**Załącznik nr 2c do SWZ 22/ZP/2022**

**Część 3 – Oprogramowanie do zarządzania infrastrukturą IT na 230 stanowisk z licencją na 36 miesięcy**

1. Przedmiotem zamówienia jest dostawa z wdrożeniem oprogramowania zapewniającego kompleksowy monitoring infrastruktury IT oraz stanowisk użytkowników oprogramowania Zamawiającego.

**2. Wykaz funkcjonalności w poszczególnych obszarach funkcjonalności oprogramowania:**

2.1. Oprogramowanie musi pozwalać na monitorowane stacji roboczych opartych o systemy

Windows, Linux oraz Mac.

2.2. Monitorowanie powinno być dostępne również dla urządzeń typu: firewall, router, przełącznik,

VoIP, jak również drukarek pracujących w środowisku sieciowym oraz urządzeń obsługujących SNMP.

2.3. Serwer oprogramowania powinien działać w 64-bitowym systemie operacyjnym min. Windows

Serwer 2019 oferującym 2 rdzenie CPU, 4GB RAM.

2.4. Konsole zarządzania powinny pracować w 64-bitowym systemie operacyjnym Microsoft

Windows w konfiguracji 2 rdzenie CPU / 4 GB RAM

2.5. Minimalne wymagania dla agenta na stacjach roboczych nie powinny wykraczać poza 2

rdzeniowy CPU, 1GB RAM, i 32/64 bitowy system operacyjny Windows XP

2.6. Oprogramowanie Agenta powinno współpracować z posiadanymi rozwiązaniami

bezpieczeństwa firmy ESET.

2.7. Monitorowanie infrastruktury IT z uwzględnieniem stacji roboczych, serwerów, sieciowych

urządzeń aktywnych, urządzeń SNMP.

2.7.1. System powinien wykrywać urządzenia w sieci poprzez skanowanie ping oraz arp-ping.

2.7.2. Wykrywanie urządzeń na podstawie informacji odczytanych z AD.

2.7.3. Graficzna wizualizacja stanu urządzeń.

2.7.4. Wizualizacji poprzez tworzenie map i schematów dla urządzeń i połączeń.

2.7.5. Monitorowanie serwisów TCP/IP, HTTP, POP3, SMTP, FTP wraz z możliwością definiowania

własnych rodzajów.

2.7.6. Monitorowanie czasu odpowiedzi i procent utraconych pakietów

2.7.7. Monitorowanie serwerów pocztowych ze szczególnym uwzględnieniem:

2.7.7.1. czas logowania,

2.7.7.2. czas wysyłania,

2.7.7.3. stanu powiadomienia (e-mail, SMS i inne),

2.7.7.4. wykonywania operacji testowych,

2.7.8. Monitorowanie serwerów WWW i adresów URL.

2.7.9. Monitorowanie czasu ładowania strony internetowej, zmiany treści na stronie internetowej i

statusu protokołu HTTPS.

