Załącznik nr 3 do SWZ

Przedmiot zamówienia: Kompleksowy system do zarządzania zasobami IT, użytkownikami oraz bezpieczeństwem w ramach projektu „Podniesienie poziomu cyberbezpieczeństwa w Urzędzie Miejskim w Grudziadzu”.

1. **Architektura / budowa:**
   - **1.1.** System musi umożliwić bezproblemową i stabilną obsługę co najmniej 450 Klientów jednocześnie.
   - **1.2.** System musi posiadać co najmniej 8 dostępów administracyjnych (tzw. użytkownik nazwany) umożliwiające jednoczesne działania administratorów w konsoli systemu.
   - **1.3.** Architektura / budowa:
     - **1.3.1.** Klient – komponent odpowiedzialny za zarządzanie komputerem, zbieranie danych oraz przesyłanie danych do serwera z wykorzystaniem bezpiecznego połączenia, pracujący w trybie usługi systemowej.
       - **1.3.1.1.** Połączenie klient – serwer, Komunikacja odbywa się z wykorzystaniem TLS 1.3.
       - **1.3.1.2.** Serwer i klient posiadają certyfikaty SSL (4096 bitowe).
     - **1.3.2.** Konsola administracyjna – przeznaczona do zarządzania całym systemem, w formie w pełni funkcjonalnej aplikacji internetowej (webowej). Pozwala na realizację pełnego zarządzania systemem oraz zasobami, wyposażona w mechanizmy do edycji/modyfikacji/usuwania i analizy danych, zawierająca mechanizmy raportowania (nie jest dopuszczalne stosowanie aplikacji webowej do przeglądania danych oraz innej aplikacji do wprowadzania/edycji danych).
     - **1.3.3.** Panel pracownika – aplikacja webowa, niewymagająca dodatkowego logowania, dostępna dla pracowników i uruchamiana na komputerach pracowników udostępniająca wybrane dane z konsoli administracyjnej oraz pozwalająca na interakcję z pracownikiem w wybranych obszarach zgodnie ze specyfikacją opisaną poniżej.
     - **1.3.4.** Serwer – oprogramowanie odpowiadające za utrzymywanie komunikacji i wymianę danych z Klientami.
     - **1.3.5.** Baza danych powinna umożliwiać pracę na silniku Microsoft SQL w wersji bezpłatnej lub komercyjnej.
   - **1.4.** Konfiguracja Architektury:
     - **1.4.1.** Komponenty Klient, konsola administracyjna, serwer, baza danych muszą się aktualizować samodzielnie za pośrednictwem bezpiecznego połączenia z serwerów aktualizacji producenta systemu.
     - **1.4.2.** Czas aktualizacji wszystkich komponentów systemu: serwer, konsola administracyjna, baza danych, agenci - nie może przekroczyć 24h od wydania przez producenta nowej wersji dowolnego komponentu. Agenci na komputerach muszą się zaktualizować samodzielnie w czasie nie dłuższym niż 1h od pobrania aktualizacji od producenta, przy czym aktualizacja Klientów musi przebiegać
       w pełni automatycznie z wykorzystaniem funkcjonalności wbudowanej w system (bez użycia zewnętrznych narzędzi, np. MS Active Directory). W przypadku, gdy połączenie pomiędzy systemem a serwerem aktualizacji producenta nie jest dostępne musi być możliwość dokonania aktualizacji manualnie poprzez

pobranie od producenta paczki aktualizacyjnej w postaci jednego pliku z kompletną aktualizacją.

1.4.3. System musi w sposób w pełni automatyczny z wykorzystaniem serwera aktualizacji producenta aktualizować wzorce aplikacji, pakietów, pomoc i inne wbudowane bazy wiedzy.

1.4.4. Klient do działania nie może wymagać instalacji komponentów pomocniczych typu .NET Framework lub innych z wyłączeniem komponentów WMI.

1.4.5. Klient musi być dostępny dla administratora z poziomu webowej interfejsu konsoli administracyjnej zawsze w najnowszej wersji wydanej przez producenta (bez konieczności pobierania go od producenta), w postaci pliku *.msi gotowego do zainstalowania (bez konieczności dodatkowego wykonywania zmian/ustalania parametrów) w pliku *.msi.

1.4.6. Klient musi być możliwy do zainstalowania za pośrednictwem MS Active Directory, za pomocą skryptów lub manualnie, poprzez uruchomienie na danej stacji roboczej.

1.4.7. System zapewnia możliwość stworzenia instalatora (.exe) z wbudowanymi, zaszyfrowanymi poświadczeniami dla dowolnego konta. Funkcja ta umożliwia instalację usługi bezpośrednio na kontach użytkowników – zarówno lokalnych, jak i domenowych, korzystając z uprawnień zdefiniowanych dla instalatora w konsoli systemu.

1.4.8. Klient musi pracować w trybie niewidocznym dla użytkownika (usługa systemowa).

1.4.9. System powinien umożliwiać generowanie unikatowego identyfikatora Klienta – wygenerowanego losowo i unikatowo (np. za pomocą mechanizmu typu GUID) lub w sposób powtarzalny dla danego komputera) na podstawie kombinacji parametrów wybranych przez użytkownika systemu spośród następujących: nazwy producenta BIOS, numeru seryjnego komputera, system UUID, nazwy komputera, dowolnego oraz losowego ciągu znaków.

1.4.10. Klient musi mieć definiowalny priorytet pracy (ABOVE_NORMAL, NORMAL, BELOW_NORMAL, IDLE), przy czym w każdym momencie administrator może automatycznie z poziomu konsoli administracyjnej systemu wydać polecenie zmiany tej konfiguracji na dowolnej grupie komputerów.

1.4.11. Klient musi wspierać wiele różnych adresów serwera rozumianych jako adresy w sieci lokalnej, rozległej (VPN) oraz za NATem i potrafić wykorzystać adres dostępny (na którym następuje połączenie z serwerem) w dowolnym momencie działania, bez konieczności restartu Klienta.

1.4.12. System musi umożliwiać komunikację pomiędzy Klientami a serwerem w sieciach lokalnych, rozległych, także gdy komputery znajdują się za NATem.

1.4.13. System musi mieć możliwość współpracy komponentów Klient i serwer w taki sposób, aby serwer mógł współpracować ze wszystkimi poprzednimi wersjami Klientów.

1.5. System musi mieć wbudowane mechanizmy automatycznej konserwacji/utrzymania zgodnie ze zdefiniowanym harmonogramem.

1.5.1. Automaty powinny realizować co najmniej:

1.5.1.1. Usuwanie zbędnych danych z systemu (dane z monitoringu uruchamianych aplikacji, uruchamianych procesów, odwiedzonych stron www, wydrukowanych dokumentów, indeksowanie bazy danych, kopie bezpieczeństwa przyrostowe i nie przyrostowe, zmniejszanie bazy danych.

1.5.2. Harmonogram musi mieć możliwość ustalenia częstotliwości wykonywania zadania (godzina, dzień, tydzień, miesiąc), możliwość zmiany wartość

parametrów wejściowych do wykonania danej konserwacji, a także zatrzymania/uruchomienia wybranych pozycji harmonogramu w dowolnym momencie.

2. **Wymagania systemowe:**

2.1. Konsola administracyjna musi działać w pełni responsywnie (niezależnie od wielkości i rozdzielczości ekranu urządzenia wyświetlającego) na dowolnej przeglądarce stron WWW zgodnej z HTML5 (np. Internet Explorer 11, FireFox, Chrome, Opera).

2.2. Klient musi działać na systemach 32 i 64 bitowych: Windows Server 2012/2012R2/2016/2019/2022, Windows 7/8/8.1/10/11, MacOS 10.7/10.8, Linux dla wersji: Ubuntu v.11.04 lub wyższa, Debian v.6.0 lub wyższa, RedHat v.6.0 lub wyższa, CentOS v.6.0 lub wyższa, Fedora v.16 lub wyższa.

2.2.1. Klient wspiera poniższe przeglądarki internetowe w zakresie monitorowania aktywności użytkownika w sieci: Opera wersja 63.0.3368.94, Chrome wersja 77.0.3865.90, FireFox wersja 69.0.2

2.3. Serwer musi działać na systemach 64 bitowych: Windows Server 2016/2019/2022, Windows 7/8/8.1/10/11.

2.4. Serwer www musi być oparty o platformę Microsoft 64 bit (Windows Server 2016/2019/2022, Windows 10 oraz Java 8 (JRE lub JDK), Apache Tomcat 8+.

2.5. Baza danych musi działać na silniku Microsoft SQL Server 2014/2016/2017/2019/2022 w wersji 64 bitowych zarówno komercyjnych jak i bezpłatnych (np. Microsoft SQL Server Express Edition).

2.6. System musi mieć możliwość pracy w środowisku wirtualnym Microsoft Hyper-V oraz VMWare.

3. **Interfejsy:**

3.1. System musi umożliwiać wielokrotny, zgodny z harmonogramem lub na życzenie, import użytkowników, komputerów, struktury organizacyjnej (całości bądź wybranego kontenera) z usługi MS Active Directory, przy czym import struktury organizacyjnej musi następować we wskazane miejsce struktury organizacyjnej zdefiniowanej w systemie.

3.1.1. Import obiektów z MS Active Directory musi być odporny na zmianę nazw obiektów (nazwy użytkownika, struktury organizacyjnej itp.) – podczas import zmienione dane muszą zostać odpowiednio zaktualizowane wg klucza UUID.

3.1.2. Import z Active Directory musi wspierać obsługę protokołów SSL oraz TLS.

3.1.3. Import z Active Directory musi umożliwiać podanie więcej niż jednej domeny.

3.2. System musi umożliwiać import użytkowników z zewnętrznego pliku CSV.

3.3. System musi posiadać wbudowany, w pełni definiowalny przez administratora interfejs do importu innych niż komputery urządzeń (np. pendrive, monitory, switche itp.) wraz z danymi o kosztach zakupu, nr dokumentu zakupowego, dostawcy, daty zakupu, gwarancji. Interfejs dodatkowo musi umożliwiać importowanie użytkowników, struktur i licencji. Import musi umożliwiać pobieranie danych z CSV, Excel, Microsoft SQL Server, MySQL, PostgreSQL z wykorzystaniem sterownika ODBC (np. z pliku tekstowego, pliku *.xls, pliku *.xml) w sposób jednorazowy lub zgodnie
ze zdefiniowanym harmonogramem. Import aktualizuje te same dane wcześniej zaimportowane.

3.4. System musi umożliwiać pobieranie danych z komputerów (wyników skanowania) metodą bezpośredniego połączenia, za pośrednictwem serwera pocztowego (MAIL), za pośrednictwem serwera HTTP/HTTPS.

3.5. System zapewnia integrację z modelem LLM.

4. Funkcjonalności systemu zarządzania infrastrukturą IT:

4.1. Funkcjonalność Klienta:

4.1.1. System musi umożliwiać pełne zdalne zarządzanie Klientami (w sposób masowy i jednostkowy) w zakresie: uruchamiania i wyłączania Klienta, zmiany konfiguracji, uruchamiania skanowania, przekazania dowolnych zadań do wykonania (poleceń systemu operacyjnego).

4.1.2. Klient musi mieć możliwość konfiguracji zakresu skanowania plików w oparciu o nazwę plików (z uwzględnieniem znaków wieloznacznych), lokalizację na konkretnym dysku, datę utworzenia pliku oraz wielkość.

4.1.3. Klient musi mieć możliwość wyświetlenia dowolnego komunikatu w postaci HTML wysłanego z poziomu konsoli administracyjnej, konsola musi udostępnić dane o dacie i godzinie wyświetlenia komunikatu oraz użytkowniku, który go wyświetlił.

4.2. Funkcjonalność konsoli administracyjnej:

4.2.1. Konsola musi być w pełni polskojęzyczna oraz dodatkowo posiadać wersje językową angielską.

4.2.2. Interfejs konsoli musi być wyposażony w intuicyjne mechanizmy obsługi, musi zapewniać pełną obsługę funkcjonalną (dodawanie/modyfikacja/usuwanie).

4.2.3. Konsola administracyjna musi posiadać minimum 140 dashboardów – dashboard użytkownika, dashboard prezentujący parametry infrastruktury, dashboard prezentujący parametry sieci, dashboard prezentujący informacje o bezpieczeństwie.

4.2.4. Dashboard użytkownika jest budowany samodzielnie przez użytkownika poprzez wybór szybkiego skrótu do dowolnego ekranu aplikacji lub wybór widżetu.

4.2.5. Dashboard prezentujący parametry sieci zawiera widżety pogrupowane w kategorie: Czat, Gry, Peer to peer, Streaming, Usługa podstawowa, Usługa podstawowa (szyfrowana), Złośliwe oprogramowanie.

4.2.5.1. Lista monitorowanych usług: AIM/ICQ, BGMP, BGP, BitTorrent, Blaster, Dabber, DHCPv6 (client), DHCPv6 (server), Direct Connect, DNS, FTP (connection control), FTP (data port), FTPS (TLS/SSL)(connection control), FTPS (TLS/SSL)(data port), Gopher protocol, HTTP, HTTP Proxy, HTTPS, IMAP, IMAPS, IMAPv3, iperf, IRC, IRC, iSCSI, LDAP, LDAP (SSL), LDP, LogMeIn Hamachi, MMP, MPP, MS Exchange Routing, MS Media Server, MS SQL Server (monitor), MS SQL Server (server), MSDP, MSN, Mu Online, Mxit, MySQL, Nessus, NetBIOS (Datagram Service), NetBIOS (Name Service), NetBIOS (Session Service), NetBus, NNTP, NNTP (TLS/SSL), NTP, OpenVPN, POP3, POP3S, PostgreSQL, PPTP, Printer-IPP, Printer-RAW, Print-spooler, Rbot/Spybot, RDP, rsyns, RTCP, RTP, RTSP, Sasser, SFTP, SIP, SIP(TLS), SLP, SMB, SMTP,SMTPS, SNMP, SOCKS proxy, SSH, Steam, Structured Query Language (SQL) Services, TACACS, Telenet (TLS/SSL), Telnet, TSP, UUCP, VMware Server, VMware VAMI, WASTE, WHOIS, WINS, XMPP/Jabber, Yahoo, Messenger.

4.2.6. Dla każdej z usług prezentowane są relacje do wszystkich komputerów zawierające połączenia: powolne, nieosiągalne, rozłączone i poprawne wraz z czasami połączeń.

