Załącznik nr 1 – opis przedmiotu zamówienia

Dotyczy: Realizacji projektu grantowego „Cyberbezpieczny Samorząd”
Umowa o powierzenie grantu o numerze FERC.02.02-CS.01-001/23/2218/ FERC.02.02-CS.01-001/23/2024

Opis przedmiotu zamówienia

„Zakup urządzeń i oprogramowania” dla Gminnego Ośrodka Pomocy Społecznej w Szczytnikach w ramach projektu Cyberbezpieczny Samorząd

Spis

I. Dostawa, wdrożenie i konfiguracja serwera wraz z systemem operacyjnym oraz licencjami dostępowymi

1) Urządzenia muszą być fabrycznie nowe, pochodzić z autoryzowanego kanału sprzedaży producenta i reprezentować model bieżącej linii produkcyjnej. Nie dopuszcza się urządzeń: odnawianych, demonstracyjnych lub powystawowych.

2) Nie dopuszcza się urządzeń posiadających wadę prawną w zakresie pochodzenia sprzętu, wsparcia technicznego i gwarancji producenta.

3) Elementy, z których zbudowane są urządzenia muszą być produktami producenta urządzeń lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta serwera.

4) Urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach producenta.

5) Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w języku polskim lub angielskim w formie papierowej lub elektronicznej.

6) Urządzenia na etapie dostawy pomiędzy producentem, a zamawiającym nie mogą podlegać modyfikacjom.

Serwer o poniższej charakterystyce:

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	• Obudowa Rack o wysokości max 1U z możliwością instalacji min. 8 dysków 2.5” • Obudowa wyposażona w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze. • Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne.
Płyta główna	• Płyta główna z możliwością zainstalowania do dwóch procesorów. • Obsługa procesorów 32 rdzeniowych. • Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. • Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. • Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Chipset	• Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
Procesor	• Zainstalowany jeden procesor 16-rdzeniowy, min. 2.8 GHz (częstotliwość bazowa), klasy x86, dedykowany do pracy z zaoferowanym serwerem, umożliwiający osiągnięcie wyniku min. 335 w

	teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.
RAM	• Minimum 128 GB DDR5 RDIMM 5600MT/s,
Funkcjonalność pamięci RAM	• Demand Scrubing, • Patrol Scrubing, • Permanent Fault Detection
Gniazda PCI	• minimum jeden slot PCIe x16 generacji 4
Kontroler RAID	• Sprzętowy kontroler dyskowy, posiadający o Min. 8 GB nieulotnej pamięci cache, o Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60. o Wsparcie dla dysków samoszyfrujących
Dyski twarde	• Zainstalowane o 3 x dysk SSD SATA o pojemności min. 960 GB, 6Gb, 2,5“ Hot-Plug. o 3 x dysk SAS o pojemności min. 2.4TB, 12Gb, 10 tys. obr./min., 2,5“ Hot-Plug. • Możliwość zainstalowania dwóch dysków M.2 NVMe SSD o pojemności min. 960GB z możliwością konfiguracji RAID 1.
Interfejsy sieciowe/FC/SAS	• Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT • 2 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) • W zestawie z serwerem muszą znajdować się 2 kable DAC 10GbE SFP+/SFP+ min. 3m, dostarczone przez producenta serwera • W zestawie z serwerem wykonawca dostarczy 3 patchcordy RJ-45 cat 6 o długości minimum 3m
Elementy montażowe	• Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych • Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych
Wbudowane porty	• 4 x USB z czego nie mniej niż 1x USB 3.0, • 2x VGA
Video	• Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
Zasilacze	• Redundantne, Hot-Plug min. 700W klasy Titanium
System operacyjny/dodatkowe oprogramowanie	• Dostarczona przez producenta oferowanego serwera licencja na Windows Server 2022 Standard, licencja dożywotnia pokrywająca wszystkie fizyczne rdzenie w serwerze

	• Wraz z serwerem zamawiający wymaga dostarczenia 5 licencji CAL na użytkowników
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 • Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem • Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).
Karta Zarządzania	• Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: o zdalny dostęp do graficznego interfejsu Web karty zarządzającej; o zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); o szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; o możliwość podmontowania zdalnych wirtualnych napędów; o wirtualną konsolę z dostępem do myszy, klawiatury; o wsparcie dla IPv6; o wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; o możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; o możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; o integracja z Active Directory; o możliwość obsługi przez dwóch administratorów jednocześnie; o wsparcie dla dynamic DNS; o wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.

	○ możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera ○ możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera oraz z możliwością rozszerzenia funkcjonalności o: ○ Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej ○ Przesyłanie danych telemetrycznych w czasie rzeczywistym ○ Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze ○ Automatyczna rejestracja certyfikatów (ACE)
Oprogramowanie do zarządzania	• Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: ○ Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych ○ integracja z Active Directory ○ Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta ○ Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish ○ Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram ○ Szczegółowy opis wykrytych systemów oraz ich komponentów ○ Możliwość eksportu raportu do CSV, HTML, XLS, PDF ○ Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. ○ Grupowanie urządzeń w oparciu o kryteria użytkownika ○ Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji ○ Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach ○ Szybki podgląd stanu środowiska ○ Podsumowanie stanu dla każdego urządzenia ○ Szczegółowy status urządzenia/elementu/komponentu ○ Generowanie alertów przy zmianie stanu urządzenia. ○ Filtry raportów umożliwiające podgląd najważniejszych zdarzeń ○ Integracja z service desk producenta dostarczonej platformy sprzętowej ○ Możliwość przejęcia zdalnego pulpitu ○ Możliwość podmontowania wirtualnego napędu ○ Kreator umożliwiający dostosowanie akcji dla wybranych alertów ○ Możliwość importu plików MIB ○ Przesyłanie alertów „as-is” do innych konsol firm trzecich ○ Możliwość definiowania ról administratorów

	○ Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów ○ Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) ○ Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta ○ Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów ○ Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. ○ Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. ○ Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile ○ Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. ○ Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. ○ Zdalne uruchamianie diagnostyki serwera. ○ Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. ○ Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
Certyfikaty	• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 • Serwer musi posiadać deklaracja CE. • Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest

	wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku - **Wykonawca złoży dokument potwierdzający spełnianie wymogu.** • Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022.
Dokumentacja użytkownika	• Zamawiający wymaga dokumentacji w języku polskim lub angielskim. • Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Warunki gwarancji	• Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 7 lat. • Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. • Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie Producenta (dla krytycznych zgłoszeń serwisowych) • Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. • Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. • Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. • Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. • Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego. • Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym

	aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. • Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki: o Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego. o Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy. o Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. o Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu. o Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. • Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. • Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.

Montaż, konfiguracja, uruchomienie, wdrożenie:

- Usługa wdrożenia musi obejmować montaż i uruchomienie oferowanego sprzętu we wskazanym miejscu przez Zamawiającego,
- Na oferowanym serwerze musi zostać przeprowadzona aktualizacja firmware'u. Urządzenie zostanie skonfigurowane zgodnie z najlepszymi praktykami, a następnie zainstalowane zostanie oprogramowanie do wirtualizacji (Windows Server Hyper-V),

- Przy wykorzystaniu zaoferowanych licencji Microsoft muszą zostać utworzone dwie nowe maszyny wirtualne z systemem Windows Server 2022 Standard,
- Na jednej z utworzonych maszyn zostanie uruchomiona usługa kontrolera domeny wraz z usługami wymaganymi do jej prawidłowego działania.
  Wykonawca musi utworzyć konta dla wszystkich użytkowników (maksymalnie 5 kont) oraz skonfigurować politykę domenową z uwzględnieniem wytycznych zamawiającego,
- Wszystkie komputery zamawiającego z systemem w wersji Professional (maksymalnie 5 urządzeń) zostaną przez wykonawcę podłączone do domeny, a na każdym komputerze przeprowadzona zostanie migracja profilu lokalnego do domenowego połączona z konfiguracją dla tych urządzeń profili mobilnych,
- Prace wdrożeniowe będą prowadzone w terminie uzgodnionym z Zamawiającym (w dzień roboczy, w godzinach 8:00 – 16:00),
- Podczas wdrożenia zostanie przeprowadzone instruktażowe szkolenie z wdrożonych systemów.

II: Dostawa i wdrożenie systemu do wykonywania kopii zapasowych

Pamięć masowa NAS o minimalnych wymaganiach:

Procesor	Czterordzeniowy o taktowaniu co najmniej 2,2GHz np. AMD Ryzen V1500B lub równoważny procesor czterordzeniowy osiągający w testach PassMark - CPU Mark wynik nie gorszy niż 4600 pkt. W przypadku zaoferowania procesora równoważnego, wynik testu musi być opublikowany na stronie https://www.cpubenchmark.net/mid_range_cpus.html (z dnia ogłoszenia postepowania lub nowszy).
Obudowa	Rack 2U o wymiarach max. 89 × 483 x 408 mm
Montaż RACK	Tak; do szafy RACK 19’; szyny teleskopowe w zestawie
Pamięć RAM	32GB pamięci SO-DIMM DDR4 ECC
Ilość obsługiwanych dysków	8 dysków o maksymalnej pojemności 20TB każdy z możliwością podłączenia zewnętrznej półki, która rozszerza pojemność serwera o kolejne 4 dyski
Zainstalowane dyski	5 dysków HDD klasy Enterprise w formacie 3,5” znajdujących się na liście kompatybilności producenta macierzy NAS o min. pojemności 12TB; możliwość aktualizacji oprogramowania dysku z poziomu NAS
Interfejsy sieciowe	4 x Gigabit (10/100/1000); Wsparcie dla Link Agregation 2x 10GbE SFP+ W zestawie wykonawca dostarczy dwie kompatybilne wkładki SFP+ SR LC MM 300m.
Porty	2 x USB 3.2, 1 x eSATA, 1x PCIe 3 x 4-liniowe gniazdo x8, port konsoli x1
Wskaźniki LED	Power on, Status, HDD1 -8
Obsługa RAID	Basic, JBOD, RAID 0,1,5,6,10, SHR + Obsługa Hot Spare dla SHR,RAID 1,5,6,10
Funkcje RAID	Możliwość zwiększania pojemności i migracja między poziomami RAID online.
Licencja na Kamery IP	W zestawie dwie licencje na jedną kamerę z możliwością rozszerzenia do 40.
Protokoły	SMB, AFP, NFS, FTP, WebDAV, CalDAV, iSCSI, Telnet, SSH, SNMP, VPN (PPTP, OpenVPN™, L2TP)
Usługi	Wsparcie dla High Availability Serwer VPN

	Serwer pocztowy dla kilku domen Stacja monitoringu Windows ACL Integracja z Windows ADS Firewall z kontrolą ruchu Serwer WWW Serwer plików Manager plików przez WWW Szyfrowana replikacja zdalna na kilka serwerów w tym samym czasie Antyvirus Klient VPN Usługa DDNS Oprogramownie do backup stacji roboczych, serwerów fizycznych i środowiska wirtualizacji VMware
Obsługa migawek	• Maksymalna liczba migawek folderów współdzielonych: 1 024 • Maksymalna liczba migawek systemu: 65 536
Zarządzanie dyskami	SMART, sprawdzanie złych sektorów, dynamiczne mapowanie uszkodzonych sektorów,
Język GUI	Polski, Angielski
Gwarancja i serwis	5 lat gwarancji door-to-door producenta NAS lub autoryzowanego partnera producenta 5 lat gwarancji door-to-door producenta dysków lub autoryzowanego partnera producenta
Waga	Max. 12 KG
Certyfikaty	CE
System plików	Dyski wewnętrzne Btrfs EXT4. Dyski zewnętrzne Btrfs, FAT, NTFS, EXT3, EXT4, HFS+, exFAT*(z dodatkową licencją)
Liczba wolumenów	Do 64
Liczba iSCSI Targetów	Do 128
Liczba iSCSI LUN	Do 256
Liczba kont użytkowników	2048
Liczba grup	256
Liczba udziałów	512
Ilość jednoczesnych połączeń	1000 dla CIFS/AFP/NFS/FTP/WebDAV; 2,000 po rozszerzeniu RAM
Zasilanie	Zasilacz 2x 350W
Chłodzenie	FAN x 2 80 x 80 mm

Oprogramowanie do backupu:

Należy dostarczyć oprogramowanie tego samego producenta co pamięć masowa NAS umożliwiające ochronę dwóch maszyn wirtualnych oraz 5 stacji roboczych.
Oprogramowanie nie może wymagać dokupowania dodatkowych licencji w celu ochrony stacji roboczych, serwerów oraz maszyn wirtualnych.

