Załącznik Nr 1 do SIWZ
jednocześnie Załącznik nr 1 do Umowy

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)

Przedmiotem Zamówienia jest podniesienie funkcjonalności posiadanego przez Zamawiającego systemu monitorowania urządzeniami sieciowymi poprzez:

Część 1

Dostawa licencji

- podniesienie funkcjonalności wdrożonego u Zamawiającego systemu Axence nVision poprzez wyrównanie posiadanych przez Zamawiającego modułów oprogramowania w części jednostek;
- podniesienie funkcjonalności wdrożonego u Zamawiającego systemu Axence nVision poprzez uzupełnienie liczby posiadanych licencji do łącznej ilości 2400 licencji każdego z modułów systemu celem wdrożenia w kolejnych jednostkach organizacyjnych.

Wykonawca udzieli licencji na czas nieoznaczony / Wykonawca zapewni, że Licencja udzielona jest na czas nieoznaczony.

Dostarczone oprogramowanie musi posiadać usługę wsparcia serwisowego realizowaną przez producenta oprogramowania przez okres nie krótszy niż 36 miesięcy od dnia dostarczenia licencji.

Zamawiający aktualnie posiada następującą ilość poszczególnych modułów systemu:

nazwa modułu	Ilość licencji obecnie
Network	1205
Inventory	1205
Users	1205
Helpdesk	1205
Dataguard	1125

Zamawiający dopuszcza dostawę oprogramowania równoważnego do w/w pod warunkiem:

- Wykonawca na własny koszt przeprowadzi pełen proces migracji Systemu we wszystkich lokalizacjach, w których został już wdrożony. Migracja dotyczyć musi zarówno migracji serwerów jak i agentów zainstalowanych na końcówkach. Podczas migracji muszą zostać odwzorowane wszystkie zdefiniowane przez Zamawiającego ustawienia.
- Proces migracji Systemu nie może w żaden sposób wpływać na pracę działającego środowiska, w szczególności proces migracji nie może wymuszać konieczności czasowego wyłączenia maszyn Zamawiającego.

- Proces migracji nie może generować dla Zamawiającego żadnych dodatkowych kosztów w tym związanych z zakupem dodatkowego oprogramowania, licencji czy urządzeń.
- Proces dostawy i migracji zostanie zakończony w terminie 30 dni od dnia podpisania umowy.
- Dostarczone przez Wykonawcę oprogramowanie będzie spełniało przynajmniej opisane niżej wymagania minimalne.

Część 2

Szkolenia

- szkolenie pracowników Helpdesk z funkcjonalności dostarczonego systemu;
- szkolenie administratorów systemu z funkcjonalności dostarczonego systemu.

- **Realizacja zamówienia**

Część 1

Wykonawca dostarczy licencje w formie papierowej lub elektronicznej w terminie do 5 dni roboczych od dnia podpisania umowy.

Część 2

Wykonawca przeprowadzi szkolenia w terminie do 45 dni od dnia podpisania umowy. Każde szkolenie musi zostać przeprowadzone dla dwóch grup szkoleniowych w dwóch różnych terminach. Szczegółowe terminy szkoleń zostaną uzgodnione przez Wykonawcę z Zamawiającym nie później niż 14 dni kalendarzowych przed planowanym terminem rozpoczęcia danego szkolenia. Wykonawca przygotuje dokument potwierdzający ukończenie szkolenia (certyfikat), który otrzyma każdy uczestnik kończący szkolenie. Wszelkie koszty związane z przeprowadzeniem szkoleń są ponoszone przez Wykonawcę i zawierają się w cenie Zamówienia.

- **Wymagania minimalne:**

Część 1

Dostawa licencji

– funkcjonalności systemu monitorowania urządzeniami sieciowymi

System musi posiadać budowę modułową, składającą się z serwera zarządzającego, zdalnych konsoli oraz Agentów. Moduły mają 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.

Monitorowanie infrastruktury (bezagentowo) musi obejmować serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle przynajmniej w zakresie:

- Serwisów TCP/IP, http, HTTPS, POP3, SMTP, IMAP, MAPI, FTP i innych wraz z możliwością definiowania własnych serwisów. System musi monitorować m.in. czas ich odpowiedzi i procent utraconych pakietów.
- Serwerów pocztowych:
  - system musi monitorować zarówno serwis odbierający, jak i wysyłający pocztę,
  - program musi 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 musi mieć możliwość wykonywania operacji testowych,
  - program musi mieć możliwość wysłania 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.).
- 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.
- Serwisów Windows: monitor serwisów Windows musi alarmować gdy serwis przestanie działać oraz pozwalać na jego uruchomienie/zatrzymanie/zrestartowanie.
- Wydajności systemów Windows:
  - obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy.

