

OPIS PRZEDMIOTU ZAMÓWIENIA

System Koordynacji Działań Straży Miejskiej Wrocławia

„SKD SMW”

Spis treści

[1. Wprowadzenie 4](#_Toc81503990)

[1.1. Cel dokumentu 4](#_Toc81503991)

[1.2. Definicje i skróty 4](#_Toc81503992)

[1.3. Zakres zamówienia 7](#_Toc81503993)

[1.4. Ograniczenia formalno-prawne 8](#_Toc81503994)

[2. Ogólny opis systemu 10](#_Toc81503995)

[2.1. Kontekst funkcjonowania 10](#_Toc81503996)

[2.2. Charakterystyka użytkowników 11](#_Toc81503997)

[2.3. Główne funkcje systemu 12](#_Toc81503998)

[2.4. Założenia i zależności 13](#_Toc81503999)

[3. Wymagania funkcjonalne i poza funkcjonalne 13](#_Toc81504000)

[3.1. Ogólne 13](#_Toc81504001)

[3.2. Wymogi w zakresie interoperacyjności 14](#_Toc81504002)

[3.3. Administracja systemem 17](#_Toc81504003)

[3.4. Dziennik obsługujący zgłoszenia i interwencje dyżurnego SMW 18](#_Toc81504004)

[3.5. Aplikacja Mobilna SKD PATROL SM – Wymagania 20](#_Toc81504005)

[3.6. Udostępnianie danych do portalu OPEN DATA WROCŁAW 27](#_Toc81504006)

[3.7. e-Usługi publiczne 28](#_Toc81504007)

[3.8. Wymiana danych z CZK UM Wrocławia 29](#_Toc81504008)

[3.9. Wymiana danych z WPiO 29](#_Toc81504009)

[3.10. Wymiana danych z WZN 29](#_Toc81504010)

[4. Straż Miejska 29](#_Toc81504011)

[4.1. Funkcjonariusze 29](#_Toc81504012)

[4.2. Centralny rejestr zgłoszeń 30](#_Toc81504013)

[4.3. Siły i środki 32](#_Toc81504014)

[4.4. Blokady na koła 33](#_Toc81504015)

[4.5. Ewidencja druków 33](#_Toc81504016)

[4.6. Rejestr zapytań CEPIK 36](#_Toc81504017)

[4.7. Rejestr zapytań ŹRÓDŁO 36](#_Toc81504018)

[4.8. Formularze działań i interwencji 36](#_Toc81504019)

[4.9. Dziennik RSOW 37](#_Toc81504020)

[4.10. Kartoteka sprawców 38](#_Toc81504021)

[4.11. Karty MRD-5 38](#_Toc81504022)

[4.12. Statystyki 38](#_Toc81504023)

[4.13. Odholowane pojazdy 39](#_Toc81504024)

[4.14. Obsługa wykroczeń drogowych 40](#_Toc81504025)

[5. Pozostałe wymagania 42](#_Toc81504026)

[5.1. Architektura systemu 42](#_Toc81504027)

[5.2. Wymagania wydajnościowe 42](#_Toc81504028)

[6. Wymagania bezpieczeństwa 43](#_Toc81504029)

[6.1. Bezpieczeństwo danych 44](#_Toc81504030)

[6.2. Bezpieczeństwo Danych Osobowych (RODO) 45](#_Toc81504031)

[6.3. Bezpieczeństwo serwerów aplikacyjnych 46](#_Toc81504032)

[6.4. Serwer baz danych wymagania 47](#_Toc81504033)

[7. Elementy infrastruktury informatycznej, którą Zamawiający zamierza udostępnić do realizacji zamówienia 48](#_Toc81504034)

[8. Warunki realizacji umowy 49](#_Toc81504035)

[8.1. Warunki dostawy i odbioru 49](#_Toc81504036)

[8.2. Scenariusze testowe 49](#_Toc81504037)

[8.3. Przygotowanie danych 50](#_Toc81504038)

[8.4. Odbiór Systemu (w tym poszczególnych Aplikacji) 50](#_Toc81504039)

