

Załącznik nr 1 – Opis przedmiotu zamówienia

W ramach przedmiotowego postępowania wymagane jest dostarczenie dla 850 zasobów oraz 6 kont dedykowanych pracowników obsługi informatycznej licencji, realizujących poniższe wymagania podstawowe oraz funkcjonalne.

1. Wymagania podstawowe dla Systemu

- 1.1 Instalacja wszystkich modułów oprogramowania w postaci pojedynczej kompilacji (jeden plik wykonywalny).
- 1.2 Wszystkie funkcjonalności modułów oprogramowania dostępne są w chwili instalacji oprogramowania.
- 1.3 Oprogramowanie musi zapewniać możliwość jednoczesnej pracy co najmniej 6 pracowników obsługi informatycznej oraz przechowywanie informacji o co najmniej 850 elementach konfiguracji w bazie konfiguracji.
- 1.4 Oprogramowania działa agentowo.
- 1.5 Wszystkie moduły oprogramowania są ze sobą wzajemnie zintegrowane.
- 1.6 Interfejs oprogramowania musi być dostępny w języku polskim i angielskim.
- 1.7 Dostęp do wszystkich modułów oprogramowania, w tym pełna konfiguracja systemu musi być w całości realizowana poprzez interfejs przeglądarki internetowej bez konieczności instalowania dodatkowych komponentów.
- 1.8 Oprogramowanie musi zapewniać dostęp do interfejsu z przeglądarek – Edge, Chrome, Firefox.
- 1.9 Oprogramowanie musi umożliwić realizację połączeń z aplikacją poprzez bezpieczny kanał komunikacji, oparty co najmniej na protokole https i certyfikatach kwalifikowanych.
- 1.10 Oprogramowanie musi umożliwiać integrację użytkowników aplikacji z grupą roboczą, domenami Active Directory lub katalogiem LDAP, pojedyncze logowanie do aplikacji oraz autentykację SAML bez konieczności instalowania dodatkowych aplikacji.
- 1.11 Oprogramowanie serwera musi pracować na użytkowanym przez Zamawiającego systemie operacyjnym Microsoft Windows w wersji 64 bitowej oraz współpracować z bazą danych PostgreSQL (Postgres) oraz MS SQL.
- 1.12 Oprogramowanie serwera musi posiadać własny serwer www.
- 1.13 Oprogramowanie musi posiadać własny wbudowany interfejs, przez który odbywa się konfiguracja bazy danych.
- 1.14 Oprogramowanie musi posiadać wbudowany interfejs, pozwalający na łatwe wykonywanie kopii zapasowych i ich odtwarzania, bez potrzeby dodatkowego edytowania plików konfiguracyjnych, również z możliwością jednoczesnej archiwizacji załączników.
- 1.15 Oprogramowanie musi posiadać wbudowany interfejs pozwalający na konfigurację powiadomień, bez potrzeby dodatkowego edytowania plików konfiguracyjnych.
- 1.16 Oprogramowanie musi posiadać własną wersję darmowej aplikacji mobilnej, na systemy Android i iOS.
- 1.17 Oprogramowanie musi posiadać możliwość uruchomienia dwuskładnikowego logowania przy użyciu poczty elektronicznej.

2. Wymagania funkcjonalne dla Systemu

- 2.1 System musi posiadać możliwość zarządzania urządzeniami z systemami Windows (10 i wyższe), Linux (Ubuntu 10.04, Red Hat Enterprise Linux 8 i wyżej, CentOS 8, Fedora 19, mandriva 2010, Debian 7, Linux Mint 13, OpenSuse 11, Suse enterprise Linux 11), macOS (wersja 10.7 i wyższe), Android (wersja 5.0 i wyższe), IOS (wersja 4.0 i wyższe).
- 2.2 System musi rozpoznawać stacje robocze w ramach usługi katalogowej ora grupy roboczej.