Wymagania dla kopi zapasowej fizycznego systemu Windows:

- Obsługiwane platformy: Windows 10 Creators Update (wszystkie wersje), Windows 10 (wszystkie wersje), Windows 8.1 (wszystkie wersje), Windows 7 SPl (wszystkie wersje), Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016 i Windows Server 2019
- Obsługa systemu plików NTFS
- Tryby tworzenia kopii zapasowych: całe urządzenie, wolumin systemowy i niestandardowa kopia zapasowa woluminu
- Metody przywracania: przywracanie całego urządzenia, przywracanie na poziomie plików/folderów, przywracanie na poziomie woluminów i natychmiastowe przywracanie do VMware vSphere, Microsoft Hyper-V
- Tworzenie kopii zapasowej na podstawie obrazu w celu utworzenia kopii zapasowej całego urządzenia, w tym konfiguracji danych i system
- Kopie zapasowe oparte na agencie, które umożliwiają tworzenie kopii zapasowych i przywracanie danych, na przykład przenoszenie zmienionych bloków między migawkami
- Korzystając z usługi Microsoft VSS Changed Błock Tracking, można wykonać przyrostową kopię zapasową
- Okno kopii zapasowej umożliwiające użytkownikom dostosowanie dozwolonego i odrzuconego czasu tworzenia kopii zapasowych
- Obsługa wstawiania argumentów (adres IP serwera NAS, nazwa użytkownika, hasło) do instalatora .msi w celu masowego wdrażania programu (Agenta)

Wymagania dla kopi zapasowej maszyn wirtualnych:

- Obsługa platform VMware vSphere: VMware vSphere 5.0, 5.1, 5.5, 6.0, 6.5 i 6.7
- Obsługiwane wersje VMware vSphere: VMware free ESXi, VMware vSphere Essentials, VMware vSphere Essentials Plus, VMware vSphere Standard, VMware vSphere Advanced, VMware vSphere Enterprise i VMware vSphere Enterprise Plus
- Obsługa wszystkich wersji sprzętu wirtualnego VMware, w tym 62TB VMDK
- Obsługiwane wersje Microsoft Hyper-V: Hyper-V 2016 i 2019
- Obsługa maszyn wirtualnych 1. I 2. generacji Hyper-V, w tym dysków VHDX o pojemności 64 TB i wirtualnych wersji sprzętowych od 5.0 do 9.0
- Aby utworzyć kopię zapasową programu Microsoft Hyper-V, wymagany jest wolumin systemowy hosta z co najmniej 512 MB wolnego miejsca
- Kopia zapasowa oparta na obrazie w celu utworzenia kopii zapasowej całego urządzenia, w tym konfiguracji systemu i danych
- Kopia zapasowa bez agenta
- Wykorzystanie VMware Changed Błock Tracking in Hyper-V Resilient Change Tracking do wykonywania przyrostowej kopii zapasowej
- Okno tworzenia kopii zapasowej umożliwiające użytkownikom dostosowanie dozwolonego i odrzuconego czasu tworzenia kopii zapasowej
- Metody przywracania: przywracanie całego urządzenia, przywracanie plików/folderów systemu operacyjnego gościa i natychmiastowe przywracanie do systemu VMware vSphere, Microsoft Hyper-
- W przypadku przywracania na poziomie plików systemu operacyjnego gościa obsługiwane systemy plików to NTFS i FAT32, a obsługiwane systemy plików Linux to NTFS, FAT32, ext3, I ext4

- Tworzenie kopii zapasowych z uwzględnieniem aplikacji dla maszyn wirtualnych VMware vSphere lub Microsoft Hyper-V działających w systemie Microsoft Windows 2003 z dodatkiem SPl lub nowszym (z wyłączeniem Nano Server z powodu braku struktury VSS)
- Obsługa tworzenia kopii zapasowych systemów operacyjnych i
- aplikacji obsługiwanych przez VMware vSphere i Microsoft Hyper- V

Montaż, konfiguracja, uruchomienie:

- Usługa wdrożenia musi obejmować montaż i uruchomienie oferowanego sprzętu
- we wskazanym miejscu przez Zamawiającego
- Na zaoferowanym urządzeniu musi zostać przeprowadzona aktualizacja oprogramowania systemowego.
- Urządzenie zostanie skonfigurowane zgodnie z najlepszymi praktykami, pod katem używania go
- jako miejsce przechowywania kopii dla zaoferowanego oprogramowaniem do backupu,
- Na zaoferowanym urządzeniu wykonawca zainstaluje i skonfiguruje oferowane oprogramowanie do backupu,
- Wykonawca zainstaluje na wszystkich stacjach klienckich (do 5 stacji) dostarczane oprogramowanie do backupu oraz skonfiguruje na nich zadania backupu z uwzględnieniem wytycznych zamawiającego oraz najlepszych praktyk,
- Wykonawca zainstaluje na Hyper-V (dwie maszyny wirtualne Windows Server 2022) dostarczane oprogramowanie do backupu oraz skonfiguruje na nich zadania backupu z uwzględnieniem wytycznych zamawiającego oraz najlepszych praktyk,
- Prace wdrożeniowe będą prowadzone w terminie uzgodnionym z Zamawiającym (w dzień roboczy, w godzinach 8:00 – 16:00).
- Podczas wdrożenia zostanie przeprowadzone instruktażowe szkolenie z wdrożonych systemów obejmujące przynajmniej omówienie konfiguracji i funkcji konsoli administracyjnej oprogramowania do backupu, procesu odzyskiwania danych oraz najlepszych praktyk dla rozwiązań backupowych.

III: Dostawa, montaż i konfiguracja przełącznika sieciowego.

Nazwa komponentu	Wymagane minimalne parametry techniczne przełącznika
Typ przełącznika	Zarządzalny
Porty	• 48 x 10/100/1000 Mb/s • 4 x 10 Gigabit SFP+
Zasilanie	100-240V 50-60 Hz
Montaż	Możliwość montażu w szafie Rack
Wydajność przełączania	Min. 175 Gb/s
Szybkość przekierowań pakietów	Min. 130 Mp/s

Rozmiar tablicy adresów MAC	16 000 wpisów
Bufor pakietów	3 MB
Niezawodność MTBF	1,452,667 godzin
Maks. Wymiar	445 x 288 x 44 mm
Maks. Waga	3.96 kg
Cechy i funkcje przełącznika	• Obsługa protokołu kontroli agregacji łączy (LACP) IEEE 802.3ad • Obsługa do 4094 sieci VLAN jednocześnie • Obsługa mapowania VLAN One-to-One • Przekaźnik protokołu dynamicznej konfiguracji hosta (DHCP) na warstwie 2 • Zapobieganie blokowaniu HOL • Wykrywanie pętli zwrotnej • Trasowanie pakietów IPv4 z dużą prędkością Do 990 tras statycznych i do 128 interfejsów IP • Do 4 jednostek w stosie. Do 200 portów zarządzanych jako pojedynczy system z funkcją failover sprzętowym • Protokół Secure Shell (SSH) • Warstwa bezpiecznych gniazd (SSL) • Uwierzytelnianie oparte na sieci Web • Ochrona źródła IP (IPSG) • Dynamiczna inspekcja ARP (DAI) • Powiązanie IP/MAC/Portu (IPMB) • Technologia Bezpiecznego Rdzenia (SCT) • Obsługuje uwierzytelnianie RADIUS i TACACS • Zapobieganie atakom DoS • Listy kontroli dostępu (ACL) Obsługa do 1024 reguł Limit odrzucania lub ograniczania szybkości transmisji na podstawie źródłowego i docelowego adresu MAC, identyfikatora VLAN, adresu IPv4 lub IPv6, etykiety przepływu IPv6, protokołu, portu, punktu kodowego usług zróżnicowanych (DSCP)/pierwszeństwa IP, portów źródłowych i docelowych protokołu Transmission Control Protocol/User Datagram Protocol (TCP/UDP), priorytetu 802.1p, typu Ethernet, pakietów protokołu ICMP (Internet Control Message Protocol), pakietów IGMP, flagi TCP; listę ACL można stosować zarówno po stronie wejściowej, jak i wyjściowej. • Zdalne monitorowanie (RMON) • Kopiowanie lustrzane sieci VLAN • Agent sFlow

	• Protokół Link Layer Discovery Protocol (LLDP) (802.1ab) z rozszerzeniami LLDP-MED • Aplikacje IPv6: Web/SSL, serwer Telnet/SSH, ping, traceroute, Simple Network Time Protocol (SNTP), Trivial File Transfer Protocol (TFTP), SNMP, RADIUS, syslog, klient DNS (Domain Name System), klient Telnet, klient DHCP, automatyczna konfiguracja DHCP, przekaźnik DHCP IPv6, kontroler dostępu do terminala Access Control System Plus (TACACS+)
Gwarancja	Ograniczona dożywotnia gwarancja door-to-door producenta wraz z dostępnością wsparcia producenta przez pierwszy rok trwania gwarancji
Akcesoria	W zestawie wykonawca dostarczy dwie kompatybilne z urządzeniem wkładki SFP+ SR LC MM 300m wraz z dwoma patchordami optycznymi o dł. min. 2m

Montaż, konfiguracja, uruchomienie:

1. Usługa musi obejmować montaż i uruchomienie oferowanego sprzętu we wskazanym miejscu przez Zamawiającego
2. Wykonawca wdroży oferowane urządzenie:
    a. Konfiguracja portu/agregacji.
    b. Rejestracja oraz upgrade urządzenia.
    c. Konfiguracja VLAN na interfejsie urządzenia.
    d. Weryfikacja działania VLAN na portach urządzenia.

IV: Dostawa, wdrożenie i konfiguracja oprogramowania do gromadzenia i analizy logów

I. Przedmiot zamówienia:
    1. Przedmiotem zamówienia jest dostawa, wdrożenie oraz konfiguracja rozwiązania do centralnego zbierania, przechowywania i analizy logów z urządzeń i systemów informatycznych w infrastrukturze Zamawiającego. Rozwiązanie ma umożliwiać monitorowanie, analizę i raportowanie zdarzeń w czasie rzeczywistym oraz przechowywanie logów zgodnie z wymogami prawnymi i regulacyjnymi.
    2. Wykonawca dostarczy licencje na oprogramowanie niezbędne do działania systemu, umożliwiające pełne wykorzystanie funkcjonalności opisanych w niniejszym dokumencie. Licencje muszą być ważne przez co najmniej 24 miesiące od momentu wdrożenia rozwiązania.

