

Załącznik nr 1
do Zapytania ofertowego nr **BA-WZ.25.12.2021.BP.3**

Opis Przedmiotu Zamówienia

Dostarczenie i wdrożenie licencji do oprogramowania służącego do monitorowania, audytowania i ewidencji podzespołów i sprzętu IT (stacji roboczych) Zamawiającego wraz z obsługą zgłoszeń serwisowych typu HelpDesk oraz udzielenie rocznego wsparcia (maintenance).

Zamawiający posiada obecnie usługę katalogową Active Directory. W usłudze katalogowej jest dostępne ok. 350 kont aktywnych oraz 362 stacji roboczych. Zadaniem Wykonawcy będzie wdrożenie zaproponowanego rozwiązanie wraz z konfiguracją i produkcyjnym uruchomieniem, przeprowadzenie instruktażu dla administratorów Zamawiającego oraz opracowaniem dokumentacji powdrożeniowej.

I. Specyfikacja przedmiotu zamówienia:

1. Udzielenie bezterminowej licencji do oprogramowania wraz z modułami pozwalającego monitorować, audytować, inwentaryzować, zarządzać stacjami roboczymi, wraz z zintegrowanym modułem HelpDesk (system ticketowy) dla Zamawiającego wraz z prawem do aktualizacji oprogramowania i wsparciem (maintenance) na okres 12 miesięcy dla:
 - a) 362 licencji **w ramach zamówienia podstawowego**,
 - b) w liczbie maksymalnej do 50 licencji **w ramach prawa opcji** - w przypadku licencji do oprogramowania w ramach prawa opcji, prawo do aktualizacji licencji dostarczonych w ramach opcji zakończy się w tym samym terminie co ważność licencji wraz z prawem do aktualizacji nabytych w ramach zamówienia podstawowego..
2. Wdrożenie wraz z konfiguracją zaproponowanego rozwiązania.
3. Opracowania dokumentacji powdrożeniowej wraz z przeniesieniem autorskich praw majątkowych do tej dokumentacji .
4. Przeprowadzenie instruktażu dla administratorów

II. Podstawowe wymagania całego systemu, rozwiązanie powinno:

1. Oprogramowanie powinno posiadać bezterminową licencję.
2. Oprogramowanie powinno posiadać interfejs użytkownika w języku polskim.
3. Wsparcie techniczne mailowe oraz telefoniczne w języku polskim.
4. Przechowywanie danych w bazie MS SQL (wersja płatna i darmowa).
5. Możliwość automatycznego usuwania danych z audytu oraz monitoringu starszych niż wybraną ilość dni, co powinno zapewniać automatyczne pilnowanie wielkości bazy.
6. Wzajemna integracja wszystkich funkcjonalności (modułów) systemu. Korzystanie z tych samych słowników, katalogu użytkowników, informacji o majątku itp.
7. System powinien umożliwiać logowanie do systemu z różnymi poziomami uprawnień. Możliwość podziału bazy danych na homogeniczne całości (możliwość odizolowania np. poszczególnych jednostek organizacyjnych pod względem zarządzania w systemie oraz pracy z wynikami na podstawie uprawnień użytkowników systemu).
8. Automatyczne przypisywanie użytkowników do komputerów
9. Podział i przydzielanie komputerów do grup według struktury organizacyjnej, lokalizacji i użytkownika
10. Możliwość przypisania administratora do pewnej grupy komputerów

