Załącznik Nr 1

**OPIS PRZEDMIOTU ZAMÓWIENIA**

**Zakup oprogramowania do audytów bezpieczeństwa, kontroli legalności oprogramowania oraz szyfrowania danych zgodnie z KRI.**

**System do zarządzania infrastrukturą it**

Ilość komputerów: 100

Ilość administratorów: 3

Zdalne wykonanie instalacji, konfiguracji i profilowanie systemu

Minimum 2 godziny szkolenia z obsługi dostarczonego systemu

Wsparcie producenta i dostęp do aktualizacji: 12 miesięcy

Licencja wieczysta. Licencja bezterminowa na oprogramowanie musi objąć co najmniej 100 stanowisk komputerowych z 12 miesięcznym wsparciem serwisowym

Wykonawca systemu zapewni co najmniej roczną usługę SLA (umowa poziomu usług) dla różnych kategorii błędów, w szczególności dla błędu krytycznego sytemu uniemożliwiającego korzystanie z oprogramowania lub blokującego realizację kluczowych procesów biznesowych klienta (unieruchomienie lub zawieszenie się systemu, znaczące zakłócenie pracy dla co najmniej 10% użytkowników Oprogramowania) i wymagającego jak najszybszej naprawy bądź obejścia, czas reakcji dla błędu krytycznego wyniesie do 4 godzin od momentu zgłoszenia błędu a czas naprawy do 12 godzin od momentu zgłoszenia błędu.

Architektura systemu

* 1. Agent – komponent odpowiedzialny za zarządzanie komputerem, zbieranie danych oraz przesyłanie danych do serwera z wykorzystaniem bezpiecznego połączenia, pracujący w trybie usługi systemowej.
	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).
	3. Panel pracownika – aplikacja webowa 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.
	4. Serwer – oprogramowanie odpowiadające za utrzymywanie komunikacji i wymianę danych z agentami.
	5. Baza danych pracująca na silniku Microsoft SQL Server w wersjach wyspecyfikowanych poniżej.
	6. Komponenty Agent, konsola administracyjna, serwer, baza danych muszą mieć możliwość aktualizacji samodzielnej za pośrednictwem bezpiecznego połączenia z serwerów aktualizacji producenta systemu.
	7. System musi umożliwiać komunikację pomiędzy agentami a serwerem w sieciach lokalnych, rozległych, także gdy komputery znajdują się za NATem.
	8. Wbudowany mechanizm automatycznej konserwacji/utrzymania zgodnie ze zdefiniowanym harmonogramem realizujący co najmniej: usuwanie zbędnych danych z systemu.

Wymagania systemowe

1. Konsola administracyjna ma działać w pełni responsywnie (niezależnie od wielkości i rozdzielczości ekranu urządzenia wyświetlającego) na dowolnej przeglądarce stron WWW zgodnej z HTML5 (np. Edge, Firefox, Chrome, Opera).
2. Agent ma pracować na systemach 32 i 64 bitowych: Windows Server 2016/2019/2022, Windows 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.
3. Serwer ma działać na systemach 64 bitowych: Windows Server 2016/2019/2022, Windows 10/11.
4. Serwer www ma być oparty o platformę Microsoft 64 bit (Windows Server 2016/2019/2022, Windows 10/11) oraz Java 8 (JRE lub JDK), Apache Tomcat 8+.
5. Baza danych ma działać na silniku Microsoft SQL Server 2016/2019 w wersji 64 bitowej komercyjnej.
6. Możliwość pracy w środowisku wirtualnym Microsoft Hyper-V oraz VMWare.
7. System ma umożliwiać wielokrotny, zgodny z harmonogramem lub na życzenie, import użytkowników, komputerów, struktury organizacyjnej z usługi MS Active Directory.

