



URZĄD MIEJSKI W KOWARACH

URZĄD MIEJSKI * UL. 1 MAJA 1A * 58-530 KOWARY * TEL. +48 75 643 92 22 * TEL. +48 75 718 24 16
FAX: +48 75 761 31 73 * E-MAIL: bok@kowary.pl * www.kowary.pl

WOK.271.1.2021

Kowary, 19.05.2021 r.

ZAPROSZENIE DO SKŁADANIA OFERT

Na podstawie art. 2 ust.1 pkt. 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. Z 2019r., poz. 2019 z późn. zm.), Urząd Miejski w Kowarach zaprasza do składania ofert na dostawę licencji oprogramowania do monitorowania i nadzorowania sieci.

Oprogramowanie to powinno posiadać następującą charakterystykę:

Lp.	Szczegółowy zakres przedmiotu zamówienia wymagany przez Zamawiającego
1	<p>Wymogi ogólne:</p> <p>a 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 obsługiwany użytkownikiem. Instalacja Serwera oraz Konsol zarządzających wymaga 64-bitowego systemu operacyjnego Windows.</p> <p>b 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, zgodnie z RODO, usuwanie danych wybranego użytkownika bez konieczności usunięcia informacji o stacji roboczej.</p> <p>c 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. Działania administratorów powinny być logowane oznacza to, że program musi posiadać dziennik z listą czynności wykonanych przez administratorów, które zmodyfikowały obiekty znajdujące się w systemie.</p> <p>d Oprogramowanie powinno posiadać obszar funkcjonalny w formie platformy WWW, który pozwala na tworzenie wielu interaktywnych paneli informacyjnych (dashboardów) z responsywnymi widgetami. Na każdym z dashboardów widgety powinny móc być rozłożone na siatce o rozmiarze ustalonym przez administratora. Obszar pozwala na wyświetlanie danych z całego systemu.</p> <p>e Oprogramowanie powinno umożliwiać zarządzanie przynajmniej 80 stacjami roboczymi</p>
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 funkcji

	<p>a MONITOROWANIE INFRASTRUKTURY (BEZAGENTOWO) musi obejmować serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle w zakresie:</p> <ul style="list-style-type: none"> • 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. • wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z wykorzystaniem jako tła zaimportowanych obrazków • serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program monitoruje czas ich odpowiedzi i procent utraconych pakietów. • zablokowania mapy urządzeń przed przypadkową edycją. • serwerów pocztowych: <ul style="list-style-type: none"> ○ 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, pułapek SNMP i ewidencjonowanie odebranych z nich danych, • monitoringu routerów i przełączników wg: <ul style="list-style-type: none"> ○ zmian stanu interfejsów sieciowych, ○ ruchu sieciowego, ○ podłączonych stacji roboczych, ○ ruchu generowanego przez podłączone stacje robocze • Program powinien posiadać własny, wbudowany kompilator plików MIB umożliwiający dodawanie definicji dla modułów SNMP • serwisów Windows: monitor serwisów Windows powinien informować gdy serwis przestanie działać oraz pozwalać na jego uruchomienie/zatrzymanie/zrestartowanie. • wydajności systemów Windows: <ul style="list-style-type: none"> ○ obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy. <p>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).</p>
	<p>b INWENTARYZACJA - program powinien automatycznie gromadzić informacje o sprzęcie i oprogramowaniu na stacjach roboczych oraz:</p> <ul style="list-style-type: none"> • Prezentować szczegóły dotyczące sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp. • Obejmować m.in.: zestawienie posiadanych konfiguracji sprzętowych, wolne miejsca 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 użytkownika 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 jakiegokolwiek 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, kontaktach lokalnych użytkowników, harmonogramie zadań itp.
- Umożliwia utworzenie listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI) znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem metadanych plików użytkownika: obrazów (wymiary obrazka), video (długość filmu), audio (długość nagrania), archiwów (liczba plików w środku, rozmiar po wypakowaniu). 10.
- Umożliwia wymianę plików do i ze stacją roboczą poprzez funkcję Menedżera plików. Działania administratorów wykonywane w tej funkcji są logowane.