4.2.7. Dashboard prezentujący informacje o bezpieczeństwie zawiera widżety zawierające informacje: błędy serwera zadań, błędy smart, komputery bez BitLockera, komputery bez połączenia z serwerem, komputery z błędami typu critical / error / warning, duży transfer sieciowy, komputery bez Klienta, komputery offline, komputery online, komputery z naruszoną polityką dlp, komputery z nieaktualną polityką dlp, liczba administratorów lokalnych w systemie (online), logowanie w godzinach nocnych, monitorowanie transferu do dysków chmurowych, nieautoryzowana pamięć usb, nowe komputery, nowe urządzenia w sieci, oprogramowanie zabronione, przekroczone cal, przekroczone licencje, subskrypcje, które wygasły, systemy bez wsparcia, wielokrotne logowanie, wysokie użycie CPU, wysokie użycie ram, zaległe szkolenia wideo, zaległe wiadomości elearning, zbyt mało miejsca na hdd, zmiany na kontach użytkowników, zmiany tcp/ip.

4.2.8. Konsola administracyjna musi być wyposażona w panel zawierający graficzne widżety prezentujące dane w postaci wykresu kołowego i słupkowego bądź w formie tabeli z danymi.

4.2.9. Dane na widżetach muszą być aktualizowane automatycznie.

4.2.10. Widżety muszą być skojarzone dziedzinowo ze wszystkimi obszarami zarządzania infrastrukturą, a każdy obszar powinien być reprezentowany odpowiadające mu widżety (np. w obszarze zarządzania komputerami system powinien być wyposażony w widżety zawierające: ilość komputerów w ramach danego typu, ilość komputerów on/off-line, strukturę komputerów wg ilości pamięci RAM, ilość komputerów wg ilości wolnego miejsca na dysku, ilość komputerów wg dat ostatnich połączeń).

4.2.11. System musi posiadać filtr roboczy, przeszukujący całą tabelę po zdefiniowanym słowie.

4.2.12. System musi umożliwiać i zapamiętywać w profilu użytkownika indywidualną personalizację interfejsu konsoli administracyjnej (wybór wyświetlanych kolumn, ich kolejność, język, definiowanie filtrów, kolejność sortowania, wyświetlane widżety, ich konfigurację i kolejność).

4.2.12.1. System musi oferować możliwość dodawania własnych pól zarówno w głównym widoku, jak i w obszarze zarządzania użytkownikami. Te definiowalne pola powinny być w pełni funkcjonalne i umożliwiać:

4.2.12.1.1. Dodawanie nazwy kolumny, określenie jej typu oraz możliwość ograniczenia liczby znaków, które można wprowadzić.

4.2.12.1.2. Wśród obsługiwanych typów pól znajdują się: tekst, liczba całkowita, liczba, data, data i czas, combobox.

4.2.12.2. W ramach personalizacji widoku, system powinien oferować możliwość zastosowania filtrów dostosowujących zawartość danego widoku. Filtry te powinny:

4.2.12.2.1. Bazować na kolumnach dostępnych w danym widoku.

4.2.12.2.2. Umożliwiać selekcję operacji filtrujących takich jak: równość, nierówność, większość, mniejszość, obecność lub brak wartości.

4.2.12.2.3. Pozwalać na łączenie filtrów przy użyciu logicznych operatorów „AND” (i), „OR” (lub), „NOT AND” (i nie), „NOT OR” (lub nie).

4.2.12.2.4. Być zapamiętywane przez system dla konkretnej sesji użytkownika i pozostawać aktywne po ponownym zalogowaniu.

4.2.13. Dane prezentowane na wszystkich widokach/zakładkach w systemie muszą być dynamicznie filtrowane w oparciu o reguły utworzone przez dowolnego użytkownika systemu. Reguły muszą być zapamiętywane i dostępne w kolejnych sesjach oraz oparte co najmniej o: nazwę komputera, IP, rodzaj systemu operacyjnego, identyfikator Klienta, strukturę organizacyjną, stan Klienta (włączony/wyłączony), nazwę użytkownika zalogowanego, producenta sprzętu, dostawcę sprzętu, lokalizację komputera, dowolnie zdefiniowaną przez użytkownika wartość (np. kolor obudowy komputera). Użytkownik może wybrać za jednym razem więcej niż jedną regułę. Zmiana wybranej reguły powoduje aktualizację wyświetlonego widoku.

4.2.14. Dane prezentowane na wszystkich widokach/zakładkach w systemie muszą mieć możliwość filtrowania kolumnowego.

4.2.15. System musi umożliwiać definiowanie poziomu uprawnień dla grupy oraz użytkownika (odczyt, usuwanie, modyfikowanie, wydruk) do wszystkich widoków danych oraz wybranych elementów struktury organizacyjnej, musi być wyposażony w opcję dziedziczenia uprawnień. Odebranie praw do widoku lub zakładki na widoku powoduje ukrycie opcji.

4.2.16. Lista użytkowników / administratorów systemu musi być importowana i aktualizowana zgodnie z harmonogramem w oparciu o mechanizm RBAC (Role Base Access Control) z wybranego obiektu Active Directory. Użytkownik wyłączony/usunięty/zablokowany w Active Directory automatycznie traci prawa do korzystania z konsoli administracyjnej systemu.

4.2.17. Konsola musi umożliwiać wykonywanie poszczególnych poleceń na wielu rekordach, w szczególności na wszystkich rekordach, również tych, które nie są widoczne w konsoli w ramach jednej strony (zaznacz wszystko).

4.2.18. Konsola administracyjna musi zawierać szczegółowe informacje dotyczące pracy wszystkich komputerów: wersja Klienta, stanu Klienta (włączony/wyłączony), zalogowanego użytkownika, historii czasu włączenia i wyłączenia komputera.

4.2.19. Konsola musi umożliwić bezpośrednie przejście do witryny internetowej producenta z poziomu repozytorium producentów (o ile taka jest dostępna).

4.2.20. Konsola musi umożliwić bezpośrednie przejście do strony producenta zawierającej dodatkowe dane konfiguracyjne na temat konkretnego komputera w oparciu o Service Tag lub inny unikatowy identyfikator.

4.2.21. Konsola musi zawierać w sobie pełną dokumentację systemu, dokumentacja musi być na bieżąco aktualizowana poprzez automatyczne mechanizmy aktualizacji z serwera aktualizacji producenta.

4.3. Funkcjonalność panelu pracownika:

4.3.1. Automatyczne uruchamianie panelu oraz autoryzacja w momencie zalogowania użytkownika do systemu operacyjnego.

4.3.2. Zakres informacji w panelu jest definiowany przez administratora w formie schematów przypisywanych dla wybranych grup pracowników.

4.3.3. Panel pracownika użytkowany przez kierownika zawiera dodatkowo dane dostępne w panelach podległych pracowników w formie danych skumulowanych i analitycznych.

4.3.4. Wszelkie informacje udostępniane w panelu pracownika pogrupowane są w logiczne sekcje, z możliwością indywidulanego bądź grupowego włączania / wyłączania (ukrywania) sekcji.

4.3.5. Sekcje informacyjne panelu pracownika:

4.3.5.1. Zalogowany użytkownik – imię i nazwisko, IP, nazwa komputera, informacje z AD – Nazwa użytkownika, Imię, Nazwisko, E-mail, Firma, Dział, Stanowisko, Struktura org., Kraj, Województwo, Miasto, Ulica, Kod pocztowy, Telefon, Telefon komórkowy, Adres, Biuro, Skrytka pocztowa.

4.3.6. Dashboard :

4.3.6.1. Mój komputer – wykorzystanie RAM, Dysk, CPU.

4.3.6.2. Produktywność - czas zalogowania, aktywność, produktywność.

4.3.6.3. Wiadomości – lista ostatnich wiadomości przesłanych pracownikowi.

4.3.6.4. Skróty – definiowane przez administratora skróty do adresów URL, z możliwością edycji tytułu, opisu, koloru tekstu i tła.

4.3.6.5. Moje zgłoszenia – zgłoszenia do wsparcia technicznego (nowe, otwarte, rozwiązane).

4.3.6.6. Baza wiedzy – najczęściej odwiedzane artykuły wsparcia technicznego.

4.3.7. Sprzęt:

4.3.7.1. Komputery przypisane do pracownika (nr seryjny, MAC, IP, data ostatniego logowania).

4.3.7.2. Komputery używane przez pracownika (nr seryjny, MAC, IP, data ostatniego logowania).

4.3.7.3. Urządzenia przypisane do pracownika (nr seryjny, typ, IP).

4.3.8. Oprogramowanie:

4.3.8.1. Lista używanego oprogramowania (nazwa aplikacji, wersja, Producent, użycie w okresie ostatnich 3, 6, 12 miesięcy, data ostatniego uruchomienia).

4.3.9. Informacja o czasie pracy:

4.3.9.1. Lista otwartych sesji pracownika lub grupy pracowników (data zalogowania, nazwa komputera, IP, rodzaj połączenia (LAN, NAT, VPN), czas zalogowania).

4.3.9.2. Lista ostatnich sesji użytkownika lub grupy użytkowników (początek, koniec, czas trwania sesji, nazwa komputera, IP).

4.3.9.3. Lista używanego oprogramowania (nazwa aplikacji, wersja, producent, data ostatniego uruchomienia, użycie aplikacji w ostatnich 3, 6, 12 miesiącach).

4.3.9.4. Aktywność użytkownika lub użytkowników w aplikacjach (aplikacja, kategoria aplikacji, łączny czas korzystania, czas korzystania aktywnego, czas korzystania pasywnego).

4.3.9.5. Aktywność użytkownika lub użytkowników w Internecie (adres URL, informacja o stronie www –kategoria strony czy strona jest produktywna, łączny czas korzystania, czas aktywności, czas pasywności).

4.3.9.6. Wydruki – lista wydrukowanych dokumentów – data, godzina, nazwa drukarki, nazwa dokumentu.

4.3.10. Wsparcie techniczne – helpdesk.

4.3.10.1. System musi udostępniać formularz zgłoszenia awarii.

4.3.10.2. System musi udostępniać informacja o wszystkich dokonanych zgłoszeniach.

4.4. Zarządzanie licencjami:

4.4.1. System musi umożliwiać zarządzanie licencjami w ramach dowolnego elementu struktury organizacyjnej (dla wybranej struktury organizacyjnej pokazuje liczbę instalacji i liczbę licencji w danym modelu licencjonowania wraz z listą komputerów).

4.4.2. System musi dawać możliwość wykonywania (historia) wielu audytów legalności i zapamiętywać wyniki tych audytów w odniesieniu do systemów operacyjnych jak i aplikacji/pakietów, z uwzględnieniem segmentu struktury organizacyjnej.

4.4.3. Zarządzanie oprogramowaniem musi następować z podziałem na aplikacje i pakiety oprogramowania.

4.4.4. System musi pozwalać na zdefiniowanie dowolnej ilości tzw. „standardów oprogramowania", które definiują 3 kategorie oprogramowania: „oprogramowanie zalecane" – pozycje z tej listy są wymagane do zainstalowania obowiązkowo na każdym komputerze, „oprogramowanie dodatkowe" - pozycje z tej listy mogą być zainstalowane (nie jest to wymagane) a instalacja odbywa się na wniosek samego użytkownika lub jego przełożonego, „oprogramowanie nieokreślone" – oprogramowanie nie należące do żadnej z dwóch powyżej zdefiniowanych kategorii a zidentyfikowane na komputerze.

4.4.5. System umożliwia zdefiniowanie listy aplikacji zabronionych.

4.4.6. System umożliwia utworzenie schematów (kolekcji) oprogramowania zabronionego i w momencie pojawienia się ich na komputerze przystępuje do automatycznego odinstalowania w trybie cichym (bez interfejsu).

4.4.7. System musi umożliwiać kategoryzację uruchamianych procesów.

4.4.7.1. Umożliwia zdefiniowanie dowolnej kategorii oprogramowania/pliku/procesu i samodzielnej przydzielenie oprogramowania/pliku/procesu do kategorii.

4.4.7.2. W oparciu o Machine learning system umożliwia analizę procesów oraz przypisanie im odpowiednich kategorii oraz kontrolowanie użytkowników pod kątem uruchamianych procesów.

4.4.7.3. Automatyczne przypisanie kategorii do każdego uruchomionego procesu.

4.4.7.4. Niezależność od zewnętrznych dostawców bazy wzorców procesów.

4.4.8. System zbiera szczegółowe informacje o systemie operacyjnym (wersja, edycja, service pack, poprawki, data instalacji).

4.4.9. System umożliwia odczytywanie identyfikatorów i kluczy produktowych dla systemu operacyjnego oraz dowolnego oprogramowania, tam, gdzie jest to tylko technicznie możliwe.

4.4.10. System wspiera następujące typy licencji: Enterprise, Licensed concurrent, Licensed Name, Licensed per Processor, Licensed per Seat, Licensed per Server, OEM, OEM Downgrade, Open, Select, MOLP Open Value (Company wide), MOLP Open Value (non-Company wide), MOLP Open Value Subscription, CAL, SAAS, Trial, Shareware, Cal Per User.

4.4.11. System automatycznie klasyfikuje i rozlicza licencje OEM dla systemów operacyjnych oraz licencje typu freeware dla aplikacji.

4.4.12. System musi pomijać w rozliczeniu licencje wygasłe (po terminie ważności) i informować administratora o wygasaniu licencji.

4.4.13. System musi umożliwiać wyróżnianie licencji zabezpieczonych kluczami sprzętowymi.

4.4.14. System automatycznie wskazuje liczbę posiadanych licencji oraz liczbę używanego oprogramowania (pokazuje braki oraz nadwyżki).

4.4.15. System automatycznie uwzględnia i rozlicza licencje typu Upgrade i Downgrade wg zdefiniowanych przez użytkownika reguł.

4.4.16. System umożliwia ewidencję licencji (data zakupu, cena, dostawca, nr faktury, typ licencji, klucz produktowy, identyfikator produktowy, data wygaśnięcia, nr dokumentu OT, nr zapotrzebowania) poprzez rejestrację dokumentów

źródłowych (faktur zakupu) z możliwością dołączenia dowolnych załączników z repozytorium.

4.4.17. System umożliwia przypisanie licencji do użytkownika i/lub komputera oraz udostępnia informację o licencjach zarejestrowanych i jednocześnie wolnych (nieprzypisanych).