Funkcjonalności systemu zarządzania infrastrukturą IT

* 1. Inwentaryzacja sprzętu komputerowego
* ma umożliwiać automatyczną inwentaryzację komputerów z zainstalowanym agentem znajdujących się w sieci lokalnej oraz poza siecią lokalną (za NATem)
* ma zbierać szczegółowe informacje o sprzęcie (producent, model, data produkcji, numer seryjny) w oparciu o klasy WMI (Windows Management Instrumentation) oraz odczytuje informacje o zainstalowanych kościach pamięci: producent, numer seryjny (Serial Number), numer części (Part Number), rozmiar, częstotliwość, taktowania, a także skanować  dyski twarde (z podaniem typu interfejsu, numeru seryjnego oraz informacji SMART)
* ma monitorować parametry obciążenia komputerów: procesor, dyski, pamięć i sieć
* ma ewidencjonować pliki na komputerach (nazwa, rozmiar, rodzaj, lokalizacja, w przypadku plików wykonywalnych: wersja, producent) oraz wykazywać zmiany w systemie plików (dodano plik, usunięto plik)
* ma pozwalać na zdalne trwałe (bez możliwości odzyskania) usunięcie dowolnego pliku/plików na dowolnie zdefiniowanej grupie komputerów.
* ma umożliwiać ewidencję zdarzeń serwisowych dowolnego typu (np. naprawy sprzętu, wymiany części)
* ma umożliwiać samodzielną definicję, ewidencję oraz wydruk wszelkiego typu protokołów (przyjęcie, przekazanie do użytkowania, likwidacja)
	1. Inwentaryzacja urządzeń podłączanych do komputera
* ma automatycznie identyfikować i klasyfikować urządzenia podłączane do komputera (pendrive, monitor zewnętrzny, pamięć masowa, telefon, urządzenie multimedialne itp.)
* ma pozwalać na przypisanie podłączonego urządzenia do komputera oraz użytkownika
* ma umożliwiać uzyskanie informacji kto, kiedy i na jakim komputerze posługiwał się urządzeniem zewnętrznym, pozwalając na jego jednoznaczne zidentyfikowanie
* ma umożliwiać utworzenie dowolnej ilości list urządzeń USB dozwolonych do stosowania - tzw. białe listy urządzeń USB na podstawie zdefiniowanych reguł (dozwolone/niedozwolone) wg kryteriów: użytkownik, dzień tygodnia, okres (data od, godzina od, data do, godzina do), urządzenie USB, komputer, data obowiązywania reguły
1. Inwentaryzacja urządzeń innych niż komputery
	* ma umożliwiać inwentaryzację manualną dowolnych zasobów np. drukarki, switche, routery, monitory, pamięci masowe itp
	* ma posiadać 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
	* skaner SNMP ma łączyć zinwentaryzowane urządzenia (np. komputery, drukarki) z danymi uzyskanymi w procesie skanowania IP/port
	* wbudowany, konfigurowalny skaner sieci, ma pozwalać na monitorowanie aktywnych usług oraz zweryfikowanie czy znalezione skanerem komputery posiadają agenta
	* ma umożliwiać niezwłoczną i automatyczną identyfikację podłączonych urządzeń do sieci
	* ma posiadać możliwość generowania map sieci bazujących na danych zebranych ze skanowania sieci, według dowolnych filtrów użytkownika
	* ma umożliwiać przypisanie urządzenia do użytkownika, ewidencję napraw, kosztów zakupu i serwisu, przypominać o upływającym terminie gwarancji oraz pozwalać na dołączanie do urządzeń dokumentów z repozytorium wewnętrznego systemu
	* pozwalać na kopiowanie (duplikację) dowolnego urządzenia dowolną ilość razy.
	1. Inwentaryzacja oprogramowania. Zarządzanie licencjami
	* ma udostępniać szczegółowe informacje o systemie operacyjnym (wersja, edycja, service pack, poprawki, data instalacji)
	* ma ewidencjonować/inwentaryzować aplikacje na komputerach oraz umożliwiać wykonywanie audytów legalności, mieć możliwość zdefiniowania listy aplikacji zabronionych a także zdalnego odinstalowania oprogramowania
	* mieć możliwość odczytu identyfikatorów i kluczy produktowych dla systemu operacyjnego oraz dowolnego oprogramowania (tam gdzie jest technicznie możliwe)
	* ma wspierać 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