2.7.10. Obsługa szyfrowania SSL/TLS w powiadomieniach e-mail.

2.7.11. Obsługa urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją:

2.7.12. Obsługa komunikatów syslog i pułapek SNMP i ewidencjonowanie logów.

2.7.13. Monitoring aktywnego sprzętu sieciowego (firewalle, routery, przełączniki) w zakresie:

2.7.13.1. zmian stanu interfejsów sieciowych,

2.7.13.2. ruchu sieciowego,

2.7.13.3. podłączonych stacji roboczych z graficzną prezentacją przełącznika,

2.7.13.4. ruchu generowanego przez podłączone do portów stacje robocze

2.7.14. Monitorowanie serwisów Windows.

2.7.15. Wyświetlania statystyk urządzenia.

2.7.16. Monitorowanie wydajności systemów Windows

2.8. Inwentaryzacja zasobów IT w czasie rzeczywistym w zakresie fizycznym i logicznym.

2.8.1. Prezentacja pełnej specyfikacji komputera/stacji roboczej.

2.8.2. Zestawienie konfiguracji sprzętowej.

2.8.3. Powiadamianie o niezbędnej aktualizacji/rozszerzenia urządzenia.

2.8.4. Zestawienie zainstalowanych aplikacjach oraz aktualizacjach systemu operacyjnego.

2.8.5. Agregacja informacji o zmianach przeprowadzonych na wybranej stacji roboczej.

2.8.6. Możliwość wysyłania powiadomienia w przypadku zainstalowania programu lub jakiejkolwiek

zmiany konfiguracji sprzętowej komputera

2.8.7. Możliwość odczytania numeru seryjnego (klucza licencyjnego).

2.8.8. Możliwość automatycznego zarządzania instalacjami i deinstalacjami oprogramowania poprzez

określenie paczek aplikacji wymaganych oraz nieautoryzowanych.

2.8.9. Możliwość przeglądu informacji o konfiguracji systemu, np. komend startowych, zmiennych

środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań.

2.8.10. Możliwość tworzenia listy plików użytkowników z określonym rozszerzeniem 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).

2.8.11. Możliwość wymiany plików do i ze stacją roboczą poprzez funkcję Menedżera plików.

2.8.12. Możliwość przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym

miejscu oraz automatycznego aktualizowania zgromadzonych informacji.

2.8.13. Tworzenia powiązań między zasobami a urządzeniami.

2.8.14. Tworzenia powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak i

zsynchronizowanymi z domeną AD).

2.8.15. Wskazania osób uprawnionych do użycia zasobów.

2.8.16. Możliwość definiowania własnych typów zasobów (elementów wyposażenia), ich atrybutów

oraz wartości - dla danego urządzenia lub oprogramowania istnieje możliwość dodawania

dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer dokumentu

zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu gwarancji, termin

kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie e-mail o

zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, lub własny

komentarz.

2.8.17. Możliwość określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich

zasobów.

2.8.18. Możliwość określenia atrybutów dodatkowych tylko dla wybranych typów zasobów.

2.8.19. Możliwość definiowania własnych list jednokrotnego wyboru jako dodatkowe informacje o

zasobie.

2.8.20. Możliwość importu danych z zewnętrznego źródła.

2.8.21. Możliwość przechowywania dowolnych dokumentów w postaci załączników.

2.8.22. Możliwość tworzenia powiązań między zasobami a dokumentami w relacji 1:N.

2.8.23. Możliwość oznaczania statusów zasobów, np. w użyciu, w naprawie, zutylizowany itp.,

2.8.24. Ewidencja czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie,

konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie

czynności.

2.8.25. Generowanie zestawień wszystkich zasobów, w tym urządzeń i zainstalowanego na nich

oprogramowania.

2.8.26. Generowanie protokołów przekazania zasobów.

2.8.27. Archiwizacja i porównywania audytów zasobów.

2.8.28. Tworzenia i drukowanie kodów dla zasobów które posiadają numer inwentarzowy.

2.8.29. Definiowania alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data” z

atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnie licencja/gwarancja”).

2.8.30. Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie

archiwów ZIP

2.8.31. Prezentacja informacji o aplikacjach używanych w organizacji.

2.8.32. Tworzenie własnych wzorców aplikacji.

2.8.33. Tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp.

2.8.34. Informacje o komputerach, na których aplikacja została wykryta.

2.8.35. Zarządzanie posiadanymi licencjami.

2.8.36. Wskazywanie osób odpowiedzialnych za licencję.

2.8.37. Wskazanie użytkowników licencji.

2.8.38. Tworzenia powiązań między licencjami a dokumentami w relacji 1:N.

2.8.39. Rozbudowane zarządzanie licencjami poprzez: przypisywanie do użytkownika, przypisywanie

do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych,

przypisywanie wg różnych wersji aplikacji na jednym urządzeniu.

