# Wymagania ogólne w zakresie dostawy oprogramowania do zarządzania infrastrukturą IT.

* + - 1. Dostarczone oprogramowanie musi być wolne od wad prawnych.
      2. Niedopuszczalne jest oprogramowanie prototypowe.
      3. Wymagania licencyjne dla dostarczonego oprogramowania:
* Licencjobiorcą licencji będzie Starostwo Powiatowe w Ostrołęce.
* Licencje muszą zostać wystawione na czas nieoznaczony (bezterminowy).
* Oferowane licencje muszą pozwalać na użytkowanie oprogramowania zgodnie z przepisami prawa.
* Licencja na oprogramowanie nie może w żaden sposób ograniczać sposobu pracy użytkowników końcowych (np. praca w sieci LAN, praca zdalna poprzez Internet). Użytkownik może pracować w dowolny dostępny technologicznie sposób.
* Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do wykonania kopii bezpieczeństwa oprogramowania w ilości, którą uzna za stosowną.
* Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do instalacji użytkowania oprogramowania na serwerach zapasowych uruchamianych w przypadku awarii serwerów podstawowych.
* Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do korzystania z oprogramowania na dowolnym komputerze klienckim (licencja nie może być przypisana do komputera/urządzenia).
* Wykonawca zapewni minimum 12 miesięczną gwarancję producenta oprogramowania, która obejmie gwarancję aktualizacji oprogramowania do najnowszej wersji oprogramowania w okresie objętym gwarancją.
* opcjonalnie możliwość przedłużenia Umowy Serwisowej na kolejne 12 miesięcy (przy zachowaniu ciągłości usługi) w cenie nie większej niż 20% wartości licencji (liczonej od ceny katalogowej licencji, aktualnej w dniu wyceny przedłużenia Umowy Serwisowej)
* dostępność oprogramowania w dowolnej konfiguracji modułowej (funkcjonalnej) według rzeczywistych indywidualnych potrzeb użytkownika.
* możliwość dokupienia modułów (rozszerzenia funkcjonalności) oraz zwiększenia liczby zarządzanych stacji roboczych w ramach jednej licencji w dowolnym czasie.

# Zasada równoważności rozwiązań.

1. Za równoważne do wyspecyfikowanego rozwiązania Zamawiający uzna rozwiązanie o tym samym przeznaczeniu, cechach technicznych, jakościowych i funkcjonalnych odpowiadających cechom technicznym, jakościowym i funkcjonalnym wskazanych w opisie przedmiotu zamówienia, lub lepszych, oznaczonych innym znakiem towarowym, patentem lub pochodzeniem.
2. Rozwiązanie równoważne musi pozwalać na zrealizowanie zakładanego przez Zamawiającego celu poprzez parametry wydajnościowe i funkcjonalne, mające wpływ na skuteczność działania, takie same lub lepsze od wskazanych wymagań minimalnych.
3. Użycie w opisie przedmiotu zamówienia nazw rozwiązań, służy ustaleniu minimalnego standardu wykonania i określenia właściwości i wymogów technicznych założonych w dokumentacji technicznej dla projektowanych rozwiązań.
4. Wykonawca zobligowany jest do wykazania, że oferowane rozwiązania równoważne spełnią zakładane wymagania minimalne. Wykonawca, który złoży ofertę na produkty równoważne musi do oferty załączyć dokumenty zawierające dokładny opis oferowanych produktów, z którego wynikać będzie zachowanie warunków równoważności. Wykonawca, który posługuje się równoważnymi certyfikatami musi je załączyć do oferty. Przez certyfikat równoważny Zamawiający rozumie certyfikat analogiczny co do zakresu z certyfikatami wskazanymi z nazwy, który potwierdza spełnianie normy charakteryzującej się cechami właściwymi dla normy wymienionej przez Zamawiającego, wystawiony przez niezależny podmiot uprawniony do wystawiania certyfikatów.
5. Brak określenia „minimum” oznacza wymaganie na poziomie minimalnym, a Wykonawca może zaoferować rozwiązanie o lepszych parametrach.
6. W celu zachowania zasad neutralności technologicznej i konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych, przy czym za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności nie odbiega lub jest lepsze od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym.
7. Nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym. W związku z tym, Wykonawca może zaproponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób.
8. Przez bardzo zbliżoną (podobną) wartość użytkową rozumie się podobne, z dopuszczeniem nieznacznych różnic nie wpływających w żadnym stopniu na całokształt systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, dla których to warunków rozwiązania te są dedykowane. Rozwiązanie równoważne musi zawierać dokumentację potwierdzającą, że spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wyspecyfikowanego.