	* ma umożliwiać 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
	* ma zbierać informacje o uruchamianych aplikacjach (m.in. czas uruchomienia, nazwa zalogowanego użytkownika, nazwa aplikacji, szczegóły aktywności użytkownika)
2. Zdalna administracja komputerami
	* możliwość wykonywania poleceń powłoki, uruchamianie aplikacji, 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
	* skaner ma umożliwiać wykrywanie komputerów z technologią Intel VPro/AMT wraz z identyfikacją IP technologii Vpro, portu VPro, wersji Vpro, Serial Over LAN oraz zarządzać komputerami z technologią Intel vPro, w tym: zdalne włączać, wyłączać komputer, konfigurować BIOS, uruchamiać komputer przy użyciu obrazu ISO lub IMG znajdującego się w dowolnej lokalizacji, połączyć się komputerem w trybie graficznym (od VPro v.6)
	* za pomocą technologii Ultra VNC: ma umożliwiać zdalne podłączenie do wielu komputerów jednocześnie, przejąć ekran, klawiaturę i myszkę użytkownika, zdalnie uruchamiać aplikacje, zarządzać usługami i restartować komputer. Umożliwiać podłączenia do obecnie zalogowanego użytkownika oraz w trybie RDP (wylogowania użytkownika i przejęcia dostępu)
	* umożliwiać zdefiniowanie dowolnego własnego zadania jednorazowego bądź cyklicznego z poziomu konsoli administracyjnej z wykorzystaniem poleceń cmd, windows powershell. Każde wykonanie zadania musi mieć odzwierciedlenie w statusie wykonania zadania (poprawne, z błędem) oraz udostępniać informację zwrotną o przebiegu wykonania (godzina, data, status)
	* zezwalać na wykonywanie zapytań WMI oraz edycję rejestrów bez zdalnego połączenia do urządzenia
	* umożliwiać wykonanie poleceń z uprawnieniami dowolnego użytkownika (Uruchom jako)
	* ewidencjonować logowania użytkowników do danego komputera, również w przypadku podłączania się wielu użytkowników jednocześnie, tak w sieci lokalnej, jak i poza NAT
3. Zarządzanie magazynem IT
	* obsługiwać dowolną ilości magazynów w różnych lokalizacjach
	* obsługiwać dokumenty PZ, WZ, MM+, MM-, LI
	* ewidencjonować materiały w magazynach w oparciu o metodę FIFO (pierwsze przyszło pierwsze wyszło)
	* obsługiwać kody kreskowe dla materiałów w magazynach
	* informować o wartości materiałów w poszczególnych magazynach, aktualnych stanach magazynowych, dokumentach dotyczących danego materiału w dowolnym magazynie
4. Repozytorium
	* umożliwić 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
5. Kody kreskowe
	* umożliwić generowanie kodów kreskowych (jedno i dwuwymiarowych) 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
	* informować o błędzie generacji kodu, np. na skutek niewłaściwej długości wprowadzonego ciągu znaków w stosunku do danego standardu kodu
	* mieć możliwość masowego wydruk kodu / kodów
	* obsługa kodów kreskowych nie może wymagać instalacji czcionek
	* mieć możliwość współpracy z zewnętrznymi czytnikami kodów
6. Komunikacja za pomocą wiadomości
	* mieć możliwość tworzenie wiadomości tekstowych zgodne z HTML z możliwością eksportu / importu treści, celem automatycznego wysyłania do urządzeń, użytkowników lub dowolnych grup odbiorców,
	* wiadomości wysyłane jednorazowo lub cyklicznie powinny być zgodnie z definiowalnym harmonogramem
	* predefiniowane szkolenia: „Klasyfikowanie informacji stanowiących tajemnicę przedsiębiorstwa”, „Kontrola zabezpieczeń i obiegu informacji stanowiących tajemnicę przedsiębiorstwa”, „Postępowanie w przypadku naruszenia tajemnicy”, „Udostępnienie informacji stanowiących tajemnicę”
	* użytkownik otrzymujący wiadomość ma być powiadamiany wizualne i dźwiękowo
	* wiadomości o podwyższonym priorytecie – alerty – mają wyświetlać się na środku ekranu, z widoczną treścią wiadomości
	* dla wiadomości innych niż alerty użytkownik ma być możliwość natychmiastowego odczytania wiadomości lub jej odłożenia (na określony czas np. 10 minut, 1, 2 lub 4 godziny) celem późniejszego odczytania