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).
- określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów,
- określenia atrybutów dodatkowych tylko dla wybranych typów zasobów
- definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie,

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.
- Informacje o aplikacjach używanych w organizacji.
- Tworzenie własnych wzorców aplikacji.
- Tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp.
- Informacje o komputerach, na których aplikacja została wykryta.
- Zarządzanie posiadanymi licencjami.
- Wskazywanie osób odpowiedzialnych za licencję.
- Wskazanie użytkowników licencji.
- Tworzenia powiązań między licencjami a dokumentami w relacji 1:N. 10.
- Rozbudowane zarządzanie licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie

	<p>wg różnych wersji aplikacji na jednym urządzeniu.</p> <ul style="list-style-type: none"> • 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. <p>Okna audytowe powinny posiadać możliwość filtrowania elementów per jednostka organizacyjna</p>
	<p>c OBSŁUGA UŻYTKOWNIKÓW- program powinien umożliwiać monitorowanie aktywności użytkowników pracujących na komputerach z systemem Windows poprzez monitorowanie:</p> <ul style="list-style-type: none"> • 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 użytkownika 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. <p>Program ponadto powinien posiadać możliwość:</p> <ul style="list-style-type: none"> • 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. • definiowania godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone. <p>Program powinien posiadać Grupy użytkowników oraz Grupy Inteligentne, które będą służyć do lepszego zarządzania użytkownikami, polityką monitorowania oraz blokowania aplikacji i stron internetowych.</p>
d	<p>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.</p>

Moduł pomocy zdalnej będzie umożliwiać również:

- pobieranie listy użytkowników z Active Directory,
- zarządzanie dostępem pracowników HelpDesku do zgłoszeń poprzez rozbudowany system zarządzania regułami widoczności zgłoszeń,
- zarządzanie dostępem do czatu w 3 poziomach uprawnień: pełny dostęp, brak dostępu lub dostęp ograniczony wyłącznie do pomocy technicznej,
- tworzenie własnego drzewa kategorii zgłoszeń wraz z możliwością grupowania kategorii w folderach (do 4 poziomów kategorii),
- automatyczne przypisywanie konkretnych pracowników helpdesk do zgłoszeń w określonych kategoriach lub pochodzących od określonych grup użytkowników,
- procesowanie zgłoszeń użytkowników z wiadomości e-mail,
- tworzenie formularzy z niestandardowymi polami opisowymi, dedykowanymi do wybranych kategorii zgłoszeń,
- wykonywanie operacji na wielu zgłoszeniach równocześnie,
- dołączanie załączników do zgłoszeń,
- rozbudowane wyszukiwanie zgłoszeń i artykułów w bazie wiedzy,
- szybki dostęp do ostatnich zgłoszeń, artykułów bazy wiedzy i załączników,
- wprowadzenie komentarza oraz informacji o czasie poświęconym na rozwiązanie w kreatorze wyświetlanym przy zamykaniu zgłoszenia,
- zrzuty ekranowe (podgląd pulpitu),
- dystrybucję oprogramowania przez Agenty,
- dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików MSI),
- zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecenia operacji następuje kolejowanie zadania dystrybucji pliku,
- zarządzania procesami systemu Windows (w zakresie: zakończ proces, zakończ drzewo procesu, uruchom nowy proces w sesji użytkownika wraz z parametrami),
- wymiany plików do i ze stacji roboczej poprzez funkcję Menedżera plików

e 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 dyskiety.
- 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.

System umożliwia monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika.

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	Program powinien być objęty gwarancją producenta w okresie min 12 miesięcy od czasu wdrożenia

Oferty proszę składać drogą e-mailową na adres informatyk@kowary.pl.

W ofercie proszę o podanie producenta oraz nazwę oprogramowania oraz opis oferowanych modułów zgodnych z podanymi wymaganiami, a także o podanie sumarycznej ceny brutto zawierającej ewentualne koszty dostarczenia.

Termin składania ofert: do dnia **31 maja 2021 r.** Kryterium wyboru oferty będzie najniższa cena.

Termin realizacji zamówienia to 7 dni od momentu otrzymania zamówienia przez wykonawcę.

Urząd Miejski w Kowarach zastrzega sobie prawo do rezygnacji z zamówienia w przypadku, gdy oferty spełniające wymogi przekroczą szacowany koszt zamówienia.

Postępowanie prowadzi:

Maciej Janas

Urząd Miejski w Kowarach, pokój nr 28

tel. (75) 64 56 117