4.4.18. System umożliwiać zbieranie informacji na temat uruchamianych aplikacji na inwentaryzowanych komputerach (m.in. czas uruchomienia, nazwa zalogowanego użytkownika, nazwa aplikacji). System musi posiadać mechanizm zabezpieczający przed powstaniem niekompletnych lub niewłaściwych zapisów w wyniku braku zasilania lub innych awarii inwentaryzowanego systemu/sprzętu).

4.4.19. System musi udostępniać informację o uruchamianych aplikacjach w okresie 3/6/12 miesięcy oraz udostępniać datę ostatniego uruchomienia.

4.4.20. System musi umożliwiać podgląd historii zmian aplikacji i pakietów na komputerach.

4.4.21. System musi umożliwiać zdalne odinstalowanie oprogramowania na jednym bądź wybranych komputerach.

4.4.22. System musi udostępniać informacje o stopniu wykorzystania aplikacji / pakietów dla modeli licencjonowania oprogramowania typu CAL w podziale na analizę godzinową/dzienną/miesięczną w zadanym okresie. W/w informacja winna być przedstawiona również w postaci graficznej.

4.4.23. System musi udostępniać informacje o stopniu wykorzystania oprogramowania typu web dla modeli licencjonowania oprogramowania typu CAL w podziale na analizę godzinową/dzienną/miesięczną w zadanym okresie. W/w informacja winna być przedstawiona również w postaci graficznej.

4.5. Wzorce aplikacji i pakietów:

4.5.1. System ma posiadać wbudowaną bazę wzorców dostawcy oprogramowania posiadającą co najmniej 4 tys. wzorców aplikacji, 1,3 tys. Producentów.

4.5.2. System musi udostępniać informacje dotyczące plików, na podstawie których zidentyfikowana została dana aplikacja.

4.5.3. System musi prezentować informacje o ilości i dacie publikacji posiadanej bazy wzorców oprogramowania.

4.5.4. System musi posiadać możliwość definiowania własnych wzorców aplikacji i pakietów (składających się z aplikacji) w oparciu o definiowalne reguły rozpoznawania.

4.5.5. Własne wzorce aplikacji i pakietów muszą mieć pierwszeństwo w procesie rozpoznawania aplikacji i pakietów.

4.5.6. System musi mieć możliwość zamawiania bezpośrednio z poziomu konsoli administracyjnej u producenta systemu wzorców oprogramowania z możliwością wskazania dla jakiego komputera / komputerów wzorce mają być utworzone. Zamówione i utworzone przez Producenta wzorce muszą automatycznie (bez ingerencji administratora systemu) zostać zaimportowane do systemu.

4.5.7. System musi rozpoznawać wersję i edycję zainstalowanych pakietów Microsoft Office (tam, gdzie jest to technicznie możliwe (np. Microsoft Office 2007 Professional, Microsoft Office 2007 Standard, Microsoft Office 2003 Standard itd.).

4.6. Inwentaryzacja sprzętu komputerowego:

4.6.1. System musi umożliwiać: automatyczną inwentaryzację komputerów znajdujących się w sieci lokalnej oraz komputerów znajdujących się poza siecią lokalną (za NATem).

4.6.2. System musi zbierać szczegółowe informacje o sprzęcie (producent, model, data produkcji, numer seryjny) w oparciu o klasy WMI (Windows Management Instrumentation). Szczegółowość odczytywania danych musi być parametryzowana za pomocą definiowanego zapytania w standardzie WMI Query Language.

4.6.3. System ma umożliwiać skanowanie kości pamięci RAM (z podaniem jednoznacznej specyfikacji kości, typu, numeru seryjnego oraz informacji o taktowaniu).

4.6.4. System ma odczytywać informacje o zainstalowanych kościach pamięci: producent, numer seryjny (Serial Number), numer części (Part Number), rozmiar, częstotliwość, taktowania.

4.6.5. System musi mieć możliwość odczytywania danych z dowolnego miejsca rejestru systemowego. Musi istnieć możliwość łączenia (konkatenacji) kilku pozycji
z różnych miejsc rejestru oraz możliwość automatycznego, rekurencyjnego wyszukiwania wartości podanego klucza począwszy od wskazanego miejsca w hierarchii kluczy rejestru.

4.6.6. System ma umożliwiać automatyczne skanowanie monitorów podłączonych do komputera (ze wskazaniem producenta, modelu, numeru seryjnego, przekątnej ekranu).

4.6.7. System ma umożliwiać skanowanie dysków twardych (z podaniem typu interfejsu, numeru seryjnego oraz informacji SMART).

4.6.8. System musi umożliwić budowanie powiadomień administracyjnych w oparciu o dowolne atrybuty tabeli SMART dysku.

4.6.9. System prowadzi szczegółową ewidencję zmian konfiguracji sprzętu.

4.6.10. System udostępnia informacje o występowaniu plików na komputerach (nazwa, rozmiar, rodzaj, wielkość, lokalizacja, w przypadku plików wykonywalnych: wersja, producent).

4.6.11. System musi umożliwiać dokonanie klasyfikacji pliku wg dowolnie zdefiniowanych kategorii (np. audio, wideo, graficzne, erotyczne/pornograficzne, archiwa, wykonywalne.

4.6.12. System pozwala na zdalne trwałe (bez możliwości odzyskania) usunięcie dowolnego pliku/plików na dowolnie zdefiniowanej grupie komputerów.

4.6.13. System udostępnia informacje o zmianach w systemie plików (dodano plik, usunięto plik).

4.6.14. System umożliwia dodawanie notatek do każdej pozycji sprzętu.

4.6.15. System musi umożliwiać ewidencję zdarzeń serwisowych dowolnego typu (np. naprawy sprzętu, wymiany części).

4.6.15.1. System musi umożliwiać definiowanie typów serwisów.

4.6.15.2. System musi umożliwiać definiowanie wartości serwisu.

4.6.15.3. System musi umożliwiać definiowanie daty ważności serwisu oraz daty gwarancji.

4.6.16. System musi pozwalać na dołączanie do urządzeń dokumentów z repozytorium.

4.6.17. System umożliwia samodzielną definicję, ewidencję oraz wydruk wszelkiego typu protokołów (przyjęcie, przekazanie do użytkowania, likwidacja).

4.7. Inwentaryzacja urządzeń podłączanych do komputera.

4.7.1. System automatycznie identyfikuje i klasyfikuje urządzenia podłączane do komputera (pendrive, kamera, aparat, monitor zewnętrzny, pamięć masowa, telefon, urządzenie multimedialne itp.).

4.7.2. System pozwala na automatycznie lub ręczne przypisanie podłączonego urządzenia do komputera oraz użytkownika.

4.7.3. System ewidencjonuje historię podłączanych urządzeń zewnętrznych w zakresie: komputer, data, godzina, kto podłączył, czy urządzenia było podłączane na innym komputerze, czy urządzenie było podłączane przez innego użytkownika).

4.8. Inwentaryzacja urządzeń sieciowych.

4.8.1. System musi być wyposażony we wbudowany, konfigurowalny w zakresie IP oraz portów, pracujący zgodnie z harmonogramem skaner SNMP. Skaner musi wykryć typ urządzenia na danym IP/porcie i zwracać podstawowe informacje o tym urządzeniu (nazwa, producent, opis). Skaner musi obsługiwać SNMP w wersji 1/2c/3.

4.8.2. Skaner SNMP musi kojarzyć (łączyć) zinwentaryzowane urządzenia (np. komputery, drukarki) z danymi uzyskanymi w procesie skanowania IP/port.

4.8.3. System musi zbierać informacje o jakości połączenia:

4.8.4. Czas odpowiedzi serwisów (usług) podawany w milisekundach:

4.8.4.1. Średni czas odpowiedzi.

4.8.4.2. Minimalny czas odpowiedzi.

4.8.4.3. Maksymalny czas odpowiedzi.

4.8.5. Ilość dostarczonych informacji – pakietów dostarczonych, straconych oraz procent strat.

4.8.6. System musi być wyposażony we wbudowany, konfigurowalny skaner sieci, pozwalający na monitorowanie aktywnych usług oraz zweryfikowanie czy znalezione skanerem komputery posiadają Klienta.

4.8.6.1. Posiada niezwłoczną i automatyczną identyfikację podłączonych urządzeń do sieci.

4.8.6.2. Baza wzorców musi zawierać ponad 100 monitorowanych portów i usług.

4.8.6.3. System musi umożliwiać administratorowi definiowanie dodatkowych portów do monitorowania i przypisywanie do nich usług, a także modyfikowanie istniejących rekordów, obejmujących: port TCP, kategorię, nazwę usługi oraz nazwę skróconą.

4.8.7. System musi posiadać możliwość generowania map sieci bazujących na danych zebranych ze skanowania sieci.

4.8.7.1. System musi umożliwiać generowanie map według dowolnych filtrów użytkownika.

4.9. Inwentaryzacja sprzętu:

4.9.1. System musi umożliwiać inwentaryzację manualną (ewidencję) sprzętu innego niż komputery: np. drukarki, switche, routery, monitory, pamięci masowe itp.

4.9.1.1. System musi umożliwiać bazy typów urządzeń, o dowolne typy.

4.9.2. System umożliwia wprowadzanie dowolnych notatek oraz zdarzeń serwisowych.

4.9.3. System musi monitorować zmiany ewidencyjne i ruchy sprzętu.

4.9.4. System musi umożliwiać przypisanie urządzenia do użytkownika, ewidencję napraw, gwarancji.

4.9.5. System musi mieć możliwość przypominania o upływającym terminie gwarancji.

4.9.6. System musi pozwalać na dołączanie do urządzeń dokumentów z repozytorium wewnętrznego systemu.

4.9.7. System udostępnia informację o wartości wprowadzonego sprzętu.

4.9.8. System musi umożliwiać samodzielną definicję, ewidencję oraz wydruk wszelkiego typu protokołów oraz zapewniać automatyczną numerację tych dokumentów zapewniającą unikatowość.

4.9.9. System musi pozwalać na kopiowanie (duplikację) dowolnego urządzenia dowolną ilość razy.

4.9.10. System musi pozwalać na ewidencję umów utrzymaniowych (SLA) w odniesieniu do zaewidencjonowanych licencji oraz urządzeń w zakresie co najmniej: nazwa, okres, data dokumentu, numer dokumentu, dostawca, osoba kontaktowa, wartość, opis, warunki oraz umożliwiać dołączenie dowolnej ilości załączników z repozytorium i powiązanie umowy utrzymaniowej z dowolną ilością zasobów (urządzenia, licencje).

4.10. Ochrona danych (DLP):

4.10.1. System automatycznie tworzy listę podłączanych do komputerów urządzeń USB.

4.10.2. System automatycznie klasyfikuje podłączane urządzenia (pamięć masowa, pendrive, aparat fotograficzny, urządzenie multimedialne itp.).

4.10.3. System umożliwia uzyskanie informacji kto, kiedy i na jakim komputerze posługiwał się urządzeniem zewnętrznym, pozwalając na jego jednoznaczne zidentyfikowanie.

4.10.4. System umożliwia utworzenie listy urządzeń USB dozwolonych do stosowania - tzw. białej listy urządzeń USB.

4.10.5. System ma możliwość zidentyfikowania urządzenia USB i wprowadzenia go do systemu za pośrednictwem konsoli administracyjnej oraz wbudowanego do konsoli oprogramowania/skryptu, pozwalając na zidentyfikowanie jednocześnie wielu urządzeń USB (multiplekser USB).

4.10.6. System musi umożliwiać zdefiniowanie reguł stanowiących podstawę użytkowania urządzeń USB (dozwolone/niedozwolone) na inwentaryzowanych komputerach wg kryteriów: użytkownik, dzień tygodnia, okres (data od, godzina od, data do, godzina do), urządzenie USB, komputer, data obowiązywania reguły.

4.11. Szyfrowanie dysków wewnętrznych:

4.11.1. System musi identyfikować partycje dysków twardych zaszyfrowane BitLockerem.

4.11.2. System musi posiadać wbudowane mechanizmy do masowego zdalnego szyfrowania BitLockerem i wspierać metody XTS_AES_256, XTS_AES_128, AES_256, AES_128 oraz typy zabezpieczeń TPM+Pin, TPM, Passphrase.

4.11.3. Ochrona danych na wbudowanych dyskach twardych musi być realizowana przez silne szyfrowanie całej zawartości dysku/dysków z wykorzystaniem MS API BitLocker oraz umożliwiać uwierzytelnianie użytkownika przed uruchomieniem startu systemu operacyjnego ze wsparciem metod silnego uwierzytelnienia.

4.11.4. Ochrona danych przez szyfrowanie całej zawartości dysku oznacza, że szyfrowaniu podlegają wszystkie informacje zapisane na dysku twardym (łączenie z system operacyjnym, sterownikami, zainstalowanymi programami, danymi itp.).

4.11.5. Funkcjonalność szyfrowania / deszyfrowania nie może być realizowana w oparciu o dodatkowego Klienta na stacji roboczej, lecz musi być integralnym rozwiązaniem oferowanego systemu.

4.11.6. System musi umożliwiać zdalne szyfrowanie / deszyfrowanie partycji systemowych oraz niesystemowych oraz prezentować w konsoli administracyjnej bieżący postęp procesu.

4.11.7. Szyfrowanie partycji niesystemowych polega na wprowadzeniu przez użytkownika hasła.

4.11.8. Proces szyfrowania odbywa się w sposób niewidoczny dla użytkownika komputera i może być realizowany w czasie jego pracy na komputerze. Szyfrowanie nie może być zostać wyłączone przez użytkownika.

4.11.9. Proces szyfrowania może być zatrzymany podczas hibernacji oraz wyłączenia systemu, ale jest kontynuowany po wzbudzeniu / włączeniu komputera.

4.11.10. System przechowuje klucze szyfrujące w konsoli administracyjnej, przy czym klucze są dostępne po dodatkowym uwierzytelnieniu administratora.

4.11.11. System musi umożliwiać szyfrowanie / deszyfrowanie komputerów w sieci lokalnej oraz poza NATem.

4.12. Szyfrowanie dysków zewnętrznych USB:

4.12.1. System musi identyfikować partycje dysków zewnętrznych zaszyfrowane BitLockerem.

4.12.2. System musi posiadać wbudowane mechanizmy do masowego zdalnego szyfrowania / deszyfrowania BitLockerem i wspierać metody XTS_AES_256, XTS_AES_128, AES_256, AES_128 oraz typ zabezpieczeń Passphrase.