	* ma mieć zabezpieczenie (np. synchronizowany z serwerem znacznik czasowy) odporne na zmiany czasu na lokalnym komputerze (użytkownika) a pozwalać na jednoznaczne ustalenie daty i godziny dostarczenia i odczytania wiadomości
	* ma być dostępna historia przesyłania wiadomości i odczytywania wiadomości przez użytkowników
	* ma mieć możliwość tworzenia cyklu wiadomości szkoleniowych, dla których można wygenerować elektroniczną listę uczestników przeszkolonych (z odczytanym całym szkoleniem)
7. Monitorowanie drukarek sieciowych i wydruków
	* system ma posiadać posiada możliwość ewidencji wszystkich generowanych wydruków niezależnie od miejsca ich generowania oraz typu drukarki (lokalna, sieciowa)
	* ewidencja wydruków ma obejmować: nazwę i wielkość dokumentu, datę i godzinę wydruku, nazwę użytkownika drukującego, IP i nazwę komputera z którego dokonano wydruku, format dokumentu, informację o jedno bądź dwustronnym wydruku, informację o wydruku mono/kolor
	* 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
8. Monitorowanie stron www
	* system ma posiadać możliwość monitorowania odwiedzanych stron www niezależnie od typu używanej przeglądarki internetowej
	* ewidencja otwieranych stron musi dotyczyć wielu jednocześnie otwartych zakładek, również, gdy otwierana jest strona z połączeniem szyfrowanym (https) i obejmuje co najmniej: nazwę i adres IP komputera, nazwę użytkownika, datę i godzinę, adres strony, łączny czas korzystania, czas aktywności, czas pasywności
	* system ma umożliwiać analizę treści rtc stron www oraz przypisanie im – w oparciu o treść – odpowiednich kategorii oraz kontrolowanie użytkowników pod kątem odwiedzanych stron
	* każda odwiedzona strona ma otrzymać 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
9. Worktime manager dla administratora
	* ma być wyposażony w zestaw statystycznych danych o pracy użytkownika i zdefiniowanych grup użytkowników
	* dane mają być prezentowane w formie interaktywnych widgetów oraz w formie danych analitycznych
	* prezentacja danych ma odbywać się poprzez wskazanie pracownika lub grupy pracowników oraz wybranie okresu danych źródłowych
	* ma umożliwiać wyświetlanie informacji o użytkowniku pobranych z Active Directory. Informacje mają się aktualizować zgodnie z harmonogramem połączenia z domeną
	* ma posiadać widgety 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
10. Monitorowanie dziennika zdarzeń
	* ma posiadać możliwość monitorowania dziennika zdarzeń wszystkich komputerów
	* ewidencja zdarzeń ma następować w oparciu o definiowalną kategorię zdarzenia: critical, error, warning, info, audit failure, audit success, debug oraz typ dziennika: aplikacja, bezpieczeństwo, system
	* ma pozwalać na zdefiniowanie ewidencji zdarzeń z komputerów na podstawie kategorii zdarzenia, musi zawierać: datę i godzinę zdarzenia, nazwę i adres IP komputera, typ zdarzenia, opis zdarzenia.
	* ma umożliwiać monitorowanie komunikatów Syslog.
11. Repozytorium CMDB – centralna baza systemu ma umożliwiać import i eksport danych zarówno poprzez API jak też za pomocą wbudowanego import/eksporta, na którą składają się:
	* Active Directory - lista serwerów LDAP, z których są importowane i aktualizowane dane o użytkownikach. System ma pozwalać na wprowadzanie dowolnej ilości serwerów dla różnych domen
	* kontenery dokumentów - grupy, do których można przypisywać zapisane w systemie dokumenty w celu sortowania
	* kategorie aplikacji - lista kategorii, do których przynależą wykorzystywane przez użytkowników aplikacje
	* budżet - zestawienie typów budżetów (kosztów) zaewidencjonowanych w systemie
	* komputery - lista zinwentaryzowanych komputerów, podzielonych wg typu autoryzacji. Widok rekordu zawiera szczegółowe dane dotyczące danego komputera
	* dokumenty - repozytorium dokumentów zapisanych w systemie