2.8.40. Audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby

posiadanych licencji.

2.8.41. Zarządzanie posiadanymi licencjami: raport zgodności licencji.

2.8.42. Możliwość przypisania do programów numerów seryjnych, wartości.

Możliwość instalacji zdalnej programów na stacjach roboczych zarówno na pojedynczym PC jak

również grupie komputerów. Możliwość instalacji zdalnej programów dla pojedynczego konta AD

oraz dla grupy kont AD.

2.9. Monitorowanie aktywności użytkowników systemu informatycznego.

2.9.1. Monitorowanie czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia

pracy)

2.9.2. Monitorowanie procesów (każdy proces ma całkowity czas działania oraz czas aktywności

użytkownika) wraz informacją o uruchomieniu na podwyższonych uprawnieniach.

2.9.3. Monitorowanie rzeczywistego użytkowania programów.

2.9.4. Monitorowanie listy odwiedzanych stron WWW (liczba odwiedzin stron z nagłówkami, liczbą i

czasem wizyt).

2.9.5. Monitorowanie transferu sieciowego użytkowników (ruch lokalny i transfer internetowy

generowany przez użytkownika).

2.9.6. Monitorowanie zleceń wydruków.

2.9.7. Monitorowanie nagłówków przesyłanej w aplikacjach klienckich poczty e-mail.

2.9.8. Możliwość blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania

całego ruchu WWW dla stacji roboczej, na której zalogowany jest

użytkownik, z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających

korzystania z danych domen oraz wybranych lub dowolnych sub-domen (np. \*.domena.pl). Reguły w

postaci listy domen tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane

pomiędzy grupami lub kontami.

2.9.9. Możliwość blokowania ruchu na wskazanych portach TCP/IP.

2.9.10. Możliwość blokowania pobierania poprzez przeglądarki internetowe plików z określonym

rozszerzeniem.

2.9.11. 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.

2.9.12. Definiowanie zakresu czasu w których monitorowanie użytkowników jest wyłączone.

2.10. Obsługa wewnętrznego Help Desk – zdalnej pomocy użytkownikom systemu

informatycznego.

2.10.1. Możliwość prowadzenia kontroli stacji roboczej użytkownika z dostępem do pulpitu i

zdalnego dostępu (w tym z dostępem bez zgody użytkownika i opcja, kiedy użytkownik decyduje o

udzieleniu dostępu).

2.10.2. Obsługa funkcji zdalnego dostępu do stacji roboczej przez użytkownika, który uzyskał takie

uprawnienia przez administratora systemu.

2.10.3. Pobieranie listy użytkowników z Active Directory.

2.10.4. Zarządzanie lokalnymi kontami Windows.

2.10.5. Zarządzanie dostępem pracowników Help Desk do zgłoszeń poprzez rozbudowany system

zarządzania regułami widoczności zgłoszeń.

2.10.6. Zarządzanie dostępem do czatu w 3 poziomach uprawnień: pełny dostęp, brak dostępu lub

dostęp ograniczony wyłącznie do pomocy technicznej.

2.10.7. Tworzenie własnego drzewa kategorii zgłoszeń wraz z możliwością grupowania kategorii w

folderach (do 4 poziomów kategorii), opisami kategorii oraz klauzulą RODO.

2.10.8. Automatyczne przypisywanie pracowników helpdesk do zgłoszeń w określonych kategoriach

lub pochodzących od określonych grup użytkowników.

2.10.9. Procesowanie zgłoszeń użytkowników z wiadomości e-mail

2.10.10. Tworzenie formularzy z niestandardowymi polami opisowymi, dedykowanymi do wybranych

kategorii zgłoszeń.

2.10.11. Wykonywanie operacji na wielu zgłoszeniach równocześnie.

2.10.12. Dołączanie załączników do zgłoszeń.

2.10.13. Wyszukiwanie zgłoszeń i artykułów w bazie wiedzy.

2.10.14. 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.

