systemu ze strony producenta po podaniu numeru seryjnego. Sprzęt wyprodukowany w Europie, nie wcześniej niż w 2022 roku. Laptop trwale oznaczony logo producenta. Mysz bezprzewodowa Na sprzęcie powinien być umieszczony symbol legalności systemu operacyjnego w formie naklejki/hologramu potwierdzający jego autentyczność
Pakiet biurowy	Microsoft Office 2021 Licencja komercyjna, wieczysta

Komputer przenośny – laptop – ilość 1 szt.:

Nazwa komponentu	Wymagane minimalne parametry techniczne
Typ:	Komputer przenośny
Zastosowanie:	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, dostępu do Internetu oraz poczty elektronicznej.
Ekran:	15,6" o rozdzielczości FHD (min. 1920x1080 przy 60Hz) z powłoką przeciwodblaskową, matryca WVA, kąty widzenia $170^0/170^0$
Procesor:	4 rdzenie, 8 wątków, ze zintegrowaną grafiką, cache 12MB, osiągający w teście PassMark CPU Mark wynik min. 10500 punktów (należy dołączyć wydruk ze strony https://www.cpubenchmark.net z wynikiem testu dla oferowanego procesora)
Pamięć operacyjna:	min. 16GB z możliwością rozbudowy do 32GB, jeden slot wolny
Parametry pamięci masowej:	Dysk SSD PCIe NVMe o pojemności min. 500GB, prędkość odczytu/zapisu: 3500/2300 MB/s Dysk HDD 2,5” 2TB SATA3
Karta graficzna:	Zintegrowana z procesorem z dynamicznie przydzielaną pamięcią współdzieloną.
Wyposażenie multimedialne:	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, wbudowane głośniki
Płyta główna:	Wyposażona przez producenta w dedykowany chipset dla oferowanego procesora.
Napęd ODD:	brak
Komunikacja:	Wbudowana karta sieci bezprzewodowej 802.11 a/b/g/n/ac/ax, moduł Bluetooth w wersji min. 5.2, karta sieciowa 10/100/1000 ze złączem RJ-45
Klawiatura:	Układ klawiszy US, możliwość 4 stopniowej regulacji podświetlenia oraz zmiany koloru podświetlenia, wydzielony blok klawiszy numerycznych
Bateria i zasilanie:	Komputer wyposażony w baterię o pojemności min. 73Wh (umożliwiającą pracę do 16 godzin wg. danych producenta) oraz zasilacz.
Gwarancja:	Min. 12 miesięcy door-to-door. Gwarancja musi być realizowana przez producenta lub autoryzowanego serwis-partnera producenta.

	Możliwość sprawdzenia konfiguracji oraz okresu gwarancji na stronie producenta po podaniu numeru seryjnego sprzętu.
Certyfikaty:	Certyfikat CE, ISO14001, ISO9001 lub równoważne
System operacyjny:	Zainstalowany i aktywowany system operacyjny z wieczystą licencją w polskiej wersji językowej zapewniający dostęp do domeny. Klucz systemu musi być zapisany trwale w BIOS i umożliwiać instalację systemu operacyjnego z nośnika bezpośrednio z wbudowanego złącza lub napędu lub zdalnie bez potrzeby ręcznego wpisywania klucza licencyjnego. W pełni będzie integrował się z istniejącą usługą Active Directory, w tym GPO (m.in. automatyzacja procesów instalacji oprogramowania). System operacyjny ma pozwalać na uruchomienie i pracę z większością aplikacji biurowych dostępnych na rynku. Pełna polska wersja językowa. Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta systemu. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi). Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników
Wymagania dodatkowe:	Wbudowana kamera internetowa trwale zainstalowana w obudowie matrycy, wbudowany mikrofon i głośniki, czytnik kart pamięci, czytnik linii papilarnych, złącza USB – min. 4 szt. w tym 1x USB 3.2 Gen2 Type-A, 1x USB 3.2 Gen2 Type-C i 1x Thunderbolt 4, wyjście HDMI, Touchpad, TPM 2.0, gniazdo Kensington Lock, waga max 1,7 kg, sprzęt fabrycznie nowy, oryginalnie zapakowany, bez śladów użytkowania. Możliwość pobrania sterowników oraz obrazu systemu ze strony producenta po podaniu numeru seryjnego. Sprzęt wyprodukowany w Europie, nie wcześniej niż w 2022 roku. Laptop trwale oznaczony logo producenta. Mysz bezprzewodowa. Na sprzęcie powinien być umieszczony symbol legalności systemu operacyjnego w formie naklejki/hologramu potwierdzający jego autentyczność
Pakiet biurowy	Microsoft Office 2021 Licencja komercyjna, wieczysta

