Nr sprawy: RP.271.1.2.2022 **Załącznik nr 1**

Zakup oprogramowania sieciowego dla Urzędu Miasta i Gminy Mrocza w ramach realizacji projektu „Cyfrowa Gmina"

OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiotem zamówienia jest zakup oprogramowania sieciowego dla Urzędu Miasta i Gminy Mrocza w ramach realizacji projektu „Cyfrowa Gmina".

2. Określone parametry należy traktować jako minimalne.

3. Wskazane w opisie przedmiotu zamówienia znaki towarowe, patenty lub pochodzenie mają charakter pomocniczy dla określenia parametrów przedmiotu zamówienia. Zamawiający dopuszcza możliwość zastosowania rozwiązań równoważnych o parametrach technicznoużytkowych nie gorszych niż podane w opisie przedmiotu zamówienia. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego jest zobowiązany wykazać, że oferowana przez niego dostawa spełnia wymagania określone przez Zamawiającego.

4. Zamawiający wymaga by oprogramowanie było fabrycznie nowe.

5. Wykonawca realizujący przedmiot zamówienia, zobowiązany jest do przeszkolenia pracowników Urzędu Miasta i Gminy w Mroczy z obsługi oprogramowania, które dostarczył.

6. Poniżej znajdują się lista z wymaganiami co do przedmiotu zamówienia.

System zarządzający dla: Urząd Miasta i Gminy Mrocza – 1 sztuka

- Specjalistyczne modularne oprogramowanie systemowe do zarządzania infrastrukturą sieciową, serwerami oraz komputerami w firmie/instytucji. Oprogramowanie zakupione jednorazowo licencją dożywotnią na minimum 70 stanowisk z możliwością nabycia aktualizacji w razie potrzeby.
- Wymagane pełne szkolenie z zakupionego oprogramowania dla dwóch osób .
- System musi składać się z siedmiu modułów:

a) Moduł sieciowy

- monitorowanie wskaźników wilgotności i temperatury
- monitorowanie serwera i łącza internetowego
- kontrola nad procesami systemowymi
- obsługa szyfrowania AES, DES i 3DES dla protokołu SNMPv3
- skanowanie sieci, wykrywanie urządzeń i serwisów TCP/IP
- interaktywne mapy sieci, mapy użytkownika, oddziałów, mapy inteligentne
- jednoczesna praca wielu administratorów, zarządzanie uprawnieniami, dzienniki dostępu
- serwisy TCP/IP: poprawność i czas odpowiedzi, statystyka ilości odebranych/utraconych pakietów (PING, SMB, HTTP, POP3, SNMP, IMAP, SQL itp.)
- liczniki WMI: obciążenie procesora, zajętość pamięci, zajętość dysków, transfer sieciowy itp.
- możliwość nakładania na urządzenie liczników wydajności wg szablonu (wzorca)
- działanie Windows: zmiana stanu usług (uruchomienie, zatrzymanie, restart), wpisy dziennika zdarzeń
- liczniki SNMP v1/2/3 (np. transfer sieciowy, temperatura, wilgotność, napięcie zasilania, poziom tonera i inne)
- kompilator plików MIB
- obsługa pułapek SNMP
- routery i switche: mapowanie portów
- obsługa komunikatów syslog
- alarmy zdarzenie – akcja

- powiadomienia (pulpitowe, e-mail, SMS) oraz akcje korekcyjne (uruchomienie programu, restart komputera itp.
- raporty (dla urządzenia, oddziału, wybranej mapy lub całej sieci)

b) Moduł spisu zasobów IT

- zarządzanie wszelkimi zasobami, za które odpowiada dział IT
- szczegółowe informacje i ewidencja czynności wykonywanych na zasobach w trakcie całego cyklu życia, możliwość definiowania statusów i pól oraz generowanie protokołu przekazania sprzętu
- widok zasobów, aplikacji, dokumentów, licencji dla poszczególnego użytkownika lub osobny widok według zasobów przypisanych do urządzeń
- jednoczesne przypisywanie dokumentu do wielu zasobów
- Mobilny Asystent Inwentaryzacji dla systemu Android
- generator dokumentów na podstawie szablonów
- automatyczne numerowanie dodawanych zasobów i dokumentów wg zdefiniowanego wzorca numeracji
- rozbudowany system zarządzania aplikacjami i licencjami, identyfikacja realnego zużycia licencji
- rozliczanie dowolnego typu licencji w tym modelowanie licencji chmurowych
- rozliczanie licencji według użytkownika, urządzenia, numeru seryjnego lub na podstawie wersji zainstalowanej aplikacji
- Historia użycia konkretnej licencji oprogramowania
- audyt inwentaryzacji sprzętu i oprogramowania
- wgląd w licencje przypisane do użytkownika pracującego na wielu urządzeniach
- zdalny dostęp do managera plików z możliwością usuwania plików użytkownika
- informacje o wpisach rejestrowych, plikach i archiwach .zip na stacji roboczej
- szczegółowe informacje o konfiguracji sprzętowej konkretnej stacji roboczej
- zarządzanie instalacjami/dezinstalacjami oprogramowania w oparciu o menedżera pakietów
- 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

c) Zarządzanie użytkownikami

- pełne zarządzanie użytkownikami, bazujące na grupach i politykach bezpieczeństwa
- dane są gromadzone i przyporządkowywane do konkretnego użytkownika
- zwiększenie poziomu bezpieczeństwa firmy: możliwość blokowania niebezpiecznych domen WWW przed przypadkowym wejściem i pobraniem złośliwego oprogramowania
- ochrona pracowników przed wiadomościami phishingowymi i atakami APT
- optymalizacja organizacji pracy
- rozróżnienie, na którym urządzeniu dana czynność została wykonana
- minimalizacja zjawiska cyberslackingu i zwiększenie wydajności pracowników
- redukcja kosztów wydruku
- blokowanie stron WWW
- blokowanie uruchamianych aplikacji
- monitorowanie wiadomości e-mail (nagłówki) – antyphishing
- szczegółowy czas pracy (godzina rozpoczęcia i zakończenia aktywności oraz przerwy
- 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)