2.10.15. Zrzuty ekranowe (podgląd pulpitu).

2.10.16. Dystrybucja oprogramowania przez funkcjonalność agenta

2.10.17. Dystrybucja oraz uruchamianie plików za pomocą Agentów (w tym plików MSI).

2.10.18. Zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecania operacji

następuje kolejkowanie zadania dystrybucji pliku.

2.10.19. Możliwość skonfigurowania automatyzacji procesowania zgłoszeń wraz z powiadomieniami

wysyłanymi do określonych aktorów w zgłoszeniu.

2.10.20. Obsługa usług (SLA) wraz z raportami np. przekroczeń SLA wraz z podsumowaniem

2.10.21. Generowanie raportów obsługi helpdesk.

2.10.22. Zdalne wykonywanie poleceń poprzez agenta (np. utworzenie / edycja konta lokalnego

użytkownika systemu).

2.10.23. Zarządzania procesami systemu Windows.

2.10.24. Wymiany plików do i ze stacji roboczej poprzez funkcję menedżera plików.

2.11. Ochrona danych przed nieuprawnionym dostępem do danych.

2.11.1. Możliwość blokowanie urządzeń i nośników danych.

2.11.2. 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

2.11.3. Blokowanie urządzeń i interfejsów fizycznych: USB, gniazda kart pamięci, SATA, dyski

przenośne, napędy CD/DVD.

2.11.4. Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth.

2.11.5. Blokownie dotyczy tylko urządzeń służących do przenoszenia danych - inne urządzenia

(drukarka, klawiatura, mysz itp.) mogą być podłączane.

2.11.6. Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z

możliwością ograniczenia alarmów tylko do nośników niezaufanych.

2.11.7. Funkcje wspierające bezpieczeństwa systemu: integracja i zarządzanie ustawieniami np.

Windows Defender.

2.11.8. Funkcje wspierające bezpieczeństwo systemu:

2.11.9. Monitorowanie stanu szyfrowania dysków BitLocker.

2.11.10. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu modułu TPM.

2.11.11. Zarządzanie prawami dostępu do urządzeń:

2.11.11.1. Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików.

2.11.11.2. Autoryzowanie urządzeń firmowych

2.11.11.3. Blokowanie urządzeń prywatnych

2.11.11.4. Blokowanie określonych typów urządzeń dla wybranych użytkowników.

2.11.11.5. Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całe jsieci.

2.11.11.6. Możliwość usuwania z listy znanych urządzeń tych nośników, które np. zostały

zutylizowane.

2.11.12. Audyt operacji na plikach na urządzeniach przenośnych:

2.11.12.1. Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych.

2.11.12.2. Podłączenie/odłączenie urządzenia przenośnego.

2.11.13. Monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika.

2.11.14. Integracja z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników

oraz grup domenowych. Przydzielanie uprawnień również do kont użytkowników lokalnych.

**3. Wymagania w zakresie licencji i integracji:**

3.1. Wieczysta licencja na oprogramowanie.

3.2. Podstawowy moduł zarządzania środowiskiem dla nielimitowanej liczby monitorowanych

urządzeń.

3.3. Instalacja wielu zdalnych konsol administracyjnych w środowisku udostępnionym przez

Zamawiającego – spełniającym wymogi oprogramowania Wykonawcy.

3.4. Umowa serwisowa obejmująca aktualizacje i pomoc techniczną na okres nie krótszy niż 36

miesięcy.

3.5. Modułowość oprogramowania pozwalająca Zamawiającemu na dowolną konfigurację według

aktualnych potrzeb.

3.6. **Obsługa 230 stacji roboczych** przez wszystkie moduły i funkcjonalności oprogramowania z

możliwością zwiększenia tej liczby w dowolnym czasie.

**4. Warunki udzielenia licencji:**

4.1. Licencje na oprogramowanie dostarczone będą do siedziby Zamawiającego w formie papierowej lub elektronicznej: klucze lub licencje dostępne do pobrania na stronie www producenta oprogramowania.