11. Możliwość integracji systemu z Active Directory - wsparcie wielu domen - dla komputerów oraz osób można ustawić dowolną ilość domen lub kontenerów, które będą synchronizowane
12. Możliwość cyklicznej synchronizacji użytkowników i komputerów, lokalizacji, jednostek organizacyjnych z Active Directory. Po synchronizacji możliwość automatycznego uruchomienia dowolnych poleceń SQL.
13. Możliwość instalacji agentów z Konsoli zarządzającej oraz możliwość dystrybucji agentów (audyt/monitoring) za pomocą GPO (paczki msi).
14. Możliwość audytu za pośrednictwem serwera FTP
15. TCP/IP serwer – usługa systemowa nasłuchująca na dowolnie wybranym porcie umożliwiająca komunikację z agentem
16. Możliwość pracy systemu w: sieciach rozproszonych, sieciach spiętych VPN-em, w Internecie (za NAT-em). Możliwość wyboru protokołu TCP/IP lub FTP.
17. Możliwość eksportu dowolnych tabeli oraz raportów do formatów: .csv, .xls, .xlsx, .html, .pdf, .rtf, .jpeg, .png.
18. Bezpośrednie wysyłanie danych z tabeli za pomocą maila.
19. Portal webowy dla całego systemu – możliwość przeglądania wyników z audytu oraz monitoringu za pośrednictwem przeglądarki www według definiowanych uprawnień. Możliwość przeglądania tylko własnych wyników, posiadania roli menedżera jednostki organizacyjnej lub lokalizacji, lub administratora. Portal powinien posiadać „Drill down”, co umożliwia rozbicie wyświetlanych danych na poszczególnych użytkowników.
20. Możliwość ustawienia tabelki - widoczność, szerokość i kolejność poszczególnych kolumn może zostać zapisana.
21. Dostosowanie pasku menu Ribbon. Można ustawić własny toolbar oraz zreorganizować pozycje w menu.
22. W zależności od uprawnień użytkownika w Konsoli możliwość ukrycia odpowiednich elementów interfejsu, np. administrator majątku po zalogowaniu widzi tylko elementy dotyczące majątku.
23. Konsola powinna automatycznie wykrywać rodzaj platformy systemu operacyjnego (32b/64b).
24. Tworzenie kopii zapasowej bazy danych bezpośrednio z konsoli programu
25. W związku z rozporządzeniem RODO system powinien umożliwiać monitorowanie modyfikacji w katalogu osób oraz anonimizację danych użytkowników.

Synchronizacja z Active Directory:

1. Zunifikowane ustawienia połączenia z AD dla komputerów oraz osób.
2. Wsparcie wielu domen - dla komputerów oraz osób można ustawić dowolną ilość domen lub kontenerów, które będą synchronizowane.
3. Automatyczne zmiany stanu komputerów usuniętych z AD - system powinien automatycznie zmieniać stan na Usunięty w przypadku komputerów, które zostały usunięte lub wyłączone w Active Directory.
4. Wczytanie nowych komputerów z AD i zapisanie ich DB – zapisywanie do bazy danych nowych komputerów znalezionych w AD, które nie zostały jeszcze zaudytowane.
5. Automatyczna synchronizacja obiektów nie tylko dla osób, ale również dla komputerów.

III. Funkcja audytu

Podstawowe wymagania:

1. Audyt sprzętu i oprogramowania

2. Ewidencja i zarządzanie majątkiem
3. Zarządzanie licencjami
4. Zdalna instalacja oprogramowania
5. Zdalne zarządzanie komputerami

Audyt

1. Możliwość przeprowadzenia audytu na komputerach z systemami: Windows 8.1, Windows 10, Windows 2012 Serwer, Windows Serwer 2016, Windows Serwer 2019
2. Możliwość audytu w trybie jawnym i „ukrytym” (bez wymaganej interakcji po stronie użytkownika)
3. Zbieranie szczegółowych informacji o sprzęcie i jego podzespołach (procesorach, pamięciach, płytach głównych, dyskach twardej, nośnikach danych, urządzeniach wej/wyj, itp.) wraz z numerami seryjnymi (lub możliwość ręcznego dopisania numerów seryjnych).
4. Identyfikacja systemu operacyjnego wraz z kluczem licencyjnym i numerem seryjnym
5. Identyfikacja oprogramowania, a w przypadku składników pakietu MS Office identyfikacja wersji, klucza licencyjnego i numeru seryjnego (o ile znajduje się lokalnie na komputerze).
6. Możliwość regulacji szczegółowości rozpoznawania wersji dla każdego programu (np. możliwość grupowania wersji 4.x lub 4.1.x, itd.)
7. Możliwość zbierania informacji o wszystkich plikach na dysku (definiowanie dowolnych rozszerzeń, wszystkie typy plików)
8. Dodatkowe informacje z rejestrów systemowych i MSI
9. Możliwość dołączania elektronicznych dokumentów do wybranych pozycji w majątku lub licencji (faktury, dokumenty, oprogramowanie, drivery itd.)
10. Możliwość zebrania dodatkowych informacji podczas audytu za pomocą ankiety wyświetlonej na ekranie użytkownika
11. Audyt urządzeń z systemem Android za pomocą aplikacji mobilnej. Zbieranie danych na temat zainstalowanych programów oraz informacji o sprzęcie. Audytowane urządzenie z Androidem powinno automatycznie być wpisane do majątku tak jak w przypadku komputera, włącznie z możliwością wydrukowania protokołu zdawczo-odbiorczego.
12. Audytowanie urządzeń z Androidem w ramach standardowych licencji.
13. Integracja funkcjonalności/modułu Audytu z funkcjonalnością/modułem HelpDesk – dostęp do aktualnych wyników z audytu przez webowy interfejs z poziomem uprawnień serwisanta.

