****

|  |
| --- |
| **ZAŁĄCZNIK NR 2** |

Pieczęć Wykonawcy

**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**

Wykonawca jest zobowiązany podać dokładny opis oferowanej dostawy w prawej kolumnie tabeli „szczegółowy zakres przedmiotu zamówienia oferowany przez Wykonawcę”. Nie dopuszcza się wpisywania określeń ogólnych typu „tak”, „spełnia”, „zgodne” itp. chyba, że wymagają tego zapisy opisu przedmiotu zamówienia.

Zamawiający odrzuci ofertę, której parametry nie będą spełniały wymagań opisu przedmiotu zamówienia.

**Dostawa licencji oprogramowania do monitorowania i nadzorowania sieci. Oprogramowanie to powinno posiadać następującą charakterystykę:**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Szczegółowy zakres przedmiotu zamówienia wymagany przez Zamawiającego** | **Szczegółowy zakres przedmiotu zamówienia oferowany przez Wykonawcę:** |
| 1 | Wymogi ogólne:   1. Oprogramowanie powinno posiadać budowę modułową i składać się z serwera zarządzającego, zdalnych konsoli oraz Agentów. Komunikacja pomiędzy Serwerem a Agentami i Konsolami powinna być nawiązywana przy użyciu szyfrowanego protokołu (TLS lub SSL). Moduły muszą umożliwiać kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych oraz pomoc w formie interaktywnego połączenia sieciowego z obsługiwanym użytkownikiem. 2. Dane, które dotyczą działań pracownika na komputerze, a więc: historia aktywności, polityka korzystania z Internetu oraz aplikacji, dostęp do zewnętrznych nośników danych itp., powinny być odseparowane od danych stricte technicznych tj. informacji o stacji roboczej. Powinny one być również grupowane w osobnym, dedykowanym oknie, aby możliwe było, zgodne z RODO, usuwanie danych wybranego użytkownika bez konieczności usunięcia informacji o stacji roboczej. 3. Dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, powinien być objęty kontrolą na poziomie wybranych Administratorów – w programie powinna być możliwość nadawania kontom administracyjnym różnych poziomów dostępu oraz uprawnień zarówno do grup urządzeń, jak i użytkowników. | |
| 2 | Program powinien być dostępny w języku polskim i angielskim wraz z podręcznikiem użytkownika w formie strony internetowej. Należy podać link do strony zawierającej podręcznik użytkownika. |  |
| 3 | Serwer bazy danych, na której działają wszystkie oferowane moduły powinien umożliwiać pracę dla nieograniczonej ilości użytkowników oraz nielimitowanej pojemności bazy. Należy wskazać nazwę bazy danych dla oferowanego rozwiązania uwzględniając powyższe wymogi. |  |
| 4 | Wymogi dotyczące poszczególnych funkcjonalności |  |
|  | 1. MONITOROWANIE INFRASTRUKTURY (BEZAGENTOWO) 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). * wizualizacji stanu urządzeń w postaci ikon urządzeń na mapach sieci. * wizualizacji połączeń pomiędzy urządzeniami a przełącznikami i informacji, do którego portu przełącznika podłączone jest dane urządzenie. * 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 powinien monitorować zarówno serwis odbierający, jak i wysyłający pocztę,   + program powinien mieć 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 powinien posiadać możliwość wykonywania operacji testowych,   + program powinien wysyłać powiadomienia, jeśli serwer pocztowy nie działa. * monitorowania serwerów WWW i adresów URL. * obsługi szyfrowania SSL/TLS w powiadomieniach e-mail. * obsługi urządzeń SNMP wspierających SNMP v1/2/3 (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.) za pomocą nazw. * szyfrowania AES, DES i 3DES dla protokołu SNMPv3, * obsługi komunikatów syslog i pułapek SNMP, * monitoringu routerów i przełączników wg:   + zmian stanu interfejsów sieciowych,   + ruchu sieciowego,   + podłączonych stacji roboczych,   + ruchu generowanego przez podłączone stacje robocze * Program powinien posiadać własny, wbudowany kompilator plików MIB. * serwisów Windows: monitor serwisów Windows powinien informować gdy serwis przestanie działać oraz pozwalać na jego uruchomienie/zatrzymanie/zrestartowanie. * wydajności systemów Windows:   + obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy.   Program powinien posiadać Inteligentne Mapy i Oddziały/Jednostki organizacyjne, które służą do lepszego zarządzania logiczną strukturą urządzeń w przedsiębiorstwie (Oddziały/Jednostki organizacyjne) oraz tworzą dynamiczne mapy wg własnych filtrów (Mapy Inteligentne). |  |
|  | 1. INWENTARYZACJA - program powinien 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.   Moduł inwentaryzacji sprzętu powinien umożliwiać prowadzenie bazy ewidencji majątku IT w zakresie:   * przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji, * definiowania własnych typów (elementów wyposażenia), ich atrybutów oraz wartości – dla danego urządzenia lub oprogramowania istnieje możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer i skan faktury zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu i skan gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, inny dowolny załącznik (np. plik .DOCX, .XLSX, .PDF), skan dowolnego dokumentu, czy też własny komentarz; dodatkowo powinien istnieć możliwość importu danych z zewnętrznego źródła (.CSV), * generowania zestawienia wszystkich środków trwałych, w tym urządzeń i zainstalowanego na nich oprogramowania, * archiwizacji i porównywania audytów środków trwałych, * tworzenia kodów kreskowych w Środkach Trwałych, * drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla środków trwałych, które posiadają numer inwentarzowy, * inwentaryzacji sprzętu posiadającego kody kreskowe za pomocą aplikacji mobilnej na system Android, * inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline).   Dostępne muszą być Agenty inwentaryzacji na systemy Android, macOS oraz Linux.  Inwentaryzacja oprogramowania powinna zapewniać funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez:   * Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP. * Zarządzanie posiadanymi licencjami. * Łatwy 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 jednostka organizacyjna |  |