- 2.3 System musi umożliwiać dodawanie załączników do informacji o sprzęcie komputerowym takich jak: faktury, gwarancje w dowolnym formacie.
- 2.4 System musi umożliwiać instalację i deinstalację aplikacji z indywidualnymi ustawieniami dla pojedynczych stacji, określonych grup roboczych, użytkowników lub grup użytkowników.
- 2.5 System musi umożliwiać tworzenie list aplikacji, które będą mogły być instalowane przez samego użytkownika z poziomu stacji roboczej, tzw. Portal samoobsługowy.
- 2.6 System musi posiadać wbudowane funkcje zarządzania i wdrażania łąt systemowych i aktualizacji na stacjach roboczych oraz serwerach, w szczególności rozpoznawać sekwencje instalacji. Funkcje wdrażania łąt obejmują co najmniej oprogramowanie: systemy operacyjne Windows: Vista, 7, 8, 10, 2008, 2012, 2016, Microsoft Office, Google Chrome, Mozilla Firefox, Adobe Reader, Adobe Acrobat, Java.
- 2.7 System musi posiadać możliwość włączenia opcji testowania i zatwierdzania poprawek na wybranej grupie komputerów testowych przed instalacją poprawek w całym środowisku produkcyjnym.
- 2.8 System musi posiadać wbudowane narzędzia rozpoznawania podatności stacji roboczych na zagrożenia w oparciu o brakujące łąty systemowe.
- 2.9 System musi posiadać architekturę umożliwiającą zarządzanie stacjami roboczymi w sieci LAN, WAN bezpośrednio z poziomu serwera centralnego.
- 2.10 System musi posiadać wbudowane narzędzia zarządzania sprzętem komputerowym, w szczególności rozpoznaje komponenty sprzętowe oraz oprogramowanie zainstalowane na stacjach roboczych.
- 2.11 System musi posiadać wbudowane narzędzia zdalnego dostępu (sesji) z wykorzystaniem technologii ActiveX, HTML 5, z możliwością uzyskania potwierdzenia użytkownika oraz ma możliwość włączenia opcji nagrywania tych sesji.
- 2.12 System musi umożliwiać wdrażanie polityk konfiguracji dla systemów Windows, w szczególności polityk dostępu do interfejsu USB, zużycia energii, konfiguracji drukarek i przeglądarek Edge, Chrome, Firefox.
- 2.13 System musi posiadać możliwości konfiguracji polityk dostępu do USB umożliwiających blokowanie co najmniej poniższych typów urządzeń, a także mieć możliwość wykluczania z listy zablokowanych konkretnych urządzeń o danym identyfikatorze urządzenia lub danego dostawcy, a dla dysków przenośnych tych, które są szyfrowane za pomocą rozwiązania BitLocker: Mysz, stacja dysków (takie jak napędy USB, zewnętrzne dyski twarde), CD ROM, urządzenia przenośne (takie jak telefony komórkowe, kamery cyfrowe i przenośne odtwarzacze multimedialne), bluetooth, obraz (takie jak kamery USB i skanery), drukarka, modem, urządzenia USB Apple (takie jak iPad, iPhone i iPod, łączące się z programem iTunes).

- 2.14 System musi posiadać wbudowane narzędzia systemowe umożliwiające zdalne uruchomienie stacji roboczych, zdalne zamykanie stacji roboczych, skanowanie, czyszczenie i defragmentację dysków.
- 2.15 System musi posiadać rozbudowany system zarządzania użytkownikami z podziałem na administratora, audytora, gościa, menadżera zasobów, menadżera łąć, z możliwością dodawania nowych ról z określonymi uprawnieniami.
- 2.16 System musi posiadać możliwość włączenia opcji uwierzytelniania dwuskładnikowego, dzięki któremu dostęp do systemu odbywać się będzie poprzez podanie swojego hasła dostępu (lokalnego lub Active Directory) oraz drugiego składnika w postaci jednorazowego hasła wysyłanego e-mailem (funkcja OTP) lub tokenu z aplikacji uwierzytelniającej.
- 2.17 System musi posiadać możliwość uruchamiania instalatora aplikacji z uprawnieniami dowolnego użytkownika.
- 2.18 System musi umożliwiać dodawanie i rozliczanie licencji aplikacji.
- 2.19 System musi umożliwiać wykrywanie zakazanego oprogramowania i uruchamiania działania naprawcze, w tym automatyczne odinstalowanie niepożądanego oprogramowania.
- 2.20 System musi posiadać możliwość włączenia pomiaru wykorzystania wskazanej aplikacji.
- 2.21 System musi posiadać możliwość blokowania plików wykonywalnych EXE poprzez reguły oparte na ścieżce aplikacji lub wartości hash.
- 2.22 System musi umożliwiać uruchamianie zdalnego Menedżera Systemu dla systemu operacyjnego Windows bez potrzeby uruchamiania połączenia zdalnego sesją RDP, który pozwoli na: podgląd i zamykanie uruchomionych procesów na stacji roboczej, podgląd, uruchamianie, zatrzymywanie, zmianę stanu usług na stacji roboczej, uruchamianie zdalnego wiersza poleceń, podgląd, dodawanie i modyfikację rejestru systemowego stacji roboczej, przegląd logów systemowych stacji roboczej, podgląd menedżera urządzeń, podgląd udziałów sieciowych.
- 2.23 System musi umożliwiać generowanie następujących raportów:
 - 2.23.1 Raporty Active Directory:
 - a) aktualnie zalogowani użytkownicy,
 - b) często zalogowani użytkownicy, rzadko logujący się użytkownicy,
 - c) nieaktywni użytkownicy,
 - d) historia logowania użytkownika,
 - e) historia logowania użytkowników na poszczególnych komputerach,
 - f) wykorzystania aplikacji w skali całej organizacji.
 - 2.23.2 Raporty dotyczące poprawek:
 - a) narażone systemy,
 - b) narażone poprawki,
 - c) obsługiwane poprawki,
 - d) brakujące poprawki czekające na zatwierdzenie,
 - e) systemy wymagające ponownego uruchomienia.
 - 2.23.3 Raporty inwentaryzacji:
 - 2.23.4 Raporty dotyczące sprzętu:
 - a) komputery wg systemu operacyjnego,
 - b) komputery wg producenta,
 - c) komputery wg pamięci,
 - d) komputery wg wykorzystania dysku,