4.12.3. Ochrona danych na zewnętrznych urządzeniach USB musi być realizowana przez silne szyfrowanie całej zawartości dysku z wykorzystaniem MS API BitLocker oraz umożliwiać uwierzytelnianie użytkownika przed dostępem do danych ze wsparciem metod silnego uwierzytelnienia.

4.12.4. Funkcjonalność szyfrowania / deszyfrowania nie może być realizowana w oparciu o dodatkowego Klienta na stacji roboczej, lecz musi być integralnym rozwiązaniem oferowanego systemu.

4.12.5. Szyfrowanie partycji urządzeń USB polega na wprowadzeniu przez użytkownika hasła.

4.12.6. System musi umożliwiać zdalne szyfrowanie / deszyfrowanie partycji urządzeń USB oraz prezentować w konsoli administracyjnej bieżący postęp procesu.

4.12.7. Proces szyfrowania odbywa się w sposób niewidoczny dla użytkownika komputera i może być realizowany w czasie jego pracy na komputerze. Szyfrowanie nie może być zostać wyłączone przez użytkownika.

4.12.8. System przechowuje klucze szyfrujące w konsoli administracyjnej, przy czym klucze są dostępne po dodatkowym uwierzytelnieniu administratora.

4.13. Zdalna administracja komputerami:

4.13.1. System ma automatyczne wykonywać dowolne polecenia na dowolnych komputerach: wykonywanie poleceń powłoki, uruchamianie aplikacji, instalacja/deinstalacja oprogramowania, zmiany w rejestrach systemowych (dodawanie, usuwanie, modyfikowanie), usuwanie oraz kopiowanie plików i folderów, dostarczanie wyników zwróconych przez wykonane zadanie do bazy danych i prezentowanie ich w konsoli zarządzającej, możliwość wykonywania zadań z uprawnieniami dowolnego użytkownika.

4.13.1.1. System musi posiadać predefiniowane zadania (polecenia) możliwe do wykonania zdalnie – niezwłocznie lub zgodnie z harmonogramem

o funkcjonalnościach typowego harmonogramu Windows; zadania powinny być podzielone na typy: administracyjne, bezpieczeństwo, konserwacyjne a użytkownik może utworzyć dowolny nowy typ zadania.

4.13.1.2. Minimalne zadania predefiniowane: wyświetlanie aktywnych połączeń sieciowych, czyszczenie buforu DNS, pobranie listy zalogowanych użytkowników, ping, tracert, pobranie listy procesów, wyłączenie/włączenie komputera, wyłączenie/włączenie usługi, wyłączenie/włączenie/restart zapory Windows, włączenie usługi Windows Update, pobranie zmiennych środowiskowych, opróżnienie kosza, usunięcie plików tymczasowych, wymuszenie sprawdzenia dostępności aktualizacji Windows Update, wymuszenie aktualizacji zasad grup (AD), konserwację dysku twardego.

4.13.1.3. Każde wykonanie zadania musi mieć odzwierciedlenie w statusie wykonania zadania (poprawne, z błędem) oraz udostępniać informację zwrotną o przebiegu wykonania (godzina, data, status).

4.13.1.4. System musi umożliwiać zdefiniowanie dowolnego własnego zadania z poziomu konsoli administracyjnej z wykorzystaniem poleceń cmd, Windows PowerShell. System posiada co najmniej 70 predefiniowanych poleceń. System musi umożliwiać użytkownikom automatyczne definiowanie poleceń cmd/PowerShell. Funkcjonalność ta pozwala na wprowadzanie opisów zadanych czynności, a następnie, wykorzystując zaawansowane algorytmy AI, system automatycznie generuje adekwatne skrypty.

4.13.1.5. Zaawansowany Asystent AI do Przygotowywania Skryptów do precyzyjnego tworzenia szczegółowych skryptów.

4.13.1.6. System musi wspierać obsługę dowolnych poleceń powłoki na stacjach roboczych (kopiowanie plików, usuwanie plików, przenoszenie plików, zmiana ustawień systemu, wykonywanie programów, instalacja oprogramowania, instalacja poprawek itp.).

4.13.1.7. System musi umożliwić wykonanie poleceń z uprawnieniami dowolnego użytkownika (Uruchom jako).

4.13.1.8. System musi umożliwiać tworzenie zadań cyklicznych dla komputerów.

4.13.1.9. Obsługa zadań cyklicznych musi następować w cyklu dziennym: co n dni, w każdy dzień powszedni, nowe zadanie n dni od wykonania, tygodniowym: w wybrane dni co n tygodni, nowe zadanie n tygodni od wykonania, miesięcznym: co x miesięcy n-tego dnia, pierwszy/drugi/trzeci/czwarty/ostatni poniedziałek/wtorek/środa/czwartek/piątek/sobota/niedziela/dzień wolny/dzień powszedni co n miesięcy, nowe zadanie n miesięcy od wykonania, rocznym: n dzień w wybranym miesiącu, w pierwszy/drugi/trzeci/czwarty/ostatni, w dowolny dzień tygodnia, dzień wolny/dzień powszedni wybranego miesiąca, nowe zadanie n lat od wykonania.

4.13.1.10. System musi obsługiwać zadania cykliczne: bez daty końcowej, z końcem cyklu po n wystąpieniach, z końcem cyklu w określonej dacie.

4.13.2. System musi posiadać wbudowany skaner wyposażony w harmonogram skanowania umożliwiający wykrywanie (rozpoznawanie) komputerów z technologią Intel VPro/AMT wraz z identyfikacją IP technologii Vpro, portu VPro oraz wersji Vpro.

4.13.2.1. System musi umożliwiać zarządzanie komputerami z technologią Intel vPro, w tym: Serial Over LAN, zdalne włączanie, wyłączanie komputera,

zdalna konfiguracja BIOS, uruchomienie zdalnie komputera przy użyciu obrazu ISO lub IMG znajdującego się w dowolnej lokalizacji.

4.13.2.2. System ma umożliwiać połączenie się z wybranym komputerem w trybie graficznym (od VPro v.6).

4.13.3. System musi umożliwiać za pomocą technologii Ultra VNC: przejęcie ekranu, klawiatury i myszki użytkownika, zdalne uruchamianie aplikacji, zarządzanie usługami i restart komputera, zdalną instalacja oprogramowania, poprawek i aktualizacji (service pack, patch).

4.13.3.1. System umożliwia zdalne podłączenie do wielu komputerów jednocześnie i podgląd oraz operowanie na pulpitach tych komputerów w technologii Ultra VNC.

4.13.3.2. System musi umożliwiać uruchomienie do 6 sesji Ultra VNC na jednym ekranie.

4.13.3.3. System musi umożliwiać uruchomienie sesji Ultra VNC w trybie podłączenia się do obecnie zalogowanego użytkownika oraz w trybie RDP (wylogowania użytkownika i przejęcia dostępu).

4.14. System musi umożliwiać zdalne połączenia do wielu komputerów jednocześnie, podgląd i operowanie na pulpitach tych komputerów w technologii WEBRTC.

4.14.1. System musi umożliwiać instalację oraz konfigurację instalatora WEBRTC, co obejmuje określenie serwera, portu lokalnego oraz portu zewnętrznego (opcjonalnie). Dzięki temu, między innymi, umożliwiona zostaje komunikacja za pomocą WEBRTC niezależnie od sieci, w której znajduje się urządzenie końcowe.

4.14.2. System musi umożliwiać za pomocą technologii WEBRTC: przejęcie ekranu, klawiatury i myszki użytkownika, zdalne uruchamianie aplikacji, zarządzanie usługami i restart komputera, zdalną instalację oprogramowania, poprawek i aktualizacji (service pack, patch).

4.14.3. System musi umożliwiać poprzez technologię WEBRTC zdalne zarządzanie plikami (tworzenie, kopiowanie, usuwanie, przesyłanie).

4.14.4. System musi umożliwiać wykorzystanie wiersza poleceń (cmd) oraz PowerShell bez konieczności podłączenia do komputera.

4.14.4.1. W trybie administratora.

4.14.4.2. Na uprawnieniach zalogowanego użytkownika.

4.14.5. System musi umożliwiać nagrywanie sesji połączeń WEBRTC.

4.14.6. System powinien umożliwiać komunikację z użytkownikiem podczas sesji, włączając możliwość wykorzystania kamery i mikrofonu, jeśli urządzenie to obsługuje.

4.14.7. System powinien oferować konfigurację różnych trybów połączenia, takich jak:

4.14.7.1. Przejęcie sesji bez wymaganej zgody aktualnie zalogowanego użytkownika.

4.14.7.2. Przejęcie sesji bez wymaganej zgody użytkownika, z wyświetleniem komunikatu o dzieleniu sesji podczas jej trwania.

4.14.7.3. Przejęcie sesji z wymaganą zgodą użytkownika.

4.14.7.4. Przejęcie sesji z wymaganą zgodą użytkownika oraz wyświetleniem komunikatu o dzieleniu sesji.

4.14.7.5. „Tryb RDP”, pozwalający na wylogowanie użytkownika i rozpoczęcie nowej sesji na urządzeniu.

4.14.8. Wprowadzenie poświadczeń systemowych w trybie UAC.

4.14.9. Połączenie w trybie WEBRTC, powinno umożliwiać wprowadzenie poświadczeń do systemu w trybie UAC podczas sesji.

4.14.10. Połączenie w trybie WEBRTC, powinno oferować wyłączenie trybu wprowadzania danych przez zalogowanego użytkownika, co umożliwia podgląd sesji:

4.14.10.1. Bez wymaganej zgody aktualnie zalogowanego użytkownika.

4.14.10.2. Bez wymaganej zgody użytkownika, z wyświetleniem komunikatu o dzieleniu sesji.

4.14.10.3. Z wymaganą zgodą użytkownika.

4.14.10.4. Z wymaganą zgodą użytkownika oraz wyświetleniem komunikatu o dzieleniu sesji.

4.14.11. Ponadto system powinien zapewniać:

4.14.11.1. Blokadę urządzeń wskazujących dla użytkownika zalogowanego na urządzeniu.

4.14.11.2. Możliwość kopiowania tekstu do i z urządzenia, na którym odbywa się sesja.

4.14.11.3. Udostępnienie sesji „gościowi”.

4.14.11.4. Nagrywanie sesji WEBRTC.

4.14.11.5. Wykonanie zrzutu ekranu podczas sesji WEBRTC.

4.14.11.6. Wyświetlenie komunikatu PowerShell podczas sesji WEBRTC.

4.14.11.7. Podczas połączenia WEBRTC wykonanie akcji takich jak Wake-up, Run-commands, Sleep, Reset, Power off, Uninstall Klient.

4.14.12. Tryb WEBRTC powinien również oferować ustawienia dotyczące:

4.14.12.1. Jakości.

4.14.12.2. Skalowania.

4.14.12.3. Częstotliwości wyświetlania klatek.

4.14.12.4. Konfiguracji przycisków myszy.

4.14.12.5. Odwrócenia działania przewijania.

4.14.12.6. Blokady po połączeniu.

4.14.12.7. Zmiany trybu wyświetlania (dopasowany, rzeczywisty, dopasowany do okna).

4.14.13. System musi umożliwiać uruchomienie do 12 sesji WEBRTC na jednym ekranie.

4.15. System musi zezwalać na wykonywanie zapytań WMI bez zdalnego połączenia do urządzenia.

4.16. System musi zezwalać na edycję rejestrów urządzenia bez wykorzystania zdalnego połączenia pulpitu.

4.17. Zdalne Zarządzanie Zaporą (Firewall):

4.17.1. System powinien umożliwiać monitorowanie stanu zapory w czasie rzeczywistym, zapewniając aktualne informacje o jej działaniu.

4.17.2. System powinien zapewniać zdalne sterowanie zaporą na dowolnych komputerach, co obejmuje:

4.17.2.1. Definiowanie i zarządzanie złożonymi zasadami zapory z centralnego panelu administracyjnego.

4.17.3. System powinien umożliwiać szybkie identyfikowanie i reagowanie na potencjalne zagrożenia, zwiększając bezpieczeństwo sieci.

4.17.4. System powinien oferować kontrolę ruchu sieciowego, umożliwiając zarządzanie dostępem do zasobów sieciowych.

4.18. Automatyzacja:

4.18.1. System ma mieć możliwość ustalania harmonogramu, zgodnie z którym uruchamiane są czynności konserwacyjne, naprawcze, porządkujące.

4.18.2. Harmonogram musi mieć możliwość ustalenia częstotliwości wykonywania danej czynności (godzina, dzień, tydzień, miesiąc), możliwość zmiany wartość parametrów wejściowych, a także zatrzymania/uruchomienia harmonogramu uruchomienia dla każdej z czynności.

4.18.3. System musi mieć możliwość definiowania czynności wykonywanych automatycznie.

4.18.4. System musi być wyposażony w następujące mechanizmy automatyzacji: wykonywanie kopii bezpieczeństwa bazy danych, identyfikacja aplikacji i pakietów, porządkowanie bazy danych / odbudowa indeksów, usuwanie nadmiarowych danych w bazie danych, usuwanie zewnętrznych plików (logów).

4.18.5. System musi być wyposażony w mechanizmy informowania - wysyłania komunikatów (alerty) o: zasobach zakazanych (pliki erotyczne i pornograficzne), zasobach multimedialnych (pliki multimedialne), nowych komputerach w bazie danych, braku skanowania komputerów, brakach w licencjach, niewłaściwych datach systemowych komputerów, urządzeniach bez użytkowników, zdublowanych systemach operacyjnych, zakazanych procesach/stronach www /aplikacjach, wygasaniu serwisu lub licencji, przekroczeniu wielkości bazy danych, nadmiernym obciążeniu dysków twardych, nadmiernym obciążeniu sieci, nadmiernym obciążeniu sieci na komputerze, nadmiernym obciążeniu procesora, nadmiernym obciążeniu pamięci RAM, małej ilości wolnego miejsca na dysku, upływającej gwarancji.

4.19. Zarządzanie magazynem IT:

4.19.1. System musi umożliwiać obsługę magazynu IT.

4.19.2. System musi umożliwiać obsługę dowolnej ilości magazynów w różnych lokalizacjach.

4.19.3. System musi umożliwiać obsługę dokumentów PZ, RW, WZ, MM+, MM-, LI.

4.19.4. System musi prowadzić ewidencję materiałów w magazynach w oparciu o metodę FIFO (pierwsze przyszło, pierwsze wyszło).

