

OPIS PRZEDMIOTU ZAMÓWIENIA

Oprogramowanie do zarządzania infrastrukturą IT – licencja bezterminowa

1	Moduły systemu:	Program musi umożliwiać pełny monitoring sieci, pozwalać na ewidencję i zarządzanie zasobami IT, na zarządzanie użytkownikami, posiadać system helpdesku, umożliwiający zdalną pomoc techniczną, oraz posiadać funkcje kontroli dostępu do danych. Program obsługiwać będzie 1 serwer +30 hostów
2	Monitoring sieci:	<p>wskazywanie aktualnych danych o wydajności serwera i łącza internetowego</p> <p>obsługa szyfrowania AES, DES i 3DES dla protokołu SNMPv3</p> <p>skanowanie sieci, wykrywanie urządzeń i serwisów TCP/IP</p> <p>możliwość tworzenia interaktywnych map sieci, map użytkownika, map inteligentnych</p> <p>możliwość zarządzania uprawnieniami, wgląd do dzienników dostępu</p> <p>monitoring poprzez serwisy TCP/IP: poprawność i czas odpowiedzi, statystyka ilości odebranych/utraconych pakietów (PING, SMB, HTTP, POP3, SNMP, IMAP, SQL itp.)</p> <p>musi posiadać liczniki WMI: obciążenie procesora, zajętość pamięci, zajętość dysków, transfer sieciowy itp.</p> <p>umożliwienie współpracy z systemem Windows poprzez zmianę stanu usług (uruchomienie, zatrzymanie, restart), wpisy dziennika zdarzeń</p> <p>musi posiadać liczniki SNMP v1/2/3 (np. transfer sieciowy, temperatura, wilgotność, napięcie zasilania, poziom tonera i inne)</p> <p>kompilator plików MIB</p> <p>obsługa pułapek SNMP</p> <p>mapowanie portów</p> <p>obsługa komunikatów syslog</p> <p>alarmy zdarzenie – akcja</p> <p>powiadomienia (pulpitowe, e-mail, SMS) oraz akcje korekcyjne (uruchomienie programu, restart komputera itp.)</p> <p>raporty (dla urządzenia, oddziału, wybranej mapy lub całej sieci)</p>
3	Ewidencja i zarządzanie zasobami IT	<p>zarządzanie wszelkimi zasobami, za które odpowiada dział IT</p> <p>szczegółowe informacje i ewidencja czynności wykonywanych na zasobach w trakcie całego cyklu życia, możliwość definiowania statusów i pól oraz generowanie protokołu przekazania sprzętu</p> <p>widok zasobów, aplikacji, dokumentów, licencji dla poszczególnego użytkownika lub osobny widok według zasobów przypisanych do urządzeń</p> <p>jednoczesne przypisywanie dokumentu do wielu zasobów</p> <p>system zarządzania aplikacjami i licencjami, identyfikacja realnego zużycia licencji</p> <p>rozliczanie dowolnego typu licencji w tym modelowanie licencji chmurowych</p> <p>rozliczanie licencji według użytkownika, urządzenia, numeru seryjnego lub na podstawie wersji zainstalowanej aplikacji</p> <p>audyt inwentaryzacji sprzętu i oprogramowania</p> <p>wgląd w licencje przypisane do użytkownika pracującego na wielu urządzeniach</p> <p>zdalny dostęp do menedżera plików z możliwością usuwania plików użytkownika</p> <p>informacje o wpisach rejestrowych, plikach i archiwach .zip na stacji roboczej</p> <p>szczegółowe informacje o konfiguracji sprzętowej konkretnej stacji roboczej</p>