IV. Raportowanie

Wymagania:

1. Informowanie o wygasających licencjach i gwarancjach
2. Zbiorcze statystyki audytu dla poszczególnych jednostek organizacyjnych oraz lokalizacji.
3. Raport zainstalowanego oprogramowania w sieci, zestawienia licencjonowanych i nielicencjonowanych programów.
4. Rozmiar wolnego miejsca na partycjach dysków (w MB i w %).
5. Ilość, rozmiar, rozszerzenie oraz dokładna lokalizacja (ścieżka dostępu) plików danych i plików multimedialnych.
6. Automatyczne porównywanie zmian pomiędzy stanem aktualnym a poszczególnymi audytami dla oprogramowania i sprzętu.

7. Możliwość filtrów automatycznych, szybkiego fulltextowego wyszukiwania w tabelach oraz obliczeń statystycznych w kolumnach.
8. Raportowanie za pomocą wykresów (z tego minimum 5 rodzajów wykresów 3D).
9. Możliwość tworzenia dokumentów dotyczących przekazania majątku, np.: protokół przekazania komputera, telefonu, monitora, karta majątku itp.
10. Otwarta baza SQL (możliwość tworzenia własnych raportów – zapytań SQL bezpośrednio z programu).
11. Wbudowany designer raportów, możliwość pracy z szablonami raportów.
12. Dashboard - kokpit nawigacyjny. Najważniejsze informacje dotyczące oprogramowania, licencji, sprzętu, majątku IT, z możliwością dostosowania na jednym ekranie.
13. Działania na majątku powinny umożliwiać generowanie raportów bezpośrednio z formularza działania. Możliwość ustawienia domyślnego raportu dla poszczególnych działań.

V. Licencjonowanie i baza wzorców

1. Zarządzanie posiadanymi licencjami – bieżące śledzenie licencji i porównywanie zakupionych licencji z użytkowanymi.
2. Możliwość wprowadzania licencji Upgrade, czasowych, ewidencja licencji CAL, MOLP, OEM.
3. Możliwość przypisania różnych programów lub wielu wersji programu do jednej licencji. Licencje powinny być automatycznie przeliczane wg ustawionego priorytetu (np. pod jedną pozycję wpisujemy 10szt. licencji systemu operacyjnego a licencja może obowiązywać dla Windows 8.1 oraz Windows 10)
4. Zarządzanie oraz przypisywanie licencji ma być w pełni zautomatyzowane. Dla multilicencji lub licencji retailowych powinna być możliwość oprócz automatycznego przypisywania również automatycznego odbierania odbierania licencji. Jeżeli program zostanie usunięty z komputera, licencja wróci do puli wolnych licencji. Jeżeli program zostanie zaktualizowany to, jeżeli licencja na to pozwala, zostanie przeniesiona na aktualną wersję programu.
5. Identyfikacja zainstalowanego oprogramowania na podstawie własnej bazy wzorców aplikacji, programów i pakietów – system sam natychmiast automatycznie.
6. Bezterminowe uprawnienia do aktualizacji bazy wzorców aplikacji, programów i pakietów (bez konieczności wykupienia wsparcia, subskrypcji, abonamentu itp.).
7. Rozpoznawanie oprogramowania na podstawie wzoru generycznego (automatyczne wykrycie i rozpoznanie nowej wersji oprogramowania już wcześniej zidentyfikowanego programu)
8. Możliwość edycji bazy wzorców – tworzenie reguł, wyjątków