II. Wymagania techniczne dotyczące rozwiązania
    1. Rozwiązanie powinno działać na systemie operacyjnym na licencji Open Source.

2. System centralnego składowania dzienników zdarzeń powinien być zainstalowany na fizycznym serwerze będącym na wyposażeniu Zamawiającego lub wirtualnej maszynie.
3. System powinien być oparty na komponentach z licencjonowaniem Open Source.
4. Zamawiający przeznaczy na potrzeby rozwiązania sprzętowego maszynę wirtualną lub serwer fizyczny.
5. System powinien umożliwiać tworzenie użytkowników za pomocą zewnętrznego źródła tożsamości (Active Directory) lub ręczne definiowanie kont w samym rozwiązaniu.
6. System powinien umożliwiać zdefiniowanie i skonfigurowanie dowolnej liczby źródeł danych, takich jak Syslog UDP/TCP, Plaintext UDP/TCP, RAW UDP/TCP, NetFlow UDP, JSON, Beat, CEF UDP/TCP. Powinna być dostępna opcja definiowania dowolnych portów komunikacji.
7. System powinien umożliwiać ekstrakcję fragmentów wpisów logów, które mogą być używane do filtrowania danych, tworzenia zapytań dla powiadomień i alertów, oraz budowania widoków w interfejsach.
8. System powinien umożliwiać tworzenie widoków w formie interfejsów, które mogą być udostępniane w trybie ReadOnly (tylko do odczytu) na urządzeniach z funkcją SMART-TV lub w dowolnej przeglądarce WWW.
9. System powinien pozwalać na tworzenie powiadomień (alertów) opartych na regułach uwzględniających napływające dane z dzienników systemowych.
10. System powinien umożliwiać tworzenie paczek, które będą składać się ze skonfigurowanych źródeł nasłuchu danych wejściowych, strumieni formatujących dane wejściowe oraz interfejsów.

III. Wdrożenie systemu

1. Wykonawca przeprowadzi instalację oraz pełną konfigurację systemu do zbierania logów, zapewniając jego optymalne działanie zgodnie z wymaganiami Zamawiającego.
2. Wykonawca zobowiązuje się do przeprowadzenia integracji systemu z istniejącymi urządzeniami oraz systemami Zamawiającego, takimi jak serwery, urządzenia sieciowe, stacje robocze oraz inne systemy, które generują logi.
3. Wykonawca zainstaluje system operacyjny na wybranym przez Zamawiającego serwerze fizycznym lub maszynie wirtualnej.
4. Wykonawca zweryfikuje źródła czasu na urządzeniach i systemach wysyłających logi do systemu centralnego składowania dzienników zdarzeń. Jeśli urządzenia nie posiadają wspólnego zegara czasu, Wykonawca zaproponuje rozwiązanie uspójniające zegary czasów w sieci Zamawiającego.
5. Wykonawca przeprowadzi instalację oraz wstępną konfigurację systemu, w tym konfigurację polityki dostępu dla pracowników zespołu IT Zamawiającego.
6. System zostanie skonfigurowany pod kątem retencji przechowywania danych zgodnie z przepisami prawnymi oraz dobrymi praktykami.
7. Wykonawca skonfiguruje urządzenia i systemy w sieci Zamawiającego do wysyłania dzienników zdarzeń (logów) do centralnego systemu składowania dzienników zdarzeń.
8. Definiowanie portów nasłuchu: System zostanie skonfigurowany w sposób umożliwiający segmentację nasłuchu logów, aby odseparować dane napływające z różnych typów urządzeń i systemów.

9. Analiza logów i konfiguracja ekstraktorów: Wykonawca przeprowadzi wstępną analizę napływających logów i skonfiguruje ekstraktory, które będą wydzielać wybrane segmenty danych.
10. Wykonawca skonfiguruje interfejsy prezentujące dane w postaci tabelarycznej lub graficznej oraz zautomatyzuje analizę napływających logów.
11. Wykonawca skonfiguruje mechanizmy powiadamiania oraz alertowania oparte na analizie logów.
12. System zostanie skonfigurowany do wysyłania powiadomień poprzez email lub Microsoft Teams w przypadku wykrycia niepokojących sytuacji.
13. Wykonawca przeprowadzi szkolenie dla pracowników Zamawiającego z obsługi wdrożonego systemu, w zakresie obsługi nowego systemu, w tym zarządzania logami, tworzenia raportów, obsługi interfejsów oraz zarządzania alertami
14. Wykonawca dostarczy pełną dokumentację wdrożonego rozwiązania, w tym instrukcje obsługi, opis konfiguracji oraz procedury awaryjne.
15. Po zakończeniu wdrożenia, Wykonawca przeprowadzi testy systemu w obecności Zamawiającego w celu potwierdzenia spełnienia wszystkich wymagań określonych w zamówieniu. Odbiór końcowy nastąpi po pozytywnym zakończeniu testów.

V: Dostawa i wdrożenie zasilaczy awaryjnych UPS

A. Dostawa 5 sztuk rozwiązanie zasilania awaryjnego typ 1

PARAMETR	CECHA/WARTOŚĆ/WŁAŚCIWOŚĆ
Minimalne wymagania techniczne dla jednostki UPS	Moc znamionowa jednostki nie mniej niż 520W / 950VA Topologia line-interactive Temperatura eksploatacji 0 - 40 °C • Wilgotność względna podczas pracy 0 - 95 % • Wysokość n.p.m. podczas pracy 0-3000 m • Klasa energetyczna sprzętu przeciwprzepięciowego 273 J
Parametry wejściowe	• Nominalne napięcie wejściowe 230V • Częstotliwość wejściowa 50/60Hz • Standard wtyczki: Schuko CEE 7/7P
Parametry wyjściowe	• Napięcie wyjściowe 230V • Zniekształcenia napięcia wyjściowego +/- 10% (przy pracy na akumulatorze) • Częstotliwość na wyjściu (zsynchronizowana z siecią zasilającą) 50/60Hz +/- 1 Hz • Typ przebiegu: Schodkowa aproksymacja sinusoidy • Złącza/gniazda wyjściowe: 4 gniazda Schuko z zabezpieczeniem przeciwprzepięciowym oraz podtrzymaniem zasilania.
Akumulatory i czas podtrzymania	• Typ akumulatora bezobsługowy szczelny akumulator kwasowo-ołowiowy z elektrolitem w postaci żelu • Czas autonomii: 29 sekund dla pełnego obciążenia 6 minut 42 sekundy dla połowy obciążenia • Typowy czas ładowania 6-8 godzin

	• Oczekiwana żywotność akumulatora (lata) 3 – 5 • Baterie wymieniane na gorąco
Komunikacja i zarządzanie	• Gniazdo RJ45 Gigabit • Diody LED wskazująca na status zasilania: zasilanie z sieci energetycznej: zasilanie z akumulatora • Alarm dźwiękowy: Praca na baterii, niski poziom naładowania baterii, wyłączenie baterii, wykrycie wymiany akumulatora
Certyfikaty, zgodności oraz gwarancja	• CE / EN/IEC-62040-1 / EN/IEC-62040-2 • 2 letnia gwarancja producenta door to door na naprawę lub wymianę urządzenia
Oprogramowanie	Oprogramowanie do zarządzania zasilaczami UPS do bezpiecznego wyłączania i zarządzania energią dla komputerów stacjonarnych, serwerów i stacji roboczych, wykorzystujące dedykowane połączenia szeregowe lub USB i oferujące: • Monitorowania i zarządzania zasilaczy UPS • Bezobsługowego, bezpiecznego wyłączania podczas problemów z zasilaniem • Bezpieczny dostęp do internetowego interfejsu użytkownika (UI) • Możliwość dokładnego określania czasu i sekwencji wyłączania za pomocą dziennika zdarzeń • Identyfikacja potencjalnych zagrożeń, możliwość eksportowania dziennika zdarzeń

B. Dostawa i wdrożenie Rozwiązanie zasilania awaryjnego typ 2

PARAMETR	**CECHA/WARTOŚĆ/WŁAŚCIWOŚĆ**
Minimalne wymagania techniczne dla jednostki UPS	Moc znamionowa jednostki nie mniej niż 1980W / 2200VA Montaż w szafie Rack Technologia Line Interactive Temperatura eksploatacji 0 - 40 °C • Wilgotność względna podczas pracy 0 - 95 % • Wysokość n.p.m. podczas pracy 0-3000 m • Hałas słyszalny w odległości 1 m od powierzchni urządzenia 55.0dBA • Rozpraszanie ciepła w trybie online 215.0BTU/godz. • Klasa energetyczna sprzętu przeciwprzepięciowego 375J
Parametry wejściowe	• Nominalne napięcie wejściowe 230V • Częstotliwość wejściowa 50/60 Hz +/-3 Hz (automatyczne wykrywanie) • Typ gniazda wejściowego: - IEC-320 C20, • Zmienny zakres napięcia wejściowego w trybie podstawowym 160 - 286V
Parametry wyjściowe	• Napięcie wyjściowe 230V • Częstotliwość na wyjściu (zsynchronizowana z siecią zasilającą) 50/60Hz +/- 3 Hz • Inne napięcia wyjściowe 220, 240

	• Typ przebiegu sinusoida • Złącza/gniazda wyjściowe (8) IEC 320 C13 (1) IEC 320 C19
Akumulatory i czas podtrzymania	• Typ akumulatora bezobsługowy szczelny akumulator kwasowo-ołowiowy z elektrolitem w postaci żelu szczelny • Czas autonomii: 5 minut 27 sekundy dla pełnego obciążenia 16 minut 6 sekund dla połowy obciążenia • Typowy czas ładowania 3 godziny • Oczekiwana żywotność akumulatora (lata) 3 – 5 • Baterie wymieniane na gorąco
Komunikacja i zarządzanie	• Gniazdo do montażu karty WEB/SNMP- Smart Slot x1 • Wstępnie zainstalowana karta zarządzania siecią do monitorowania i zarządzania UPS. • Porty komunikacyjne: RJ-45, SmartSlot, USB • Panel sterowania: Wielofunkcyjna konsola sterownicza i informacyjna LCD Alarm dźwiękowy: Alarm przy zasilaniu akumulatora: alarm przy bardzo niskim poziomie naładowania akumulatora: konfigurowalne opóźnienia • Awaryjny wyłącznik zasilania (EPO) Tak
Certyfikaty, zgodności oraz gwarancja	• RCM, CE, EN62040-1, EN62040-2 • 3 letnia gwarancja door-to-door producenta na naprawy lub wymiany (bez akumulatora) i 2 lata gwarancji door-to-door producenta na akumulator
Oprogramowanie	• Dostępne oprogramowanie do zarządzania/monitorigu (niektóre wersje odpłatne) z VMware® ESXi (VMware® ESXi Server 6.5 Update 3 (vMA 6.5), VMware® ESXi Server 6.5 Update 2 (vMA 6.5)); Microsoft® Hyper-V (Windows® Hyper-V Server 2019, 2012 R2); Windows® Server 2019, 2016, 2012; Windows® 10, 7; Red Hat® Enterprise Linux; SuSE® Linux®.

Montaż, konfiguracja, uruchomienie:

- Usługa wdrożenia musi obejmować montaż i uruchomienie oferowanego sprzętu w siedzibie zamawiającego,
- Wykonawca zainstaluje darmową aplikację dostarczoną przez producenta zasilacza awaryjnego i skonfiguruje połączenie pomiędzy urządzeniem, a hostem, aby zapewnić bezpieczne wyłączanie w przypadku przedłużającego się braku zasilania,
- Prace wdrożeniowe będą prowadzone w terminie uzgodnionym z Zamawiającym (w dzień roboczy, w godzinach 8:00 – 16:00).
- Podczas wdrożenia zostanie przeprowadzone instruktażowe szkolenie z wdrożonych systemów.