4.2. W przypadku licencji dostępnych w formie elektronicznej na stronie producenta, Wykonawca przekaże dane autoryzacyjne lub Zamawiający poda konto do portalu producenta, jakie posiada, a do którego licencje mają być dołączone.

# **5. Zakres prac wdrożeniowo-szkoleniowych:**

**Wdrożenie** (w siedzibie Zamawiającego, minimum dwa dni robocze)**:**

* 1. Zakres minimalnych prac w obszarze wstępnej konfiguracji dostarczanego rozwiązania:
  + Instalacja dostarczonego systemu na wskazanym przez Zamawiającego serwerze Windows.
  + Konfiguracja programu antywirusowego w obszarze wyjątków wymaganych do poprawnej pracy wdrażanego systemu. Omówienie wyjątków z Zamawiającym.
  + Konfiguracja stosowanych przez Zamawiającego zapór sieciowych w obszarze dopuszczenia wymaganej, minimalnej komunikacji sieciowej zapewniającej poprawną pracę wdrażanego systemu. Omówienie wymaganych reguł z Zamawiającym.
  + Instalacja konsol zarządzających na wskazanych przez Zamawiającego stacjach roboczych personelu IT.
  + Wstępna konfiguracja wdrażanego systemu w obszarze parametrów ogólnych tj. retencja danych, reguły kopii zapasowej bazy danych, synchronizacja z AD).
  + Konfiguracja uprawnień poszczególnych pracowników działu IT do wdrażanego systemu.
  + Instalacja we wskazanym przez Zamawiającego pomieszczeniu dostarczonej wraz z oprogramowaniem bramki SMS wraz z jej integracją w protokole SOAP z w/w oprogramowaniem. Kartę SIM Zamawiający udostępni w momencie montażu urządzenia.
  + Przygotowanie procedury instalacji agenta i jej testy (w zależności od środowiska: konfiguracja reguł GPO w Active Directory/konsola centralna antywirusa/ręczna procedura) wraz z testem działania test działania polisy.

5,2. Zakres minimalnych prac w obszarze wdrożenia mechanizmu umożliwiającego wsparcie Zamawiającego w procesie zarządzania czasem i analizy aktywności użytkowników systemów informatycznych:

* + Konfiguracja kategoryzacji aktywności pracowników w zakresie grupowania aktywności w kontekście typu użytej aplikacji, np. Word, Excel, Notepad czy Wordpad to aplikacje typu „Praca na dokumentach”.
  + Konfiguracja reguł klasyfikujących pracę użytkowników na służbowym sprzęcie w zakresie aplikacji ocenianych pozytywnie (produktywnie).
  + Konfiguracja reguł klasyfikujących pracę użytkowników na służbowym sprzęcie w zakresie aplikacji ocenianych negatywnie (nieproduktywnie).
  + Zdefiniowanie polityk monitorowania minimalnego poziomu produktywności i czasu nieproduktywnego.
  + Zdefiniowanie reguł wyjątków w zakresie negatywnego oceniania aktywności w poszczególnych aplikacjach, np. portal Facebook dla pracowników działu promocji to aktywność pozytywna, a dla reszty pracowników działanie negatywne w kontekście oceny pracy.
  + Konfiguracja reguł dostępu poszczególnych pracowników do swoich danych i ich oceny.
  + Konfiguracja reguł dostępu do danych pracowników dla poszczególnych kierowników/dyrektorów wydziałów/departamentów/zespołów.