- e) komputery wg wieku,
 - f) komputery wg typu urządzenia,
 - g) zmapowane dyski logiczne.
- 2.23.5 Raporty dotyczące oprogramowania:
- a) oprogramowanie według producenta,
 - b) ostatnio zainstalowane oprogramowanie,
 - c) niedozwolone oprogramowanie,
 - d) wykorzystanie oprogramowania przez komputer,
 - e) klucze produktu oprogramowania,
 - f) komputery z/bez określonego oprogramowania,
 - g) podsumowanie zasad pomiaru użytkowania oprogramowania,
 - h) oprogramowanie specyficzne dla użytkownika.
- 2.23.6 Raporty dotyczące licencji:
- a) zgodność licencji,
 - b) licencje do odnowienia.
- 2.23.7 Raporty dotyczące systemu:
- a) użytkownicy grupy systemu,
 - b) komputery wg usług.
- 2.23.8 Raporty dotyczące gwarancji:
- a) gwarancja niedługo wygaśnie,
 - b) gwarancja wygasła,
 - c) niezidentyfikowane komputery.
- 2.23.9 Raporty bezpieczeństwa:
- a) szczegóły antivirus,
 - b) szczegóły bitlocker,
 - c) szczegóły firewall.
- 2.23.10 Raporty skanowania plików multimedialnych:
- a) szczegóły pliku wg kategorii,
 - b) szczegóły pliku wg rozszerzenia,
- 2.23.11 Raporty dotyczące USB – Raport wykorzystania USB.
- 2.24 System musi umożliwiać planowanie raportów i przesyłanie ich w formie pliku PDF, XLSX, CSV na podany adres e-mail.
- 2.25 System musi umożliwiać tworzenie niestandardowych raportów w oparciu o kryteria dostępne z systemu.
- 2.26 System musi umożliwiać tworzenie niestandardowych raportów w oparciu o wysyłanie zapytań SQL do bazy danych z poziomu konsoli zarządzającej.
- 2.27 System musi pozwalać otrzymywać SMS-y dotyczące alertów inwentaryzacyjnych.
- 2.28 System musi umożliwiać kopiowanie plików do folderów, kopiowanie wielu plików i kopiowanie folderów.
- 2.29 System musi umożliwiać zarządzanie flotą urządzeń mobilnych typu smartfony i tablety z zainstalowanymi systemami operacyjnymi: Android 5.0 i wyższe, iOS 4 i wyższe.
- 2.30 System musi pozwalać zatwierdzać uprawnienia żądane przez aplikacje Mac, konfigurując zasady kontroli preferencji polityki prywatności.
- 2.31 System musi obsługiwać usługę VPN Per-App dla urządzeń Mac.