4.19.5. System musi umożliwiać obsługę kodów kreskowych dla materiałów w magazynach.

4.19.6. System musi udostępniać informację o wartościach materiałów w poszczególnych magazynach, stanach materiałów w magazynach, dokumentach dotyczących danego materiału w dowolnym magazynie.

4.19.7. System musi umożliwiać automatyczne łączenie wygenerowanych dokumentów z zasobami systemu, takimi jak osoby, urządzenia.

4.19.8. System musi zapewniać możliwość przeglądu wszystkich wygenerowanych dokumentów.

4.20. Repozytorium:

4.20.1. Konsola administracyjna musi być wyposażona w repozytorium dokumentów dowolnego typu.

4.20.2. Repozytorium musi umożliwiać: dodawanie nowych dokumentów dowolnego typu, przeszukiwanie, oznaczanie dokumentów (znaczniki TAG) więcej niż jednym znacznikiem, podgląd dokumentów, dołączanie dokumentów z repozytorium w dowolnym miejscu systemu, uzyskanie informacji w jakich miejscach systemu dany dokument repozytorium występuje.

4.20.3. Repozytorium musi umożliwić definiowanie kontenerów na dokumenty.

4.21. Kody kreskowe:

4.21.1. System wspiera obsługę kodów kreskowych jedno i dwuwymiarowych.

4.21.2. System wspiera parametryzację kodu w zakresie wielkości graficznej kodu.
4.21.3. System pozwala w każdym momencie na zmianę typu i atrybutów kodu.
4.21.4. System informuje o błędzie generacji kodu, np. na skutek niewłaściwej długości wprowadzonego ciągu znaków w stosunku do danego standardu kodu.
4.21.5. Istnieje możliwość podglądu kodu oraz jednostkowego i masowego wydruku kodu / kodów.
4.21.6. System musi generować kody kreskowe (jedno i dwuwymiarowe) dla każdego zaewidencjonowanego urządzenia w standardzie wybranym przez użytkownika: aztec, codabar, code128, code39, dataMatrix, EAN128, EAN13, EAN8, interleaved2of5, ITF14, PDF417, POSTNET, qrcode, royalMailCBC, UPCA, UPCE, USPSIntelligentMail.
4.21.7. Obsługa kodów kreskowych nie może wymagać instalacji czcionek.
4.21.8. Parametry kodu kreskowego (wymiary, wielkość i typ czcionki) muszą być definiowalne.

4.22. Wysyłanie wiadomości:
4.22.1. Komunikator.
4.22.1.1. System musi oferować funkcję komunikatora, umożliwiającą bezpośrednią wymianę wiadomości pomiędzy użytkownikiem komputera z zainstalowanym Klientem a administratorem systemu.
4.22.1.2. Powinien zapewniać możliwość inicjowania czatu przez administratora.
4.22.1.3. Użytkownik powinien mieć opcję rozpoczęcia rozmowy za pomocą ikony na pasku zadań, która automatycznie uruchamia się zgodnie z konfiguracją Klienta.
4.22.1.4. System musi przechowywać historię konwersacji.
4.22.1.5. Powinien informować administratora poprzez powiadomienie w konsoli systemowej o nowych wiadomościach od użytkowników.
4.22.2. Wiadomość Jednorazowa:
4.22.2.1. System powinien umożliwiać wysyłanie jednorazowych wiadomości w trybie natychmiastowym jako ALERT.
4.22.2.2. Musi oferować możliwość wysłania wiadomości z opcją odłożenia na później (na 10 minut, 1, 2, 4 godziny) dla późniejszego odczytu.
4.22.2.3. Powinien zapewniać historię wysyłania i odbierania wiadomości przez użytkowników, z możliwością edycji treści w edytorze HTML.
4.22.2.4. Wiadomość powinna być dostępna do wysłania do określonej grupy, wybranych komputerów lub użytkowników.
4.22.2.5. System musi umożliwiać konfigurację czasu wygaśnięcia wiadomości.
4.22.3. Wiadomości Cykliczne:
4.22.3.1. Powinien pozwalać na tworzenie szablonów wiadomości do regularnego użytku.
4.22.3.2. Musi zapewniać funkcję odłożenia wysyłania wiadomości dla późniejszego odczytu, z możliwością edycji treści w edytorze HTML.
4.22.3.3. System powinien rejestrować historię wysyłania i odczytywania wiadomości przez użytkowników.
4.22.3.4. Powinien umożliwiać wysłanie wiadomości do zdefiniowanej grupy, wybranych komputerów lub użytkowników.
4.22.3.5. Musi oferować opcję konfiguracji terminu, po którym wiadomość wygaśnie.
4.22.4. System szkolenia pracowników za pomocą wiadomości.

4.22.4.1. System musi mieć możliwość zdefiniowania pakietów tekstowych (kontent) celem automatycznego wysyłania do urządzeń i użytkowników komputerów.

4.22.4.2. System musi posiadać predefiniowane szkolenia: „Klasyfikowanie informacji stanowiących tajemnicę przedsiębiorstwa", „Kontrola zabezpieczeń i obiegu informacji stanowiących tajemnicę przedsiębiorstwa", „Postępowanie w przypadku naruszenia tajemnicy", „Udostępnienie informacji stanowiących tajemnicę".

4.22.4.3. Formatowanie treści musi być zgodne z HTML.

4.22.4.4. System musi mieć możliwość edycji treści (zmiana kolejności, usuwanie, dodawanie nowych).

4.22.4.5. System musi mieć programowalny harmonogram wysyłania treści do dowolnej grupy odbiorców.

4.22.4.6. Użytkownik otrzymujący wiadomość musi być powiadamiany wizualne i dźwiękowo o otrzymaniu nowej wiadomości.

4.22.4.7. Użytkownik musi mieć możliwość natychmiastowego odczytania wiadomości lub jej odłożenia (na 10 minut, 1, 2 lub 4 godziny) celem późniejszego odczytania.

4.22.4.8. System musi udostępnia historię przesyłania wiadomości i odczytywania wiadomości przez użytkowników.

4.22.4.9. System musi generować elektroniczną listę uczestników przeszkolonych (z odczytanym całym szkoleniem).

4.23. System musi posiadać możliwość eksportu / importu treści.

4.24. Monitorowanie drukarek sieciowych i wydruków:

4.24.1. System musi posiadać możliwość ewidencji wszystkich generowanych wydruków niezależnie od miejsca ich generowania oraz typu drukarki (lokalna, sieciowa).

4.24.2. Ewidencja wydruków musi obejmować: nazwę i wielkość dokumentu, datę i godzinę wydruku, nazwę użytkownika drukującego, IP i nazwę komputera, z którego dokonano wydruku, format dokumentu, informację i jedno bądź dwustronnym wydruku, informację o wydruku mono/kolor.

4.24.3. System dla każdego wydruku, dla każdej drukarki musi obliczać rzeczywisty koszt wydruku w oparciu o wbudowany definiowalny przez administratora systemu, cennik wydruków obejmujący cenę papieru (w zależności od formatu) oraz cenę materiałów eksploatacyjnych (toner, tusz) dla danej drukarki, typu wydruku, rozmiaru papieru.

4.24.4. System musi generować zestawienia pozwalające ustalić miejsca powstawania kosztów wydruków (komórki organizacyjne, użytkownicy) oraz stopień obciążenia poszczególnych urządzeń drukujących.

4.24.5. System musi prognozować ilość i koszt wydruków na wszystkich drukarkach w okresie kolejnych 3,6,12 miesięcy.

4.24.6. System musi pozwalać na grupowanie (kojarzenie) drukarek wg sterowników.

4.24.7. Dla każdej z drukarek SNMP system musi udostępniać informacje: nr seryjny, IP, MAC, bieżący status drukarki, całkowitą ilość wydrukowanych stron, ilość wydrukowanych stron od uruchomienia, błędy, alerty, dostępne porty, stan pokryw, interfejsów sieciowych, rodzaj i ilości pamięci całkowitej i wykorzystanej, informacje o poziomie materiałów eksploatacyjnych.

4.25. Monitorowanie stron www:

4.25.1. System musi posiadać możliwość monitorowania odwiedzanych stron www niezależnie od typu używanej przeglądarki internetowej.

4.25.2. Ewidencja otwieranych stron musi dotyczyć wielu jednocześnie otwartych zakładek.

4.25.3. Ewidencja otwieranych stron musi działać również, gdy otwierana jest strona z połączeniem szyfrowanym (https).

4.25.4. Ewidencja musi obejmować co najmniej: nazwę i adres IP komputera, nazwę użytkownika, datę i godzinę, adres strony, łączny czas korzystania, czas aktywności, czas pasywności.

4.25.5. W oparciu o algorytmy sztucznej inteligencji - machine learning oraz deep learning system umożliwia analizę treści stron www oraz przypisanie im – w oparciu o treść – odpowiednich kategorii oraz kontrolowanie użytkowników pod kątem odwiedzanych stron.

4.25.5.1. Każda odwiedzona strona otrzymuje atrybuty: czy SSL, czy jest bezpieczna, czy zawiera przekierowania, czy znajduje się na liście CERT, czy znajduje się na liście stron hazardowych, czy kategoria strony jest bezpieczna, czy jest produktywna.

4.26. Monitorowanie serwerów WWW:

4.26.1. System musi umożliwiać monitorowanie wybranych serwerów www.

4.26.1.1. System musi przedstawiać informację o działaniu wybranych serwerów oraz ich aktywności.

4.26.1.2. System musi posiadać możliwość weryfikacji treści (tekstu) dostępnego na monitorowanej stronie.

4.26.1.3. System w sposób graficzny musi przedstawiać działanie serwerów WWW wraz z wyszczególnieniem informacji dla każdego wybranego serwera (status, bieżący czas odpowiedzi, średni czas odpowiedzi za ostatnie 12 miesięcy, aktywność za ostatnie 3, 6, 12 miesięcy).

4.27. Monitorowanie dziennika zdarzeń:

4.27.1. System musi posiadać możliwość monitorowania dziennika zdarzeń wszystkich komputerów.

4.27.2. System musi pozwalać na zdefiniowanie ewidencji zdarzeń z komputerów na podstawie kategorii zdarzenia.

4.27.3. Ewidencja musi zawierać: datę i godzinę zdarzenia, nazwę i adres IP komputera, typ zdarzenia, opis zdarzenia.

4.28. System musi umożliwiać monitorowanie komunikatów Syslog.

4.29. Monitorowanie pracy komputerów.

4.29.1. System musi posiadać możliwość monitorowania daty włączenia i wyłączenia komputera niezależnie czy znajduje się w sieci lokalnej czy też poza nią i prezentować czas pracy komputera w układzie graficznym.

4.29.2. System musi posiadać ewidencję daty i godziny przyłączenia i odłączenia komputera od systemu monitorującego.

4.29.3. System musi ewidencjonować zdarzenia związane z logowaniem się użytkowników do danego komputera, również w przypadku podłączania się wielu użytkowników jednocześnie.

4.29.4. Monitorowanie sesji zdalnych połączeń:

4.29.4.1. System musi prowadzić ewidencję sesji zdalnych połączeń na każdym komputerze.

4.29.4.2. Informacja o nawiązanej sesji musi zawierać co najmniej: nazwę i adres IP komputera, z którego nastąpiło połączenia, nazwę użytkownika nawiązującego połączenie, nazwę i adres IP komputera docelowego, adres portu połączenia.

4.30. Monitorowanie sensorów:

4.30.1. System musi umożliwić integrację z systemem monitoringu warunków środowiskowych poprzez odczyt wartości z wykorzystaniem SNMP.
4.30.2. Czujniki muszą być grupowane wg typu oraz lokalizacji.
4.30.3. System musi prezentować położenie czujników na mapie wbudowanej w system.
4.30.4. System musi umożliwić odczyt informacji z czujników temperatury, wilgotności oraz odczytywać zmiany stanu czujników zalania oraz otwarcia drzwi.
4.30.5. System musi przechowywać odczytane dane w bazie danych przez zadany okres.
4.30.6. System musi umożliwić wysyłanie alertów poprzez email, sms oraz prezentować informację w konsoli o przekroczeniu monitorowanych parametrów.
4.30.7. System musi umożliwić graficzną prezentację danych zebranych z monitorowanych czujników.

4.31. Repozytorium CMDB.
4.31.1. System musi posiadać wbudowaną centralną bazę systemu umożliwiająca import i eksport danych zarówno poprzez API jak też za pomocą wbudowanego import/eksporta, na którą składają się:
4.31.1.1. Active Directory - lista skonfigurowanych z konsolą serwerów LDAP, z których są importowane i aktualizowane dane o użytkownikach. System pozwala na wprowadzanie dowolnej ilości serwerów dla różnych domen.
4.31.1.2. Kontenery dokumentów - grupy, do których można przypisywać zapisane w systemie dokumenty w celu sortowania.
4.31.1.3. Kategorie aplikacji - lista kategorii, do których przynależą wykorzystywane przez użytkowników aplikacje.
4.31.1.4. Budżet - zestawienie typów budżetów (kosztów) zaewidencjonowanych w systemie.
4.31.1.5. Komputery - lista zinwentaryzowanych komputerów, podzielonych wg typu autoryzacji. Widok rekordu zawiera szczegółowe dane dotyczące danego komputera.
4.31.1.6. Dokumenty - repozytorium dokumentów zapisanych w systemie.
4.31.1.7. eLearning - zdefiniowane wiadomości typu eLearning. Wykorzystywane są do wysyłania użytkownikom szkoleń wbudowanych w system, zgodnie ze zdefiniowanym harmonogramem.
4.31.1.8. Kategorie plików - lista typów plików kategoryzowanych przez system. Administrator ma możliwość zdefiniowania własnych grup, do których pliki będą przydzielane, według wpisanej maski.
4.31.1.9. Pliki - lista zinwentaryzowanych plików ze wszystkich komputerów.
4.31.1.10. Licencje - zestawienie licencji zapisanych w bazie systemu, które administrator może przypisywać do poszczególnych użytkowników.
4.31.1.11. Typy licencji - lista typów licencji.
4.31.1.12. Lokalizacje - lista zdefiniowanych lokalizacji, do których administrator może przypisać poszczególnych użytkowników. W odróżnieniu od struktury organizacyjnej dane nie są importowane z Active Directory.
4.31.1.13. Typy urządzeń - lista typów urządzeń.
4.31.1.14. Urządzenia - lista urządzeń podzielonych wg typu.
4.31.1.15. Producenci / Dostawcy - lista producentów i dostawców.
4.31.1.16. Pamięć masowa - zestawienie dysków twardych z komputerów.
4.31.1.17. Porty sieciowe - lista monitorowanych portów sieciowych.
4.31.1.18. Usługi sieciowe - lista monitorowanych usług sieciowych.