5.3. Zakres minimalnych prac w obszarze wdrożenia mechanizmów umożliwiających zarządzanie i kontrolę nośników zewnętrznych:

* + Konfiguracja podstawowych reguł pracy modułu/funkcjonalności pozwalającej na aktywne blokowanie nieznanych (nieautoryzowanych) nośników danych.
  + Konfiguracja reguł dopuszczających nośniki danych autoryzowane i przepisanie odpowiednich reguł do poszczególnych pracowników oraz grup pracowników, w tym opisanie dopuszczonych nośników.
  + Konfiguracja monitorowania folderów lokalnych na stacjach roboczych pracowników (np. profil użytkownika).
  + Konfiguracja powiadomienia pracownika o dokonanym przez niego naruszeniu polityki obcych nośników.
  + Konfiguracja powiadamiania działu IT (wskazanych osób z działu) o naruszeniu polityki nośników przez pracownika organizacji.
  + Konfiguracja automatycznych raportów w zakresie naruszeń reguł nośników zewnętrznych.
  1. Zakres minimalnych prac w obszarze wdrożenia mechanizmów umożliwiających realizację zdalnej pomocy technicznej w sieci Zamawiającego:
  + Zdefiniowanie kont pracowników obsługujących zgłoszenia w ramach dostarczanej platformy HelpDesk.
  + Analiza obecnych procesów obsługi zgłoszeń serwisowych oraz przeniesienie do wdrażanego systemu obsługi zgłoszeń serwisowych kategorii poszczególnych zgłoszeń.
  + W ramach poszczególnych kategorii zgłoszeń zdefiniować niestandardowe formularze zgłoszeń, pozwalające na uzyskiwanie precyzyjnych informacji o rodzaju problemu. Np. dla kategorii „Problemy z wydrukiem” dodać dodatkowe pytania kontrolne pozwalające uzyskać takie informacje jak: czy drukarka jest włączona, czy drukarka nie wyświetla komunikatu o wymianie tonera lub braku papieru, czy drukarka nie sygnalizuje inne problemu technicznego (np. zacięty papier).
  + Zdefiniowanie reguł określających widoczność zgłoszeń w poszczególnych kategoriach dla poszczególnych pracowników systemu obsługi zgłoszeń.
  + Zdefiniowanie reguł określających mechanizm automatycznego rozdzielania zgłoszeń w poszczególnych kategoriach dla poszczególnych pracowników systemu obsługi zgłoszeń.
  + Zdefiniowanie priorytetów obsługi zgłoszeń serwisowych wraz z ich automatycznym przypisaniem do poszczególnych kategorii.
  + Zdefiniowanie metryk SLA pilnujących i powiadamiających pracowników obsługi zgłoszeń o ich przekroczeniu

5.5. Zakres minimalnych prac w obszarze wdrożenia mechanizmów umożliwiających realizację obowiązku nadzoru nad aktywności wynikającą z pracy na sprzęcie służbowym:

* + Konfiguracja domyślnych reguł monitorowania pracy dla poszczególnych kont pracowników. Ustawienia muszą obejmować monitorowania takich obszarów jak aktywność w aplikacjach i przeglądarkach WWW, ogólny czas pracy wraz z przerwami w aktywności powyżej zdefiniowanego limitu, rejestr drukowanych dokumentów oraz korespondencji mail opartej na kliencie poczty (np. Outlook czy Thunderbird). Omówienie możliwości stosowania wyjątków dla wybranych grup oraz pojedynczych kont.
  + Konfiguracja domyślnych reguł blokowania praw do uruchomienia przez użytkowników aplikacji dodanych przez IT do listy zakazanych. Omówienie możliwości stosowania dodatkowych zmian w blokadach dla wybranych grup oraz pojedynczych kont.
  + Konfiguracja domyślnych reguł blokowania praw do pobierania określonych przez IT typów plików z wykorzystaniem przeglądarki. Omówienie możliwości stosowania dodatkowych zmian w blokadach dla wybranych grup oraz pojedynczych kont.
  + Konfiguracja domyślnych reguł blokowania dostępu do zdefiniowanych stron internetowych. Omówienie możliwości stosowania dodatkowych zmian w blokadach dla wybranych grup oraz pojedynczych kont.
  + Konfiguracja wstępnej klasyfikacji aktywności w aplikacjach desktopowych oraz na stronach WWW na podstawie danych zebranych w pierwszym dniu pracy wdrażanego systemu. Przykładowo: Word, Excel przypisane do kontenera „Praca na dokumentach”, a Płatnik to kontenera „Finansowo-Księgowe”.