VI: Dostawa urządzeń UTM wraz ze wsparciem oraz wdrożeniem

OBSŁUGA SIECI

1. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.

ZAPORA KORPORACYJNA (Firewall)

2. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.
3. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.
4. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).
5. Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.
6. Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia.
7. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.
8. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.
9. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.
10. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.
11. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).
12. System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.

INTRUSION PREVENTION SYSTEM (IPS)

13. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.
14. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.
15. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
16. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
17. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia.

18. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS.
19. Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.
20. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.
21. Po zakupie stosownej licencji moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV).
22. Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.
23. Urządzenie ma posiadać moduł wykrywania typu i wersji oprogramowania sieciowego, którego ruch jest filtrowany przez urządzenie. Moduł musi działać na urządzeniu. Nie dopuszcza się stosowania rozwiązania z agentem instalowanym na komputerach w sieci. Moduł ma nie tylko wykrywać oprogramowanie ale również wykrywać i informować o lukach i podatnościach występujących w wykrytym oprogramowaniu.

KSZTAŁTOWANIE PASMA (Traffic Shapping)

24. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
25. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.
26. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).
27. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.

OCHRONA ANTYWIRUSOWA

28. Urządzenie ma umożliwiać zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania).
29. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji.
30. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
31. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.
32. Urządzenie ma być dostarczone wraz z komercyjnym, europejskim skanerem Antywirusowym.
33. Urządzenie ma być dostarczone wraz z komercyjnym, europejskim skanerem Antywirusowym oraz umożliwiać skanowanie plików w oparciu o Sandboxing zlokalizowany w Internecie na serwerach producenta. Nie dopuszcza się aby analiza była przeprowadzana na urządzeniu lub wymagała instalacji dodatkowego urządzenia lub oprogramowania. Nie dopuszcza się również żeby analiza była przeprowadzana przez firmy trzecie.

OCHRONA ANTYSPAM

34. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
35. Ochrona antyspam ma działać w oparciu o:
    a. białe/czarne listy,
    b. DNS RBL,
    c. Skaner heurystyczny.
36. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.
37. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.

WIRTUALNE SIECI PRYWATNE (VPN)

38. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
39. Urządzenie ma wspierać co najmniej następujące typy sieci VPN:
    a. PPTP VPN,
    b. IPSec VPN,
    c. SSL VPN.
40. SSL VPN ma działać co najmniej w trybach tunelu i portalu.
41. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.
42. Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal)
43. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
44. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf.
45. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.

FILTR DOSTĘPU DO STRON WWW

46. Urządzenie ma posiadać wbudowany filtr URL.
47. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 77 kategorii tematycznych stron internetowych. Rozszerzony URL Filtering posiada miliony sklasyfikowanych stron internetowych. Klasyfikacja URL musi się odbywać w oparciu o komunikację z serwerami producenta znajdującymi się w sieci Internet, a nie na bazie danych przechowywanej lokalnie w urządzeniu..
48. Administrator ma mieć możliwość dodawania własnych kategorii URL.
49. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej:
    a. blokowanie dostępu do adresu URL,
    b. zezwolenie na dostęp do adresu URL,
    c. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.
50. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
51. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.
52. Filtr URL musi uwzględniać komunikację po protokole HTTPS.

53. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
54. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.
55. Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch

UWIERZYTELNIANIE

56. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o:
    a. lokalną bazę użytkowników (wewnętrzny LDAP),
    b. zewnętrzną bazę użytkowników (zewnętrzny LDAP),
    c. usługę katalogową Microsoft Active Directory.
57. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.
58. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły:
    a. SSL,
    b. Radius,
    c. Kerberos.
59. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.
60. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.
61. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.
62. Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS).
63. Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP).
64. Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.

ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)

65. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
66. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:
    a. równoważenie względem adresu źródłowego,
    b. równoważenie względem połączenia.
67. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.
68. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover).
69. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza.

70. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).
71. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.

ROUTING (TRASOWANIE)

72. Urządzenie ma umożliwiać statyczne trasowanie pakietów.
73. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
74. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).
75. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.

ADMINISTRACJA URZĄDZENIEM

76. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
77. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.
78. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.
79. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
80. Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.
81. Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH)
82. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.
83. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.
84. Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup.
85. Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.
86. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła.
87. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording).
88. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services).
89. Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników.
90. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).
91. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.
92. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie:
    a. manualnego eksportu do pliku w dowolnym momencie czasu,

   b. automatycznego eksportu do serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu
93. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzących bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora.
94. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.
95. Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.

RAPORTOWANIE

96. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
97. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
98. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.
99. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.
100. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.
101. System raportowania ma umożliwiać eksport wyników raportu do formatu CSV.
102. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.
103. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.
104. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).

POZOSTAŁE USŁUGI I FUNKCJE

105. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.
106. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).
107. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.
108. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny).
109. Urządzenie ma posiadać usługę DNS Proxy.
110. Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN.
111. Urządzenie musi mieć zaimplementowane Open API
112. Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie.
113. Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP.
114. Urządzenie musi oferować możliwość zwiększenia wydajności takich parametrów jak przepustowości firewall, IPS, Antywirus, VPN. Zwiększenie wydajności odbywa się wyłącznie

przez zmianę licencji i nie wymaga ingerencji w komponenty fizyczne urządzenia czy wymianę samego urządzenia.

GWARANCJA I SERWIS

115. Urządzenie ma być objęte 24-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa.
116. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.

PARAMETRY SPRZĘTOWE

117. Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash.
118. Urządzenie ma być wyposażone w zintegrowany port na kartę microSD.
119. Liczba portów Ethernet 2,5Gbps – min. 8.
120. Liczba portów światłowodowych 1Gbps – min. 1.
121. Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.
122. Przepustowość Firewall (1518 bajtów UDP) – minimum 4Gbps.
123. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 2Gbps.
124. Przepustowość filtrowania Antywirusowego – minimum 500Mbps.
125. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 1Gbps.
126. Maksymalna liczba tuneli VPN IPSec – minimum 100.
127. Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) – minimum 50.
128. Maksymalna liczba tuneli typu SSL VPN (tryb portalu) – minimum 50.
129. Obsługa interfejsów 802.11q (VLAN) – minimum 128
130. Liczba równoczesnych sesji – minimum 300 000 i nie mniej niż 20 000 nowych sesji/sekundę.
131. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.
132. Urządzenie nie ma limitu na liczbę użytkowników.
133. Liczba reguł filtrowania – minimum 8 192.
134. Liczba tras statycznego routingu – minimum 512.
135. Liczba tras dynamicznego routingu – minimum 10 000.
136. Urządzenie ma umożliwiać podłączenie zewnętrznego nadmiarowego zasilacza (zasilanie redundantne). Stan pracy każdego zasilacza musi być sygnalizowany bezpośrednio na obudowie urządzenia.
137. Urządzenie musi być wyposażone w moduł TPM.

Usługa wdrożenia musi obejmować montaż, podłączenie i uruchomienie oferowanego sprzętu w siedzibie Zamawiającego. Wdrożenie musi być przeprowadzone przez certyfikowanego inżyniera wykonawcy. Po wdrożeniu należy przeszkolić wskazanego pracownika Zamawiającego, szkolenie powinno obejmować 5 godzin.

Zakres wdrożenia UTM:

- Konfiguracja sieci (interfejsy i routing).
- Konfiguracja firewalla (limit reguł – 20).
- Konfiguracja NAT (limit reguł – 10).
- Konfiguracja IPS – zgodnie z wymaganiami klienta.
- Konfiguracja dodatkowych usług sieciowych tj. DHCP, DNS Proxy.
- Konfiguracja dostawców Internetu (maksymalnie 2 dostawców).
- Konfiguracja VPN:
    - IPSec Site-to-Site (limit 2 tuneli) – zgodnie z otrzymanymi od klienta parametrami tuneli.
    - Client-to-Site – konfiguracja urządzenia i jednej wzorcowej stacji klienckiej.
- Integracja usługi Active Directory, integracja obejmująca m.in.:
    - Uwierzytelnianie użytkowników przy połączeniach VPN z konfiguracją 2FA na email.
    - Konfigurację profili bezpieczeństwa również dla ruchu zaszyfrowanego w celu pełnej analizy zagrożeń.
    - Konfigurację integracji pozwalającej na zarządzanie ruchem do zasobów sieci oraz Internetu w oparciu o przynależność do grup w Active Directory. Polityki powinny działać również w momencie przepinania się między sieciami fizycznymi np. LAN, WiFi

VII: Dostawa i wdrożenie systemu do inwentaryzacji i zarządzania zasobami informatycznymi (sprzętu i oprogramowania) na potrzeby Urzędu Gminy i Gminnego Ośrodka Pomocy Społecznej

Wymagania ogólne dla systemu zarządzania

1. Oprogramowanie musi posiadać polski oraz angielski interfejs językowy.
2. Oprogramowanie musi posiadać architekturę trójwarstwową składającą się z Bazy Danych, Serwera Aplikacji, Agenta/Konsoli zarządzającej.
3. Oprogramowanie musi umożliwiać obsługę dedykowanych kluczy szyfrujących podczas komunikacji pomiędzy agentami, serwer aplikacji i konsolą zarządzającą.
4. Odczyt informacji dotyczących parametrów sprzętowych komputera musi odbywać się za pośrednictwem agenta systemu instalowanego na komputerach użytkowników.
5. Agent systemu nie może nasłuchiwać na żadnym porcie sieciowym po stronie stanowiska komputerowego użytkownika.
6. Oprogramowanie musi umożliwiać wybór instalacji agenta w trybie standardowym oraz bezpiecznym tj. braku wkompilowanych funkcji takich jak zdalne zarządzanie, transfer plików, zdalny pulpit.
7. 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.

8. Oprogramowanie musi posiadać dodatkową autoryzację użytkownika konsoli zarządzającej za pomocą usługi Google Authenticator oraz Microsoft Authenticator.
9. Oprogramowanie musi posiadać moduł zarządzania uprawnieniami do poszczególnych funkcjonalności systemu dla operatorów konsoli zarządzającej zgodny z modelem RBAC (Role Based Access Control).
10. Oprogramowanie musi umożliwiać nadawanie oraz odbieranie uprawnień w czasie rzeczywistym (brak konieczności przelogowania użytkownika konsoli systemu).
11. Oprogramowanie musi umożliwiać blokadę wybranych uprawnień konkretnego użytkownika niezależnie od uprawnień wynikających z przypisanych ról.
12. Oprogramowanie musi umożliwiać zastosowanie dwóch konsol: jednej dla urzędu gminy i jednej dla jednostki podległej, co pozwoli na jednoczesną pracę dwóch administratorów.
13. Oprogramowanie musi współpracować z serwerem MSSQL Server 2008R2-2019
14. Oprogramowanie, w zakresie wszystkich warstw, nie może wymagać do prawidłowej pracy komponentów Java.
15. Oprogramowanie serwera aplikacji musi posiadać funkcjonalność centralnego wysyłania wybranych powiadomień mailowych .
16. Oprogramowanie musi posiadać moduł zarządzania uprawnieniami do danych w zakresie wybranych jednostek organizacyjnych oraz typów zasobów poszczególnych użytkowników konsoli. Wszelkie raporty, zestawienia oraz funkcje obejmują wtedy tylko wynikowe obiekty.
17. 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).
18. Oprogramowanie agentów musi posiadać obsługę sesji terminalowych Windows.
19. 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).
20. Oprogramowanie musi posiadać raport przedstawiający różnice w konfiguracji poszczególnych agentów w stosunku do konfiguracji globalnej.
21. Oprogramowanie musi posiadać mechanizm logowania zmian w konfiguracji agentów przez użytkowników konsoli (data, czas, login, poprzednia i nowa wartość).
22. Oprogramowanie musi posiadać mechanizm analizy czasu pracy komputera, informujący użytkownika (alert oraz wymuszone działanie – restart) o przekroczeniu zadanego czasu pracy bez restartu systemu operacyjnego.
23. 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.
24. 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.
25. Oprogramowanie musi posiadać kreator powiązań (mapowanie atrybutów) dowolnych atrybutów obiektów z usługi katalogowej do wskazanych atrybutów zasobów systemowych.
26. Oprogramowanie musi umożliwiać współpracę z nieograniczoną ilością kontrolerów domen z zachowaniem podległej struktury drzewiastej.
27. Oprogramowanie musi umożliwiać automatyczny import informacji dotyczących przynależności użytkowników oraz stanowisk komputerowych do grup struktury katalogowej.