VI. Zarządzanie majątkiem

Wymagania:

1. Możliwość ewidencjonowania dowolnego sprzętu komputerowego (skaner, drukarka, pendrive, switch, komórka itd.)
2. Możliwość zachowania danych dotyczących wycofanego komputera w bazie danych nie zajmując licencji systemu audytującego.
3. Możliwość importu sprzętu do programu z pliku csv
4. Możliwość dodania własnych pól dla obiektu majątku
5. Rejestrowanie napraw sprzętu
6. Przeglądy majątku - umożliwia wykonywanie cyklicznych działań, takich jak regularne przeglądy, testy czy serwis. System ostrzega o zbliżających się przeglądach za pośrednictwem komunikatów, lub wysyłając maila pod wskazane adresy.
7. Możliwość wykonania działania na majątku na wielu pozycjach równocześnie. Zbiorcze działania muszą umożliwiać szybkie przenoszenie do magazynu, przeniesienia pomiędzy jednostkami, lokalizacjami lub osobami.

8. Możliwość generowania raportów w postaci list majątku, kart, specyfikacji, protokołów przeniesienia, usunięcia z możliwością uruchamiania bezpośrednio z ekranu Majątku i dodatkowo przy wykonywaniu działania na majątku. Generowanie raportów bezpośrednio z formularza działania. Nowe raporty, jako wariant karty (jedna pozycja na jednej stronie) oraz listy (skrótowy raport, lista pozycji na jednej stronie). Raport dla kodów kreskowych. Możliwość samodzielnego tworzenia i modyfikowania kart/wzorów raportów.
9. Generowanie raportów do zdalnego zatwierdzenia przez użytkowników np. w przypadku przypisania sprzętu do nowego użytkownika. Proces powinien odbywać się przez portal www.
10. System powinien posiadać aplikację na urządzenia z systemem Android do skazywania kodów kreskowych (zamiast terminali). Możliwość identyfikacji majątku według kodu kreskowego oraz od razu sprawdzenia czy pozycja znajduje się w bazie majątku. Możliwość wprowadzanie nowych pozycji majątku podczas inwentaryzacji z określeniem dokładnego położenia majątku (piętro, pokój, użytkownik itp.), daty inwentaryzacji.
11. Inwentaryzacja za pomocą dedykowanego webowego portalu aplikacji. System powinien wysłać mail-a do pracowników z linkiem umożliwiającym potwierdzenie lub skorygowanie informacji o posiadanym sprzęcie.
12. Automatyczne tworzenie historii komputera – możliwość stwierdzenia, kiedy np. doszło do zmiany użytkownika komputera bez aktywnego wprowadzenia informacji o przeniesieniu.
13. Możliwość powiązania dokumentów oraz licencji z konkretną jednostką organizacyjną oraz lokalizacją

VII. Zdalne zarządzanie

1. Możliwość zdalnego zarządzania stacjami: przejęcie kontroli (przejęcie obecnej sesji użytkownika), przesyłanie wiadomości, sprawdzenie jakości połączenia, możliwość kopiowania plików, przejmowanie monitora, myszy, klawiatury; zdalne wyłączanie komputera, zdalny restart.
2. Skanowanie otwartych i zamkniętych portów
3. Skanowanie stanu usług w momencie audytu
4. Zdalne zarządzanie usługami (status, sposób uruchomienia)
5. Remote Desktop Protocol (RDP) – zdalny pulpit dostępny bezpośrednio z programu
6. Zdalny pulpit również poza siecią lokalną - połączenie powinno być realizowane za pomocą elementu pośredniczącego, który może być umieszczony w strefie zdemilitaryzowanej (DMZ) lub gdziekolwiek w Internecie.

