Dostawa i wdrożenie informatycznego systemu zarządzania zasobami i użytkownikami, na który składają się monitoring infrastruktury, inwentaryzacja, monitoring pracy, helpdesk, ochrona danych przed wyciekiem.

Wymagania względem licencji:

1. Dostarczone licencje na oprogramowanie muszą być bezterminowe.
2. Dostarczone licencje oprogramowanie muszą być dostarczone z 12 miesięcznym wsparciem producenta, liczonym od daty zakończenia wdrożenia. W ramach wsparcia wymagany jest dostęp do nowych wersji systemu oraz wsparcia technicznego producenta.
3. Dostarczone licencje na oprogramowanie muszą objąć co najmniej 250 stanowisk roboczych i nie mogą mieć ograniczeń ilościowych dotyczących liczby obsługiwanych innych zasobów, jak drukarki, monitory czy urządzenia sieciowe.

Podstawowe informacje techniczne o Przedmiocie Zamówienia:

1. System musi posiadać budowę modułową i składać się z serwera zarządzającego, zdalnych konsoli oraz agentów.
2. Komunikacja pomiędzy składnikami systemu musi być nawiązywana przy użyciu szyfrowanego protokołu TLS 1.2.
3. Baza danych musi być oparta na darmowym silniku PostgreSQL.
4. Dane z monitoringu działań pracownika na stanowisku roboczym muszą być odseparowane od informacji o stacji roboczej. Musi być zachowana zgodność z RODO, która umożliwia usunięcie danych o pracowniku bez konieczności usuwania danych stacji roboczej.
5. System musi być dostosowany do pracy w środowisku wysokiej wirtualizacji, cienkich klientów (Thin Client), infrastruktury VDI.
6. Dostęp do danych osobowych oraz danych z monitoringu musi być objęty kontrolą na poziomie wybranych Administratorów Systemu. Konta administracyjne muszą dzielić się na Głównego Administratora oraz Administratorów o różnym poziomie dostępu i uprawnień. Główny Administrator musi móc zarządzać uprawnieniami konfiguracyjnymi systemu dla innych kont z rolą administracyjną.
7. Program musi posiadać ochronę (hasło Głównego Administratora) przed usunięciem lub ingerencją użytkownika (nawet z prawami administracyjnymi na stacji roboczej).
8. System musi być dostępny w polskiej i angielskiej wersji językowej.

Poniżej zawarty został opis funkcjonalności poszczególnych modułów systemu.

1. **Monitorowanie infrastruktury**. System musi spełniać wymagania, takiej jak:
    - Wykrywanie urządzeń wpiętych w sieć wewnętrzną poprzez skanowanie ping oraz arg-ping (bezagentowe).
    - Wizualizacja graficzna stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci.
    - Wizualizacja połączeń pomiędzy urządzeniami a przełącznikami i informacji, do którego portu przełącznika podłączone jest dane urządzenie.
    - Wykrywanie serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program musi monitorować czas odpowiedzi serwisów i procent utraconych pakietów.
    - W przypadku serwerów pocztowych:

  - program musi monitorować zarówno serwis odbierający, jak i wysyłający pocztę,
  - program musi mieć możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS),
  - program musi mieć możliwość wykonywania operacji testowych,
  - program musi mieć możliwość wysyłania powiadomień, w przypadku gdy serwer pocztowy nie odpowiada.
- System musi umożliwiać monitorowanie serwerów WWW i adresów URL.
- System musi obsługiwać szyfrowanie SSL/TLS w powiadomieniach e-mail.
- System musi obsługiwać urządzenia SNMP wspierające SNMP v1/2/3 z szyfrowaniem oraz autoryzacją oraz monitorować wartości za pomocą nazw zmiennych oraz OID.
- System musi obsługiwać komunikaty syslog i pułapki SNMP.
- System musi umożliwiać monitoring routerów i przełączników według:
  - zmian stanu interfejsów sieciowych,
  - ruchu sieciowego,
  - podłączonych stacji roboczych (w tym graficzna prezentacja panelu switcha),
  - ruchu generowanego przez podłączone do portów stacje robocze.
- Monitorowanie serwisów Windows – oprogramowanie musi alarmować gdy serwis przestanie działać oraz musi umożliwiać jego uruchomienie, zatrzymanie i zrestartowanie.
- Monitorowanie wydajności systemów Windows.
- Oprogramowanie musi posiadać funkcję kompilatora plików MIB.
- System musi umożliwiać tworzenie graficznych map zarządzania logiczną strukturą urządzeń.