28. Oprogramowanie musi posiadać raport przedstawiający informacje nt. grup struktury katalogowej wraz przynależącymi do nich użytkownikami.
29. Oprogramowanie musi umożliwiać tworzenie dynamicznych grup stanowisk w oparciu o kreator zawierający filtry (AND, OR) w zakresie min. wersja OS, nazwa oraz wersja wybranej aplikacji, RAM, CPU, HDD, jednostka organizacyjna, jednostka lokalizacyjna, architektura (x32, x64), zainstalowane oprogramowanie, wersja oprogramowania, lista usług systemowych, producent oraz model komputera, poziom uprawnień użytkownika, zainstalowana usługa systemowa, ostatnie uruchomienie systemu, obecność pliku EXE na dysku, predefiniowane atrybuty komputera (np. dostawca, numer faktury, data zakupu).
30. 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.
31. Oprogramowanie musi umożliwiać dynamiczne zawężanie wyników wyszukiwania ww. widoków na podstawie prezentowanych w nich atrybutów.
32. Oprogramowanie musi umożliwiać graficzną prezentację aktualnego stanu aktywności agenta (online/offline) z dokładnością do 1 minuty.
33. Oprogramowanie musi umożliwiać zapisywanie w bazie danych informacji o uruchomieniu i wyłączeniu komputera oraz zalogowaniu i wylogowaniu użytkownika.

Inwentaryzacja konfiguracji komputerów

1. Oprogramowanie musi umożliwiać wydruk kartoteki sprzętowej stanowiska komputerowego.
2. Oprogramowanie musi umożliwiać samodzielną edycję wyglądu kartoteki sprzętowej, protokołów przekazania oraz zwrotu zasobów za pomocą graficznego kreatora wyglądu.
3. Oprogramowanie musi umożliwiać zapisywanie edytowanych szablonów (min. kartoteka sprzętowa, protokoły przekazania/zwrotu zasobów) w kontekście zalogowanego operatora konsoli zarządzającej.
4. 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
5. Oprogramowanie musi umożliwiać okresową automatyczną inwentaryzację parametrów sprzętowych stanowiska: HDD, RAM, CPU, karta sieciowa, system operacyjny, karta graficzna itp.
6. Oprogramowanie Agenta musi umożliwiać audyt off-line, poprzez uruchomienie skanera (z GUI) bez konieczności instalacji, oraz zapis wyników do pliku w postaci zaszyfrowanej.
7. Oprogramowanie musi umożliwiać analizę sprzętową:
8. - płyty głównej w zakresie model, producent, nr. seryjny,
9. - CPU w zakresie nazwy, modelu, producenta, częstotliwości,
10. - HDD w zakresie numeru seryjnego dysku, numeru seryjnego partycji, rozmiaru pamięci,
11. - RAM w zakresie wielkości pamięci,
12. - karty sieciowej w zakresie model, adres IP, adres MAC,
13. - karty graficznej w zakresie model.
14. Oprogramowanie musi umożliwiać odczyt informacji dotyczących systemu operacyjnego w zakresie nazwy, wersji, daty instalacji, zainstalowanych poprawek, dostępnych kluczy licencyjnych, produkt ID.
15. Oprogramowanie musi umożliwiać odczyt informacji sieciowych w zakresie adresu IO, adresu MAC, nazwy sieciowej.
16. Oprogramowanie musi umożliwiać odczyt informacji sprzętowych z BIOS w zakresie nazwy BIOS, daty, producenta.

17. Oprogramowanie musi umożliwiać przegląd historii zmian parametrów sprzętowych komputerowych.
18. Oprogramowanie musi umożliwiać globalny przegląd stanowisk komputerowych pod względem parametrów sprzętowo-systemowych.
19. Oprogramowanie musi zawierać raport stanowisk komputerowych posiadających co najmniej jedno konto z uprawnieniami administratora.
20. Oprogramowanie musi umożliwiać odczyt urządzeń podłączonych do stanowiska komputerowego przez interfejs USB, z możliwością odczytania nazwy urządzenia, producenta, modelu oraz numeru seryjnego (o ile urządzenie dostarcza ww. informacji)
21. Oprogramowanie musi umożliwiać globalną analizę urządzeń podłączonych do stanowisk komputerowych przez interfejs USB
22. Oprogramowanie musi umożliwiać integrację z zewnętrzną usługą Dell API w celu automatycznego odczytania informacji na temat okresu gwarancji stanowiska komputerowego na podstawie odczytanego przez agenta identyfikatora (ServiceTag)
23. 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

1. Oprogramowanie musi umożliwiać automatyczną inwentaryzację zainstalowanego na komputerach oprogramowania.
2. Oprogramowanie musi umożliwiać globalny przegląd wszystkich programów zainstalowanych na komputerach.
3. Oprogramowanie musi umożliwiać tworzenie zestawień zainstalowanych typów programów (freeware, shareware itp.).
4. Oprogramowanie musi umożliwiać tworzenie wykazów z zainstalowanym, dowolnie wybranym programem.
5. Oprogramowanie musi umożliwiać tworzenie zestawień zainstalowanych systemów operacyjnych na komputerach.
6. Oprogramowanie musi umożliwiać tworzenie wykazów stanowisk z brakiem zainstalowanego, dowolnie wybranego, programu.
7. Oprogramowanie musi posiadać wbudowany mechanizm umożliwiający, poprzez GUI konsoli, zdalną grupową dezinstalację oprogramowania np. pakietów MS Office.
8. Oprogramowanie musi umożliwiać oznaczanie kolorem aplikacji zabronionych oraz zgodnych ze standardem wraz z możliwością raportowania wg w/w klasyfikacji.
9. Oprogramowanie musi umożliwiać zablokowanie na stacji roboczej wybranych procesów celem uniemożliwienia ich uruchomienia przez użytkownika.
10. 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

1. Oprogramowanie musi posiadać wbudowaną bazę sygnatur aplikacji (produktów) wraz z możliwością automatycznej aktualizacji wzorców ze strony Producenta oprogramowania
2. Oprogramowanie musi umożliwiać zdefiniowanie własnych sygnatur aplikacji (produktów) wykorzystywanych
3. w procesie automatycznego audytu licencji (rozliczenie ilościowe).

4. 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.
5. Oprogramowanie musi umożliwiać zapis historii wykonywanych audytów licencji.
6. Oprogramowanie musi umożliwiać tworzenie bazy licencji systemowo/programowych i przypisywanie ich do stanowisk komputerowych oraz użytkowników.

Centralna baza danych

1. Oprogramowanie musi umożliwiać tworzenie własnych typów elementów konfiguracji (CI)
2. Oprogramowanie musi umożliwiać dodawanie dowolnych atrybutów dla typów CI w szczególności: wartości logiczne, data/czas, numeryczne, tekstowe, słownikowe
3. Oprogramowanie musi umożliwiać tworzenie podrzędnych i nadrzędnych typów CI
4. Oprogramowanie musi umożliwiać dziedziczenie atrybutów przez elementy konfiguracji posiadające typ nadrzędny
5. Oprogramowanie musi umożliwiać tworzenie dowolnych typów relacji do obsługi połączeń pomiędzy różnymi typami CI
6. Oprogramowanie musi umożliwiać tworzenie atrybutów dla relacji
7. Oprogramowanie musi umożliwiać prezentowanie powiązań pomiędzy elementami konfiguracji w formie struktury płaskiej oraz graficznej
8. Oprogramowanie musi umożliwiać zbiorczy podgląd relacji pomiędzy poszczególnymi elementami konfiguracji
9. Oprogramowanie musi umożliwiać modelowanie struktury relacji pomiędzy usługami, sprzętem, organizacją oraz pracownikami
10. Oprogramowanie musi umożliwiać nadzór nad wpływem zmian na poszczególne elementy konfiguracji
11. Oprogramowanie musi umożliwiać import elementów konfiguracji ze źródeł takich jak usługa katalogowa, skaner sieci, zewnętrzne pliki płaskie (CSV)
12. Oprogramowanie musi umożliwiać tworzenie oraz edycję własnych list elementów konfiguracji
13. Oprogramowanie musi umożliwiać wyszukiwanie i analizę elementów konfiguracji wg posiadanych atrybutów
14. Oprogramowanie musi umożliwiać tworzenie własnych typów relacji z określaniem nazwy relacji podstawowe i odwrotnej
15. Oprogramowanie musi umożliwiać tworzenie własnych formularzy dla wszystkich elementów konfiguracji

Zarządzanie zasobami oraz użytkownikami

1. Oprogramowanie musi umożliwiać tworzenie własnych szablonów widoków zasobów z określeniem analizowanych typów zasobów, widocznych atrybutów oraz informacji nt. powiązań pomiędzy zasobami.
2. Oprogramowanie musi umożliwiać tworzenie własnych atrybutów o typach co najmniej: tekst, liczba, bit, data, wartość słownikowa dla wybranego typu zasobu.
3. Oprogramowanie musi umożliwiać zapis oraz przegląd historii zmian dowolnego atrybutu zasobu w zakresie: operator, data, czas, poprzednia oraz nowa wartość.