	* kategorie plików - lista typów plików kategoryzowanych przez system. Administrator ma możliwość zdefiniowania własnych grup, do których pliki będą przydzielane, według wpisanej maski
	* pliki - lista zinwentaryzowanych plików ze wszystkich komputerów
	* licencje - zestawienie licencji zapisanych w bazie systemu, które administrator może przypisywać do poszczególnych użytkowników
	* typy licencji - lista typów licencji
	* lokalizacje - lista zdefiniowanych lokalizacji, do których administrator może przypisać poszczególnych użytkowników. W odróżnieniu od struktury organizacyjnej dane nie są importowane z Active Directory
	* typy urządzeń - lista typów urządzeń
	* urządzenia - lista urządzeń podzielonych wg typu
	* producenci / Dostawcy - lista producentów i dostawców
	* pamięć masowa - zestawienie dysków twardych z komputerów
	* porty sieciowe - lista monitorowanych portów sieciowych
	* usługi sieciowe - lista monitorowanych usług sieciowych
	* udostępnione zasoby sieciowe - lista udostępnionych zasobów sieciowych
	* sieci - lista definiowalnych ręcznie sieci, do których administrator może ręcznie przypisywać komputery
	* systemy operacyjne - zestawienie unikalnych systemów operacyjnych
	* struktura org. - zestawienie struktur organizacyjnych zdefiniowanych bądź importowanych z Active Directory
	* kategorie procesów - lista kategorii, do których będą przypisywane procesy aplikacji uruchamianych przez użytkowników. Klasyfikacja procesów odbywa się za pomocą algorytmów sztucznej inteligencji
	* serwery - lista zinwentaryzowanych serwerów
	* usługi - zestawienie usług działających na komputerach
	* oprogramowanie - lista zinwentaryzowanego i monitorowanego oprogramowania
	* pamięć masowa USB - lista urządzeń pamięci masowej USB
	* administratorzy - lista administratorów i użytkowników systemu, z możliwością nadawania im indywidulanych uprawnień do wybranych funkcjonalności w systemie oraz danych użytkowników w ramach struktur organizacyjnych w zakresie przeglądania, edytowania, eksportowania i usuwania danych
	* użytkownicy / pracownicy - lista pracowników
	* kategorie WWW - lista kategorii stron WWW wykorzystywanych w procesie klasyfikacji stron internetowych. Klasyfikacja oparta o sztuczną inteligencję
	* serwisy WWW - lista monitorowanych serwisów WWW
12. Eksport danych
	* możliwość wyeksportowania wybranych lub wszystkich danych do formatu xls, csv, pdf, OpenOffice calc, html, mht, xml, jpeg, png, gif, bmp
	* generowanie raportu ma odbywać się po stronie serwera a nie klienta
	* generowanie raportów ma odbywać się bezpośrednio z każdego widoku w aplikacji z zastosowaniem bieżących filtrów
	* ma umożliwiać ustalenia harmonogramu umożliwiającego cykliczne wysyłanie raportów oraz zapisywanie ich w dowolnym miejscu
13. Powiadomienia
	* komunikaty w formie alertów w konsoli, wiadomości email wysyłanych na wybrane adresy oraz wiadomości SMS na wskazane numery telefonów
	* mieć możliwość tworzenia wielu komunikatów w oparciu o te same zdarzenia z określeniem innych grup obiorców lub parametrów
	* mieć możliwość edycji treści wysyłanych powiadomień oraz korzystania z danych umieszczonych w systemie w treści powiadomienia
14. Automatyzacja
	* mieć możliwość ustalania harmonogramu, zgodnie z którym uruchamiane są czynności konserwacyjne, naprawcze, porządkujące wraz z częstotliwością wykonywania danej czynności (godzina, dzień, tydzień, miesiąc)
	* mieć zdefiniowane czynności wykonywane są automatycznie
	* mieć dostępne 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)

18. Inne

* system ma umożliwiać zdalne, masowe szyfrowanie dysków wewnętrznych oraz zewnętrznych np. nośników USB za pośrednictwem API MS Bitlocker. Klucze do odszyfrowania mają być dostępne są z poziomu konsoli administracyjnej
* system ma umożliwiać zdalną instalacja– zdalne instalowanie plików **msi** oraz **exe** w trybie cichym