## Zadanie 2: Dostarczenie licencji na oprogramowanie monitorująco-inwentaryzacyjne

Proponowane oprogramowanie: ……………………………………………..

| **L.p.** | **Parametr** | **Wymagane minimalne wartości parametru** | **Proponowane wartości parametru** |
| --- | --- | --- | --- |
| OMI1 | **Monitorowanie infrastruktury** | Wykrywanie urządzeń w sieci poprzez skanowanie ping |  |
| OMI2 | Wizualizacja stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci |  |
| OMI3 | Wizualizacja połączeń pomiędzy urządzeniami a przełącznikami i informacji, do którego portu przełącznika podłączone jest dane urządzenie |  |
| OMI4 | Monitorowanie serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program monitoruje czas ich odpowiedzi i procent utraconych pakietów |  |
| OMI5 | Monitorowanie serwerów pocztowych:   * program monitoruje zarówno serwis odbierający, jak i wysyłający pocztę, * 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. |  |
| OMI6 | Monitorowanie serwerów WWW i adresów URL |  |
| OMI7 | Obsługa szyfrowania SSL/TLS w powiadomieniach e-mail |  |
| OMI8 | Obsługa urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją |  |
| OMI9 | Obsługa komunikatów syslog i pułapek SNMP |  |
| OMI10 | Monitoring routerów i przełączników wg:   * zmian stanu interfejsów sieciowych, * ruchu sieciowego, * podłączonych stacji roboczych, * ruchu generowanego przez podłączone do portów stacje robocze. |  |
| OMI11 | Monitorowanie serwisów Windows: monitor serwisów Windows alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie/zatrzymanie/zrestartowanie. |  |
| OMI12 | Monitorowanie wydajności systemów Windows, np. obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy. |  |
| OMI13 | **Parametry inwentaryzacyjne i audytowe** | Program powinien automatycznie gromadzić informacje o sprzęcie i oprogramowaniu na stacjach roboczych, oferować zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade |  |
| OMI14 | Tak |  |
| OMI15 | patchcord UTP, kat. 6, 1.0m, niebieski – 50 szt. |  |
| OMI10 | Monitoring routerów i przełączników wg:   * zmian stanu interfejsów sieciowych, * ruchu sieciowego, * podłączonych stacji roboczych, * ruchu generowanego przez podłączone do portów stacje robocze. |  |
| OMI11 | Monitorowanie serwisów Windows: monitor serwisów Windows alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie/zatrzymanie/zrestartowanie. |  |
| OMI12 | Monitorowanie wydajności systemów Windows, np. obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy. |  |
| OMI13 | **Parametry inwentaryzacyjne i audytowe** | Program powinien automatycznie gromadzić informacje o sprzęcie i oprogramowaniu na stacjach roboczych, oferować zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade. |  |
| OMI14 | Informowanie o zainstalowanych aplikacjach oraz aktualizacjach Windows co bezpośrednio umożliwia audytowanie i weryfikację użytkowania licencji w organizacji. |  |
| OMI15 | Zbieranie informacji w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd. |  |
| OMI16 | Wysyłanie powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera. |  |
| OMI17 | Odczytywanie numeru seryjnego (klucze licencyjne). |  |
| OMI18 | Automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych. |  |
| OMI19 | Przegląd informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp. |  |
| OMI20 | Przechowywanie wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji. |  |
| OMI21 | Definiowanie własnych typów (elementów wyposażenia), ich atrybutów oraz wartości – dla danego urządzenia lub oprogramowania powinna istnieć 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, nazwa firmy serwisującej, inny dowolny załącznik (np. plik .DOCX, .XLSX, .PDF), skan dowolnego dokumentu, czy też własny komentarz. |  |
| OMI22 | Import danych z zewnętrznego źródła (.CSV). |  |
| OMI23 | Generowanie zestawienia wszystkich środków trwałych, w tym urządzeń i zainstalowanego na nich oprogramowania. |  |
| OMI24 |  | Archiwizacja i porównywanie audytów środków trwałych |  |
| OMI25 | Tworzenie kodów kreskowych w Środkach Trwałych. |  |
| OMI26 | Drukowanie kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla środków trwałych, które posiadają numer inwentarzowy. |  |
| OMI27 | Inwentaryzacja sprzętu posiadającego kody kreskowe za pomocą aplikacji mobilnej na system Android |  |
| OMI28 | Inwentaryzacja stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline) |  |
| OMI29 | Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowania archiwów ZIP. |  |
| OMI30 | Audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji – w każdej chwili istnieje możliwość wykonania aktualnych raportów audytowych. |  |