2. **Inwentaryzacja**. W zakresie inwentaryzacji system musi umożliwiać:
   - Automatyczne gromadzenie informacji o sprzęcie i oprogramowaniu na stacjach roboczych.
   - Automatycznie generowanie:
     - zestawienia posiadanych konfiguracji sprzętowych,
     - wolnym miejscu na dyskach,
     - średniego wykorzystania pamięci,
     - informacje o koniecznym upgrade.
   - System musi wyświetlać informacje o zainstalowanych aplikacjach oraz aktualizacjach Windows.
   - System musi zbierać informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej, tj. instalacji i deinstalacji aplikacji, zmian adresu IP itd.
   - Wysyłanie powiadomień w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera.
   - System musi umożliwiać odczytanie numeru seryjnego (kluczy licencyjnych).
   - System musi umożliwiać automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych.
   - System musi umożliwiać przegląd informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp.

- System musi umożliwiać utworzenie listy plików użytkowników z określonym rozszerzeniem znalezionych na stacjach roboczych oraz ich zdalne usuwanie.
- System musi mieć możliwość wymiany plików do i ze stacją roboczą poprzez funkcję menadżera plików. Działania Administratorów wykonywane w tej funkcji muszą być logowane.

W zakresie prowadzenia **baz ewidencji majątku IT**:

- System musi umożliwiać przechowywanie wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji.
- Wymagana jest możliwość definiowania własnych typów wyposażenia, ich atrybutów oraz wartości oraz możliwość importu danych z zewnętrznego źródła (np. CSV).
- Generowanie zestawień wszystkich środków trwałych, w tym urządzeń i zainstalowanego na nich oprogramowania.
- Archiwizacja i porównywanie audytów środków trwałych.
- Tworzenie kodów kresowych w środkach trwałych.
- Drukowanie kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla środków trwałych, które posiadają numer inwentarzowy.
- Inwentaryzacja sprzętu posiadającego kody kreskowe za pomocą aplikacji mobilnej (należy wskazać dedykowany system dla aplikacji).
- System musi móc przeprowadzać inwentaryzację stacji roboczych niepodłączonych do sieci.
- Możliwość definiowania alarmów z powiadomieniami e-mail dla dowolnych pól typu data ze szczegółów środków trwałych lub licencji (np. powiadomienie o wygasającej licencja/gwarancja).
- Agenty inwentaryzacji muszą być dostępne dla systemów Android, macOS oraz Linux.

Funkcje **inwentaryzacji oprogramowania** musza umożliwiać:

- Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP.
- Zarządzanie posiadanymi licencjami.
- Audyt legalności oprogramowania oraz powiadamiania w przypadku przekroczenia liczby posiadanych licencji.
- Tworzenie raportów zgodności licencji.
- Przypisanie do programów numerów seryjnych lub wartości.

3. **Monitorowanie aktywności pracowników** oraz **zarządzanie czasem pracy** poprzez:
   - Faktyczny czas aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy).
   - Monitorowanie procesów wraz z informacją o uruchomieniu na podwyższonych uprawnieniach.
   - System musi obrazować rzeczywiste użytkowanie programów (procentowa wartość wykorzystania aplikacji), czas używania aplikacji w stosunku do łącznego czasu, przez który aplikacja była uruchomiona (informacja, na którym komputerze wykonano daną aktywność).
   - Budowaniu bazy informacji o edytowanych przez użytkownika dokumentach.

- Lista odwiedzanych stron WWW, przy czym musi być podana liczba odwiedzin stron z nagłówkami, liczbą i czasem wizyt.
- System musi monitorować ruch lokalny i transfer internetowy generowany przez użytkowników.
- Oprogramowanie musi monitorować wydruki.
- Oprogramowanie musi monitorować nagłówki przesłanej przez użytkownika poczty e-mail.

Dodatkowo system musi umożliwiać:

- Blokowanie stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla danej stacji roboczej z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych subdomen.
- Blokowanie ruchu na wskazanych portach TCP/IP.
- Blokowanie pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem.
- Wysyłanie 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 liczbę stron w ciągu dnia.
- Przygotowanie metryki ustawień monitorowania użytkownika w postaci raportu.
- Generowanie raportów dla użytkowników Active Directory.
- Blokowanie uruchamiania aplikacji.