VIII. Zdalna dystrybucja

1. Instalacja (bez ograniczenia wielkości pliku instalacyjnego), odinstalowanie, odinstalowanie paczek msi, kopiowanie, kasowanie plików i katalogów, uruchamianie skryptów lub plików, wyłączenie i restart komputera, wylogowanie użytkownika (również poza siecią lokalną)
2. Możliwość zdefiniowania kilku serwerów, z których będą przebiegały instalacje.
3. Możliwość zdefiniowania serii działań, które są zależne od siebie, z kontrolą poprawności wykonania działania, jeśli będzie nieprawidłowe, następne działanie nie zostanie uruchomione.
4. Możliwość zaplanowania instalacji niezależnie od tego czy wybranego komputery są włączone lub wyłączone
5. Przewodnik dystrybucji, który umożliwia zaplanowanie instalacji na wybranych komputerach. Zdefiniowanie dni, w których ma przebiegać instalacja oraz czasu, w którym mają być wykonywane zaplanowane działania.

IX. Alertowanie zdarzeń

1. Za pomocą maila oraz „wyskakujących okien” – powiadomień.
2. Możliwość definiowania dni poprzedzających notyfikację związaną z zdarzeniem (np. miesiąc przed, tydzień przed, dzień przed i każdy dzień po terminie).
3. Powiadomienia o wygasających licencjach i gwarancjach.
4. Dzielne raporty z audytu z możliwością definiowania min. 3 własnych raportów
5. Wysyłanie powiadomień związanych ze zbliżającym się terminem przeglądu, lub listą urzędzeń, na których nie zostały wykonane czynności serwisowe w terminie.
6. Wysyłanie alertów/maila w przypadku usunięcia użytkownika z Active Directory z informacją o tym, że powinien oddać przypisany mu majątek IT.
7. Dostęp do raportów z poziomu przeglądarki www.

X. Funkcja monitorowania

Podstawowe wymagania:

1. Monitoring i blokowanie aplikacji
2. Monitoring i blokowanie stron www
3. Monitoring i blokowanie dysków USB
4. Monitoring wydruków
5. Monitoring obciążenia komputerów

Monitoring

1. Monitoring czasu pracy w aplikacji, ilość uderzeń w klawiaturę, ilość kliknięć myszką, podział czasu działania aplikacji na czas pracy (od momentu włączenia do momentu wyłączenia aplikacji) oraz czas aktywności (rzeczywisty czas aktywności użytkowników, okno „on top” na ekranie), statystyki wg czasu, grup, aplikacji
2. Możliwość ustawienia czasu nieaktywności (timeout naliczania aktywności) - po określonym czasie nieaktywności, licznik czasu spędzonego pracą w aplikacji, zostanie zatrzymany.
3. Informacje o odwiedzanych przez użytkowników stronach www: czas, statystyki wg domeny, czasu, użytkownika, konkretnych stron, czas pracy, czas aktywności użytkownika, dokładny adres strony www – aktywny odnośnik, tytuł strony.
4. Monitoring obciążenia procesora i wykorzystania pamięci
5. Monitoring ruchu na kartach sieciowych komputera. Monitorowana jest ilość pobranych (download) oraz wysłanych (upload) danych.
6. Monitoring wydruków (jakie dokumenty, ile, z jakiej drukarki, kiedy, jaki użytkownik drukował, wysokość i szerokość kartki, liczba kopii, kolor, wydruk obustronny)
7. Monitoring zmian na dyskach USB (zmiana nazwy pliku, wielkości, kasowanie pliku, itp.)
8. Monitoring zmian w wybranych katalogach zarówno lokalnych jak i sieciowych (zmiana nazwy pliku, wielkości, kasowanie pliku, modyfikacja itp.)
9. Podstawowe informacje o komputerze użytkownika (dane użytkownika, nazwa komputera, zalogowany użytkownik, adres IP, adres MAC)
10. Ustawienie przedziału czasowego monitoringu (np. od 7:00 do 15:00), wyłączenie monitorowania w weekendy itp..
11. Automatyczna aktualizacja agentów monitoringu – możliwość określenia częstotliwość sprawdzania nowej wersji agentów lub konfiguracji. Możliwość określenia częstotliwość wysyłania wyników monitoringu ze stacji.
12. Możliwość wyłączenia poszczególnych dziedzin monitoringu: www, aplikacje, obciążenie procesora, obciążenie pamięci RAM, monitoring wydruków, czas zalogowania / wylogowania użytkownika.