- 2.32 System musi umożliwiać konfigurację tras DNS i Forwarding w Always-on VPN dla urządzeń z systemem Android.
- 2.33 System musi umożliwiać rozpoznawanie i dodawanie urządzeń poprzez: ręczne dodawanie urządzeń, zbiorcze dodawanie urządzeń z pliku CSV, uwierzytelnione dodawanie z jednorazowym kodem i/lub poświadczeniami użytkownika AD.
- 2.34 System musi umożliwiać konfigurację polis / profili - konfiguracja ustawień polis dostępu do zasobów organizacyjnych.
- 2.35 System musi umożliwiać nakładanie restrykcji – szyfrowanie pamięci wewnętrznej urządzenia, ograniczanie użytkownika kamery, Youtube, przeglądarki, itp.
- 2.36 System musi posiadać funkcję Geofencing – możliwość ograniczenia korzystania z urządzeń mobilnych do wybranych regionów geograficznych.
- 2.37 System musi posiadać funkcję Organizacyjny dostęp - zapewnia dostęp do organizacyjnych zasobów jak e-mail, Wi-Fi, VPN.
- 2.38 System musi umożliwiać tworzenie grup urządzeń - tworzenie logicznych grup urządzeń w oparciu o departamenty, lokalizacje i wdrażania polis, restrykcji i dystrybucji aplikacji do wszystkich urządzeń w grupie.
- 2.39 System musi posiadać moduł zarządzania zasobami, który wyświetla informacje o urządzeniu: szczegóły sprzętu, certyfikaty, zainstalowane aplikacje.
- 2.40 System musi posiadać moduł zarządzania bezpieczeństwem obejmujący: kod dostępu: Wymuszenie kodu w celu blokowania nieautoryzowanego dostępu, zdalna blokada: W celu uniknięcia niepowołanego użycia utraconego urządzenia, pełne czyszczenie: usunięcie wszystkich danych z telefonu w celu wycieku danych po kradzieży, organizacyjne czyszczenie: usunięcie tylko danych organizacyjnych i pozostawienie danych prywatnych.
- 2.41 System musi pozwalać na dystrybucję certyfikatów CA na urządzenia z systemem iOS oraz Android, przy użyciu profilu certyfikatu.
- 2.42 System musi lokalizować urządzenia z systemem Windows 10, nawet bez instalowania aplikacji MDM w urządzeniach.
- 2.43 System musi pozwalać na konteneryzację urządzeń z Androidem w wersji 5.0 lub nowszej.
- 2.44 System musi pozwalać na konfiguracje uprawnień i konfiguracje aplikacji.
- 2.45 System musi pozwalać na cichą instalację aplikacji dla systemu Android.
- 2.46 System musi pozwalać na rejestrację urządzeń mobilnych z systemem Windows 10.
- 2.47 System musi pozwalać na reset urządzenia nawet po wygaśnięciu poświadczeń AD.
- 2.48 System musi umożliwiać śledzenie i zabezpieczenie utraconych urządzeń przy użyciu trybu utraconego dla urządzeń z systemem Android oraz IOS.
- 2.49 System musi pozwalać na automatyzację przypisywania użytkowników urządzeniom z funkcją DEP.
- 2.50 System musi pozwalać na przesyłanie zbiorcze szczegółów APN, co ułatwia dystrybucję zasad APN.
- 2.51 System musi pozwalać na wyświetlanie niestandardowych wiadomości i zapewnianie funkcji połączeń na ekranie blokady zagubionego urządzenia itp. na urządzeniach z systemem Android oraz iOS.
- 2.52 System musi pozwalać na powiadomienia e-mail administratorów, gdy zarządzanie urządzeniem zostało odwołane przez użytkowników.
- 2.53 System musi pozwalać na zmianę nazwy urządzenia podczas przekazywania urządzenia.