Część 5 - Dostawa oprogramowania

Oprogramowanie do backupu – minimalne wymagania:

- Oprogramowanie może być dostarczane w dwóch scenariuszach:
  - Cloud(Software as Service),
  - On-premise.
- Istnieje możliwość migracji w obie strony pomiędzy środowiskiem on-premise oraz cloud.
- Interfejs systemu dostępny jest w języku:
  - polskim,
  - angielskim,
- Oprogramowanie nie preferuje platformy sprzętowej, nie jest profilowane pod konkretnego dostawcę sprzętu serwerowego oraz pamięci masowych,

- Oprogramowanie może być uruchomione w kontenerze docker,
- Możliwość instalacji oraz uruchomienia serwera zarządzania na hostach fizycznych, maszynach wirtualnych czy też kontenerach docker opartych o systemy:
  - Debian: 9+
  - Ubuntu: 16.04+
  - Fedora: 29+
  - centOS: 7+
  - RHEL: 6+
  - openSUSE: 15+
  - SUSE Enterprise Linux (SLES): 12 SP2+
  - Windows Client: 7, 8.1, 10 (1607+)
  - Windows Server: 2008 R2+,
- System wykonuje kopię własnej bazy danych, która umożliwia odtworzenie wszystkich ustawień i całej konfiguracji,
- Oprogramowanie działa w architekturze wykluczającej pojedynczy punkt awarii(awaria jednego z komponentów nie spowoduje przestoju),

Wsparcie techniczne:

- Pomoc techniczna w językach:
  - polskim,
  - angielskim.
- Materiały samopomocowe:
  - Baza wiedzy:
    - polski,
    - angielski

Zarządzanie:

- Zarządzanie całością działania systemu (backup, przywracanie)z poziomu jednej konsoli webowej,
- Zarządzanie całym systemem poprzez dashboardy,
- Gradacja uprawnień kont administratorów z poziomu panelu zarządzającego,
- System posiada wbudowane predefiniowane zadania backupowe,
- System umożliwia tworzenie zadań backupowych w oparciu o kalendarz,
- Automatyczne oraz ręczne uruchamianie kopii zapasowych zgodnie z ustalonym harmonogramem,
- Automatyczne oraz ręczne uruchamianie procesu przywracania zgodnie z ustalonym harmonogramem,
- Monitorowanie postępu działania zadania,
- Posiada system powiadamiania poprzez e-mail o zdarzeniach w następujących przypadkach:
  - Zadanie zostało zakończone pomyślnie,
  - Zadanie zostało zakończone z ostrzeżeniami,
  - Zadanie zostało zakończone z błędem,
  - Zadanie zostało anulowane,
  - Zadanie nie zostało uruchomione.
- System generuje alerty na konsoli WEB w przypadku zaistnienia określonego zdarzenia systemowego.

- Możliwość zdefiniowania okna backupowego dla każdego z zadań,
- Oprogramowanie posiada wbudowany menadżer haseł do przechowywania kluczy szyfrujących oraz poświadczeń do magazynów,
- System pozwala na klonowanie planów kopii zapasowych,
- System umożliwia reset hasła administratora w przypadku jego utraty,
- Oprogramowanie umożliwia definiowanie retencji według schematów:
  - GFS(Grandfather-Father-Son),
  - FIFO(First-In, First-Out).
- Oprogramowanie umożliwia tworzenie kont użytkowników nie będących administratorami,
- Konta użytkowników mogą być tworzone poprzez import pliku CSV,
- Oprogramowanie umożliwia tworzenie grup urządzeń,
- Oprogramowanie zapewnia zoptymalizowaną trasę transmisji danych poprzez możliwość wybrania dowolnego workera(urządzenia, które odpowiadać będzie za pobieranie danych z konkretnych usług) oraz browsera(urządzenia, które będzie wykorzystywane do przeszukiwania m.in. magazynów).
- System pozwala na zarządzanie multi-tenantowe - umożliwia tworzenie wielu kont administracyjnych z dedykowanymi rolami oraz uprawnieniami, jak m. in.:
  - System Administrator,
  - Backup operator,
  - Restore operator,
  - Viewer.