4.31.1.19. Udostępnione zasoby sieciowe - lista udostępnionych zasobów sieciowych.
4.31.1.20. Sieci - lista definiowalnych ręcznie sieci, do których administrator może ręcznie przypisywać komputery.
4.31.1.21. Systemy operacyjne - zestawienie unikalnych systemów operacyjnych.
4.31.1.22. Struktura org. - zestawienie struktur organizacyjnych zdefiniowanych bądź importowanych z Active Directory.
4.31.1.23. Kategorie procesów - lista kategorii, do których będą przypisywane procesy aplikacji uruchamianych przez użytkowników. Klasyfikacja procesów odbywa się za pomocą algorytmów sztucznej inteligencji.
4.31.1.24. Serwery - lista zinwentaryzowanych serwerów.
4.31.1.25. Usługi - zestawienie usług działających na komputerach.
4.31.1.26. Oprogramowanie - lista zinwentaryzowanego i monitorowanego oprogramowania.
4.31.1.27. Pamięć masowa USB - lista urządzeń pamięci masowej USB.
4.31.1.28. Administratorzy - lista administratorów systemu.
4.31.1.29. Użytkownicy / pracownicy - lista pracowników.
4.31.1.30. Kategorie WWW - lista kategorii stron WWW wykorzystywanych w procesie klasyfikacji stron internetowych. Klasyfikacja oparta o sztuczną inteligencję.
4.31.1.31. Serwisy WWW - lista monitorowanych serwisów WWW.

4.32. Worktime manager:
4.32.1. System musi być wyposażony w zestaw statystycznych danych o pracy użytkownika i zdefiniowanych grup użytkowników.
4.32.2. System musi umożliwiać definiowanie dowolnej ilości grup użytkowników przypisanych do dowolnej ilości przełożonych.
4.32.2.1. System musi umożliwiać prezentację szczegółowych informacji o przypisanej grupie bezpośrednio w panelu pracownika na pulpicie przełożonego, który jest przypisany do tej grupy.
4.32.3. Dane muszą być prezentowane w formie interaktywnych widgetów oraz w formie danych analitycznych.
4.32.4. Dane dla grup użytkowników muszą być skumulowane oraz analityczne.
4.32.4.1. Prezentacja danych odbywa się poprzez wskazanie pracownika lub grupy pracowników oraz wybranie okresu danych źródłowych.
4.32.4.2. Informacje prezentowane w panelu: informacja o otwartych sesjach, informacja o sesjach historycznych, informacja o czasie zalogowania użytkownika, informacja o czasie pracy komputera, informacja o aktywności użytkownika w aplikacjach, informacja o produktywności użytkownika
w aplikacjach, informacja o produktywności, wykorzystywanych aplikacjach, odwiedzonych stronach www z podziałem na kategorie stron, informacja o uruchomionych procesach z podziałem na kategorie, informacja o aktywności na stronach www, informacja o wykonanych wydrukach (nazwa dokumentu, data i godzina wydruku, drukarka, ilość stron, rodzaj wydruku – czarno-biały czy w kolorze, koszt wydruku), informacja o transferze sieciowym, informacja o zależności czasu pracy w trybach: zalogowany/ uśpiony/ wylogowany.
4.32.5. System musi umożliwić wyświetlanie informacji o użytkowniku pobranych z Active Directory. Informacje powinny być aktualizowane zgodnie z harmonogramem połączenia z domeną.

4.32.6. System musi prezentować w formie tabelarycznej informacje o dokumentach (np. protokoły przekazania i zwrotu sprzętu), komputerach i urządzeniach, które zostały przypisane użytkownikowi.

4.32.7. System musi posiadać widżety prezentujące dane w wybranym przedziale czasu: czas zalogowania – dni, czas pracy komputera – dni, aktywność w aplikacjach, produktywność w aplikacjach, produktywność w czasie pracy, czas pracy w aplikacjach, czas spędzony na stronach www wg kategorii stron, czas spędzony w aplikacjach (procesach) wg kategorii procesu, czas aktywność na stronach www, stron wydruku wg dokumentów, transfer sieciowy, czas pracy wg zalogowany/ wylogowany / uśpiony, czas aktywności w godzinach pracy.

4.33. Raportowanie i eksport danych:

4.33.1. Systemu musi umożliwiać wyeksportowania wybranych lub wszystkich danych do formatu xls, csv, OpenOffice calc, html, mht, xml, jpeg, png, gif, bmp.

4.33.2. System musi mieć możliwość kategoryzowania raportów (spośród wszystkich raportów) oraz dodawania raportów użytkownika (zaprojektowanych przez użytkownika).

4.33.3. System musi umożliwiać generowanie raportów bezpośrednio z każdego widoku w aplikacji z zastosowaniem bieżących filtrów.

4.33.4. Generowanie raportu musi odbywać się po stronie serwera a nie klienta.

4.33.5. System musi umożliwiać wieloinstancyjność raportowania (wiele otwartych raportów jednocześnie z wielu widoków).

4.33.6. System musi mieć możliwość generowania i wyświetlania dowolnych wieloparametrycznych raportów w standardzie SAP Crystal Reports (rpt) oraz Stimulsoft.

4.33.7. System musi umożliwiać eksport danych z raportu do formatów: RPT, PDF, XLS, DOC, RTF.

4.33.8. System musi obsługiwać raporty parametryczne z parametrami statycznymi (wprowadzanymi w momencie generowania raportów) oraz dynamicznymi (pobieranymi z bazy danych w momencie generowania raportu).

4.33.9. System musi posiadać co najmniej 150 zdefiniowanych raportów dotyczących obszarów funkcjonalnych.

4.33.9.1. Raporty z zakresu komputerów:

4.33.9.1.1. Komputery – Karta graficzna – Procesor.
4.33.9.1.2. Komputery – Serwery wg systemu operacyjnego.
4.33.9.1.3. Komputery wg procesora – Skrócony.
4.33.9.1.4. Komputery wg procesora – Wszystkie.
4.33.9.1.5. Komputery wg producenta – Skrócony.
4.33.9.1.6. Komputery wg producenta – Wszyscy.
4.33.9.1.7. Komputery wg struktur organizacyjnych – Skrócony.
4.33.9.1.8. Komputery wg struktury organizacyjnej – Wszystkie.
4.33.9.1.9. Komputery wg systemów operacyjnych – Skrócony.
4.33.9.1.10. Komputery wg systemów operacyjnych – Wszystkie.
4.33.9.1.11. Komputery wg typu – Desktop.
4.33.9.1.12. Komputery wg typu – Hyper-V.
4.33.9.1.13. Komputery wg typu – Mobile.
4.33.9.1.14. Komputery wg typu – Nieokreślone.
4.33.9.1.15. Komputery wg typu – Server.
4.33.9.1.16. Komputery wg typu – Virtual Machine.
4.33.9.1.17. Komputery wg typu – VMWare.
4.33.9.1.18. Komputery wg typu – Wszystkie typy.

4.33.9.1.19. Zestawienie komputerów wg typu – Skrócony.
4.33.9.1.20. Komputery online.
4.33.9.1.21. Komputery niezautoryzowane.
4.33.9.1.22. Komputery offline.
4.33.9.1.23. Komputery online.
4.33.9.1.24. Komputery w magazynie.
4.33.9.1.25. Komputery w naprawie.
4.33.9.1.26. Komputery wszystkie.
4.33.9.1.27. Komputery wycofane.
4.33.9.1.28. Komputery zablokowane.
4.33.9.1.29. Komputery zautoryzowane.
4.33.9.1.30. Komputery zlikwidowane.
4.33.9.1.31. Komputery z Intel Anti-Theft.
4.33.9.1.32. Komputery z Intel VPro.

4.33.9.2. Raporty z zakresu urządzeń:
4.33.9.2.1. Urządzenia – Notatki.
4.33.9.2.2. Urządzenia – USB – Dodane.
4.33.9.2.3. Urządzenia – USB – Wykryte.
4.33.9.2.4. Urządzenia – USB – Wszystkie.
4.33.9.2.5. Urządzenia – USB – Biała lista.
4.33.9.2.6. Urządzenia – Serwis.
4.33.9.2.7. Urządzenia – Inwentaryzacja – Kody kreskowe.
4.33.9.2.8. Urządzenia – Inwentaryzacja.
4.33.9.2.9. Urządzenia – Inwentaryzacja – Porównanie inwentaryzacji.
4.33.9.2.10. Urządzenia – Utrzymanie.
4.33.9.2.11. Urządzenia.

4.33.9.3. Raporty z zakresu sieci:
4.33.9.3.1. Sieć – Wykryte.
4.33.9.3.2. Sieć – Historia.
4.33.9.3.3. Sieć – Ostanie skanowanie.

4.33.9.4. Raporty z zakresu oprogramowania:
4.33.9.4.1. Oprogramowanie – Systemy operacyjne – Wszystkie.
4.33.9.4.2. Oprogramowanie – Systemy operacyjne – Instalacje OEM.
4.33.9.4.3. Oprogramowanie – Systemy operacyjne – Szczegóły.
4.33.9.4.4. Oprogramowanie – Systemy operacyjne – Historia audytów.
4.33.9.4.5. Oprogramowanie – Aplikacje – Wszystkie.
4.33.9.4.6. Oprogramowanie – Aplikacje – Monitorowane.
4.33.9.4.7. Oprogramowanie – Aplikacje – Szczegóły.
4.33.9.4.8. Oprogramowanie – Aplikacje – Historia audytów.
4.33.9.4.9. Oprogramowanie – Pakiety – Wszystkie.
4.33.9.4.10. Oprogramowanie – Pakiety – Szczegóły.
4.33.9.4.11. Oprogramowanie – Pakiety – Historia audytów.
4.33.9.4.12. Oprogramowanie – Bazy danych – Wszystkie.
4.33.9.4.13. Oprogramowanie – Bazy danych – Express.
4.33.9.4.14. Oprogramowanie – Bazy danych – Pozostałe.
4.33.9.4.15. Oprogramowanie – Bazy danych – per Core.
4.33.9.4.16. Oprogramowanie – Rejestry – Razem.
4.33.9.4.17. Oprogramowanie – Rejestry – Szczegóły.
4.33.9.4.18. Oprogramowanie – Rejestry – Ostatnio zainstalowane.
4.33.9.4.19. Oprogramowanie – Klucze produktu.

4.33.9.4.20. Oprogramowanie – Wykorzystanie – Użycie – Wszystkie.
4.33.9.4.21. Oprogramowanie – Wykorzystanie – Oszczędności.
4.33.9.4.22. Oprogramowanie – Wykorzystanie – CAL.
4.33.9.4.23. Oprogramowanie – Wykorzystanie – CAL WEB.
4.33.9.4.24. Oprogramowanie – Monitorowanie – Uruchomienia.
4.33.9.4.25. Oprogramowanie – Monitorowanie – Aktywność ogółem.
4.33.9.5. Raporty z zakresu osób:
4.33.9.5.1. Osoby – Protokół standardowy.
4.33.9.5.2. Osoby – Protokół rozszerzony.
4.33.9.6. Raporty z zakresu plików i multimediów:
4.33.9.6.1. Pliki i multimedia – Archiwa.
4.33.9.6.2. Pliki i multimedia – Audio.
4.33.9.6.3. Pliki i multimedia – Erotyka.
4.33.9.6.4. Pliki i multimedia – Grafika.
4.33.9.6.5. Pliki i multimedia – Wideo.
4.33.9.6.6. Pliki i multimedia – Wykonywalne.
4.33.9.6.7. Pliki i multimedia – Zmiany plików.
4.33.9.7. Raporty z zakresu magazynu:
4.33.9.7.1. Magazyn – Dokumenty.
4.33.9.7.2. Magazyn – Stany.
4.33.9.7.3. Magazyn – Materiały.
4.33.9.7.4. Magazyn.
4.33.9.8. Raporty z zakresu finansów:
4.33.9.8.1. Finanse – Urządzenia.
4.33.9.8.2. Finanse – Licencje.
4.33.9.8.3. Finanse – Wydruki wg drukarki.
4.33.9.8.4. Finanse – Wydruki wg sterownika.
4.33.9.8.5. Finanse – Wydruki użytkownicy.
4.33.9.8.6. Finanse – Magazyn.
4.33.9.9. Raporty z zakresu serwera wiadomości:
4.33.9.9.1. Serwer wiadomości – Komunikator – Historia.
4.33.9.9.2. Wiadomość cykliczna – wg wiadomości.
4.33.9.9.3. Serwer wiadomości – Komunikator – Rozmowy.
4.33.9.9.4. Serwer wiadomości – Wiadomości wysłane – wg komputera.
4.33.9.9.5. Serwer wiadomości – Wiadomości wysłane – wg odbiorcy.
4.33.9.9.6. Serwer wiadomości – Wiadomości wysłane – wg wiadomości.
4.33.9.9.7. Serwer wiadomości – Wiadomości wysłane – wg wysyłającego.
4.33.9.9.8. Serwer wiadomości – Wiadomości – Aktywne cykle.
4.33.9.10. Raporty z zakresu serwera monitorującego:
4.33.9.10.1. Serwer monitorujący – Logowanie Klientów.
4.33.9.10.2. Serwer monitorujący – eServer.
4.33.9.10.3. Serwer monitorujący – Alerty systemowe.
4.33.9.10.4. Serwer monitorujący – Historia logowań.
4.33.9.10.5. Serwer monitorujący – Dzienniki zdarzeń – Powiadomienia systemowe.
4.33.9.10.6. Serwer monitorujący – Dzienniki zdarzeń – Dzienniki.
4.33.9.10.7. Serwer monitorujący – Dzienniki zdarzeń – Sesje RDP.
4.33.9.10.8. Serwer monitorujący – Transfer sieciowy – Procesy.
4.33.9.10.9. Serwer monitorujący – Drukowanie.
4.33.9.10.10. Serwer monitorujący – Drukowanie – Razem.