13. Tworzenie dowolnej ilości profili monitoringu – możliwość określenia w jakim zakresie będą poszczególne grupy komputerów monitorowane lub ograniczane.
14. Opcja wyświetlania komunikatu o włączeniu monitoringu podczas startu agenta
15. Monitorowanie urządzeń z systemem Android. Zbierane są informacje na temat uruchamianych aplikacji, jak długo były na pierwszym planie, dokładnym czasie uruchomienia oraz wyłączenie.

Blokowanie

1. Blokowanie aplikacji – możliwość zdefiniowania aplikacji zabronionych i uniemożliwienie ich uruchomienia (także w przypadku kiedy użytkownik zmieni nazwę pliku uruchamialnego), z możliwością notyfikacji mailowej na wskazany adres lub wyświetlenia okna z ostrzeżeniem na ekranie użytkownika.
2. Blokowanie stron www, blokowanie wszystkich protokołów dla danej domeny, takich jak: http, https, ftp, imap, pop3, smtp, itp.
3. Blokowanie dysków USB wg numery seryjnego oraz sygnatury dysku.
4. Autoryzacja dysków USB - definiowanie „białej listy” dysków USB i blokowanie nieautoryzowanych.
5. Blokowanie napędów CD/DVD

Raportowanie

1. Zestawienia raportów do druku (czasowe, wg użytkownika, wg kategorii, zbiorcze itp.)
2. Wyniki monitoringu można sortować/filtrować wg jednostki organizacyjnej, lokalizacji, nazwy komputera, użytkownika....
3. Powiadamianie (alerty) mailowo np. podczas przekroczenia zdefiniowanego poziomu obciążenia RAM, procesora CPU oraz w przypadku kończącego się miejsca na dysku. (definicja poziomu w procentach oraz minimalny czas, po którym może dość do powtórnego wysyłania notyfikacji)
4. Graficzne przedstawienie wyników – 3D wykresy (minimum 5 rodzajów) z legendą lub bez legendy
5. Raporty menadżerskie graficzne wybranej grupy użytkowników (TOP 5 itp.), którzy korzystają z niepożądanych programów, gier, komunikatorów, multimediów, niepożądanych www, gier i rozrywki, portali społecznościowych, sklepów internetowych, użytkowników najwięcej drukujących dokumenty, wykonujących działania na USB, częstotliwość podłączeń USB, komputerów najbardziej obciążających CPU i RAM.
6. Dashboard dla monitoringu aktywności. Szybkie zestawienia dotyczące różnych aspektów zachowania użytkowników.
7. Dwupoziomowa kategoryzacja programów wg wykorzystania (np.: praca, zabawa, zabronione...) oraz wg typu programu (np.: gry, przeglądarki, antywirusy...)
8. Dwupoziomowa kategoryzacja stron www wg wykorzystania (zakazane, rozrywka, wiadomości, i inne) oraz ich tematów (np. dla kobiet, sport, polityka, hazard ...)
9. Oś czasu pracy - wyświetla chronologicznie działania użytkownika w ciągu dnia od momentu zalogowania się aż po wylogowanie. Raport łączący wyniki z aplikacji oraz www.
10. Dostęp do wyników z monitoringu przez www, nadawanie uprawnień dostępu do wyników wybranym osobą.

XI. Funkcja HelpDesk

Podstawowe wymagania:

1. Zarządzanie zgłoszeniami
2. Historia zgłoszeń

3. Kategorie i priorytety zgłoszeń
4. Baza wiedzy
5. Integracja z e-mailem

Ogólne

1. System umożliwia integrację z Active Directory oraz autoryzację na poziomie AD.
2. Możliwość zgłaszania problemu za pomocą maila z możliwością załączenia dowolnych załączników, które są zapisywane w historii modułu HD, również dla adresów mailowych spoza organizacji.
3. Zintegrowany moduł helpdeskowy z oprogramowaniem audytującym – wykorzystanie danych z audytu bezpośrednio w interfejsie helpdesku. Wgląd do konfiguracji (sprzęt, oprogramowanie) komputera bezpośrednio z poziomu zgłoszenia użytkownika

Raporty

1. Możliwość raportowania z poziomu konsoli i przeglądarki. Raporty ilościowe, czasowe itd.
2. Ewidencja kosztów (czas, finanse) związanych ze zgłoszeniem
3. Działania na tabelce – można filtrować, grupować pola, ustawiać szerokość, kolejność kolumn
4. Użytkownik powinien mieć możliwość obejrzenia wykresu stanu wszystkich jego zgłoszeń na głównym ekranie.