Składowanie danych:

- Oprogramowanie jest systemem multi-storageowym i umożliwia tworzenie wielu repozytoriów danych jednocześnie z poziomu jednej konsoli,
- System umożliwia składowanie danych:
  - Lokalnie:
    - Zasób SMB,
    - Zasób NFS,
    - Zasób ISCSI,
    - Zasób S3,
    - Katalog zabezpieczonego urządzenia.
  - W chmurze:
    - Amazon Web Service,
    - Magazyn zgodny z S3,
    - Dostarczanej bezpośrednio przez producenta.
- System pozwala na zdefiniowanie zapasowej ścieżki repozytorium, na wypadek niedostępności głównej lokalizacji,
- System oferuje mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykle.
- System pozwala na replikację pomiędzy dowolnymi wspieranymi magazynami według ustalonego przez administratora harmonogramu.

Odtwarzanie:

- Odtwarzanie granularne:
  - Pojedynczych plików z kopii obrazu dysku,

- Pojedynczych wiadomości z kopii skrzynki pocztowej Microsoft 365,
- Wykorzystanie funkcjonalności Bare Metal Restore(kopii zapasowej całego dysku - łącznie z partycjami i danymi startowymi) dla odtwarzania systemu po awarii, wsparcie dostępne jest dla systemów:
  - Windows: 7+,
  - Windows Server: 2008 R2+,
- Odtwarzanie Bare metal Restore może odbywać się na takim samym sprzęcie, jak ten który był backupowany, jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników oraz z możliwością dodania sterowników przez użytkownika.
- Uruchamianie procesu Bare Metal Restore odbywa się z bootowalnej płyty CD lub pendrive'a,
- Oprogramowanie umożliwia odtwarzanie systemu w scenariuszach: P2P, P2V, V2P, V2V.
- Oprogramowanie umożliwia odtwarzanie kopii obrazu dysku w wybranym formacie(VHD, VHDX, VMDK),
- Odtwarzanie zasobów plikowych bez praw dostępu(tzw. ACL),
- Odtwarzanie zasobów plikowych z prawami dostępu,
- Przywracanie plików pomiędzy systemami operacyjnymi(np. odtwarzanie danych plikowych Linux na systemie Windows),
- Odtwarzanie danych według harmonogramu,
- Przywracanie danych z określonego urządzenia/użytkownika,
- Przywracanie kopii z wybranego magazynu.
- Przywracanie danych Microsoft 365:
  - do wskazanej, dowolnej lokalizacji, na wybranym urządzeniu w formie pliku:
    - pst,
    - mbox.
  - do istniejącego konta w usłudze Microsoft 365 (tego samego lub innego, w tym w innej organizacji),
- System posiada możliwość nieodwracalnego kasowania danych,
- Przywracanie repozytoriów GIT:
  - Przywracanie pomiędzy hostingami repozytoriów(GitHub/BitBucket),
  - przywracanie między kontami.

Backup:

- Wykonywanie pełnych, różnicowych, przyrostowych kopii zapasowych, a także backupu syntetycznego dla:
  - Systemów operacyjnych:
    - Alpine 3.10+,
    - Debian: 9+,
    - Ubuntu: 16.04+,
    - Fedora: 29+,
    - centOS: 7+,
    - RHEL: 6+,
    - openSUSE: 15+,
    - SUSE Enterprise Linux(SLES): 12 SP2+,
    - macOS: 10.13+,
    - Windows: 7, 8.1, 10(1607+),
    - Windows Server: 2008 R2+,