5.6. Zakres minimalnych prac w obszarze wdrożenia mechanizmów umożliwiających realizację zadań związanych z inwentaryzacją sprzętu i oprogramowania w sieci Zamawiającego:

* + Konfiguracja zakresu pracy agenta w obszarze inwentaryzacji określonych typów plików w sieci. Np. Indeksuj pliki MP3.
  + Konfiguracja wzoru protokołu przekazania zasobu, jako elementu aktywnego w procesie wydawania i przyjmowania sprzętu od i do pracownika
  + Konfiguracja poszczególnych typów zasobów wraz ze zdefiniowaniem charakterystycznych dla nich pól opisowych.
  + Konfiguracja globalnych pól opisowych występujących przy każdym typie zasobu w ramach inwentaryzacji i opisywaniu sprzętu firmowego.
  + Konfiguracja na poszczególnych typów zasobów stałych elementów opisowych etykiety ewidencyjnej, tj. standard jej kodowania na podstawie numeru inwentaryzacyjnego oraz zdefiniowanie stałych części każdego numeru inwentaryzacyjnego.
  + Konfiguracja szablonu czynności serwisowych związanych z „cyklem życia” zasobu w organizacji.
  + Konfiguracja klasyfikacji kategorii załączanych do zasobu dokumentów/załączników.
  + Wstępna analiza zgromadzonych danych czyli omówienie mechanizmu pracy na zbiorach danych takich jak konfiguracja sprzętowa stacji roboczych oraz audyt oprogramowania.
  1. Zakres minimalnych prac w obszarze wdrożenia mechanizmów umożliwiających realizację obowiązku należytego monitorowania sieci teleinformatycznej Zamawiającego:
  + Konfiguracja podstawowych mechanizmów wykrywania sieci (serwisy używane w detekcji, poświadczenia SNMP i WMI).
  + Dodanie map reprezentujących poszczególne sieci lokalnych w infrastrukturze Zamawiającego i ich skanowanie w poszukiwaniu urządzeń sieciowych.
  + Klasyfikacja urządzeń sieciowych, w tym ich opisanie w zakresie nazwy, poziomu ważności poszczególnych urządzeń dla sieci i procesów biznesowych Zamawiającego oraz typu wizualizacji urządzeń.
  + Analiza krytycznych urządzeń sieciowych w infrastrukturze Zamawiającego pod kątem możliwości monitorowanie parametrów wydajności z wykorzystaniem protokołów sieciowych SNMP oraz WMI. Dodanie w wyniku w/w analizy monitorowania takich parametrów wydajnościowych jak:
    - Obciążenie CPU, RAM, liczba otwartych sesji czy utylizacji łącz WAN dla biegowego w sieci Zamawiającego.
    - Obciążenie CPU, RAM oraz zajętość miejsca na partycji systemowej dla serwerów Windows w sieci Zamawiającego.
    - Obciążenie CPU, RAM oraz zajętość miejsca na partycji systemowej dla serwerów Linux w sieci Zamawiającego.
    - Obciążenie CPU, RAM, zajętości miejsce oraz kondycji dysków dla macierzy NAS w sieci Zamawiającego.
    - Obciążenie i czas podtrzymania, kondycji modułu bateryjnego czy jakości napięcia wejściowego dla UPSów w sieci Zamawiającego.
    - Obciążenie CPU, RAM, stanu interfejsów dla przełączników zarządzanych w sieci Zamawiającego.
    - Obciążenie CPU, RAM, liczby podłączonych klientów dla AccessPointów w sieci Zamawiającego.
  + Zdefiniowanie progów alarmowych dla poszczególnych liczników wydajności oraz automatycznych powiadomień typu Mail i SMS. Adresy odbiorców i numery telefonów zostaną udostępnione przez Zamawiającego w momencie konfiguracji.
  + Analiza krytycznych urządzeń sieciowych w infrastrukturze Zamawiającego pod kątem możliwości monitorowanie pracy poszczególnych serwisów stosu TCP/IP. Dodanie w wyniku w/w analizy monitorowania takich serwisów stosu TCP/IP jak:
    - http/https dla wewnętrznych systemów typu IntraNet w sieci Zamawiającego.
    - mssql i inne serwisy dla usług bazodanowych w sieci Zamawiającego.
    - ping dla krytycznych urządzeń w sieci Zamawiającego.
  + Zdefiniowanie progów alarmowych dla poszczególnych monitorowanych serwisów oraz automatycznych powiadomień typu Mail i SMS. Adresy odbiorców i numery telefonów zostaną udostępnione przez Zamawiającego w momencie konfiguracji.