XII. Powiadomienia

1. Wbudowany chat - możliwość dodatkowej komunikacji pomiędzy serwisantem a zgłaszającym
2. Mailowa notyfikacja użytkownika oraz serwisanta – nowe zgłoszenie, zmiana stanu zgłoszenia i inne operacje ze zgłoszeniem.
3. Automatyczna kontrola zalegających/nierozwiązanych zgłoszeń.
4. Notyfikacja mailowa:
 - a. możliwość określenia treści maila w HTML
 - b. możliwość definicji tytułu maila
 - c. po zmianie stanu zgłoszenia, przypisaniu serwisanta, po wysłaniu wiadomości (chat)
 - d. wysyłanie maili w osobnym procesie w tle
 - e. przy każdej zmianie stanu zgłoszenia - opcja włączenia/wyłączenia powiadomienia dla poszczególnych rodzajów użytkowników (użytkownik, serwisant, menadżer)
5. Użytkownik może odpowiedzieć na Wiadomość do zgłoszenia bezpośrednio za pomocą maila. Wysłanie odpowiedzi na otrzymany mail spowoduje zaszeregowanie Wiadomości do odpowiedniego zgłoszenia w helpdesku.
6. Możliwość komunikacji ze wsparciem tylko za pomocą klienta pocztowego, bez konieczności logowania się do interfejsu webowego, zgłoszenie jednak jest zapisywane w helpdesku

XIII. Baza wiedzy

1. Baza wiedzy - tworzenie i wyszukiwanie w bazie wiedzy tworzonej z rozwiązanych zgłoszeń (opcja: zgłoszenia pojawiają się chronologicznie, bez konieczności podawania szukanej frazy. Mogą pojawiać się zgłoszenia niezależnie od stanu, lub tylko rozwiązane i zaakceptowane). Opcja – automatyczne dodawanie wszystkich rozwiązywanych zgłoszeń do bazy wiedzy.
2. Baza wiedzy – dwie oddzielne bazy wiedzy – tylko dla serwisantów oraz dla wszystkich użytkowników