  - Środowisk wirtualnych:
    - Hyper-V,
    - VMware: 6.7+.
    - Dowolne inne w sposób agentowy
  - Repozytoriów GIT:
    - GitHub,
    - Bitbucket.
- Wykonywanie pełnych, różnicowych oraz przyrostowych oraz logów transakcyjnych kopii zapasowych dla:
  - Baz danych:
    - Microsoft SQL,
    - MySQL,
    - PostgreSQL,
    - Firebird,
    - Dowolnych innych przez podpięcie skryptów pre/post.
- Szyfrowanie danych wykonywana po stronie stacji roboczej za pomocą algorytmu AES w trybie CBC z kluczem szyfrującym o długości:
    - 128 bit,
    - 192 bit,
    - 256 bit.
- Kompresja danych wykonywana po stronie stacji roboczej za pomocą algorytmów:
    - ZStandard,
    - LZ4.
- Oprogramowanie umożliwia zarządzanie poziomem kompresji,
- Wykonywanie kopii zapasowej otwartych plików(VSS),
- System umożliwia uruchamianie skryptów przed i po backupie,
- System umożliwia uruchamianie skryptów po wykonaniu migawki VSS,
- System umożliwia automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku błędów,
- Backup jednego oraz wielu dysków/całego systemu operacyjnego(Windows) ze wsparciem dla partycji MBR oraz GPT,
- Backup plikowy,
- Oprogramowanie realizuje funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie dyskowe,
- Oprogramowanie umożliwia konsolidację wersji kopii zapasowych,
- Oprogramowanie zapewnia backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia,
- Oprogramowanie pozwala na automatyczne uruchomienie kopii zapasowej podczas zamykania systemu operacyjnego.
- Oprogramowanie pozwala na backup zaszyfrowanych partycji.
- GIT
- Oprogramowanie zapewnia wsparcie dla repozytoriów lokalnych oraz zdalnych(dostępnych w usługach zewnętrznych),
- Oprogramowanie umożliwia zabezpieczenie metadanych repozytoriów(w zależności od zabezpieczanej usługi m.in.: issues, pull requests, actions/pipelines, wiki).

Licencjonowanie:

- Sposób licencjonowania opiera się na:
  - Ilości serwerów/endpointów- dla fizycznych urządzeń,
  - Ilości fizycznych hostów - dla środowisk wirtualnych,
  - Ilości repozytoriów - dla GIT.
- Licencje w wersji dożywotniej powinny pozwalać na :
  - zabezpieczenie 4 fizycznych serwerów
  - zabezpieczenie 30 fizycznych endpointów
- Wsparcie techniczne:
- Świadczone jest w języku polskim, bezpośrednio przez główną siedzibę producenta,
- Zapewnia dostęp do aktualizacji oprogramowania,
- Umożliwia korzystanie z połączeń zdalnych, systemu ticketowego oraz wsparcia telefonicznego,
- Obowiązuje przez okres min. 12 miesięcy.

Oprogramowanie do zarządzania infrastrukturą informatyczną – minimalne wymagania:

- 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.
- 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 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 przypisywania wybranych jednostek organizacyjnych, Jednostek lokalizacyjnych oraz typów zasobów do poszczególnych użytkowników konsoli. Wszelkie raporty, zestawienia oraz funkcje obejmują wtedy tylko w/w przypisane 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, predefiniowane atrybuty komputera.
- 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 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 okresowe skanowanie aktualnie uruchomionych procesów systemowych wraz z historią występowania procesu podczas wcześniejszych skanów.
- 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.

Zarządzanie zasobami oraz użytkownikami

- Oprogramowanie musi umożliwiać klonowanie wybranych typów zasobów
- 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 zdefiniowanie dodatkowych atrybutów dla wybranych relacji pomiędzy zasobami w zakresie zgodnym z atrybutami typów 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) 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.

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 musi umożliwiać optymalizację dystrybucji zadań oraz plików na komputery, pobierając brakujące fragmenty plików od agentów z tej samej podsieci (mechanizm peer-to-peer).
- Oprogramowanie w zakresie automatyzacji musi realizować m.in. następujące przypadki użycia z wykorzystaniem mechanizmu grup dynamicznych dla zadań oraz polis:
  1. 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)
  2. 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)
  3. 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
  4. 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.
  5. 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.