# Dostawa, funkcjonalność oprogramowania do zarządzania infrastrukturą IT.

**SPECYFIKACJA TECNICZNA OPROGRAMOWANIA**

Oprogramowanie powinno mieć budowę modułową, która ma składać się z serwera zarządzającego, zdalnych konsoli oraz Agentów. Komunikacja pomiędzy Serwerem a Agentami i Konsolami nawiązywana musi być przy użyciu szyfrowanego protokołu TLS 1.2. Program musi umożliwiać zmianę portu komunikacyjnego wykorzystywanego przez konsolą zarządzającą.

Moduły muszą umożliwiać kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych oraz pomocy w formie interaktywnego połączenia sieciowego z obsługiwanym użytkownikiem. Program powinien wykorzystywać darmowy silnik bazy danych z kodem źródłowym dostępnym na licencji open-source bez limitu ilości danych, baza danych nie może wymagać dodatkowego licencjonowania. Instalacja Serwera oraz Konsol zarządzających powinna wykorzystywać 64-bitowy system operacyjny Windows. Dane, które dotyczą działań pracownika na komputerze, a więc: historia aktywności, polityka korzystania z Internetu oraz aplikacji, dostęp do zewnętrznych nośników danych itp., muszą być odseparowane od danych stricte technicznych tj. informacji o stacji roboczej. Powinny być one również grupowane w osobnym, dedykowanym oknie, co pozwoli na zgodne z RODO, usuwanie danych wybranego użytkownika bez konieczności usunięcia informacji o stacji roboczej.  
Dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, musi być objęty kontrolą na poziomie wybranych Administratorów – (nadawanie kontom administracyjnym różnych poziomów dostępu oraz uprawnień zarówno do funkcji Programu, grup urządzeń, jak i użytkowników).  
  
Główny Administrator musi mieć możliwość zarządzania uprawnieniami konfiguracyjnymi programu dla innych kont z rolą administracyjną (np. może wyłączyć możliwość zdalnej deinstalacji Agenta, ograniczyć dostęp do Opcji programu oraz logów działań innych administratorów).   
Działania administratorów muszą mieć odzwierciedlenie w dzienniku z listą czynności wykonanych przez administratorów, (modyfikacja obiektów znajdujących się w systemie w tym m.in. logowanie dostępu do Opcji programu, logowanie dostępu do informacji o aktywności użytkownika, logowanie poleceń deinstalacji Agenta). Działania administratorów powinny być automatycznie eksportowane do zewnętrznego kolektora Syslog.

**WYMAGANIA W ZAKRESIE MONITOROWANIA INFRASTRUKTURY (BEZAGENTOWO)**

Monitorowanie musi obejmować serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle w zakresie:

* wykrywania urządzeń w sieci poprzez skanowanie ping oraz arp-ping
* wykrywania urządzeń na podstawie informacji odczytanych z Active Directory (wraz z informacją   
  o OU)
* wizualizacji stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci
* wizualizacji urządzeń na mapach z funkcją siatki umożliwiającej korygowanie pozycji ikon na mapie do najbliższej linii siatki
* wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z dowolnym kolorem tła.
* wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z wykorzystaniem jako tła zaimportowanych obrazków np. schematu rozmieszczenia pomieszczeń w budynku
* wizualizacji map urządzeń poprzez grupowanie urządzeń na narysowanych czworokątach   
  o dowolnym rozmiarze i kolorze
* wizualizacji map urządzeń poprzez wstawianie dowolnego tekstu na mapie
* wizualizacji połączeń pomiędzy urządzeniami a przełącznikami za pomocą linii i informacji,   
  do którego portu przełącznika podłączone jest dane urządzenie w sposób manualny oraz automatyczny
* zablokowania mapy urządzeń przed przypadkową edycją
* serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program monitoruje czas ich odpowiedzi i procent utraconych pakietów
* serwerów pocztowych:
* program monitoruje czas logowania do serwisu odbierającego oraz czas wysyłania poczty
* program ma możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie (np. gdy ważne parametry znajdą się poza zakresem)
* program ma możliwość wykonywania operacji testowych
* program ma możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa
* monitorowania serwerów WWW i adresów URL
* cyklicznego monitorowania czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS
* obsługi szyfrowania SSL/TLS w powiadomieniach e-mail
* obsługi urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją, (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.) – monitorowanie wartości za pomocą nazw zmiennych oraz OID
* obsługi komunikatów syslog i pułapek SNMP i ewidencjonowanie odebranych z nich danych
* monitoringu routerów i przełączników wg:
* zmian stanu interfejsów sieciowych
* ruchu sieciowego
* podłączonych stacji roboczych – graficzna prezentacja panelu switcha
* ruchu generowanego przez podłączone do portów stacje robocze
* serwisów Windows: monitor serwisów Windows alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie/zatrzymanie/zrestartowanie
* wyświetlania statystyk przy każdym urządzeniu na mapie takich jak: czas odpowiedzi urządzenia, czas od ostatniej poprawnej odpowiedzi, nazwa DNS, adres IP, status zarządzalności SNMP, ostrzeżenie o zdarzeniu na urządzeniu
* wydajności systemów Windows:
* obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy

W celu lepszego zarządzania logiczną strukturą urządzeń w przedsiębiorstwie (Wydziały) program powinien tworzyć dynamiczne mapy wg własnych filtrów (Mapy Inteligentne). Kryteria automatycznego filtrowania dotyczyć mogą m.in. statusu Agenta, wygenerowanych alarmów, zainstalowanych aplikacji, przynależności do oddziału, serwisów sieciowych, danych z SNMP, danych   
z inwentaryzacji urządzenia itp. Program powinien posiadać również funkcję kompilatora plików MIB, który umożliwia dodawanie definicji dla modułów SNMP.

Program powinien umożliwiać również nakładanie na urządzenia liczników wydajności WMI oraz SNMP wg szablonów definiowanie alarmów z wykorzystaniem akcji związanych ze zdarzeniami w systemie, m.in.: wysłanie komunikatu pulpitowego, wysłanie wiadomości e-mail, wysłanie SMS, wysłanie wiadomości SMS poprzez integrację z serwisem smsapi.pl, wysłanie wiadomości przez Microsoft Teams oraz Slack, uruchomienie programu, wysłanie pułapki SNMP, wysłanie pakietu Wake-On-LAN, zatrzymanie/restart usługi Windows, wyłączenie/restart komputera. Administrator powinien mieć możliwość samodzielnego budowania Alarmów Zdarzeń z wykorzystaniem ciągu przyczynowo skutkowego – np. poprzez wskazanie dowolnego zdarzenia z listy, którego wykrycie wzbudzi alarm oraz dowolną liczbę akcji wybranych z listy, które zostaną wykonane jako reakcja na wykryte zdarzenie.

Program powinien umożliwiać automatyczną konfigurację wykonywania akcji alarmów po wykryciu zdarzenia, z opóźnieniem, na końcu zdarzenia oraz cyklicznie np. co 5 minut, oraz umożliwiać dla wykonania akcji nałożenie ograniczenia czasowego np. nie wykonuj między 8:00-16:00. i pozwalać na priorytetyzację urządzeń, grupowanie wg. ważności i typu urządzenia.

Oprogramowanie powinno umożliwiać wykorzystanie w alarmowaniu skrzynek e-mail   
z wykorzystaniem autoryzacji OAuth 2.0. Program powinien mieć możliwość integracji ze sprzętową bramką GSM w celu wysyłania powiadomień SMS z wykorzystaniem protokołu netGSM (SOAP).