[8.5. Odbiór dokumentacji 51](#_Toc81504040)

[8.6. Szkolenia 52](#_Toc81504041)

[8.7. Modyfikacje 52](#_Toc81504042)

[8.8 Wprowadzanie zmian (Usuwania błędów) 53](#_Toc81504043)

[8.9. Dostosowanie, Instalacja Systemu, Konfiguracja 55](#_Toc81504044)

[8.10. Warunki i zakres licencji 55](#_Toc81504045)

[8.11. Dokumentacja 59](#_Toc81504046)

[8.11.1. Dokumentacja szkoleniowa 60](#_Toc81504047)

[8.11.2. Dokumentacja Administratora 60](#_Toc81504048)

[8.11.3. Dokumentacja użytkownika 60](#_Toc81504049)

[8.11.4. Dokumentacja powykonawcza 60](#_Toc81504050)

[8.12. Licencja na kody źródłowe 61](#_Toc81504051)

[8.13. Uzupełnianie kodów źródłowych, dokumentacji 67](#_Toc81504052)

[9. Wsparcie techniczne i gwarancja 68](#_Toc81504053)

# Wprowadzenie

# Cel dokumentu

Niniejszy dokument przeznaczony jest dla Wykonawców ubiegających się o udzielenie zamówienia publicznego i stanowi podstawę do przygotowania oferty. Dokument ten w oparciu o postanowienia umowy, będzie stanowił podstawę realizacji prac. Niniejsze opracowanie stanowić będzie bazę dla podejmowania decyzji związanych z odbiorem systemu, czyli do wnikliwej oceny wyników zrealizowanego systemu w odniesieniu do założonych kryteriów akceptacji.