4.33.9.10.11. Serwer monitorujący – Drukowanie – Razem SNMP.
4.33.9.10.12. Serwer monitorujący – Drukowanie – Prognoza.
4.33.9.10.13. Serwer monitorujący – Usługi – Wszystkie.
4.33.9.10.14. Serwer monitorujący – Usługi – Szczegóły.
4.33.9.10.15. Serwer monitorujący – Harmonogram zadań.
4.33.9.10.16. Serwer monitorujący – Sesje VNC.
4.33.9.10.17. Serwer monitorujący – Intel AMT.
4.33.9.10.18. Serwer monitorujący – Poczta wychodząca.
4.33.9.10.19. Serwer monitorujący – Strony www – Odwiedzone.
4.33.9.10.20. Serwer monitorujący – Strony www – Aktywność ogółem.
4.33.9.10.21. Serwer monitorujący – USB.
4.33.9.10.22. Serwer monitorujący – Wydajność – CPU.
4.33.9.10.23. Serwer monitorujący – Wydajność – Dysk.
4.33.9.10.24. Serwer monitorujący – Wydajność – Dysk (razem).
4.33.9.10.25. Serwer monitorujący – Wydajność – Pamięć.
4.33.9.10.26. Serwer monitorujący – Wydajność – Procesy.
4.33.9.10.27. Serwer monitorujący – Wydajność – Sieć.

4.33.9.11. Raporty z zakresu serwera zadań:
4.33.9.11.1. Serwer zadań – Logi.
4.33.9.11.2. Serwer zadań – Zadania cykliczne.

4.33.9.12. Raporty z zakresu serwera automatyzacji:
4.33.9.12.1. Serwer automatyzacji – Automaty.
4.33.9.12.2. Serwer automatyzacji – Logi.
4.33.9.12.3. Raporty z zakresu raportów.
4.33.9.12.4. Raporty – Harmonogram.
4.33.9.12.5. Raporty – Harmonogram – Historia.

4.33.9.13. Raporty z zakresu repozytorium:
4.33.9.13.1. Repozytorium – Dokumenty.
4.33.9.13.2. Repozytorium – e-Learning.
4.33.9.13.3. Repozytorium – Kategorie aplikacji.
4.33.9.13.4. Repozytorium – Kategorie plików.
4.33.9.13.5. Repozytorium – Kategorie procesów.
4.33.9.13.6. Repozytorium – Kategorie www.
4.33.9.13.7. Repozytorium – Producenci Dostawcy.
4.33.9.13.8. Repozytorium – Typy licencji.

4.33.9.14. Raporty z zakresu ustawień:
4.33.9.14.1. Ustawienia – Administratorzy – Wszystkie.
4.33.9.14.2. Ustawienia – Dane firmy.
4.33.9.14.3. Ustawienia – Struktura organizacyjna.
4.33.9.14.4. Ustawienia – Budżet.
4.33.9.14.5. Ustawienia – Sieci.

4.33.10. System musi posiadać możliwość konfiguracji harmonogramu umożliwiającego cykliczne wysyłanie raportów oraz zapisywanie ich w dowolnym miejscu.

4.33.11. Wynikiem wykonania harmonogramu jest raport w formacie pdf.

4.34. System musi zapewnić interfejs API.

4.34.1. System musi udostępniać możliwości komunikacji z systemem za pomocą REST API.

4.34.2. Komunikacja z REST API musi odbywać się w sposób szyfrowany min. Protokołem TLS 1.3 i chroniony kluczem alfanumerycznym.

4.34.3. System musi zapewniać możliwości modyfikacji i dostosowania klucza zabezpieczeń REST API i pozwalać na ustanowienie klucza o długości co najmniej 32 znaków.

4.34.4. System musi pozwalać na tworzeni requestów obsługujących parametry w formacie JSON.

4.34.5. W ramach REST API konieczne musi być możliwość pobierania danych ze wszystkich tabel systemu, zawierających dane merytoryczne.

4.34.6. System musi przyjmować requesty pozwalające na umieszczanie danych w systemie za pomocą REST API.

4.34.7. System musi dopuszczać komunikację złożoną, za pomocą sekwencji requestów REST API.

4.34.8. System musi pozwalać na automatyczną komunikację za pomocą REST API z innymi systemami z wykorzystaniem składni API systemu.

4.35. Powiadomienia:

4.35.1. System musi umożliwiać generowanie powiadomienia.

4.35.1.1. Powiadomienia muszą być w formie alertu w konsoli systemu, wiadomości email wysłanej na wybrane adresy oraz wiadomości SMS na wskazane numery telefonów.

4.35.1.2. Powiadomienie musi umożliwiać automatyczne wywalanie zadania zdefiniowanego w konsoli systemu. Dostępne polecenia CMD, Windows PowerShell (minimum 70 predefiniowanych, możliwość generowania własnych, integracja z LLM).

4.35.2. System musi umożliwiać tworzenie wybranych powiadomień wiele razy z określeniem innych grup obiorców.

4.35.3. System musi umożliwiać edycję treści wysyłanych powiadomień i możliwość korzystania z danych umieszczonych w systemie w treści powiadomienia.

4.35.4. System musi posiadać co najmniej 30 zdefiniowanych powiadomień dotyczących obszarów funkcjonalnych.

4.35.4.1. Powiadomienia z zakresu oprogramowania:

4.35.4.1.1. Odinstalowano oprogramowanie.

4.35.4.1.2. Wykryto niezgodność ze schematem oprogramowania.

4.35.4.1.3. Wykryto nowe oprogramowanie.

4.35.4.2. Powiadomienia z zakresu sieci:

4.35.4.2.1. Monitorowana usługa sieciowa przestała odpowiadać.

4.35.4.2.2. Monitorowane urządzenia z problemami.

4.35.4.2.3. Monitorowane urządzenie jest offline.

4.35.4.2.4. Problem ze stroną WWW.

4.35.4.2.5. Serwis WWW nie odpowiada.

4.35.4.2.6. Serwis WWW odpowiada niewłaściwym komunikatem.

4.35.4.2.7. Średni czas odpowiedzi usługi przekroczył wartość X ms.

4.35.4.2.8. Transfer sieciowy na komputerze przekroczył X MB / Y min.

4.35.4.2.9. W sieci pojawiły się duplikaty adresów IP.

4.35.4.2.10. W sieci pojawiły się duplikaty adresów MAC.

4.35.4.2.11. Wykryto dużą ilość danych wysyłanych przez dany port w switch'u.

4.35.4.2.12. Wykryto nowe urządzenie.

4.35.4.2.13. Wykryto urządzenie z odblokowanym portem X.

4.35.4.2.14. Wykryto urządzenie z usługą X.

4.35.4.2.15. Wykryto zmianę adres IP komputera.

4.35.4.2.16. Wykryto zmianę statusów portów w switch'u.

4.35.4.3. Powiadomienia z zakresu sprzętu:
4.35.4.3.1. Interfejs sieciowy wyłączony.
4.35.4.3.2. Parametr lub parametry S.M.A.R.T. przekroczyły dozwolone wartości.
4.35.4.3.3. Podłączono urządzenie USB.
4.35.4.3.4. Wykryto zmianę w sprzęcie (WMI).
4.35.4.3.5. Powiadomienia z zakresu systemu.
4.35.4.3.6. Mało miejsca na dysku C.
4.35.4.3.7. Pojawił się błąd w dzienniku zdarzeń Windows.
4.35.4.3.8. Wykryto problem z usługą systemu Windows.
4.35.4.3.9. Wykryto zmianę nazwy komputera.
4.35.4.3.10. Wysokie użycie pamięci RAM.
4.35.4.3.11. Zmieniono informację o systemie.
4.35.4.4. Powiadomienia z zakresu użytkownika:
4.35.4.4.1. Użytkownik odwiedził stronę WWW z wybranej kategorii.
4.35.4.4.2. Użytkownik przekroczył limit wydrukowanych stron.
4.35.4.4.3. Użytkownik przekroczył transfer sieciowy X MB / Y min.

4.36. Bezpieczeństwo:
4.36.1. System musi być wyposażony w mechanizmy definicji praw dostępu do poszczególnych widoków danych i opcji w konsoli administracyjnej.
4.36.2. Uwierzytelnianie do systemu musi być realizowane:
4.36.2.1. Z wykorzystaniem imiennego konta użytkownika i hasła.
4.36.2.2. Z wykorzystaniem imiennego konta administratorów aplikacji i hasła.
4.36.2.3. Za pośrednictwem uwierzytelniania poprzez Active Directory.
4.36.2.4. Za pośrednictwem uwierzytelniania poprzez CAS.
4.36.3. Hasła w systemie i bazach danych nie mogą w żadnym z przypadków występować w formie jawnej.
4.36.4. Siła hasła musi być definiowalna w zakresie atrybutów: ilość znaków, ilość liter, ilość znaków specjalnych, ilość małych znaków, ilość wielkich znaków, ilość cyfr, ilość znaków specjalnych, ilość znaków alfanumerycznych, lista dopuszczalnych znaków specjalnych, lista wyłączonych znaków).
4.36.5. System musi umożliwiać zastosowanie dodatkowej autentykacji podczas logowania przy użyciu certyfikatu SSL w systemie lub na tokenie (MFA).
4.36.5.1. Uwierzytelnianie z wykorzystaniem obrazu wideo.
4.36.5.2. Uwierzytelnianie z jednorazowym kodem wysyłanym na e-mail użytkownika.
4.36.5.3. Oprogramowanie musi posiadać procedurę uwierzytelnienia i autoryzacji kont operatorów w konsoli zarządzającej poprzez fizyczne zabezpieczenie sprzętowe wraz z hasłem, które umożliwia jednoczesną pracę wielu użytkownikom. Logowanie użytkowników konsoli zarządzającej musi umożliwiać integrację z kontami Active Directory/LDAP.
4.36.6. Wymagane zabezpieczenie sprzętowe musi posiadać mechanizm szyfrowania w oparciu o RSA 512/1024/RSA 2048 bit, ECDSA 192/256 bit, DES/3DES, AES 128/192/256 bit, SHA-1 / SHA-256.
4.36.6.1. Wykorzystywane klucze muszą posiadać wsparcie dla systemów Windows 7/8.1/10 i Windows Server 2012/2016/2019.
4.36.7. System musi umożliwiać blokadę dostępu po nieudanej próbie zalogowania się do systemu. Ponadto, system powinien oferować:

4.36.7.1. Podgląd wszystkich zablokowanych administratorów systemu, w tym informacje o typie, elemencie, czasie trwania blokady [s] oraz o ostatniej aktywności.

4.36.7.2. Możliwość odblokowania zablokowanego administratora systemu z poziomu konsoli administracyjnej przez osobę uprawnioną.

4.36.8. Prawa dostępu muszą opierać się na grupach i użytkownikach w zakresie: przeglądanie / edycja / usuwanie/ eksport.

4.36.9. System musi oferować możliwość podglądu wszystkich aktualnie otwartych sesji administratorów w konsoli administracyjnej, obejmując takie informacje jak: data utworzenia sesji, login, IP oraz SID.

4.36.9.1. Dodatkowo, system powinien umożliwiać wyszukiwanie zalogowanych administratorów po nazwie.

4.36.10. System musi udostępniać historię działań wybranych użytkowników/administratorów w zakresie, adresy URL i nagłówki http.

4.36.11. System musi posiadać wbudowany mechanizm automatycznej synchronizacji czasu pomiędzy Klientami oraz serwerem, gdzie wzorcowy czas jest po stronie serwera.

4.36.12. System musi posiadać mechanizmy automatycznego wykonywania kopii bezpieczeństwa w zadanych interwałach czasowych w formie kopii przyrostowej i nie przyrostowej oraz udostępniać informacje o rezultacie wykonania kopii.

4.36.13. System musi pobierać dane z widoków (view) zdefiniowanych w bazie danych a nie bezpośrednio z tabel bazy danych.

4.36.14. W przypadku wystąpienia awarii systemu i konieczności instalacji systemu na nowo system musi automatycznie z serwera aktualizacji producenta w ciągu 24 godzin dokonać aktualizacji wszystkich komponentów (konsola administracyjna, agenci, serwer, baza danych, bazy wiedzy).

4.36.15. System musi być wyposażony w mechanizmy powtórnego załadowania danych historycznych pochodzących od Klientów.

4.36.16. System musi zapewniać:

4.36.16.1. Pełne logowanie błędów w celu weryfikowania nieprawidłowości.

4.36.16.2. Przechowywanie logów systemowych.

4.36.16.3. Przechowywanie logów bezpieczeństwa.

4.36.16.4. Przechowywanie logów aktywności użytkowników i administratorów.

4.36.16.5. Pobieranie logów z Klientów z poziomu konsoli administracyjnej.

4.36.16.6. Możliwość eksportu logów.

4.36.16.7. Definiowanie maksymalnego czasu przechowywania plików log.

4.36.16.8. System musi zapewniać mechanizmy zapewniające integralność, poufność i dostępność przechowywanych informacji.

4.36.16.9. Definiowanie ścieżki do kopii zapasowej.

4.36.16.10. Definiowanie ścieżki do importu danych.

4.36.16.11. Definiowanie ścieżki do zapisu raportów.

4.36.16.12. Definiowanie serwera do importu danych.

5. **Wsparcie i pomoc**:

5.1.1. System musi posiadać dokumentację w postaci min. 20 filmów instruktażowych/nagrań z webinariów w języku polskim.

5.1.2. System musi posiadać wbudowaną dokumentację pomocy użytkownika w języku polskim.

5.1.3. Pomoc techniczna:

5.1.3.1. Musi być świadczona co najmniej w dni robocze w godzinach od 8.00-16.00.

5.1.3.2. Utrzymaniem Oprogramowania jest zapewnienie aktualizacji Oprogramowania (asysta techniczna) oraz nieprzerwanego działania Oprogramowania (usługi SLA), jak również zapewnienie świadczenia innych usług wspomagających korzystanie z Oprogramowania.

5.1.3.3. Czas trwania usługi SLA wynosi 12 miesięcy od dnia zakupu.

5.1.3.4. Usługi Utrzymania Oprogramowania obejmują:

5.1.3.4.1. Asystę techniczną.

5.1.3.4.2. Świadczenie usług SLA, w ramach, których realizowana jest:

5.1.3.4.2.1. Obsługa zgłoszeń w zakresie:

5.1.3.4.2.1.1. Reakcja na zgłoszenia błędów w określonym czasie reakcji.

5.1.3.4.2.1.2. Dokonywanie analizy przyczyn błędów.

5.1.3.4.2.1.3. Zapewnianie obejścia dla błędów występujących z przyczyn leżących po stronie oprogramowania podmiotów trzecich.