**WYMAGANIA W ZAKRESIE INWENTARYZACJI**

Program musi automatycznie gromadzić informacje o sprzęcie i oprogramowaniu na stacjach roboczych oraz:

* prezentować szczegóły dotyczące sprzętu: modelu, procesora, pamięci, płyty głównej, napędów,  
  kart itp.
* obejmować m.in.: zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach,  
  średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których  
  konieczny jest upgrade.
* informować o zainstalowanych aplikacjach oraz aktualizacjach Windows co bezpośrednio  
  umożliwia audytowanie i weryfikację użytkowania licencji w organizacji.
* zbierać informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej:  
  instalacji/deinstalacji aplikacji, zmian adresu IP itd.
* posiadać możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania  
  programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera.
* umożliwiać odczytanie numeru seryjnego (klucze licencyjne).
* umożliwiać automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez  
  określenie paczek aplikacji wymaganych oraz nieautoryzowanych.
* umożliwiać przegląd informacji o konfiguracji systemu, np. komend startowych, zmiennych  
  środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp.
* umożliwiać utworzenie listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI)  
  znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem metadanych  
  plików użytkownika: obrazów (wymiary obrazka), video (długość filmu), audio (długość nagrania), archiwów (liczba plików w środku, rozmiar po wypakowaniu).
* umożliwiać wymianę plików do i ze stacją roboczą poprzez funkcję Menedżera plików. Działania  
  administratorów wykonywane w tej funkcji są logowane.

Moduł inwentaryzacji zasobów musi umożliwiać prowadzenie bazy ewidencji majątku IT w zakresie sprzętu i programowania:

* przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz  
  automatycznego aktualizowania zgromadzonych informacji,
* tworzenia powiązań między zasobami a urządzeniami,
* tworzenia powiązań między zasobami a kontami użytkowników (zarówno lokalnymi,   
  jak i zsynchronizowanymi z Active Directory), wskazywanie osób odpowiedzialnych,
* wskazania osób uprawnionych do użycia zasobów poprzez rozbudowane mechanizmy,
* definiowania własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości  
  - dla danego urządzenia lub oprogramowania istnieje możliwość dodawania dodatkowych  
  informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer dokumentu zakupu, wartość  
  sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu gwarancji, termin kolejnego  
  przeglądu (można podać datę, po której administrator otrzyma powiadomienie e-mail  
  o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, lub  
  własny komentarz,
* określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów,
* określenia atrybutów dodatkowych tylko dla wybranych typów zasobów,
* definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie,
* importu danych z zewnętrznego źródła (.CSV),
* przechowywania dowolnych dokumentów (np. pliki .DOCX, .XLSX, .PDF), np.: skan faktury zakupu, gwarancji, dowolnego dokumentu itp.,
* tworzenia powiązań między zasobami a dokumentami w relacji 1:N,
* oznaczania statusów zasobów, np. w użyciu, w naprawie, zutylizowany itp.,
* ewidencji czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie, konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie czynności,
* generowania zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania,
* przygotowanie wielu szablonów generowanych dokumentów i protokołów przekazania  
  zasobów wraz z konfigurowalną sekcją zawierającą dane i logo organizacji,
* konfiguracji stylu automatycznego numerowania dodawanych zasobów wg zdefiniowanego  
  wzorca,
* konfiguracji stylu automatycznego numerowania dodawanych dokumentów i protokołów   
  wg zdefiniowanego wzorca,
* archiwizacji i porównywania audytów zasobów,
* tworzenia kodów kreskowych dla zasobów,
* drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code)   
  dla zasobów , które posiadają numer inwentarzowy,
* inwentaryzacji zasobów posiadających kody kreskowe za pomocą aplikacji mobilnej dla systemu Android poprzez wyszukiwanie zasobów, skanowanie etykiet, dodawanie i edycję zasobów, dodawanie czynności serwisowych, drukowanie etykiet,
* możliwość zmiany portu komunikacyjnego wykorzystywanego przez aplikację mobilną dla systemu Android,
* inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline),
* definiowania alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data”   
  z atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnie licencja/gwarancja”).