d) Helpdesk – pomoc techniczna

- tworzenie zgłoszeń serwisowych i zarządzanie nimi (przypisywanie do administratorów)
- komentarze, zrzuty ekranowe i załączniki w zgłoszeniach
- konfigurowanie pól niestandardowych, powiązanych w wybraną kategorią zgłoszenia
- automatyzacje bazujące na założeniu: warunek > akcja
- przetwarzanie zgłoszeń w trybie anonimowym (wsparcie w realizacji wymogów „Dyrektywy o Sygnalistach")
- dokumenty prawne dot. ochrony sygnalistów w tym szablon regulaminu zgłoszeń wewnętrznych wymagany przez Dyrektywę
- dwa tryby widoku - jasny i ciemny
- planowanie zastępstw w przydzielaniu zgłoszeń
- rozbudowany system raportów
- powiadomienia i widok zgłoszenia odświeżany w czasie rzeczywistym
- baza zgłoszeń z rozbudowaną wyszukiwarką
- baza wiedzy z kategoryzacją artykułów i możliwością wstawiania grafik oraz filmów z YouTube
- przejrzysty i intuicyjny interfejs webowy
- 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).

e) Kontrola dostępu do danych

- automatyczne nadawanie użytkownikowi domyślnej polityki monitorowania i bezpieczeństwa
- ograniczenie ryzyka wycieku strategicznych danych za pośrednictwem przenośnych pamięci masowych oraz urządzeń mobilnych
- zabezpieczenie sieci firmowej przed wirusami instalującymi się automatycznie z pendrive'ów lub dysków zewnętrznych
- oszczędność pieniędzy i czasu potrzebnego na odzyskanie utraconych danych
- integracja z Windows Defender: zarządzanie ustawieniami wbudowanego antywirusa wraz z możliwością alarmowania o wykrytych problemach oraz wynikach skanowania
- integracja z Windows Firewall: włączanie i wyłączanie zapory dla wybranych typów połączeń, tworzenie reguł ruchu, odczyt stanu zapory na stacjach roboczych
- 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) podłączeń 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

f) Moduł zarządzania czasem

- statystyki własnej aktywności przy komputerze w wybranym przedziale czasu: dzień / tydzień / miesiąc / dowolny okres
- wgląd we wskaźniki aktywności wszystkich podległych pracowników
- możliwość tworzenia grup złożonych z dowolnych pracowników organizacji
- dostęp dla menedżera grupy do metryki aktywności dla wszystkich jej członków
- statystyki czasu spędzonego przed komputerem
- dwa tryby widoku - jasny i ciemny
- lista aplikacji używanych przez pracowników z rozbudowaną możliwością filtrowania, przypisywania do wybranych kategorii i nadawania im odpowiednich statusów
- podgląd aplikacji używanych w grupie bądź przez indywidualnego użytkownika w dowolnym czasie
- dodawanie wyjątków przez administratora grupy, wskazujących, że dana aplikacja w tej grupie jest uznawana za produktywną
- możliwość wskazywania przez administratora statusów konkretnych aplikacji: produktywna / neutralna / nieproduktywna
- grupowanie stron internetowych oraz aplikacji z podziałem na: produktywne / nieproduktywne / neutralne
- widok najczęściej używanych aplikacji produktywnych, nieproduktywnych i neutralnych w dowolnie wybranym okresie czasu
- definiowanie minimalnego progu produktywności (czasu spędzonego w aplikacjach produktywnych) i maksymalnego progu nieproduktywności (czasu spędzonego w aplikacjach nieproduktywnych)
- cykliczne alerty wysyłane mailem o przekroczeniu zdefiniowanych progów produktywności
- możliwość ustalania okresu, po którym dane mają być usuwane z modułu
- lista kontaktów w organizacji z wbudowaną wyszukiwarką
- szybkie, bezpośrednie przejście między modułami - podgląd zrzutu ekranu wybranego użytkownika dostępny dla menedżerów i administratorów
- czas prywatny - możliwość wyłączenia analizy aktywności w czasie używania służbowego komputera do celów prywatnych.

g) Centrum dowodzenia i bezpieczeństwa

- interaktywne dashboardy i widgety prezentujące dane z modułów nVision
- dodawanie i zarządzanie nieograniczoną liczbą dashboardów
- automatyczne odświeżanie dashboardów co 1 minutę
- wyświetlanie dashboardów w trybie ciemnym i jasnym
- metryki SLA dla zgłoszeń
- możliwość dodawania widgetów ze wszystkich modułów nVision
- Lista widgetów:
- liczniki wydajności, alarmy oraz odpowiedzi serwisów TCP/IP
- zmiany w konfiguracji sprzętowej urządzeń, zmiany w konfiguracji aplikacyjnej urządzeń, alarmy dla zasobów
- statystyki wydruków, dane z używanych oraz uruchomionych aplikacji, wysycenie łącz, aktywność na stronach WWW

- statystyki z obsługi zgłoszeń, lista najnowszych oraz najstarszych nierozwiązanych zgłoszeń, metryki SLA dla zgłoszeń
- ostatnie podłączane nośniki zewnętrzne, ostatnie operacje na plikach
- produktywność dla grupy, statystyki czasu nieproduktywnego.