4. Oprogramowanie musi umożliwiać zdefiniowanie dowolnych relacji pomiędzy zasobami (np. powiązania stanowiska z pracownikiem, licencją, innym zasobem) wraz z zapisem historii relacji zasobów.
5. 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.
6. Oprogramowanie musi umożliwiać zdefiniowanie dowolnego zasobu inwentaryzacyjnego (np. telefon, drukarka, nawigacja) w strukturze drzewiastej wraz z kreatorem widocznych/wymaganych atrybutów edycyjnych.
7. Oprogramowanie musi posiadać dedykowaną (zintegrowaną z systemem) aplikację na platformę Android umożliwiającą spis z natury zinwentaryzowanych zasobów.
8. 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.
9. Oprogramowanie musi umożliwiać zaprojektowanie własnego schematu importu danych z zewnętrznego pliku CSV.
10. Oprogramowanie musi umożliwiać automatyczne tworzenie relacji pracownik-komputer na podstawie atrybutów obiektu w usłudze katalogowej.
11. Oprogramowanie musi zawierać wbudowany kreator wydruków w zakresie protokołów przekazania, zwrotu, likwidacji wraz z możliwością utworzenia dowolnego typu dokumentu
12. Oprogramowanie musi umożliwiać export ww. protokołów w formacie PDF
13. Oprogramowanie musi umożliwiać obsługę kodów kreskowych oraz QR w obrębie ww. kreatora wydruków
14. Oprogramowanie musi umożliwiać użycie w kreatorze wydruków własnego logotypu organizacji
15. Oprogramowanie musi umożliwiać użycie w kreatorze wydruków dowolnego atrybutu zasobu
16. Oprogramowanie musi umożliwiać przypisanie dowolnej firmy serwisowej z bazy organizacji do zasobu
17. Oprogramowanie musi umożliwiać przypisanie załącznika do zasobu
18. Oprogramowanie musi umożliwiać pogląd wszystkich zgłoszeń serwisowych dotyczących danego zasobu
19. Oprogramowanie musi umożliwiać podgląd zasobów (przypisanych do danego pracownika) z poziomu jego portalu użytkownika końcowego
20. Oprogramowanie musi umożliwiać zarządzanie cyklem życia zasobu
21. Oprogramowanie musi umożliwiać tworzenie niestandardowych reguł biznesowych dla zarządzania zasobami
22. Oprogramowanie musi umożliwiać seryjne dodawanie zasobów
23. Oprogramowanie musi umożliwiać automatyczne nadawanie numerów inwentaryzacyjnych dla zasobów
24. Oprogramowanie musi udostępniać kreator raportów dla zasobów
25. Oprogramowanie musi udostępniać możliwość kopiowania widoku dla określonego typu(ów) zasobu z innego typ zasobu
26. Oprogramowanie musi udostępniać możliwość kopiowania formularz dla określonego typu(ów) zasobu z innego typ zasobu
27. Oprogramowanie musi umożliwiać ewidencję magazynów
28. Oprogramowanie musi umożliwiać ewidencję lokalizacji magazynowych
29. Oprogramowanie musi umożliwiać ewidencję produktów magazynowych

30. Oprogramowanie musi udostępniać informację o stanie magazynowym(ilościowo)
31. Oprogramowanie musi umożliwiać generowanie dokumentów PZ/PW/RW/MM
32. Oprogramowanie musi umożliwiać przyjęcie zasobów ewidencjonowanych i eksploatacyjnych na magazyn
33. Oprogramowanie musi umożliwiać wydawanie zasobów ewidencjonowanych i eksploatacyjnych z magazynu
34. Oprogramowanie musi umożliwiać zwrot zasobów na magazyn
35. Oprogramowanie musi umożliwiać zmianę szablonów dokumentów PZ/PW/RW/MM
36. Oprogramowanie musi umożliwiać wyszukiwanie dokumentów po dowolnym atrybucie
37. Oprogramowanie musi umożliwiać zarządzanie organizacjami/typami organizacji (np. klient, podwykonawca)
38. Oprogramowanie musi umożliwiać dowolne przypisanie osoby do organizacji
39. Oprogramowanie musi umożliwiać tworzenia dynamicznych grup użytkowników
40. Oprogramowanie musi umożliwiać zarządzanie kontaktami osób/organizacji
41. Oprogramowanie musi umożliwiać zarządzanie nieobecnościami użytkowników
42. Oprogramowanie musi umożliwiać zarzadzanie uprawnieniami i poziomami dostępu do danych w zakresie zarządzania zasobami
43. Oprogramowanie musi umożliwiać automatyczne pobieranie danych rejestrowych kontrahentów z bazy GUS

Zdalny pulpit, zdalne zarządzanie komputerem

1. 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).
2. 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.
3. Oprogramowanie musi umożliwiać zdalne zarządzanie (bez użycia RDP/VNC itp.) lokalnymi kontami użytkowników w zakresie (tworzenie, usuwanie, edycja, zmiana hasła oraz typ konta).
4. Oprogramowanie musi umożliwiać wysyłanie polecenia Wake-on LAN.
5. Oprogramowanie musi umożliwiać zdalną dwukierunkową linię poleceń.
6. 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).
7. 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.
8. Oprogramowanie musi umożliwiać wybór aktywnych sesji terminalowych, do których chcemy się podłączyć.
9. Oprogramowanie musi umożliwiać zbiorczy podgląd zdalnych pulpitów stacji.
10. Oprogramowanie musi posiadać zarządzanie technologią iAMT, vPro w zakresie uwzględniającym min.: Serial Over Lan (SOL), IDE Redirection (IDER), Hardware KVM, Assets.
11. Oprogramowanie musi zapewniać zdalną konfigurację technologii iAMT w trybie Client Control Configuration Mode.

12. Oprogramowanie musi umożliwiać zarządzanie stacjami komputerowymi poza siecią LAN/WAN, wymagane jest tylko dowolne połączenie internetowe
13. Oprogramowanie musi umożliwiać zdalne wykonywanie zapytań WQL
14. Oprogramowanie musi umożliwiać zdalny odczyt oraz modyfikację rejestru Windows
15. Oprogramowanie musi umożliwiać pełne wykorzystanie funkcji zawartych w sekcji zdalne zarządzanie dla stacji posiadających dowolne połączenie do sieci INTERNET bez konieczności zestawiania połączenia VPN
16. Oprogramowanie musi umożliwiać przejęcie pulpitu zdalnego z poziomu konsoli zarządzającej znajdującej się poza siecią LAN organizacji poprzez połącznie konsoli ze wskazanym serwerem aplikacji.
17. Oprogramowanie musi umożliwiać prowadzenie w czasie rzeczywistym dwukierunkowej komunikacji tekstowej (chat) pomiędzy użytkownikiem a administratorem.

Automatyzacja

1. 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.
2. Oprogramowanie musi umożliwiać tworzenie zadań dystrybucji polegające na jednorazowym uruchomieniu wybranego szablonu akcji na wybranych stanowiskach komputerowych.
3. Oprogramowanie musi umożliwiać tworzenie polis uruchamianych cyklicznie na wybranych stanowiskach komputerowych wg aktualnej przynależności do struktury organizacyjnej, lokalizacyjnej lub wybranych grup dynamicznych.
4. 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.
5. 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.
6. Oprogramowanie musi umożliwiać szyfrowanie plików źródłowych dla zadań instalacji.
7. Oprogramowanie musi umożliwiać globalny przegląd postępu wykonania wybranych zadań oraz polis wraz z odczytem standardowego wyjścia (stdout) oraz standardowego wyjścia błędów (stderr).
8. Oprogramowanie musi umożliwiać tworzenie własnych szablonów akcji zawierających zdefiniowaną listę akcji pozwalających na warunkowe uruchamianie akcji zależnych (oczekiwanie na zakończenie akcji, praca w tle).
9. 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.
10. Oprogramowanie musi umożliwiać konfigurowanie dedykowanych parametrów dla każdej z ww. akcji.

11. 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.
12. Oprogramowanie musi umożliwiać ograniczenie zakresu działania zadania, polisy oraz zawężenie wszelkich raportów systemowych do stanowisk spełniających kryteria wybranej dynamicznej grupy stanowisk.
13. Oprogramowanie w zakresie automatyzacji musi realizować m.in. następujące przypadki użycia z wykorzystaniem mechanizmu grup dynamicznych dla zadań oraz polis:
    - Automatyczną instalacji aplikacji na komputerach spełniających warunki: stanowiska z Windows 10 z pamięcią RAM>4GB i zainstalowaną wybraną aplikacją w wersji mniejszej (np. 7.0)
    - Automatyczne odinstalowanie aplikacji na komputerach spełniających warunki: stanowiska z Windows 7 gdzie producentem komputera jest np. Dell i zainstalowaną wybraną aplikacją w wersji większej niż (np. 8.0)
    - Dystrybucję plików oraz folderów (ze wskazaną zawartością np. dokumenty, skróty do aplikacji) na pulpity stanowisk komputerowych spełniających warunki: stanowiska z Windows 10 z brakiem zainstalowanej wybranej aplikacji oraz nie posiadające konta użytkownika z prawami administracyjnymi
    - Uruchomienia wybranego skryptu PowerShell dla komputerów spełniających warunki: stanowiska z Windows 10 w architekturze 32 bitowej, zainstalowaną aplikacją X w wersji większej niż (np. 6.0) i brakiem zainstalowanej aplikacji Y.
    - Uruchomienia wybranych szablonów akcji w przypadku wykrycia zmiany jednostki organizacyjnej stanowiska komputerowego.
14. W przypadku wcześniej zdefiniowanych polis wymagane jest, aby zostały one automatycznie uruchomione dla nowych stanowisk komputerowych po spełnieniu warunków przynależności do określonych grup dynamicznych.
15. Oprogramowanie musi umożliwić instalację oprogramowania z plików exe, które nie posiadają instalacji w trybie cichym poprzez automatyzację procesu manualnej instalacji (nagrywanie makr w zakresie wyborów typu zaznaczenie checkbox, wybór pozycji z listy, kliknięcie przycisku, wpisanie parametru/ścieżki itp.)
16. Oprogramowanie musi posiadać repozytorium szablonów makr automatyzacji do późniejszego wykorzystania podczas procesów instalacji
17. Oprogramowanie musi zawierać funkcję testowania nagranych makr z poziomu interfejsu użytkownika
18. Oprogramowanie musi wznawiać instalację, w przypadku przerwania procesu instalacji (np. z powodu wyłączenia komputera)
19. Nagrywanie makr musi być realizowane przez wybranie/wskazanie elementu okna, na którym ma zostać wykonana akcja (np. kliknięcie, wprowadzenie tekstu, zaznaczenie)
20. Oprogramowanie musi umożliwiać wysyłanie komunikatów (Windows Notification) do wskazanych stanowisk komputerowych (wybór manualny, wg struktury organizacyjnej, lokalizacyjnej lub grupy dynamicznej)
21. Oprogramowanie musi umożliwiać wysyłanie komunikatów przed każdą zdefiniowaną akcją automatyzacji (np.: przed rozpoczęciem instalacji pakietu MSI, przed dystrybucją plików, przed uruchomieniem skryptu PowerShell)
22. Oprogramowanie musi umożliwiać automatyzację procesu konfiguracji dowolnej aplikacji Windows w celu odtworzenia zapamiętanych akcji (makr) dla wskazanych stanowisk komputerowych.

Backup danych użytkownika

1. Oprogramowanie musi umożliwiać tworzenie dowolnej ilości automatycznych zadań w zakresie archiwizacji danych – globalnie z poziomu głównej konsoli zarządzającej.
2. Oprogramowanie musi umożliwiać globalną zmianę parametrów zadań archiwizacji (ilość archiwów, kompresja, okres, zakres).
3. Oprogramowanie musi umożliwiać definiowanie rozszerzeń plików, które mają być pomijane podczas procesu archiwizacji oraz rozszerzeń plików np. *.doc, które mają być archiwizowane.
4. Oprogramowanie Agenta musi umożliwiać kopię całościową danych oraz przesyłanie plików z archiwizacji na wskazany serwer FTP.
5. Mechanizm archiwizacji danych musi być realizowany przez Agenta systemu bez udziału zdalnych sesji (typu zdalny pulpit, wywoływanie skryptów)
6. Oprogramowanie musi umożliwiać definiowanie cyklu archiwizacji.
7. Oprogramowanie musi umożliwiać automatyczne usuwanie starszych plików kopii całościowej, definiowanie globalnego zadania archiwizacji.