Inwentaryzacja oprogramowania zapewnia funkcjonalność w zakresie pozyskiwania informacji   
o oprogramowaniu i audycie licencji poprzez:

* skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP.
* informacje o aplikacjach używanych w organizacji.
* tworzenie własnych wzorców aplikacji.
* tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp.
* informacje o komputerach, na których aplikacja została wykryta.
* zarządzanie posiadanymi licencjami.
* wskazywanie osób odpowiedzialnych za licencję.
* wskazanie użytkowników licencji.
* tworzenia powiązań między licencjami a dokumentami w relacji 1:N.
* rozbudowane i konfigurowalne scenariusze zarządzania licencjami poprzez: przypisywanie   
  do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie   
  wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu.
* audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji - w każdej chwili istnieje możliwość wykonania aktualnych raportów audytowych.
* zarządzanie posiadanymi licencjami: raport zgodności licencji.
* możliwość przypisania do programów numerów seryjnych, wartości itp.
* okna audytowe powinny posiadać możliwość filtrowania elementów per oddział.

**WYMAGANIA W ZAKRESIE OBSŁUGI UŻYTKOWNIKÓW**

Program musi umożliwiać monitorowanie aktywności użytkowników pracujących na komputerach   
z systemem Windows poprzez monitorowanie:

* faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy),
* procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika) wraz  
  informacją o uruchomieniu na podwyższonych uprawnieniach,
* rzeczywistego użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji,  
  obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była  
  uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność,
* informacji o edytowanych przez użytkownika dokumentach,
* historii pracy (cykliczne zrzuty ekranowe),
* listy odwiedzanych stron WWW (liczba odwiedzin stron z nagłówkami, liczbą i czasem wizyt),
* transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez  
  użytkownika),
* wydruków m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla  
  każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był  
  drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej  
  drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek  
  poprzez identyfikację drukarek. Program ma możliwość monitorowania kosztów wydruków,
* nagłówków przesyłanej w aplikacjach klienckich poczty e-mail.

Program ponadto powinien posiadać możliwość:

* blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu  
  WWW dla stacji roboczej, na której zalogowany jest użytkownik, z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen (np. \*.domena.pl). Reguły w postaci listy domen  
  tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami.
* blokowania ruchu na wskazanych portach TCP/IP,
* blokowania pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem,
* wysyłania powiadomień gdy użytkownik: odwiedzi stronę z określonej grupy domeny; pobierze  
  lub wyśle określoną ilość danych w ciągu dnia w sieci lokalnej lub Internet; wydrukuje określoną ilość stron w ciągu dnia,
* przygotowania zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu  
  (który można dołączyć np. do akt pracownika),
* definiowania godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone.
* generowania raportów dla użytkowników Active Directory niezależnie od tego, na jakich komputerach pracowali w danym czasie.
* blokowania uruchamiania aplikacji wg maski nazwy oraz lokalizacji pliku. (np. reguły w postaci listy blokowanych plików lub lokalizacji tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami).

**WYMAGANIA W ZAKRESIE REALIZACJI ZDALNEJ POMOCY UŻYTKOWNIKOM**

W ramach kontroli stacji użytkownika program musi udostępnić podgląd pulpitu użytkownika i mieć możliwość przejęcia nad nim kontroli oraz zdefiniowania czy użytkownik powinien zostać zapytany   
o zgodę na połącznie i opcją odrzucenia takiego połącznia przez użytkownika (np. w przypadku pracowników wysokiego szczebla).

Podczas dostępu zdalnego, zarówno użytkownik jak i administrator widzą ten sam ekran. Administrator w trakcie zdalnego dostępu ma możliwość zablokowania działania myszy oraz klawiatury   
dla użytkownika.

W niniejszym programie/module powinna znajdować się baza zgłoszeń umożliwiająca użytkownikom zgłaszanie problemów technicznych poprzez dedykowany portal oraz przetwarzanie wiadomości   
e-mail, które będą przetwarzane i przyporządkowywane odpowiednim administratorom, otrzymującym automatycznie powiadomienie o przypisanym im problemie. Oprogramowanie powinno pozwalać na integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz mechanizm OAuth2.0.