Zarządzanie czasem i analiza aktywności użytkowników musi tworzyć:

- Statystyki czasu pracy i osobistej aktywności w wybranym przedziale czasu.
- Statystyki aktywności podwładnych widoczne dla przełożonego.
- Listę odwiedzanych stron internetowych i aplikacji wraz ze spędzonym na nich czasem.
- Statystyki popularności stron internetowych i aplikacji w organizacji, grupie i u poszczególnych użytkowników.
- Grupowanie stron internetowych i aplikacji z podziałem na:
  - produktywne,
  - neutralne,
  - nieproduktywne.
- Możliwość przypisania wyjątków produktywności dla poszczególnych aplikacji w wybranej grupie.
- Wskaźnik czasu poświęconego na aktywność produktywną.
- System musi móc definiować wymagany próg produktywności i limit nieproduktywności oraz umożliwiać włączenia dla nich alarmów e-mail.
- System musi umożliwiać przypisywanie kategorii aplikacjom i stronom internetowym.
- Listę kontaktów w organizacji z wbudowaną wyszukiwarką.

4. W zakresie **zdalnej pomocy i bazy wiedzy** system musi posiadać następujące funkcjonalności:
   - Kontrolę stacji użytkownika poprzez podgląd pulpitu użytkownika z możliwością przejęcia nad nim kontroli (zarówno użytkownik jak i administrator muszą widzieć ten sam ekran).

- Administrator w trakcie zdalnego dostępu musi mieć możliwość zablokowania działania myszy oraz klawiatury dla użytkownika.
- System musi umożliwiać monitorowanie przez użytkowników procesu rozwiązywania zgłoszonych przez nich problemów i aktualnych statusów, jak również musi mieć możliwość wymiany informacji z Administratorem poprzez komentarze, które muszą być wpisywane i widoczne dla obu stron.
- Oprogramowanie musi posiadać wbudowany komunikator, który musi umożliwiać przesyłanie wiadomości pomiędzy zalogowanymi użytkownikami i administratorami.
- System musi posiadać możliwość tworzenia i rozwijania bazy wiedzy pomagającej użytkownikom samodzielnie rozwiązywać najprostsze, powtarzające się problemy.
- System musi umożliwiać pobieranie listy użytkowników z Active Directory.
- System musi umożliwiać Administratorom tworzenie drzewa kategorii zgłoszeń wraz z możliwością grupowania kategorii (maksymalnie do 4 poziomów kategorii).
- System musi umożliwiać przypisywanie poszczególnych Administratorów do kategorii zgłoszeń.
- System musi umożliwiać procesowanie zgłoszeń użytkowników z wiadomości e-mail.
- Tworzenie formularzy z niestandardowymi polami opisowymi, dedykowanymi do wybranych kategorii zgłoszeń.
- Administratorzy musza mieć możliwość wykonywania operacji na wielu zgłoszeniach równocześnie.
- Oprogramowanie musi umożliwiać dołączanie załączników do zgłoszeń.
- System musi umożliwiać tworzenie i dodawanie do zgłoszenia zrzutów ekranowych.
- System musi umożliwiać dystrybucje oprogramowania oraz uruchamianie plików za pomocą dedykowanych agentów (w tym plików z rozszerzeniem MSI).
- System musi umożliwiać kolejkowanie dystrybucji plików, w przypadku gdy w trakcie trwania operacji stacja robocza jest wyłączona.
- System musi mieć możliwość skonfigurowania automatyzacji procesowania zgłoszeń.
- System musi umożliwiać planowanie nieobecności Administratorów.
- Program musi umożliwiać zdalne wykonywanie poleceń poprzez agentów na stacjach roboczych.
- System musi umożliwiać zarządzanie procesami systemu Windows w zakresie: zakończ proces, zakończ drzewo procesu, uruchom nowy proces w sesji użytkownika wraz z parametrami.
- System musi umożliwiać wymianę plików do i ze stacji roboczej poprzez wbudowaną funkcję menedżera plików.

5. Funkcjonalności dotyczące **ochrony danych przed wyciekiem** muszą umożliwiać:
   - Blokowanie urządzeń i nośników danych.
   - Blokowanie urządzeń i interfejsów fizycznych, takich jak: USB, FireWire, gniazda pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek.
   - Blokowanie interfejsów bezprzewodowych, takich jak: Wi-Fi, Bluetooth, IrDA.
   - Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do niezaufanych nośników.
   - Integrację z Active Directory poprzez zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych.
   - Przydzielanie uprawnień do kont użytkowników lokalnych.

Zarządzanie prawami dostępu do urządzeń musi umożliwiać:

- Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików.
- Autoryzowanie wewnętrznych urządzeń przenośnych: pendrive, dysków przenośnych itp., wraz z możliwością blokowania urządzeń prywatnych.
- Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników.
- Tworzenie centralnej konfiguracji poprzez ustawienie polityk dla całej sieci.

W zakresie **audytu operacji na urządzeniach przenośnych** system musi umożliwiać:

- Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych.
- Podłączenie i/lub odłączenie urządzenia przenośnego.