Zarządzanie urządzeniami USB Storage

1. Oprogramowanie musi umożliwiać zapisywanie w bazie danych informacji o kopiowaniu z/do urządzeń zewnętrznych typu: Pendrive USB, dysk zewnętrzny.
2. 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.
3. Oprogramowanie musi umożliwiać blokadę oraz autoryzację wybranych urządzeń USB w obrębie klasy USBStorage.
4. Oprogramowanie musi umożliwiać włączenie trybu ReadOnly dla klasy USBStorage
5. Oprogramowanie musi umożliwiać całkowitą blokadę klasy FDD/CD/DVD

Monitoring stanowisk komputerowych

1. Oprogramowanie musi umożliwiać zestawienie najpopularniejszych adresów (jakie stanowiska je wywoływały, kiedy) z możliwością zapisu całego adresu lub tylko głównej strony.
2. Oprogramowanie umożliwia zestawienie najaktywniejszych stanowisk (pod kątem WWW), jakie adresy odwiedzały, kiedy, wszystkie zestawienia do poziomu: jednostka organizacyjna, stanowisko, zalogowany użytkownik.
3. Oprogramowanie musi umożliwiać analizę uruchamianych aplikacji (aktywność stanowisk wg aplikacji oraz wykorzystanie zainstalowanych aplikacji wg stanowisk).
4. Oprogramowanie musi umożliwiać analizę efektywności pracy użytkowników na poszczególnych aplikacjach
5. 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).
6. Oprogramowanie musi umożliwiać tworzenie statystyk aktywności stron WWW oraz aktywności stanowisk.
7. Oprogramowanie musi umożliwiać podział stron na dozwolone i zabronione.
8. Oprogramowanie musi umożliwiać wydruki tabelaryczne oraz graficzne (wykresy aktywności).

9. Oprogramowanie musi umożliwiać okresowe tworzenie zrzutu ekranu użytkownika z możliwością przesłania go na serwer.
10. Oprogramowanie musi umożliwiać rozróżnienie stanów monitorowanego komputera w szczególności stan aktywności (focus okna), hibernacji, uśpienia oraz wylogowania
11. Oprogramowanie musi umożliwiać odczyt aktywności użytkownika w czasie rzeczywistym w zakresie min. tytuł okna, adres www przeglądanej strony z dokładnością do 1 sekundy.
12. Oprogramowanie musi umożliwiać analizę aktywności myszy oraz klawiatury dla poszczególnych monitorowanych aplikacji oraz stron internetowych (ilość kliknięć).
13. Oprogramowanie musi umożliwiać monitorowanie wszystkich prac drukowania generowanych na urządzeniach sieciowych udostępnionych przez centralny serwer wydruków i udostępnionych lokalnie przez port TCP/IP
14. 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.
15. 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.
16. Oprogramowanie musi posiadać możliwość definicji kosztów wydruku dla poszczególnych urządzeń drukujących (podział kosztu na mono/kolor).

ServiceDesk – Zarządzanie zgłoszeniami

1. 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)
2. Oprogramowanie musi umożliwiać zgłaszania przez użytkowników z poziomu przeglądarki WWW (dedykowany portal) awarii sprzętu, usług, oprogramowania i innych typów awarii zdefiniowanych przez administratora.
3. Portal ServiceDesk musi mieć możliwość obsługi przez wiodące przeglądarki WWW na urządzeniach mobilnych poprzez responsywny interfejs użytkownika.
4. Portal ServiceDesk musi umożliwiać wybór wersji językowej interfejsu (co najmniej polski i angielski).
5. Obsługa listy zgłoszeń serwisowych (incydentów i problemów) musi być realizowana przez portal ServiceDesk z zachowaniem nadanego poziomu uprawnień.
6. Oprogramowanie musi umożliwiać kontrolę obciążenia działu IT, optymalizację podziału pracy pomiędzy pracowników działu IT oraz przegląd awaryjności sprzętu.
7. Oprogramowanie musi umożliwiać uwierzytelnianie użytkowników wykorzystując bazę Active Directory poprzez protokół LDAP.
8. Oprogramowanie musi umożliwiać automatyczne autoryzowanie określonych stanowisk i użytkowników (z wykorzystaniem mechanizmy SSO), aby uniknąć każdorazowego uwierzytelniania przed korzystaniem z systemu zgłoszeń.
9. Oprogramowanie musi umożliwiać sortowanie listy zgłoszeń awarii, wg daty zgłoszenia, priorytetu, statusu.

10. Oprogramowanie musi umożliwiać filtrację zgłoszeń wg priorytetu oraz statusów zgłoszeń, stanowisk oraz inżynierów obsługujących zgłoszenia.
11. Oprogramowanie musi umożliwiać tworzenie dedykowanych list zgłoszeń z różnymi danymi, domyślnym filtrowaniem i sortowaniem.
12. Oprogramowanie musi umożliwiać określenie widoczności poszczególnych list zgłoszeń w zależności od zalogowanego użytkownika.
13. Oprogramowanie musi umożliwiać określenie widoczności zgłoszeń w zależności od kategorii i lokalizacji zgłoszeń przypisanych do zalogowanego użytkownika.
14. Oprogramowanie musi umożliwiać dostęp do zgłoszeń swoich podwładnych przez przełożonego.
15. 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.
16. Oprogramowanie musi umożliwiać tworzenie zadań w ramach konkretnego zgłoszenia z możliwością przekazania do realizacji przez innych użytkowników.
17. Oprogramowanie musi umożliwiać tworzenie globalnych zadań do realizacji przez zalogowanego użytkownika.
18. Oprogramowanie musi umożliwiać tworzenie szablonów zadań.
19. Oprogramowanie musi umożliwiać rejestrację czasu pracy poświęconego na realizację zgłoszenia przez opiekuna.
20. Oprogramowanie musi umożliwiać przesyłanie użytkownikom powiadomień pocztą elektroniczną o nowych wpisach i zmianach w zgłoszeniu.
21. Oprogramowanie musi umożliwiać edycję szablonów powiadomień email.
22. Oprogramowanie musi umożliwiać tworzenie wielopoziomowych list kategorii zawierających nazwę i opis kategorii.
23. Oprogramowanie musi umożliwiać określenie widoczności poszczególnych kategorii w zależności od zalogowanego użytkownika.
24. Oprogramowanie musi umożliwiać tworzenie pól dodatkowych na formularzu rejestracji zgłoszenia.
25. Oprogramowanie musi umożliwiać określenie widoczności poszczególnych pól dodatkowych w zależności od zalogowanego użytkownika.
26. 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.
27. Oprogramowanie musi umożliwiać edycję bazy wiedzy z poziomu przeglądarki WWW wraz z możliwością formatowania tekstu (wraz z grafiką) oraz wstawiania załączników.
28. Oprogramowanie musi umożliwiać administratorowi wprowadzenie do systemu zgłoszenia użytkownika, który nie ma dostępu do PC (np. telefoniczna informacja o awarii komputera).
29. Oprogramowanie musi umożliwiać delegowanie zgłoszenia innemu administratorowi (technikowi), jak również przejęcie innego zgłoszenia (np. w przypadku nieplanowanej nieobecności pracownika).
30. 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.

31. Oprogramowanie musi umożliwiać informowanie pracowników o planowanych działaniach, awariach za pomocą komunikatów wprowadzanych na stronę główną panelu zgłaszania usterki, bądź do poszczególnych kategorii.
32. Oprogramowanie musi umożliwiać określenie widoczności komunikatów o planowanych działaniach, awariach w zależności od zalogowanego użytkownika.
33. Oprogramowanie musi umożliwiać tworzenia baz umów serwisowych powiązanych z bazami firm serwisowych (dostawców sprzętu, oprogramowania, lokalnych serwisów). lub z zakupionym sprzętem.
34. Oprogramowanie w oparciu o bazę firm/umów serwisowych musi umożliwiać zapis przekazania zgłoszenia do serwisu zewnętrznego.
35. Oprogramowanie musi umożliwiać przesyłanie powiadomień do firm serwisowych powiązanych ze zgłoszeniem.
36. Oprogramowanie musi posiadać możliwość rejestracji w historii zgłoszenia (w komentarzach) korespondencji
37. mailowej między opiekunami zgłoszenia a firmami serwisowymi powiązanymi ze zgłoszeniem.
38. 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).
39. Oprogramowanie musi umożliwiać wyświetlenie w panelu WWW użytkownika informacji nt. powiązanych z użytkownikiem zasobów (przypisane stanowiska PC, przydzielone licencje aplikacji, wydane urządzenia).
40. Oprogramowanie musi umożliwiać wybranie zasobu w określonej kategorii powiązanego z użytkownikiem podczas rejestracji zgłoszenia.
41. Oprogramowanie musi umożliwiać tworzenie zgłoszeń cyklicznych z możliwością definiowania częstości występowania oraz typu okresu (codziennie, co tydzień, co miesiąc)
42. 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.
43. Oprogramowanie musi umożliwiać tworzenie szablonów komentarzy wykorzystywanych przez opiekunów zgłoszeń.

44. Oprogramowanie musi posiadać możliwość rejestracji zgłoszeń i komentarzy drogą mailową, zarówno przez zarejestrowanych użytkowników systemu jak i niezarejestrowanych użytkowników.
45. Oprogramowanie musi umożliwiać obsługę dowolnej ilości kont pocztowych do wysyłania powiadomień i generowania zgłoszeń/komentarzy przez email.
46. Oprogramowanie musi posiadać wbudowane raporty prezentujące m.in. realizację obsługi zgłoszeń w zakładanym SLA (statystyka miesięczna, kwartalna, roczna).
47. Oprogramowanie musi umożliwiać definiowanie własnych widoków oraz zestawień dla każdego zalogowanego użytkownika
48. Oprogramowanie musi umożliwiać zdefiniowanie własne macierzy priorytetów na podstawie pilności oraz wpływu zgłoszenia
49. Oprogramowanie musi umożliwiać zamodelowanie trzy zmianowego trybu pracy inżynierów (opiekunów zgłoszeń)
50. Oprogramowanie musi umożliwiać informowanie użytkowników o nowych zdarzeniach systemowych za pomocą notyfikacji (dymku) podczas pracy z systemem
51. Oprogramowanie musi umożliwiać tworzenie obiegu procesu decyzyjnego dla wniosków o uprawnienia lub elementy konfiguracji w oparciu o bazę CMDB
52. Oprogramowanie musi umożliwiać zaprojektowanie dowolnego formularza do wprowadzania danych z wykorzystaniem własnych atrybutów (wraz ze zmianą układu/położenia atrybutów w projektowanym widoku)
53. Oprogramowanie musi umożliwiać definicję czasów SLA w oparciu o matrycę priorytetów, statusy, kategorie lub dowolne warunki i atrybuty zgłoszenia
54. Oprogramowanie musi umożliwiać dodanie Akceptacji do już istniejącego zgłoszenia
55. Oprogramowanie musi umożliwiać definiowanie własnych reguł zarządzania w oparciu o warunki i akcje dla Prawdy i Fałszu (zdarzenie -> warunek -> akcja)
56. Oprogramowanie musi umożliwiać tworzenie wielu zgłoszeń poprzez wybór kilku użytkowników w zgłoszeniu
57. Oprogramowanie musi umożliwiać tworzenie słowników wartości dla atrybutów w oparciu o strukturę płaską lub drzewiastą
58. Oprogramowanie musi umożliwiać tworzenie atrybutów zależnych poprzez określone warunki widoczności
59. Oprogramowanie musi umożliwiać definiowanie formularzy zamykających zgłoszenie oraz zatwierdzające zmiany w zgłoszeniu
60. Oprogramowanie musi umożliwiać definiowanie reguł biznesowych za pomocą graficznego/blokowego kreatora.
61. Oprogramowanie musi umożliwiać definiowanie obiegów za pomocą graficznego/blokowego kreatora.
62. Oprogramowanie musi umożliwiać tworzenie niestandardowych raportów za pomocą kreatora.
63. Oprogramowanie musi umożliwiać definiowanie poziomu dostępu do zgłoszeń dla dynamicznych grup użytkowników.
64. Oprogramowanie musi umożliwiać definiowanie formularzy dla zgłoszeń w danej kategorii za pomocą kreatora Drag&Drop z możliwością określenia układu kolumn.
65. Oprogramowanie musi umożliwiać tworzenie dowolnej liczby Dashboard-ów dla użytkownika za pomocą kreatora Drag&Drop.
66. Oprogramowanie musi umożliwiać zmianę układu szczegółów zgłoszenia za pomocą kreatora Drag&Drop.
67. Oprogramowanie musi umożliwiać udostępniania ogłoszeń w formie Widget-u oraz okienka modalnego z wymaganym potwierdzeniem dla użytkownika.