3. Tworzenie własnych FAQ (z dodaniem załącznika)

XIV. Obsługa systemu i funkcjonalność

1. Uprawnienia – różne poziomy uprawnień w helpdesku (użytkownik, serwisant, menadżer, administrator)
2. Możliwość załączania wielu elektronicznych załączników do zgłoszenia
3. Możliwość ustawienia dostępu do podglądu posiadanego majątku użytkownika
4. Możliwość akceptacji bądź odrzucenia przez użytkowników rozwiązania zgłoszenia
5. Możliwość oceny pracy serwisanta
6. Możliwość wykonywania grupowych operacji na zgłoszeniach.
7. Wielopoziomowa kategoryzacja zgłoszeń – nieograniczona liczba poziomów
8. Przypisywanie serwisantów lub grup serwisantów do poszczególnych kategorii bądź podkategorii zgłoszeń
9. Możliwość określania priorytetów (czasu rozwiązania) zgłoszeń niezależnie dla każdej kategorii lub podkategorii
10. Możliwość określenia sztywnego SLA dla każdej kategorii lub podkategorii (np. awarię drukarki rozwiązujemy do 8 godzin, bez możliwości wyboru)
11. Naliczanie czasu potrzebnego do rozwiązania zgłoszenia
12. Możliwość zdefiniowania czasu pracy serwisu (przypisania różnego czasu pracy do poszczególnych kategorii i podkategorii zgłoszeń)
13. Możliwość pracy w trybie, w którym użytkownik określa termin rozwiązania wybierając datę z kalendarza
14. Możliwość określenia czasu pracy serwisu dla poszczególnych dni w tygodniu. Określony czas ma wpływ obliczanie terminu rozwiązania.
15. Możliwość przypisania dowolnych pól danych określonych przez administratora do wybranych kategorii zgłoszeń (można utworzyć formularz zawierający dane typu: data, łańcuch, wartość logiczna itd.)
16. Opcjonalnie nie naliczanie czasu, w którym zgłoszenie jest w stanie "Oczekujący"
17. Formatowanie HTML w szablonach notyfikacji mailowej
18. Możliwość powiązania lokalizację użytkownika z kategoriami - można zdefiniować kategorie, które będą widoczne tylko dla użytkowników (serwisantów) z danej lokalizacji lub jednostki organizacyjnej. Użytkownik nie wybiera lokalizacji, sam system to rozpoznaje.
19. Tworzenie formularzy zgłoszeń - każda kategoria może posiadać specyficzny zestaw pól, które użytkownik wypełni podczas zgłaszania.
20. Dodawanie zgłoszeń podrzędnych - rozbięcie zgłoszeń na zgłoszenia podrzędne - projektowe podejście do zgłoszeń.
21. Zatwierdzanie zgłoszeń - opcja zarządzania procesami akceptacji działań, można ustawić konieczność zatwierdzania zgłoszeń w wybranych kategoriach, dodatkowo można utworzyć wnioski o zatwierdzenie do dowolnego zgłoszenia.
22. Automatyczne tworzenie zgłoszeń ze scenariusza – opcja tworzenia scenariusza, na podstawie którego, jeżeli zgłoszenie pojawi się w wybranej kategorii, zostanie automatycznie utworzone zgłoszenia podrzędne (przykład: jeżeli w firmie pojawi się nowy pracownik, przy okazji głównego zgłoszenia zostaną wygenerowane zgłoszenia do wszystkich osób, które muszą przygotować nowe stanowisko pracy – utworzyć konta w systemach, wyposażyć w sprzęt lub na przykład przygotować służbowy samochód. Prośby o zatwierdzenie niektórych czynności do osób decyzyjnych powinny również zostać wygenerowane automatycznie.
Możliwość ustawienia dla każdej kategorii, różne poziomy zatwierdzeń (zatwierdzenie przez jednego z przypisanych zatwierdzających, czy wszyscy zatwierdzający muszą wyrazić zgodę, by móc pozytywnie zamknąć dane zgłoszenie).

XV. Instrukcja dla administratorów

1. Wykonawca przeprowadzi instrukcję powdrożeniową omawiającą wszystkie wdrożone komponenty. Instrukcja będzie dotyczyła konfiguracji oraz administracji dostarczonego oprogramowania dla administratorów Zamawiającego.
2. Instrukcję poprowadzi pracownik Wykonawcy, który brał aktywny udział w projekcie wdrożeniowym.
3. Instrukcja odbędzie się w postaci spotkań online.
4. O terminie realizacji Instrukcji Wykonawca poinformuje Zamawiającego z co najmniej dziesięciodniowym wyprzedzeniem.
5. Instrukcja musi trwać minimum 2 (słownie: dwa) dni roboczych w wymiarze, co najmniej 12 godzin zegarowych efektywnych zajęć.
6. Wykonawca zapewni uczestnikom odpowiednie materiały dotyczące Systemu zarówno w formie elektronicznej i papierowej.
7. Program Instrukcji powinien obejmować zagadnienia związane z czynnościami konfiguracyjnymi i administracyjnymi wdrożonego systemu.
8. Instrukcja musi być przeprowadzona w języku polskim.
9. W instrukcji będzie uczestniczyć maksymalnie 8 osób

XVI. Dokumentacja powdrożeniowa

Wykonawca zapewni i dostarczy w formacie DOC/DOCX dokumentację powykonawczą, która będzie:

- a) sporządzona w języku polskim;
- b) zawierać nazwę dokumentu;
- c) zawierać metrykę dokumentu (data, numer wersji, historia zmian, autor);
- d) zawierać spis treści;
- e) zawierać słownik pojęć;
- f) zawartość merytoryczną.