5.1.3.4.2.1.4. Zapewnianie obejścia dla błędów występujących z przyczyn leżących po stronie infrastruktury zamawiającego.

5.1.3.4.2.1.5. Usuwania błędów w czasie naprawy.

5.1.3.4.2.1.6. Usuwania błędów występujących z przyczyn leżących po stronie oprogramowania podmiotów trzecich – po udostępnieniu odpowiedniej aktualizacji przez producenta tego oprogramowania oraz jej uzyskaniu – w czasie naprawy.

5.1.3.5. Zapewnienia dostępności Oprogramowania.

SYGNALIŚCI

Architektura/Wsparcie:

- SLA x miesięcy
  - Czas trwania usługi SLA wynosi 12 miesięcy od dnia zakupu.
- Ilość dostępów administracyjnych
  - **Błąd! Nie można odnaleźć źródła odwołania.**

1. **Architektura / wymagania systemowe:**
   - **1.1.** Musi być kompletnym i samodzielnym systemem wspierającym pracę działu wsparcia technicznego (helpdesk). System musi zawierać moduły: zarządzanie zgłoszeniami, ewidencja magazynowa, zakupy IT, zarządzanie umowami serwisowymi, portal pomocy technicznej oraz baza wiedzy.
   - **1.2.** System musi być w pełni funkcjonalną aplikacją internetową (webową). Konsola administracyjna musi działać na dowolnej przeglądarce stron WWW zgodnej z HTML5 (np. Internet Explorer 11, Firefox, Chrome, Opera).
   - **1.3.** Bazę danych systemu musi stanowić postgresql.
   - **1.4.** System musi współpracować z czytnikiem i drukarką kodów paskowych.
   - **1.5.** System musi być zgodny z ITIL v4.
   - **1.6.** System musi zapewniać integrację z Active Directory.
   - **1.7.** System musi zapewniać integrację z systemem zarządzania zasobami IT.

1.8. System musi posiadać co najmniej 8 dostępów administracyjnych (tzw. użytkownik nazwany) umożliwiające jednoczesne działania serwisantów w konsoli systemu.

1.9. System musi zapewnić interfejs API:

1.9.1. System musi udostępniać możliwości komunikacji z systemem za pomocą REST API.

1.9.2. Komunikacja z REST API musi odbywać się w sposób szyfrowany min. Protokołem TLS 1.3 i chroniony kluczem alfanumerycznym.

1.9.3. System musi zapewniać możliwości modyfikacji i dostosowania klucza zabezpieczeń REST API i pozwalać na ustanowienie klucza o długości co najmniej 32 znaków.

1.9.4. System musi pozwalać na tworzeni requestów obsługujących parametry w formacie JSON.

1.9.5. W ramach REST API konieczne musi być możliwość pobierania danych ze wszystkich tabel systemu, zawierających dane merytoryczne.

1.9.6. System musi przyjmować requesty pozwalające na umieszczanie danych w systemie za pomocą REST API.

1.9.7. System musi dopuszczać komunikację złożoną, za pomocą sekwencji requestów REST API.

1.9.8. System musi pozwalać na automatyczną komunikację za pomocą REST API z innymi systemami z wykorzystaniem składni API systemu.

2. Zakres funkcjonalny systemu:

2.1. Zarządzanie Incydentem.

2.2. Zarządzanie Problemem.

2.3. Zarządzanie Zmianą.

2.4. Baza konfiguracji CMDB.

2.5. Zarządzanie umowami SLA.

2.6. Portal Pomocy Technicznej.

2.7. Baza wiedzy.

2.8. Zarządzanie magazynami.

2.9. Zarządzanie umowami serwisowymi.

2.10. Zarządzanie zakupami.

2.11. Ankietowanie użytkowników.

2.12. Raportowanie zgłoszeń z filtrami: urządzenie, użytkownik, jednostka organizacyjna, czas naprawy, koszt użytych do naprawy elementów, zgłoszenia w określonym przedziale czasowym.

2.13. Zarządzenie zmianą.

2.14. Webowa platforma zgłoszeń sygnalistów.

3. Moduł Zarządzanie Incydentem musi obsługiwać:

3.1. Różne typy zgłoszeń.

3.2. Dokładną rejestrację i klasyfikację incydentów.

3.3. Diagnostykę i rozwiązywanie zgłoszeń z wykorzystaniem modułu zarządzania wiedzą.

3.4. Szczegółowe raporty trendów w incydentach.

3.5. Ewidencję czasu pracy serwisanta.

3.6. Zatwierdzanie rozwiązania incydentu przez użytkownika.

3.7. Pełną historię zgłoszenia.

3.8. Możliwość ustawienia automatycznej odpowiedzi na zgłoszenia użytkowników za pomocą sztucznej inteligencji.

4. **Moduł Zarządzanie Problemem musi obsługiwać:**
   - **4.1.** Rejestracja nowego problemu lub powiązanie wielu incydentów w jeden problem.
   - **4.2.** Diagnostyka powiązanych problemów i poszukiwanie głównej przyczyny incydentów.
   - **4.3.** Tworzenie rozwiązań tymczasowych i docelowych.
   - **4.4.** Szczegółowe raporty trendów – działania prewencyjne.
   - **4.5.** Analizy, rozwiązania i zadania dodatkowe.

5. **Moduł Zarządzanie Umowami SLA w zakresie oprogramowania musi obsługiwać:**
   - **5.1.** Definiowanie reguł SLA ze względu na użytkownika, jednostkę organizacyjną przedsiębiorstwa, kategorię czy priorytet.
   - **5.2.** Automatyczną aktualizację zgłoszeń aby zapewnić zgodny z SLA czas rozwiązania.
   - **5.3.** Czuwanie nad zakończeniem rozwiązania problemu w zdefiniowanym uprzednio przedziale czasu i w razie potrzeby zastosowanie mechanizmu eskalacji (do 4 poziomów).
   - **5.4.** Pomiar jakości SLA – raportowanie.
   - **5.5.** Powiadomienia serwisantów o zbliżającym się końcu czasu przeznaczonego na rozwiązanie zgłoszenia.

6. **Moduł Portal Pomocy Technicznej musi obsługiwać:**
   - **6.1.** Przyjazny interfejs i łatwość tworzenia zgłoszeń.
   - **6.2.** Szablony standardowych zgłoszeń.
   - **6.3.** Możliwość sprawdzania statusu zgłoszeń w realizacji.
   - **6.4.** Wbudowana baza wiedzy.
   - **6.5.** Dostęp do zgłoszeń historycznych.

7. **Moduł Baza wiedzy musi obsługiwać:**
   - **7.1.** Dostęp do tworzonej przez dział IT bazy 24h/7d.
   - **7.2.** Indeksowanie przy użyciu słów – kluczy.
   - **7.3.** Rozdzielenie bazy wiedzy pomiędzy serwisantów (IT) i użytkowników końcowych z dostępem tylko do prostych rozwiązań (z którymi mogą sobie sami poradzić).
   - **7.4.** Grupowanie rozwiązań wg tematów.
   - **7.5.** Dostęp do "najbardziej popularnych" i "ostatnio dodanych" rozwiązań.

8. **Moduł Raportowanie musi obsługiwać:**
   - **8.1.** Obsługa raportów w standardzie Stimulsoft lub zgodnym.
   - **8.2.** Raporty parametryczne z parametrami statycznymi i dynamicznymi.
   - **8.3.** Predefiniowane raporty obejmujące całokształt funkcjonalności zgodne z ITIL v. 4

9. **Zarządzanie zmianą musi obsługiwać:**
   - **9.1.** Planowanie zmiany i harmonogramu projektów w webowym interfejsie GUI.
   - **9.2.** Możliwości ustawiania schematów zatwierdzeń zmiany.
   - **9.3.** Możliwości przypisania wielu osób do schematu zatwierdzeń zmiany.
   - **9.4.** Obsługa wielu zmian i projektów w oparciu o wspólny schemat kalendarza, umożliwiający kontrolę przebiegu zmiany.
   - **9.5.** Możliwości modyfikacji z poziomu GUI elementów projektu i formularza zmiany.
   - **9.6.** Automatyczne powiadomienia oraz system zatwierdzeń, wysyłane do właściwych osób.
   - **9.7.** Możliwość ograniczenia widoku zmian i planowania ze względu na uprawnienia osób.
   - **9.8.** Możliwości powiązania zmian z systemem ticketowym oraz zasobami systemu ticketowego.
   - **9.9.** Możliwości śledzenia przebiegu zmiany przez supervisora.
   - **9.10.** Możliwość zatwierdzenia przez osobę bez dostępu do systemu, o ile została uwzględniona w schemacie zatwierdzeń.

10. **Platforma zgłoszeń sygnalistów musi obsługiwać:**
   - **10.1.** Webową i powszechnie dostępną, nie wymagającą logowania platformę dostępu dla sygnalistów.
   - **10.2.** Platformę publikacji dokumentów firmowych.
   - **10.3.** Szyfrowaną dwukierunkową komunikację pomiędzy sygnalistą a osobą obsługującą na każdym etapie zgłoszenia, bez pobierania jakichkolwiek danych od sygnalisty, w tym bez pobierania adresu mailowego.
   - **10.4.** Możliwość załączania plików do formularza zgłoszenia.
   - **10.5.** Modyfikowalny formularz zgłoszenia, dostosowywany z poziomu GUI systemu przez administratora nieposiadającego fachowej wiedzy informatycznej.
   - **10.6.** Możliwość ustawienia interaktywnych formularzy zgłoszeń dla poszczególnych kategorii zgłoszeń.
   - **10.7.** Możliwość ustawienia minimalnych wymagań formularza zgłoszenia.
   - **10.8.** Zabezpieczenia captcha dla komunikacji z sygnalistą.
   - **10.9.** Możliwość dodania klauzuli RODO.
   - **10.10.** Interaktywny widok zgłoszeń sygnalistów.
   - **10.11.** Oddzielny od systemu ticketowego system uprawnień i obsługi administracyjnej.
   - **10.12.** Zabezpieczone powiadomienia o próbach ingerencji w uprawnienia użytkowników systemu.
   - **10.13.** Możliwość integracji z systemami obsługi wniosków.

11. **Bezpieczeństwo:**
   - **11.1.** System wyposażony jest w mechanizmy definicji praw dostępu do poszczególnych widoków danych i opcji w konsoli administracyjnej.
   - **11.2.** System umożliwia zablokowanie komunikacji z serwerem producenta w celu wyłączenia aktualizacji.
   - **11.3.** System umożliwia dostarczenie aktualizacji w formie offline.
   - **11.4.** Uwierzytelnianie do systemu jest realizowane:
   - **11.4.1.** Z wykorzystaniem imiennego konta użytkownika i hasła,

11.4.2. Z wykorzystaniem imiennego konta administratorów aplikacji i hasła,
11.4.3. Hasła w systemie i bazach danych nie mogą w żadnym z przypadków występować w formie jawnej,
11.4.4. Za pośrednictwem jednokrotnego uwierzytelniania poprzez Active Directory.
11.4.5. Za pośrednictwem kont LDAP.
11.4.6. Za pośrednictwem kont CAS.
11.5. System umożliwia definiowanie poziomu uprawnień dla grupy oraz użytkownika (odczyt, zapis, kasowanie) do wszystkich widoków danych oraz wybranych elementów struktury organizacyjnej, wyposażony jest w opcję dziedziczenia uprawnień. Odebranie praw do widoku lub zakładki na widoku powoduje ukrycie opcji.
11.6. Lista użytkowników / administratorów systemu jest importowana i aktualizowana zgodnie z harmonogramem w oparciu o mechanizm RBAC (Role Base Access Control) z wybranego obiektu Active Directory. Użytkownik wyłączony/usunięty/zablokowany w Active Directory automatycznie traci prawa do korzystania z konsoli administracyjnej systemu.
11.7. System posiada mechanizmy automatycznego wykonywania kopii bezpieczeństwa w zadanych interwałach czasowych w formie kopii przyrostowej i nie przyrostowej oraz może udostępniać informacje o rezultacie wykonania kopii.
11.8. System pobiera dane z widoków (ang. View) zdefiniowanych w bazie danych a nie bezpośrednio z tabel bazy danych.
11.9. W przypadku wystąpienia awarii systemu i konieczności instalacji systemu na nowo system musi automatycznie z serwera aktualizacji producenta w ciągu 24 godzin dokonać aktualizacji wszystkich komponentów (konsola administracyjna, agenci, serwer, baza danych, bazy wiedzy).
11.10. System zapewnia mechanizmy zapewniające integralność, poufność i dostępność przechowywanych informacji.

12. Pomoc techniczna:

12.1. Pomoc techniczna
12.1.1. Musi być świadczona co najmniej w dni robocze w godzinach od 8.00-16.00.
12.1.2. Utrzymaniem Oprogramowania jest zapewnienie aktualizacji Oprogramowania asysta techniczna) oraz nieprzerwanego działania Oprogramowania (usługi SLA), jak również zapewnienie świadczenia innych usług wspomagających korzystanie z Oprogramowania.
12.2. Czas trwania usługi SLA wynosi 12 miesięcy od dnia zakupu.
12.3. Usługi Utrzymania Oprogramowania obejmują:
12.3.1. asystę techniczną,
12.3.2. świadczenie usług SLA, w ramach, których realizowana jest:
12.3.2.1. obsługa zgłoszeń w zakresie:
12.3.2.1.1. reakcja na zgłoszenia błędów w określonym czasie reakcji;
12.3.2.1.2. dokonywanie analizy przyczyn błędów;
12.3.2.1.3. zapewnianie obejścia dla błędów występujących z przyczyn leżących po stronie oprogramowania podmiotów trzecich;
12.3.2.1.4. zapewnianie obejścia dla błędów występujących z przyczyn leżących po stronie infrastruktury zamawiającego;
12.3.2.1.5. usuwania błędów w czasie naprawy;

12.3.2.1.6. usuwania błędów występujących z przyczyn leżących po stronie oprogramowania podmiotów trzecich – po udostępnieniu odpowiedniej aktualizacji przez producenta tego oprogramowania oraz jej uzyskaniu – w czasie naprawy;

12.3.2.1.7. zapewnienia dostępności Oprogramowania.