Sfinansowano w ramach reakcji Unii na pandemię COVID-19

		zarządzanie instalacjami/deinstalacjami oprogramowania w oparciu o menedżera pakietów MSI
		alarmy: instalacja oprogramowania, zmiana w zasobach sprzętowych
		lista kluczy oprogramowania Microsoft
		aplikacja dla systemu Android umożliwiająca spis z natury na bazie kodów kreskowych, kodów QR
		możliwość archiwizacji i porównywania audytów
		monitorowanie harmonogramu zadań Windows
4	Zarządzanie użytkownikami	pełne zarządzanie użytkownikami, bazujące na grupach i politykach bezpieczeństwa
		gromadzenie i przyporządkowywanie danych do konkretnego użytkownika, dzięki czemu wszystkie dostępy, uprawnienia, polityka aplikacji i stron oraz polityka monitorowania będą podążały automatycznie za użytkownikiem niezależnie od komputera, na którym pracuje
		możliwość blokowania niebezpiecznych domen WWW przed przypadkowym wejściem i pobraniem złośliwego oprogramowania
		blokowanie uruchamianych aplikacji
		monitorowanie wiadomości e-mail (nagłówki) – antyphishing
		użytkowane aplikacje (aktywnie i nieaktywnie)
		odwiedzane strony WWW (tytuły i adresy stron, liczba i czas wizyt)
		audyty wydruków (drukarka, użytkownik, komputer), koszty wydruków
		użycie łącza: generowany przez użytkowników ruch sieciowy
		statyczny zdalny podgląd pulpitu użytkownika (bez dostępu)
		zrzuty ekranowe (historia pracy użytkownika ekran po ekranie)
		blokowanie uruchamiania procesów na podstawie lokalizacji pliku .EXE
		zarządzanie regułami blokowania aplikacji i stron WWW (tworzenie, grupowanie, powielanie między grupami użytkowników)
5	Helpdesk	tworzenie zgłoszeń serwisowych i zarządzanie nimi
		komentarze, zrzuty ekranowe i załączniki w zgłoszeniach
		konfigurowanie pól niestandardowych, powiązanych w wybraną kategorię zgłoszenia
		automatyzacje bazujące na założeniu: warunek » akcja
		system raportów
		powiadomienia i widok zgłoszenia odświeżany w czasie rzeczywistym
		baza zgłoszeń z rozbudowaną wyszukiwarką
		wewnętrzny komunikator (czat) z możliwością przydzielania uprawnień oraz przesyłania plików i tworzenia rozmów grupowych
		komunikaty wysyłane do użytkowników/komputerów z możliwym/obowiązkowym potwierdzeniem odczytu
		zdalny dostęp do komputerów z możliwością blokady myszy/klawiatury
		dwukierunkowa wymiana plików
		zarządzanie procesami Windows z poziomu okna informacji o urządzeniu
		zadania dystrybucji oraz uruchamiania plików (zdalna instalacja oprogramowania)
		procesowanie zgłoszeń z wiadomości e-mail
		integracja bazy użytkowników z Active Directory
		zarządzanie kontami lokalnych użytkowników Windows (tworzenie, usuwanie, edycja, reset hasła, eskalacja/deeskalacja uprawnień oraz włączanie/wyłączanie kont).



6	Kontrola dostępu do danych	automatyczne nadawanie użytkownikowi domyślnej polityki monitorowania i bezpieczeństwa
		możliwość usuwania nieistniejących/zutylizowanych nośników danych (np. USB)
		alarmy o podłączonym urządzeniu obcym (nieposiadającym atrybutu „nośnik zaufany”)
		integracja z Windows Bitlocker: odczyt stanu modułu TPM oraz zaszyfrowania woluminów
		zdefiniowanie polityki przenoszenia danych firmowych przez pracowników wraz z odpowiednimi uprawnieniami
		informacje o urządzeniach podłączonych do danego komputera
		lista wszystkich urządzeń podłączonych do komputerów w sieci
		audyt (historia) połączeń i operacji na urządzeniach przenośnych oraz na udziałach sieciowych
		zarządzanie prawami dostępu (zapis, uruchomienie, odczyt) dla urządzeń, komputerów i użytkowników
		centralna konfiguracja: ustawienie reguł dla całej sieci, dla wybranych map sieci oraz dla grup i użytkowników Active Directory
		integracja bazy użytkowników i grup z Active Directory
		alarmy: podłączono/odłączono urządzenie mobilne, operacja na plikach na urządzeniu mobilnym

WÓJT
Wiesław Kulesza