# Definicje i skróty

|  |  |
| --- | --- |
| **Administrator** | Osoba odpowiedzialna za utrzymanie zdolności operacyjnej Systemu. |
| **Aplikacja Mobilna**  | oznacza aplikację, na urządzenia przenośne. |
| **SKD PATROL SMW** | aplikacja mobilna będąca częścią Systemu, dedykowana pracownikom SMW do pracy w terenie z urządzeniami typu smartfon lub tablet. |
| **Baza Danych** | oznacza bazę danych, zawierającą dane niezbędne do działania Systemu |
| **Błąd** | oznacza wadliwe działanie Systemu, którego naprawa wymaga zmian kodu źródłowego. |
| **CEPIK** | System Informatyczny Centralnej Ewidencji Pojazdów i Kierowców zawiera informacje o pojazdach zarejestrowanych w Polsce i kierowcach posiadających polskie prawo jazdy. |
| **Czas reakcji** | oznacza wyszczególnione dni tygodnia oraz podany zakres godzin w tych dniach, podczas których muszą być dostępne operacyjne i techniczne usługi serwisowe, określone w warunkach usług gwarancyjnych; |
| **Dokumentacja** | oznacza dokumentację w formacie i formie uzgodnionej z Zamawiającym, dotyczącą wszystkich elementów Systemu:użytkownika, stanowiącą instrukcję jak użytkownik końcowy ma posługiwać się Systemem wraz z opisem dostarczanych funkcjonalności;Administratora, zawierającą między innymi: opis procedur związanych z przydzielaniem uprawnień lub parametryzacją Systemu, wykaz czynności niezbędnych do wykonania przez Administratora w celu zapewnienia prawidłowego i niezawodnego działania Systemu; powykonawczą;szkoleniową; licencję na użytkowanie Systemu. |
| **Dostawa** | oznacza dostarczenie, instalację i konfigurację Systemu na urządzeniach wskazanych przez Zamawiającego. |
| **Dyżurny** | użytkownik realizujący obsługę zgłoszeń w Systemie. |
| **Dzień roboczy/Dzień** | oznacza dzień roboczy Zamawiającego zgodnie z Regulaminem Pracy Straży Miejskiej we Wrocławiu |
| **Dzień kalendarzowy** | oznacza dzień kalendarzowy. |
| **GPS** | (ang. Global Positioning System) system nawigacji satelitarnej. |
| **IMEI** | (ang. International Mobile Equipment Identity) – indywidualny numer identyfikacyjny telefonu komórkowego GSM lub UMTS. |
| **Instalacja****Systemu** | oznacza wszystkie czynności związane z uruchomieniem i skonfigurowaniem dostarczonego Systemu i AplikacjiMobilnych |
| **Karty MRD 5** | karty rejestracyjne tworzone przez Straż Miejska i przekazywane Komendzie Miejskiej policji według wytycznych zawartych w rozporządzeniu Ministra Spraw wewnętrznych i Administracji z 2 kwietnia 1998 r w sprawie postepowania z kierowcami naruszającymi przepisy ruchu drogowego. |
| **Kod Źródłowy** | oznacza pliki źródłowe, skrypty i inne niestandardowe narzędzia, niezbędne w procesie kompilacji i konsolidacji, wykonania i dalszego utrzymywania Systemu, a także strukturę baz danych i opis struktury baz danych, słowników, definicji. |
| **Konfiguracja Systemu/Konfiguracja** | oznacza wprowadzenie wszystkich parametrów niezbędnych do prawidłowego i optymalnego funkcjonowania Systemu, w szczególności zdefiniowanie uprawnień, słowników i szablonów; |
| **Końcowy Protokół Odbioru**  | oznacza dokument podpisany przez Strony, stwierdzający, że dostarczony System zostały zrealizowany zgodniez Umową, stanowiący podstawę do wystawiania faktur przez Wykonawcę; |
| **SKD SMW** | system informatyczny wspomagający pracę Straży Miejskiej we Wrocławiu. |
| **Modyfikacja** | zakres czynności projektowych i programistycznych związanych z koniecznością usunięcia Błędu lub prac poprawiających ergonomię obsługi Systemu. Modyfikacja obejmuje również zmianę lub rozbudowę funkcjonalności Systemu w zakresie określonym przez warunki Umowy; |
| **Odbiór** | oznacza wszystkie czynności związane z przyjęciem Systemu, przez Zamawiającego z udziałem Wykonawcy, potwierdzony formalnym Protokołem Odbioru; |
| **Oprogramowanie** | oznacza oprogramowanie systemowe, narzędziowe lub ogólnego przeznaczenia; oprogramowanie systemowe obejmuje system operacyjny, zarządzanie systemem i siecią oraz oprogramowanie diagnostyczne; oprogramowanie narzędziowe obejmuje narzędzia programistyczne służące do budowy, kompilacji, modyfikacji, przystosowywania i uruchamiania Oprogramowania Aplikacyjnego, w szczególności narzędzia typu CASE, narzędzia zarządzania bazą danych, kompilatory, interpretatory;oprogramowanie ogólnego przeznaczenia obejmuje min. edytor tekstu, arkusz kalkulacyjny, itp.; |
| **Oprogramowanie Aplikacyjne**  | oznacza System;  |
| **Produkt** | oznacza Oprogramowanie, System, Dokumentację oraz inne elementy dostarczone przez Wykonawcę przedmioty zamówienia |
| **Prawa Autorskie** | oznacza prawa określone przepisami ustawy z dnia 14 lutego1994 r. o prawie autorskim i prawach pokrewnych (Dz.U. z 2006 r. Nr 90, poz. 631 z późniejszymi zmianami); |
| **Przedstawiciel** | odpowiednio upoważniony przedstawiciel Wykonawcy, zaakceptowany przez Zamawiającego, odpowiedzialny za wykonanie umowy przez Wykonawcę; |
| **Role** | oznacza grupę uprawnień, które można łącznie nadać użytkownikowi; |
| **RSOW** | rejestr spraw o wykroczenia prowadzony przez SM |
| **SMW** | Straż Miejska Wrocławia |
| **Specyfikacja** | zestawienie funkcjonalnych i technicznych wymagań dla Systemu; |
| **System** | oznacza oprogramowanie określone w przedmiocie zamówienia; |
| **UMW** | Urząd Miasta Wrocław; |
| **Wersja** | nowa wersja Systemu powstała po wprowadzeniu Modyfikacji i Zmian  |
| **Wersja Podstawowa**  | oznacza wersję Systemu obejmującą funkcjonalność oferowaną przez Wykonawcę na dzień złożenia oferty  |
| **Zamawiający** | Straż Miejska Wrocławia |
| **CZK UM** | Centrum Zarządzania Kryzysowego Urzędu Miejskiego we Wrocławiu. |
| **Zmiana w Oprogramowaniu** | zmiana Oprogramowania i Oprogramowania Aplikacyjnego, wynikająca ze zgłoszonych błędów Oprogramowania lub Oprogramowania Aplikacyjnego. |
|  |  |