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 użytkowników

- 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 zostać dostarczony w technologii PHP w formie otwartych źródeł z możliwością samodzielnej edycji kodu.
- 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 edycję kilku zgłoszeń jednocześnie po wyborze z listy zgłoszeń.
- 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 administratorowi ustalanie statusów i priorytetów z zaznaczeniem, które z nich może używać użytkownik zgłaszający problem.
- Oprogramowanie musi umożliwiać przesyłanie użytkownikom powiadomień pocztą elektroniczną o nowych wpisach i zmianach w zgłoszeniu.
- Oprogramowanie musi umożliwiać obsługę autoryzacji OAuth 2.0 w zakresie powiadomień mailowych oraz rejestracji zgłoszeń drogą mailową.
- 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 określenie widoczności poszczególnych statusów i priorytetów 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.
- Zapisane przez administratora rozwiązania incydentów tworzą bazę wiedzy (powiązaną z kategoriami) Baza ta wyświetlana jest użytkownikom podczas przeglądania kategorii zgłoszeń. 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. telefonicznie informuje, że zepsuł mu się komputer).
- 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 dostęp lub ograniczenie dostępu do ogłoszeń lub bazy wiedzy dla anonimowego użytkownika.
- Oprogramowanie musi umożliwiać tworzenia baz umów serwisowych powiązanych z bazami firm serwisowych (dostawców sprzętu, oprogramowania, lokalnych serwisów). Możliwość powiązania każdej umowy z zakupionymi licencjami oprogramowania 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 klonowanie zgłoszeń.
- 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 umożliwiać wyświetlenie w panelu WWW operatora HelpDesk informacji nt. aktywności zarejestrowanych stanowisk (on-line/off-line) oraz alertów dotyczących obciążenia CPU, RAM, HDD.
- Oprogramowanie musi posiadać wbudowane raporty prezentujące m.in. realizację obsługi zgłoszeń w zakładanym SLA (statystyka miesięczna, kwartalna, roczna).

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

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.

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 min. 12 miesięcznym supportem producenta, 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 30 stanowisk komputerowych 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 1 licencje dostępową 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 od Wykonawcy, aby w terminie 90 dni od podpisania umowy przeprowadził wdrożenie systemu zdalnie lub w siedzibie Zamawiającego
- Zamawiający wymaga od Wykonawcy, aby w terminie 90 dni od podpisania umowy przeprowadził szkolenie z obsługi systemu zdalnie lub w siedzibie Zamawiającego

Część 6 - Dostawa urządzeń drukujących

Urządzenie wielofunkcyjne laserowe A4 – 1 szt.

Minimalne wymagania techniczne:

- **Przeznaczenie produktu:** Do domu i małego biura
- **Technologia druku:** Laserowa, monochromatyczna
- **Obsługiwany typ nośnika:** Papier zwykły
- **Obsługiwane formaty nośników:** A4, A5, A6, Letter, Formaty niestandardowe
- **Podajnik papieru:** 250 arkuszy
- **Rodzaje podajników papieru:** Kasetowy + tacka
- **Liczba podajników papieru:** 2
- **Odbiornik papieru:** 120 arkuszy
- **Szybkość druku w mono:** do 34 str./min
- **Maksymalna rozdzielczość druku:** 2400 x 600 dpi
- **Maksymalna rozdzielczość kopiowania:** 600 x 600 dpi
- **Szybkość kopiowania:** do 34 str./min
- **Rozdzielczość skanowania:** 1200 x 1200 dpi
- **Podajnik dokumentów skanera:** Tak (ADF)
- **Maksymalny format skanu:** A4
- **Skanowanie bezpośrednio do e-mail:** Tak
- **Maksymalna gramatura papieru:** 230 g/m²
- **Funkcja faksu:** Tak
- **Druk dwustronny (dupleks):** Automatyczny
- **Interfejsy:** USB, Wi-Fi, LAN (Ethernet),
- **Wyświetlacz:** Wbudowany
- **Dołączone akcesoria:** Kabel zasilający, Toner startowy
- **Kolor:** Czarny
- **Gwarancja:** min. 12 miesięcy
- **Wydajność tonera:** 3000 stron, startowego 1200 stron.

Urządzenie wielofunkcyjne laserowe kolorowe A3/A4 – 1 szt.

- Technologia Laser Kolor
- Prędkość drukowania i kopiowania 35 stron na minutę A4 w kolorze i mono; dwustronnie: 35 stron na minutę A4 w kolorze i mono;
- Rozdzielczość 1200 x 1200 dpi (drukowanie)
- 600 x 600 dpi (skan/kopia)
- Czas nagrzewania Ok. 18 sekund lub mniej
- Czas pierwszego wydruku Ok. 7 sekund w mono, ok. 9,2 sekundy w kolorze
- Czas pierwszej kopii Ok. 7,4/ 9,8 sekund lub mniej w mono / kolorze (DP)
- Ok. 6,4/ 8,5 sekund lub mniej w mono / kolorze (szyba)
- Napięcie zasilania AC 220 V – 240 V, 50/60 Hz
- Poziom hałasu (ISO 7779) (poziom ciśnienia akustycznego: ISO 7779 odległość pomiarowa 1 metr)
- Kopiowanie/Drukowanie: 48,3 dB (A) w kolorze
- Certyfikaty GS, TÜV, CE – urządzenie jest produkowane zgodnie z normami jakości ISO 9001, ochrony środowiska ISO 14001
- Pamięć Standard 4GB + 32GB SSD, 320GB HDD opcjonalnie