- 2.54 System musi pozwalać na integrację z wewnętrznym urzędem certyfikacji za pomocą SCEP, aby zautomatyzować dystrybucję certyfikatów klienta na urządzenia z systemem Windows.
- 2.55 System musi pozwalać na obsługę zdalne ponowne uruchamianie urządzeń z systemem Windows 10. Aplikacja powinna pozwalać na obsługę automatycznego usuwania aplikacji / profili powiązanych po usunięciu urządzenia z grupy.
- 2.56 System musi pozwalać na nawiązanie sesji zdalnej na urządzenia Android oraz IOS.
- 2.57 System musi pozwalać na obsługę historii lokalizacji. Dzięki temu administratorzy będą mogli wyświetlać i przechowywać lokalizacje obsługiwane przez urządzenie w określonym przedziale czasu.
- 2.58 System musi pozwalać na wyszukiwanie urządzeń za pomocą numeru telefonu urządzenia.
- 2.59 System musi pozwalać na dystrybucję certyfikatów CA na urządzenia Windows.
- 2.60 System musi pozwalać na wsparcie dla zarządzania komputerami przenośnymi z systemem Windows 10, komputerami stacjonarnymi i tabletami Surface Pro.
- 2.61 System musi pozwalać na rejestrację Android Zero Touch, aby zdalnie zarejestrować flotę urządzeń, przy aktywacji urządzenia bez interwencji użytkownika.
- 2.62 System musi pozwalać na obsługę planowanej usługi Windows Azure AD Automatic Enrollment / Bulk Enrollment, aby bezproblemowo zarejestrować wiele laptopów, komputerów stacjonarnych bez interwencji użytkownika.
- 2.63 System musi pozwalać na obsługę wstępnie zdefiniowanych podstawowych ustawień aplikacji Windows przy użyciu Konfiguracji aplikacji.
- 2.64 System musi pozwalać jednym poleceniem dystrybuować aplikacje, profile i dokumenty do grup / urządzeń.
- 2.65 System musi pozwalać na zarządzanie aktualizacjami systemu operacyjnego w celu zautomatyzowania i zaplanowania aktualizacji systemu operacyjnego na urządzeniach z systemem iOS i Android
- 2.66 System musi pozwalać rejestrować urządzenia za pomocą konta Azure w MDM.
- 2.67 System musi umożliwiać skonfigurowanie adresu URL strony głównej przeglądarki dla urządzeń z systemem Windows.
- 2.68 System musi pozwalać przysyłać wewnętrzne aplikacje o rozmiarze do 1 GB.
- 2.69 System musi pozwalać administratorom wybrać strefę czasową do ustawienia na zarządzanych urządzeniach mobilnych.
- 2.70 System musi pozwalać na obsługę Google Play Protect dla urządzeń z systemem Android.
- 2.71 System musi pozwalać na zabezpieczenie korporacyjnych danych Office 365 na niezarządzanych aplikacjach.
- 2.72 System musi posiadać opcję zarządzania systemami Windows 10 poprzez Modern Management.
- 2.73 System musi pozwalać zbiorczo rejestrować więcej niż 20 komputerów z systemem Windows 1.
- 2.74 System musi pozwalać wyświetlić listę użytkowników w MDM i powiązanych z nimi urządzeniach w widoku dedykowanym.
- 2.75 System musi w ramach zasad ograniczeń zabezpieczeń pozwalać wymuszać na użytkownikach uwierzytelnianie przy użyciu identyfikatora FaceID, aby umożliwić programowi Safari i innym aplikacjom automatyczne uzupełnianie haseł i danych karty kredytowej.