Program powinien umożliwiać definiowanie automatycznie zmieniających się map urządzeń zgodnie:

- ze zdefiniowaną przez administratora systemu strukturą organizacyjną
- ze zdefiniowanymi przez administratora filtrem; minimalne kryteria, które musi umożliwiać filtr:
  - agent: stan, wersja, zainstalowany
  - alarmy: aktywne
  - aplikacje: zainstalowany program (zainstalowany lub nie), wersja aplikacji (zainstalowana lub nie)
  - usługi: monitorowane usługi, czas odpowiedzi
  - SNMP: włączone, lokalizacja, mapowanie portów
  - Właściwości urządzenia: rodzaj, nazwa, opis, adres MAC, adres IP.

W zakresie inwentaryzacji system musi 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).

Moduł inwentaryzacji sprzętu musi 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 musi 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 (musi być możliwość podania daty, po której administrator otrzyma powiadomienie o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, inny dowolny załącznik (np. plik .DOCX, .XLSX), skan dowolnego dokumentu, czy też własny komentarz; dodatkowo musi być 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 QR Code (mozaikowe) dla środków trwałych, które posiadają numer inwentarzowy,
- inwentaryzacji sprzętu posiadającego kody kreskowe za pomocą aplikacji mobilnej.

Dostępne powinny być Agenty inwentaryzacji na systemy Android, OS X oraz Linux.

Inwentaryzacja oprogramowania musi 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 musi istnieć możliwość wykonania aktualnych raportów audytowych.
- Zarządzanie posiadanymi licencjami: raport zgodności licencji.
- Możliwość przypisania do programów numerów seryjnych, wartości itp.

Okna audytowe muszą posiadać możliwość filtrowania elementów z dokładnością do jednostki.

W zakresie obsługi użytkowników system musi umożliwiać monitorowanie aktywności użytkowników pracujących na komputerach z systemem Windows poprzez analizę:

- Faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy),
- Monitorowanie procesów (każdy proces ma 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 (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 ma możliwość monitorowania kosztów wydruków,
- Nagłówków przesyłanej poczty e-mail.

System ponadto musi mieć funkcjonalność 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).

System musi mieć możliwość generowania raportów dla użytkowników Active Directory niezależnie od tego, na jakich komputerach pracowali w danym czasie.

System musi posiadać mechanizm blokowania uruchamiania aplikacji zdefiniowanej przez administratora.

System musi umożliwiać realizację zdalnej pomocy użytkownikom. W ramach kontroli stacji użytkownika musi 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 musi mieć możliwość zablokowania działania myszy oraz klawiatury dla użytkownika. W module pomocy musi znajdować się baza zgłoszeń umożliwiająca użytkownikom zgłaszanie problemów technicznych, które z kolei muszą być przetwarzane i przyporządkowywane odpowiednim administratorom, otrzymującym automatycznie powiadomienie o przypisanym im problemie. System musi umożliwiać użytkownikom monitorowanie procesu rozwiązywania zgłoszonych przez nich problemów i ich aktualnych statusów, jak również możliwość wymiany informacji z administratorem poprzez komentarze, które będą wpisywane i widoczne dla obu stron. Moduł ten musi również zawierać komunikator (czat), który musi umożliwiać przesyłanie wiadomości pomiędzy zalogowanymi użytkownikami i administratorami. Moduł pomocy musi zawierać bazę wiedzy pomagającą użytkownikom na samodzielne rozwiązywanie najbardziej typowych problemów.

Moduł pomocy zdalnej musi ponadto umożliwiać:

- pobieranie listy użytkowników z Active Directory,
- przypisywanie pracowników helpdesk do kategorii zgłoszeń,
- procesowanie zgłoszeń użytkowników z wiadomości e-mail,
- dołączanie załączników do zgłoszeń,
- 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 zlecania operacji następuje kolejkowanie zadania dystrybucji pliku,
- możliwość skonfigurowania automatyzacji procesowania zgłoszeń,
- planowanie nieobecności pracowników helpdesk,
- generowanie raportów obsługi helpdesk.

System musi posiadać możliwość ochrony danych przed wyciekiem poprzez blokowanie:

- urządzeń i nośników danych. System musi 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.
- urządzeń i interfejsów fizycznych: USB, FireWire, gniazd kart pamięci, dysków SATA, dysków przenośnych, napędów CD/DVD, stacji dyskietek.
- interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA.

Blokownie musi dotyczyć tylko urządzeń służących do przenoszenia danych - inne urządzenia korzystające z tych interfejsów (drukarka, klawiatura, mysz itp.) muszą działać prawidłowo.

System musi zapewniać zarządzanie prawami dostępu do urządzeń:

- Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików.
- Autoryzowanie urządzeń firmowych (np. szyfrowanych): pendrive'ów, dysków itp. - urządzenia prywatne są blokowane.

- Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników lub stacji roboczych.
- Centralną konfigurację poprzez ustawienie reguł (polityk) dla całej sieci lub wybranych stacji roboczych.