|  | 1. OBSŁUGA UŻYTKOWNIKÓW- program powinien 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 z 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), * 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 powinien mieć możliwość monitorowania kosztów wydruków, * Nagłówków przesyłanej poczty e-mail.   Program ponadto powinien posiadać możliwość:   * blokowania 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 sub-domen (np. \*.domena.pl), * 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. Możliwość generowania raportów dla użytkowników Active Directory niezależnie od tego, na jakich komputerach pracowali w danym czasie.   Program powinien posiadać Grupy użytkowników oraz Grupy Inteligentne, które będą służyć do lepszego zarządzania użytkownikami, polityką monitorowania oraz blokowania aplikacji i stron internetowych. |  |
|  | 1. ZDALNA POMOC UŻYTKOWNIKOM - w ramach kontroli stacji użytkownika powinien być dostępny podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli. Podczas dostępu zdalnego, zarówno użytkownik jak i administrator muszą widzieć ten sam ekran. Administrator w trakcie zdalnego dostępu będzie mieć możliwość zablokowania działania myszy oraz klawiatury dla użytkownika.   W niniejszym module musi znaleźć się baza zgłoszeń umożliwiająca użytkownikom zgłaszanie problemów technicznych, które z kolei będą przetwarzane i przyporządkowywane odpowiednim administratorom, otrzymującym automatycznie powiadomienie o przypisanym im problemie. Użytkownik powinien mieć możliwość monitorowania procesu rozwiązywania zgłoszonych problemów i ich aktualnych statusów, jak również możliwość wymiany informacji z administratorem poprzez komentarze, które będą wpisywane i widoczne dla obu stron. Moduł ten powinien zawierać również komunikator (czat), który umożliwia przesyłanie wiadomości pomiędzy zalogowanymi użytkownikami i administratorami (wraz z wyszukiwarką wiadomości) oraz bazę wiedzy pomagającą użytkownikom samodzielnie rozwiązywać najprostsze, powtarzające się problemy.  Moduł pomocy zdalnej będzie umożliwiać również:   * zarządzać zdalnie procesami Windows z poziomu okna informacji o urządzeniu, * tworzyć i konfigurować pola niestandardowych, powiązanych z wybraną kategorią zgłoszeń serwisowych w tym pól typu: czasowych, wielokrotnego i jednokrotnego wyboru, * automatycznie czyścić historię rozmów w czacie, * dwukierunkowo zarządzać plikami użytkownika w postaci managera plików dostępnego w zdalnym dostępie, * pobierać listy użytkowników z Active Directory, * przypisywać pracowników helpdesk do kategorii zgłoszeń, * procesować zgłoszenia użytkowników z wiadomości e-mail, * wykonywanie operacji na wielu zgłoszeniach równocześnie, * dołączanie załączników do zgłoszeń, * wykonywanie zrzutów ekranowych (podgląd pulpitu), * realizować dystrybucję oprogramowania przez Agenty, * realizowanie dystrybucji oraz uruchamiania plików za pomocą Agentów (w tym plików MSI), * wykonanie zadania dystrybucji plików. W przypadku gdy komputer jest wyłączony w trakcie zlecania operacji powinien następować kolejkowanie zadania dystrybucji pliku, * skonfigurować automatyzację procesowania zgłoszeń, * planować nieobecności pracowników helpdesk, * obsługę umów o gwarantowanym poziomie świadczenia usług (SLA), * generowanie raportów obsługi helpdesk, * zdalne wykonywanie poleceń poprzez Agenty (np. utworzenie / edycja konta lokalnego użytkownika systemu). |  |
|  | 1. OCHRONA DANYCH – powinna odbywać się poprzez blokowanie następujących urządzeń:  * Blokowanie urządzeń i nośników danych. Program powinien mieć możliwość zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny. * Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek. * Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA. * Blokownie powinno dotyczyć tylko urządzeń służących do przenoszenia danych - inne urządzenia (drukarka, klawiatura, mysz itp.) mogą być podłączane.   Zarządzanie prawami dostępu do urządzeń powinien odbywać się poprzez:   * Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików. * Autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive’ów, dysków itp. - urządzenia prywatne są blokowane. * Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników. * Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci.   Audyt operacji na urządzeniach przenośnych będzie odbywać się poprzez:   * Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych. * Podłączenie/odłączenie urządzenia przenośnego.   Integracja z Active Directory powinna odbywać się poprzez zarządzanie prawami dostępu przypisanymi do użytkowników grup domenowych. Przydzielanie uprawnień będzie powinno być możliwe również do kont użytkowników lokalnych.  Ochrona przed usunięciem - program powinien być zabezpieczony hasłem przed ingerencją użytkownika w jego działanie i próbą usunięcia, nawet jeśli użytkownik ma prawa administratora. |  |
| 5 | SZKOLENIE:  W ramach dostawy Wykonawca przeprowadzi szkolenie dla osób wskazanych przez Zamawiającego obejmujące min. 3 dni szkoleniowe. Szkolenie odbędzie się w siedzibie Zamawiającego. W ramach szkolenia Wykonawca zainstaluje i skonfiguruje konsolę centralną. Szkolenie powinno być przeprowadzone w całości przez osobę posiadającą certyfikację producenta oprogramowania - w ofercie należy wskazać dane osoby prowadzącej szkolenie. |  |

…………………dnia ……………… …………………………………………………

pieczęć i podpis osoby uprawnionej do składania oświadczeń woli

w imieniu Wykonawcy