- 2.76 System musi w ramach zasad ograniczeń zabezpieczeń umożliwić zabronić urządzeniom firmowym wykonywania konfiguracji zbliżeniowych dla innych urządzeń, co uniemożliwi takie ustawienia, jak kopiowanie Wi-Fi na niezatwierdzone urządzenia.
- 2.77 System musi pozwalać poznać szczegóły dotyczące sesji użytkownika oraz zakończenia aktualnie aktywnych sesji.
- 2.78 System musi pozwalać na obsługę VPN dla urządzeń z systemem Android, IOS oraz Windows 10.
- 2.79 System musi wyświetlać podstawowe informacje, takie jak IMEI, IMSI, numer telefonu itp. dla urządzeń mobilnych.
- 2.80 System musi umożliwiać zdalne ponowne uruchamianie urządzeń za pomocą jednego polecenia.
- 2.81 System musi umożliwiać konfigurację ustawień prywatności urządzenia, określenie rodzaju danych, które można gromadzić, poleceń do wykonania na urządzeniu itp.
- 2.82 System musi pozwalać na automatyzację aktualizacji aplikacji będących w sklepie aplikacji.
- 2.83 System musi posiadać zintegrowany moduł do wdrażania systemów operacyjnych, które umożliwia przechwytywanie obrazu systemu operacyjnego a następnie pozwala wdrożyć go na komputerach przenośnych i stacjonarnych.
- 2.84 System musi umożliwiać tworzenie tzw. wzorców (ang. Template) dystrybucji obrazów, które pozwalają na dystrybucję przygotowanego obrazu zgodnie z określonymi zasadami takimi jak:
 - a) zadania po dystrybucji obrazu /restart, zamknięcie systemu/,
 - b) zarządzanie tzw. SID,
 - c) możliwość nadania nazwy komputera,
 - d) dodanie komputera do domeny Windows,
 - e) instalacja dodatkowego oprogramowania.
- 2.85 System musi posiadać możliwość tworzenia zadań dystrybucji pozwalających na automatyzację procesu dystrybucji obrazów systemów.
- 2.86 System musi posiadać możliwość podpięcia przygotowanych wzorców dystrybucji (ang. Deployment Template), pozwalający na dystrybucję obrazu przy użyciu kodu, lub wybieranych systemów z dostępnej listy komputerów.
- 2.87 System musi pozwalać na import komputerów z pliku np. CSV.
- 2.88 System musi wspierać następujące metody dystrybucji obrazów: Multicast, Unicast oraz pozwala na tworzenie harmonogramu tej dystrybucji.
- 2.89 System musi posiadać możliwość przechowywania wcześniej zapisanych obrazów w swoim repozytorium.
- 2.90 System musi posiadać możliwość przechowywania informacji o sterownikach, a także zapewnia ich dystrybucję w obrazach.
- 2.91 System musi posiadać możliwość tworzenia bootowalnych mediów a także ich edycję:
 - a) PXE,
 - b) ISO,
 - c) USB.
- 2.92 System musi posiadać repozytorium możliwych do zainstalowania aplikacji po procesie dystrybucji obrazu a także posiada możliwość edycji tych aplikacji.
- 2.93 System musi posiadać możliwość migrowania profili użytkownika podczas dystrybucji obrazów.
- 2.94 System musi posiadać możliwość generowania logów a także wyświetlania listy statusów i wykonanych akcji.

3. Usługi gwarancyjne - Wsparcie

- 3.1 Wsparcie dedykowanego technika podczas wdrożenia oprogramowania w wymiarze nie krótszym niż 5 dni roboczych (40 godzin),
- 3.2 Dostęp do najnowszych aktualizacji oprogramowania (Upgrade, Update i ServicePack),
- 3.3 Zamawiający dopuszcza świadczenie pomocy technicznej środkami komunikacji elektronicznej obejmującej: kontakt telefoniczny, pocztę email, dostęp zdalny. Niezależnie od wybranej metody pomoc ma być świadczona w języku polskim.
- 3.4 Dostęp do polskojęzycznego portalu pomocy technicznej zawierającego bazę wiedzy,
- 3.5 Zamawiający wymaga zdefiniowania priorytetów zgłoszeniom pomocy technicznej na co najmniej trzy kategorie zgłoszeń: priorytet wysoki (P1) – zgłoszenie awarii, priorytet normalny (P2) – zapytanie o możliwość i sposób zrealizowania oczekiwanej funkcjonalności, priorytet niski (P3) – zgłoszenie wady lub zapytanie o przygotowanie nietypowego raportu z kwerendy w oparciu o bazę danych oprogramowania.
- 3.6 Zamawiający wymaga, aby gwarantowany czas reakcji dla poszczególnych priorytetów był nie dłuższy niż: P1 – do 1 godziny, P2 – do 4 godzin, P3 – do dwóch dni roboczych.
- 3.7 Zamawiający wymaga aby gwarantowany czas rozwiązania zgłoszenia był nie dłuższy niż: dla zgłoszeń o priorytecie P1 – do dwóch dni roboczych, P2 – do dziesięciu dni roboczych, P3 – do dwudziestu dni roboczych. Priorytet przydzielany określoneму zgłoszeniu jest ustalany przez pracownika działu pomocy technicznej w oparciu o informacje przekazane przez zamawiającego. Informacja o priorytecie nadanym zgłoszeniu dostępna jest w portalu pomocy technicznej.
- 3.8 Audyt instancji w siedzibie Zamawiającego pod kątem konfiguracji (dwa razy w okresie jednego roku od dnia podpisania protokołu odbioru).
- 3.9 Backup i aktualizacja oprogramowania w siedzibie zamawiającego (na życzenie zamawiającego).
- 3.10 Prace związane z obsługą zgłoszeń w siedzibie zamawiającego (na życzenie zamawiającego).
- 3.11 Obsługę zapytań o sposób realizacji funkcjonalności oprogramowania.
- 3.12 Opracowywanie niestandardowych raportów w ramach systemu (na życzenie zamawiającego).