| OMI31 | Zarządzania posiadanymi licencjami: raport zgodności licencji. |  |
| OMI32 | Możliwości przypisania do programów numerów seryjnych, wartości itp. |  |
| OMI33 | W zakresie obsługi użytkowników program powinien umożliwiać monitorowanie aktywności użytkowników pracujących na komputerach z systemem Windows poprzez monitorowanie faktycznego czasu aktywności, procesów(całkowity czas działania oraz czas aktywności użytkownika), 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, listy odwiedzanych stron WWW, transferu sieciowego użytkowników i wydruków (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany) |  |
| OMI34 | 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 sub-domen |  |
| OMI35 | Blokowanie ruchu na wskazanych portach TCP/IP, |  |
| OMI36 | Blokowanie pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem |  |
| OMI37 | 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 ilość stron w ciągu dnia |  |
| OMI38 | Generowanie raportów dla użytkowników Active Directory niezależnie od tego, na jakich komputerach pracowali w danym czasie. |  |
| OMI39 | Mechanizm blokowania uruchamiania aplikacji. |  |
| OMI40 | **Moduł pomocy** | Moduł pomocy użytkownikom oraz umożliwiać podgląd pulpitu użytkownika i przejęcia nad nim kontroli. |  |
| OMI41 | Administrator w trakcie zdalnego dostępu powinien mieć możliwość zablokowania działania myszy oraz klawiatury dla użytkownika. |  |
| OMI42 | W module powinna znajdować się baza zgłoszeń umożliwiająca użytkownikom zgłaszanie problemów technicznych, które z kolei są przetwarzane i przyporządkowywane odpowiednim administratorom, otrzymującym automatycznie powiadomienie o przypisanym im problemie. |  |
| OMI43 | Umożliwienie użytkownikom 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. |  |
| OMI44 | Powinien zawierać również komunikator (czat), który umożliwia przesyłanie wiadomości pomiędzy zalogowanymi użytkownikami i administratorami (wraz z wyszukiwarką wiadomości). |  |
| OMI45 | Powinien zawierać bazę wiedzy pomagającą użytkownikom samodzielnie rozwiązywać najprostsze, powtarzające się problemy. |  |
| OMI46 | Pobieranie listy użytkowników z Active Directory. |  |
| OMI47 | Przypisywanie pracowników helpdesk do kategorii zgłoszeń. |  |
| OMI48 | Procesowanie zgłoszeń użytkowników z wiadomości e-mail. |  |
| OMI49 | Wykonywanie operacji na wielu zgłoszeniach równocześnie. |  |
| OMI50 | Dołączanie załączników do zgłoszeń. |  |
| OMI51 | Zrzuty ekranowe (podgląd pulpitu). |  |
| OMI52 | Dystrybucję oprogramowania przez Agenty. |  |
| OMI53 | Dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików MSI). |  |
| OMI54 | Zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecania operacji następuje kolejkowanie zadania dystrybucji pliku. |  |
| OMI55 | Możliwość skonfigurowania automatyzacji procesowania zgłoszeń. |  |
| OMI56 | Planowanie nieobecności pracowników helpdesk. |  |
| OMI57 | Obsługę umów o gwarantowanym poziomie świadczenia usług (SLA). |  |
| OMI58 | Generowanie raportów obsługi helpdesk. |  |
| OMI59 | Zdalne wykonywanie poleceń poprzez Agenty (np. utworzenie / edycja konta lokalnego użytkownika systemu). |  |
| OMI60 | **Ochrona danych wrażliwych** | Blokowanie urządzeń i nośników danych. Program powinien posiadać 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. |  |
| OMI61 | Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek. |  |
| OMI62 | Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA.  Zarządzanie prawami dostępu do urządzeń. |  |
| OMI63 |  | Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików. |  |
| OMI64 | Autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive’ów, dysków itp. – urządzenia prywatne mają być blokowane. |  |
| OMI65 | Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników. |  |
| OMI66 | Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci. |  |
| OMI67 | Audyt operacji na urządzeniach przenośnych |  |
| OMI68 | Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych. |  |
| OMI69 | Podłączenie/odłączenie urządzenia przenośnego. |  |
| OMI70 | **Ochrona przed usunięciem** | Program powinien być zabezpieczony hasłem przed ingerencją użytkownika w jego działanie i próbą usunięcia, nawet jeśli użytkownik ma prawa administratora. |  |
| OMI71 | **Integracja z Active Directory** | Zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych. Przydzielanie uprawnień również do kont użytkowników lokalnych. |  |

.........................................................................

(podpis upełnomocnionego przedstawiciela Wykonawcy)