Program/moduł powinien umożliwiać również przetwarzanie zgłoszeń w trybie anonimowym (wsparcie w realizacji wymogów „Dyrektywy o sygnalistach”) oraz zawiera dokumenty prawne   
dot. ochrony sygnalistów w tym szablon regulaminu zgłoszeń wewnętrznych wymagany przez Dyrektywę.  
Użytkownicy powinni mieć możliwość monitorowania procesu rozwiązywania zgłoszonych przez nich problemów i ich aktualnych statusów, jak również możliwość wymiany informacji z administratorem poprzez komentarze, które są wpisywane i widoczne dla obu stron.

Program/moduł ten powinien zawierać komunikator (czat), który umożliwi prowadzenie rozmów   
w czasie rzeczywistym oraz archiwizację historii wiadomości pomiędzy zalogowanymi użytkownikami,  
pracownikami pomocy technicznej i administratorami (wraz z wyszukiwarką rozmów i wiadomości   
wg słów kluczowych oraz automatycznym oczyszczaniem historii rozmów). Ponadto pozwolić na:

* zarządzanie dostępem do czatu w 3 poziomach uprawnień: pełny dostęp, brak dostępu lub  
  dostęp ograniczony wyłącznie do pomocy technicznej
* rozmowy również między „zwykłymi” użytkownikami
* przesyłanie plików między rozmówcami w trybie online
* tworzenie pokojów tematycznych, rozmów grupowych
* oznaczanie kontaktów jako „ulubionych” na liście kontaktów
* uruchomienie z poziomu ikony dostępowej Agenta oraz bezpośrednio w interfejsie WWW heldpesku
* wyświetlanie w trybie jasnym lub ciemnym

Program/moduł powinien zawierać bazę wiedzy pomagająca użytkownikom samodzielnie rozwiązywać najprostsze, powtarzające się problemy wraz z możliwością nadawania artykułom 1 z 3 statusów (opublikowany, wewnętrzny, szkic), umożliwiać informowanie pracowników o zdarzeniach, np. planowanych przestojach w dostępie do usług, przez komunikaty z graficznym formatowaniem treści oraz łączami do artykułów w bazie wiedzy.

Dostęp do systemu zgłoszeń oraz bazy wiedzy powinien być realizowany przez dedykowany portal dostępny przez przeglądarkę internetową, który może być wyświetlany w trybie jasnym lub ciemnym. Funkcjonalność programu/modułu powinna umożliwiać również uzyskanie dostępu z prywatnego komputera tylko do swojego komputera firmowego, który pozostał w organizacji, za pomocą funkcji zdalnego dostępu przez każdego pracownika. Ponadto powinien umożliwiać również:

* pobieranie listy użytkowników z Active Directory,
* zarządzanie lokalnymi kontami Windows w zakresie: tworzenia, usuwania, aktywacji, edycji uprawnień, resetu hasła, edycji kont,
* zarządzanie dostępem pracowników HelpDesku do zgłoszeń poprzez rozbudowany system zarządzania regułami widoczności zgłoszeń,
* tworzenie własnego drzewa kategorii zgłoszeń wraz z możliwością grupowania kategorii   
  w folderach (do 4 poziomów kategorii), opisami kategorii oraz klauzulą RODO,
* automatyczne przypisywanie konkretnych pracowników helpdesk do zgłoszeń  
  w określonych kategoriach lub pochodzących od określonych grup użytkowników,
* definiowanie ścieżek akceptacji zgłoszeń – procesu, w którym użytkownik uzyskuje akceptację na realizację zgłoszenia od wyznaczonych osób w organizacji,
* przypisywanie ścieżek akceptacji zgłoszeń do określonych kategorii,
* procesowanie zgłoszeń użytkowników z wiadomości e-mail,
* integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz mechanizm OAuth 2.0,
* tworzenie formularzy z niestandardowymi polami opisowymi, dedykowanymi do wybranych kategorii zgłoszeń,
* wykonywanie operacji na wielu zgłoszeniach równocześnie,
* dołączanie załączników do zgłoszeń,
* rozbudowane wyszukiwanie zgłoszeń i artykułów w bazie wiedzy,
* szybki dostęp do ostatnich zgłoszeń, artykułów bazy wiedzy i załączników,
* wprowadzenie komentarza oraz informacji o czasie poświęconym na rozwiązanie w kreatorze wyświetlanym przy zamykaniu zgłoszenia,
* zrzuty ekranowe (podgląd pulpitu),
* zdalną modyfikację rejestrów,
* dystrybucję oprogramowania przez Agenty,
* definiowanie aplikacji dozwolonych do samodzielnej instalacji przez użytkowników z pakietów MSI w postaci Kiosku z Aplikacjami,
* przypisywanie dostępnych w Kiosku instalatorów do grup użytkowników,
* dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików MSI),
* zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecania operacji następuje kolejkowanie zadania dystrybucji pliku,
* możliwość skonfigurowania automatyzacji procesowania zgłoszeń wraz z powiadomieniami e-mail wysyłanymi do określonych aktorów w zgłoszeniu,
* planowanie nieobecności pracowników helpdesk,
* obsługę umów o gwarantowanym poziomie świadczenia usług (SLA) wraz z raportami   
  np. przekroczeń SLA wraz z podsumowaniem,
* generowanie raportów obsługi helpdesk,
* zdalne wykonywanie poleceń poprzez Agenty (np. utworzenie/edycja konta lokalnego użytkownika systemu),
* zarządzania procesami systemu Windows (w zakresie: zakończ proces, zakończ drzewo procesu, uruchom nowy proces w sesji użytkownika wraz z parametrami),
* wymiany plików do i ze stacji roboczej poprzez funkcję Menedżera plików.

Oprogramowanie powinno posiadać funkcjonalny portal informacyjny w formie platformy WWW, który pozwali na tworzenie wielu interaktywnych paneli informacyjnych (dashboardów)   
z responsywnymi widgetami, z możliwością rozmieszczenia ustalonym przez administratora.  
Zawartość każdego z paneli informacyjnych będzie automatycznie odświeżana oraz może być:

* udostępniana w trybie „tylko do odczytu” z zabezpieczeniem tokenem.
* wyświetlana w trybie jasnym lub ciemnym (nocnym).

Oprogramowanie powinno umożliwiać zarządzanie uprawnieniami administratorów   
do funkcjonalności portalu informacyjnego. Widgety powinny prezentować dane ze wszystkich modułów funkcjonalnych oprogramowania:

* liczniki wydajności, Alarmy (wraz z filtrowaniem) oraz odpowiedzi serwisów TCP/IP, Ostatnie urządzenia w sieci,
* zmiany w konfiguracji sprzętowej urządzeń z Agentami, Zmiany w konfiguracji aplikacyjnej urządzeń z Agentami, Alarmy dla Zasobów,
* statystyki z obszaru wydruków, Statystki użycia aplikacji, Użycie łącza, Aktywność WWW,
* statystyki z obsługi zgłoszeń, Lista najnowszych nierozwiązanych zgłoszeń, Lista najstarszych nierozwiązanych zgłoszeń, Zgłoszenia z naruszonym SLA, Zgłoszenia, których SLA wkrótce wygaśnie,
* ostatnio podłączone nośniki zewnętrzne, Ostatnie operacje na plikach (wraz z filtrowaniem),
* produktywność dla grupy, Statystyki czasu nieproduktywnego.

Program musi być zabezpieczony hasłem przed ingerencją użytkownika w jego działanie i próbą usunięcia, nawet jeśli użytkownik ma prawa administratora stacji roboczej, na której pracuje.  
Program powinien mieć globalną wyszukiwarkę, zwracającą wyniki obiektów różnego typu na podstawie wyszukiwanych słów kluczowych, np.: urządzenia, użytkownicy, zasoby, elementy interfejsu konsoli zarządzającej, elementy opcji.

Program musi być dostępny w języku polskim wraz z Podręcznikiem Użytkownika w formie strony internetowej.