68. Oprogramowanie musi umożliwiać zaprojektowanie dowolnego szablonu protokołu zgłoszenia.
69. Oprogramowanie musi udostępniać matrycę(wpływ/pilność) dla obliczania priorytetu zgłoszeń.
70. Oprogramowanie musi umożliwiać zmianę koloru dla statusu/priorytetu/wpływu/pilności zgłoszenia prezentowanego na liście zgłoszeń.
71. Oprogramowanie musi umożliwiać definiowanie dowolnych kolejek zgłoszeń.
72. Oprogramowanie musi umożliwiać rejestrację nieobecności administratorów z możliwością wybrania zastępstwa.

ServiceDesk – Zarządzanie wnioskami

1. Oprogramowanie musi zapewnić obsługę Workflow w zgłoszeniach serwisowych poprzez zdefiniowanie logicznych ścieżek (zbiór węzłów logicznych).
2. 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.
3. 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

1. Oprogramowanie musi umożliwiać inwentaryzację Systemów Informatycznych oraz Zbiorów danych
2. Oprogramowanie musi umożliwiać określanie powiązań pomiędzy pracownikami z Systemami Informatycznymi oraz Zbiorami danych
3. Oprogramowanie musi umożliwiać budowanie powiązanych zestawów atrybutów dla Systemów Informatycznych oraz Zbiorów danych (np. termin ważności dostępu, poziom dostępu, przetwarzanie danych wrażliwych)
4. Oprogramowanie musi umożliwiać tworzenie ścieżek decyzyjnych dla dowolnych wniosków o uprawnienia do Systemów Informatycznych oraz Zbiorów danych
5. Oprogramowanie musi umożliwiać akceptację poszczególnych etapów przez dedykowane osoby decyzyjne zdefiniowane w konfiguracji ścieżek
6. Oprogramowanie musi umożliwiać akceptację etapów ścieżki przez automatyczny wybór powiązanych opiekunów merytorycznych oraz technicznych
7. Oprogramowanie musi umożliwiać definiowanie dowolnych akcji dla poszczególnych kroków (np. zmiana opiekuna, statusu)
8. Oprogramowanie musi umożliwiać automatyczne tworzenie powiązań pracownika z Systemem informatycznym lub Zbiorem danych po akceptacji wniosku
9. Oprogramowanie musi umożliwiać obsługę procesu (wniosku) o odebranie uprawnień (koniec terminu dostępu, zwolnienie pracownika)
10. Oprogramowanie musi umożliwiać raportowanie uprawnień wg Systemów Informatycznych oraz Zbiorów danych dla poszczególnych osób
11. Oprogramowanie musi umożliwiać raportowanie uprawnień w pracowników do Systemów Informatycznych oraz Zbiorów danych
12. Oprogramowanie musi umożliwiać generowanie edytowalnej Karty Uprawnień Pracownika

ServiceDesk – Zarządzanie rezerwacjami

1. Oprogramowanie musi umożliwiać rezerwację dowolnego aktywnego zasobu w systemie.
2. Oprogramowanie musi umożliwiać kategoryzowanie rejestrowanych rezerwacji.
3. Oprogramowanie musi umożliwiać określenie widoczności poszczególnych kategorii rezerwacji w zależności od zalogowanego użytkownika.
4. Oprogramowanie musi informować o możliwych konfliktach podczas tworzenia/edycji rezerwacji z zasobem.
5. Oprogramowanie musi prezentować informacje o rezerwacjach w formie graficznej – kalendarza.
6. Oprogramowanie musi umożliwiać akceptację, odrzucenie lub anulowanie rezerwacji przez upoważnionych użytkowników.

Monitoring sieci LAN

1. 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
2. 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.
3. Oprogramowanie musi umożliwiać wizualizację ruchu sieciowego na poszczególnych portach urządzeń sieciowych wraz z wizualizacją w postaci mapy sieci dla wskazanego urządzenia typu switch, router.
4. Oprogramowanie musi umożliwiać z zdalną instalację agenta systemu z poziomu wykrytej struktury sieciowej z wykorzystaniem poświadczeń administracyjnych, w tym również stanowisk poza usługą katalogową.
5. Oprogramowanie musi umożliwiać monitorowanie stanu dowolnej usługi sieciowej TCP.
6. Oprogramowanie musi umożliwiać monitorowanie dowolnego licznika SNMP(v1/2/3) urządzenia.
7. Oprogramowanie musi umożliwiać monitorowanie stanu dowolnego urządzenia sieciowego poprzez odpytywanie typu PING.
8. Oprogramowanie musi umożliwiać tworzenie konfigurowalnych zdarzeń sieciowych powodujących wysyłanie komunikatów informacyjnych i/lub ostrzegawczych poprzez SMS i/lub Email.

Zarządzanie dokumentami

1. Oprogramowanie musi umożliwiać centralną ewidencję dokumentów
2. Oprogramowanie musi umożliwiać zawierać dedykowany formularz dodawania nowego dokumentu z możliwością edycji widocznych oraz wymaganych atrybutów dokumentu
3. Oprogramowanie musi umożliwiać dołączenie skanu dokumentu (m.in.: skany faktur, umów)
4. Oprogramowanie musi umożliwiać stworzenie dedykowanego zbioru ról i uprawnień w zakresie obsługi rejestru dokumentów
5. Oprogramowanie musi umożliwiać utworzenie pomocniczych rejestrów oraz słowników
6. Oprogramowanie musi umożliwiać przeszukiwanie bazy dokumentów oraz kontrahentów po dowolnie wskazanym atrybucie opisującym

7. Oprogramowanie musi umożliwiać utworzenie rejestru osób reprezentujących
8. Oprogramowanie musi umożliwiać analizę zmian wartości dowolnych atrybutów opisujących dokument w zakresie daty zmiany, aktualnej/poprzedniej wartości oraz osoby dokonującej zmiany

System wewnętrznego komunikatora dla użytkowników

1. Oprogramowanie musi zawierać wewnętrzny komunikator pracujący w sieci LAN, integrujący się z usługą katalogową w zakresie kont użytkowników (dane osobowe, avatar), jednostek organizacyjnych.
2. Oprogramowanie w zakresie modułu komunikatora dla użytkowników musi współpracować z serwerem MSSQL Server 2008R2-2019 lub PostrgeSQL
3. Oprogramowanie komunikatora musi umożliwiać automatyczne logowanie użytkowników pochodzących z usługi katalogowej.
4. Oprogramowanie komunikatora musi umożliwiać konwersację grupową oraz prywatną pomiędzy użytkownikami
5. Oprogramowanie komunikatora musi umożliwiać wysyłanie wiadomości powitalnych; komunikatów grupowych z raportowaniem doręczenia oraz odczytania.
6. Oprogramowanie komunikatora musi umożliwiać generowanie raportów doręczenia/odczytania wiadomości wymagających potwierdzenia.
7. Oprogramowanie komunikatora musi umożliwiać określenie maksymalnego rozmiaru transferowanego pliku (przez administratora).
8. Oprogramowanie komunikatora musi umożliwiać wysyłanie powiadomień e-mail o utworzeniu/modyfikacji użytkowników, którzy nie pochodzą z usługi katalogowej.
9. Oprogramowanie komunikatora musi umożliwiać automatyczną aktualizację wg. zadanej konfiguracji danych synchronizowanych (ze szczególnym uwzględnieniem danych o użytkownikach, jednostkach organizacyjnych z usługi katalogowej).
10. Oprogramowanie komunikatora musi umożliwiać archiwizację starych rozmów między użytkownikami.
11. Oprogramowanie komunikatora musi umożliwiać administratorowi wyłączenie globalnie możliwości zamknięcia/wylogowanie/zapisywanie poświadczeń dla klientów końcowych.
12. Oprogramowanie komunikatora musi umożliwiać administratorowi bezpieczeństwa wgląd do rozmów pracowników, wyłączenie wybranych funkcjonalności dla klienta końcowego (np. transferu plików, konferencji audio-video).
13. Oprogramowanie komunikatora musi umożliwiać wymianę plików pomiędzy zalogowanymi użytkownikami
14. Oprogramowanie komunikatora musi umożliwiać nawiązanie sesji audio oraz wideo pomiędzy zalogowanymi użytkownikami wraz z obsługą konferencji grupowych.

Wymagania formalne:

1. Dostarczone licencje na oprogramowanie muszą być bezterminowe.
2. Dostarczone licencje na oprogramowanie muszą być dostarczone z wsparciem producenta, liczonym od daty zakończenia wdrożenia do 30.06.2026r.
3. Licencja należy dostarczyć dla Urzędu Gminy oraz Gminnego Ośrodka Pomocy Społecznej.
4. Obsługa serwisowa w zakresie obsługi błędów realizowana ma być z czasem reakcji 16 godzin roboczych oraz czasem naprawy 80 godzin roboczych. W ramach wsparcia

wymagany jest dostęp do nowych wersji systemu oraz wsparcia technicznego producenta.

5. Dostarczone licencje na oprogramowanie muszą objąć co najmniej 60 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 dwie licencje dostępowe do konsoli zarządzającej.
6. 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.
7. Zamawiający wymaga od wykonawcy, aby w terminie 10 dni od podpisania umowy przeprowadził wdrożenie systemu zdalnie (wymagana co najmniej 1 sesja – 5 godzinna):
   a. Analiza przedwdrożeniowa wraz z konsultacją co do wyboru właściwej ścieżki wdrożeniowej.
   b. Instalacja oraz konfiguracja bazy danych.
   c. Instalacja oraz konfiguracja serwera.
   d. Instalacja oraz konfiguracja głównej konsoli zarządzającej.
   e. Instalacja oraz konfiguracja usługi serwera licencji (tylko dla klucza sieciowego).
   f. Określenie parametrów pracy aplikacji klienckich.
   g. Przygotowanie skonfigurowanej paczki MSI z przygotowaną wcześniej konfiguracją aplikacji klienckiej według ustaleń z Zamawiającym.
   h. Manualna instalacja testowej grupy aplikacji klienckich (maksymalnie 5 stacji) celem sprawdzenia poprawności komunikacji z bazą danych, serwerem oraz konsolą zarządzającą.
   i. Sprawdzenie poprawności instalacji paczki MSI.
   j. Sprawdzenie poprawności działania wdrożonych stref systemu (testy akceptacyjne).

Sekretarz Gminy

/-/ Dariusz Wawrzyniak