System musi zapewniać realizację audytu operacji na urządzeniach przenośnych:

- Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych.
- Podłączenie/odłączenie urządzenia przenośnego.

System musi mieć możliwość integracji z usługa katalogową Active Directory w zakresie zarządzania prawami dostępu przypisanymi do użytkowników oraz grup domenowych.

Agent na stacji roboczej musi być zabezpieczony przed ingerencją użytkownika w jego działanie i próbą usunięcia, nawet jeśli użytkownik ma prawa administratora.

Dostarczona licencja na oprogramowanie musi umożliwiać instalację dowolnej liczby serwerów zarządzania oraz konsoli zarządzających. Zamawiający musi mieć możliwość dowolnego przydziału licencji na każdy serwer zarządzania w ramach udzielonej licencji zbiorczej.

System musi być dostępny minimum w językach: polskim, angielskim, niemieckim.

Część 2

Szkolenia

– szkolenie pracowników helpdesk

- Szkolenie musi zostać przeprowadzone dla dwóch grup szkoleniowych w dwóch różnych terminach.
- Wielkość grupy szkoleniowej do 15 osób.
- Wymiar czasu szkolenia: minimum 7 godzin (jeden dzień).
- Wykonawca skieruje do realizacji zamówienia osobę w charakterze trenera, która przeprowadzi szkolenie i będzie spełniała następujące wymagania:
  - posiadała certyfikat inżyniera wydany przez producenta oprogramowania,
  - przeprowadziła co najmniej 6 szkoleń w ciągu ostatnich 12 miesięcy w zakresie zgodnym z punktem poniżej.

  Na potwierdzenie spełnienia powyższego wymogu Wykonawca przedstawi stosowne dokumenty przed podpisaniem umowy.
- Zakres szkolenia:
  - konfiguracja modułu przez administratora;
  - tworzenie zgłoszeń serwisowych, zarządzanie nimi, automatyzacja;
  - praca w module Helpdesk od strony użytkownika;
  - tworzenie polityki przypisywania zgłoszeń do pracowników helpdesk i administratorów;
  - konfiguracja wewnętrznego chatu i jego funkcjonalności;

- omówienie systemu komunikatów dla pojedynczego użytkownika i komunikatów zbiorowych;
- omówienie możliwości wykorzystania zdalnego dostępu do użytkownika z poziomu platformy Helpdesk i konsoli systemu;
- zarządzanie procesami Windows z poziomu platformy Helpdesk;
- praktyczne wykorzystanie dwukierunkowej wymiany plików;
- zdalna dystrybucja oprogramowania;
- integracja bazy użytkowników z domeną Active Directory.

- Uczestnicy po zakończeniu szkolenia będą mieli zapewniony kontakt z trenerem przez minimum 14 dni po zakończeniu szkolenia.
- Po zakończeniu szkolenia uczestnicy otrzymają dokument potwierdzający posiadaną wiedzę na poziomie pracownika Helpdesk.

– szkolenie administratorów

- Szkolenie musi zostać przeprowadzone dla dwóch grup szkoleniowych w dwóch różnych terminach.
- Wielkość grupy szkoleniowej do 10 osób.
- Wymiar czasu szkolenia: minimum 14 godzin (dwa dni).
- Wykonawca skieruje do realizacji zamówienia osobę w charakterze trenera, która przeprowadzi szkolenie i będzie spełniała następujące wymagania:
  - posiadała certyfikat administratora wydany przez producenta oprogramowania,
  - przeprowadziła co najmniej 6 szkoleń w ciągu ostatnich 12 miesięcy w zakresie zgodnym z punktem poniżej.

  Na potwierdzenie spełnienia powyższego wymogu Wykonawca przedstawi stosowne dokumenty przed podpisaniem umowy.
- Zakres szkolenia:
  - zapoznanie z najważniejszymi funkcjonalnościami systemu;
  - konfiguracja i korzystanie z poszczególnych modułów systemu;
  - monitorowanie krytycznych dla organizacji urządzeń, usług i procesów;
  - monitorowanie komponentów sieci, wydajności i pojemności;
  - wykonanie audytu oprogramowania, plików multimedialnych;
  - zarządzanie środkami trwałymi;
  - monitorowanie i analiza aktywności użytkowników;
  - standaryzacja i rozliczalność komunikacji pomiędzy użytkownikami a pracownikami IT;
  - budowa bazy wiedzy dla pracowników;
  - automatyzacja procesów związanych z obsługą zgłoszeń serwisowych;
  - zarządzanie i rozliczanie nośników zewnętrznych;
  - rozliczanie pracy na plikach wspólnych
- Uczestnicy po zakończeniu szkolenia będą mieli zapewniony kontakt z trenerem przez minimum 14 dni po zakończeniu szkolenia.

- Po zakończeniu szkolenia uczestnicy otrzymają certyfikat potwierdzający posiadaną wiedzę na poziomie administratora. Certyfikat musi być autoryzowany przez producenta systemu.