**5.8**. Zakres minimalnych prac w obszarze uruchomienia portalu WWW pozwalającego na krytycznych dla Zamawiającego danych z wdrażanego rozwiązania:

* + Zdefiniowanie dashboardow tematycznych.
  + Zdefiniowanie wigdetów z zakresem danych zaczytywanych z poszczególnych obszarów funkcjonalnych wdrożonego rozwiązania:
    - Wigdety z obszary monitorowanie sieci teleinformatycznej.
    - Wigdety z obszary inwentaryzacji sprzętu i oprogramowania.
    - Wigdety z obszaru nadzoru nad użytkownikami.
    - Wigdety z obszaru obsługi realizacji zgłoszeń serwisowych.
    - Wigdety z obszary zarzadzania i rozliczania użycia nośników zewnętrznych.
    - Wigdety z obszaru oceny produktywności pracowników.
  + Konfiguracja polityk udostępniania dashboardów
  + Konfiguracja reguł dostępu dla pracowników działu IT do zarządzania portalem.

**5.9. Szkolenie (w siedzibie Zamawiającego, minimum trzy dni robocze):**

* + 1. Zakres minimalnych prac w obszarze przeprowadzenia szkolenia dla personelu IT Zamawiającego pełniącego rolę administratora wdrażanego systemu:
  + Zakres szkolenia dla administratorów:
    - Ogólne omówienie rozwiązania i jego struktury.
    - Praca w obszarze monitorowania sieci teleinformatycznej.
    - Praca w obszarze zarządzania i inwentaryzacji sprzętem i oprogramowaniem.
    - Praca w obszarze nadzoru nad aktywności wynikającą z pracy na sprzęcie służbowym.
    - Praca w obszarze zdalnej pomocy technicznej w sieci Zamawiającego.
    - Praca w obszarze zarządzania i kontroli nośników zewnętrznych.
    - Praca w obszarze zarządzania czasem i analizy aktywności użytkowników.
    - Rozwiązywanie najczęstszych problemów.
    - Egzamin certyfikujący.
  + Czas trwania szkolenia dla administratorów:
    - Minimum 8 godzin lekcyjnych dla pracowników zarządzających całym oferowanym rozwiązaniem.
  + Szkolenie powinno się kończyć egzaminem oraz wydaniem certyfikatu.

**6. Gwarancja, licencje, wsparcie:**

1. Całość dostarczanego rozwiązania, tzn. każde z dostarczonych systemów, musi być objęte 36 miesięczną gwarancją.

2. Serwis gwarancyjny/licencyjny/wsparcie musi obejmować dostęp do poprawek i nowych wersji oprogramowania wbudowanego, które są elementem zamówienia przez cały okres obowiązywania gwarancji.

3. Zgłaszanie usterek/awarii poprzez pocztę elektroniczną, portal helpdesk lub infolinię.

4. Czas reakcji serwisu od momentu zgłoszenia - 1 godzina, czas na rozwiązanie zgłoszonej usterki/awarii - 24 godziny.