OBSŁUGA PAPIERU

- Pojemność wejściowa taca uniwersalna na 150 ark. 52–300 g/m², (baner 136-165 g/m²) A6R – SRA3 (320 x 450 mm), zakładki (136 – 256 g/m²), baner maks. 320 x 1,220 mm;
- podajnik kasetowy 2 x 500 ark., 52-300 g/m², podajnik górny A6R – A4R,
- podajnik dolny A6R – SRA3
- Moduł dupleksu W standardzie, obsługa papieru A6R-SRA3 (320 x 450 mm), 64–256 g/m²
- Pojemność wyjściowa Standardowo 500 ark. wydrukiem do dołu, maksymalnie 4300 arkuszy
- Dodatkowe informacje Wszystkie podane pojemności dotyczą papieru o grubości 0,11 mm

DRUKOWANIE

- Procesor 1.0GHz
- Emulacje PCL 6 (PCL5c / PCL-XL), KPDL3 (zgodne z Postscript 3), bezpośrednie drukowanie XPS, PDF oraz Open XPS
- Czcionki - 93 czcionki konturowe (PCL), 136 czcionek (KPDL3), 8 czcionek (Windows Vista), 1 czcionka bitmapowa, 45 typów jednowymiarowych kodów kreskowych plus dwuwymiarowy kod (PDF-417)
- Dodatkowe możliwości drukowania
- Szyfrowany druk bezpośredni PDF, drukowanie IPP, e-mail printing, WSD, wydruk bezpieczny przez SSL, IPSec, SNMPv3, szybka kopia, wydruk próbny, wydruk prywatny, przechowywanie i zarządzanie pracami
- Protokoły Drukowanie mobilne: Mobile Print app dla iOS i Android, AirPrint, Mopria, NFC, Direct WiFi, Google cloud print
- Obsługiwane Systemy Operacyjne (wydruk)Wszystkie bieżące wersje Microsoft Windows, Mac OS X wersja 10.9 lub wyższa, UNIX, LINUX oraz inne według potrzeb

KOPIOWANIE

- Maksymalny rozmiar oryginału A3
- Dodatkowe możliwości kopiowania Skanuj-raz-kopiuj-wielokrotnie, sorter elektroniczny, funkcja 2w1 / 4w1,

- powtarzanie obrazu, numerowanie stron, tryb okładek, broszura, tryb pilnej kopii, łączenie obrazów, funkcja stempla, pomijanie pustych stron, kopiowanie dowodów osobistych
- Typy ekspozycji Automatyczna, ręczna: 16 stopni
- Współczynniki zoom 5 zmniejszeń/5 powiększeń
- Zakres zoom 25 – 400 % co 1 %
- Kopiowanie ciągłe 1–9999
- Ustawienia obrazu tekst, zdjęcie, tekst + zdjęcie, mapa

SKANOWANIE

- Typ pliku PDF (skompresowany, szyfrowany, PDF/A, PDF/A-1a/b), TIFF, JPEG, Open XPS, PDF przeszukiwalny (opcja), plik MS Office(opcja)
- Rozpoznawanie oryginału Tekst + zdjęcie, zdjęcie, tekst, jasny tekst, tekst (zoptymalizowany pod OCR)
- Maksymalny format skanowania A3
- Funkcjonalności Skanera Skan do e-mail, skan do FTP, skan do SMB, skan do USB Host, skan do skrzynki, TWAIN sieciowy, skan WSD
- Dostępne rozdzielczości: 600dpi x 600dpi , 400dpi x 400dpi , 200dpi x 400dpi, 300dpi x 300dpi , 200dpi x 200dpi , 200dpi x 100dpi
- 256 odcieni szarości
- Prędkość skanowania 180 obrazów na minutę (300 dpi, A4, duplex, mono, kolor,)

INTERFEJSY

- Standardowo
- USB Host 2.0, Fast Ethernet 10Base-T/100BaseTX/1000BaseT,
- gniazdo dodatkowej karty sieciowej, gniazdo na kartę SD, gniazdo na opcjonalną kartę
- faksu

Urządzenie zawiera szafkę i komplet tonerów

Gwarancja: min. 12 miesięcy