# Zakres zamówienia

Zamówienie obejmuje następujące elementy składowe :

1. wykonanie przedmiotu zamówienia zgodnie z wymogami opisanymi w niniejszym dokumencie,
2. Instalację, konfigurację i utrzymanie systemu w okresie gwarancyjnym (12-mcy),
3. zaplanowanie i realizacja szkoleń pracowników Zamawiającego. Szkolenie dla 300 osób w siedzibie Zamawiającego, bez cateringu na sprzęcie Zamawiającego (grupa dyżurnych, grupa kierownictwa, grupa administracyjna, grupa strażników, grupy max 15 osobowe,
4. konfiguracja urządzeń mobilnych Zamawiającego,
5. dostarczenie dokumentacji technicznej i funkcjonalnej całego wdrożonego systemu (dokumentacja powdrożeniowa: zastosowane konfiguracje techniczno-sprzętowe, projekt aplikacji, instrukcja obsługi),
6. 120 roboczogodzin dodatkowych modyfikacji systemu,
7. Udzielenie nielimitowanej liczby licencji oraz gwarancji na dostarczone oprogramowanie

# Ograniczenia formalno-prawne

Wykonawca musi uwzględnić niżej wymienione akty prawne podczas realizacji prac wchodzących w skład niniejszego zamówienia:

* 1. Ustawa z dnia 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych (Dz. U.
	 z 2006 r., Nr 90, poz. 631 z późn. zm.),
	2. Ustawa z dnia 14 lipca 1983 roku o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2011 r. Nr 123, poz. 698 z późn. zm ),
	3. Ustawa o informatyzacji działalności podmiotów realizujących działania publiczne
	 z dnia 17 lutego 2005 (Dz. U. z 2013 r. poz. 235 .),
	4. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006 roku w sprawie niezbędnych elementów struktury dokumentów elektronicznych (Dz. U. 2006, Nr 206, poz. 1517),
	5. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych
	 i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych z dnia 29 kwietnia 2004 r. (Dz. U. Nr 100 poz. 1024) Załącznik Środki bezpieczeństwa,
	6. Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. nr 182 poz. 1228 z późn. zm.),
	7. Ustawa o samorządzie gminnym (tekst jednolity Dz. U. 2001 r. Nr 142, poz. 1591
	 z późn. zm.),
	8. Akty wykonawcze do w/w ustaw,
	9. Rozporządzenie prezesa rady ministrów z dnia 14 września 2011 r. w sprawie sporządzania pism w formie dokumentów elektronicznych, doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych (Dz. U. Nr 206, poz. 1216),
	10. Rozporządzenie Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji
	 w sprawie organizacji i zakresu działania archiwów zakładowych (Dz. U. Nr 14, poz. 67 z późn. zm.),
	11. Rozporządzenia Rady Ministrów z 12 kwietnia 2012 r. w sprawie Krajowych Ram
	12. Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2012 r. poz. 526),
	13. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 21 kwietnia 2011 r. w sprawie szczegółowych warunków organizacyjnych i technicznych, które powinien spełniać system informatyczny służący do identyfikacji użytkowników
	14. (Dz. U. z 2011 r. nr 93. Poz. 545),
	15. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych ( Dz. U. z 2014 r. poz. 1182, ze zm.,
	16. Ustawa z dnia 24 sierpnia 2001 r. – Kodeks postępowania w sprawach
	 o wykroczenia (Dz. U. z 2013 r. poz. 395, ze zm.),
	17. Ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego
	 (Dz. U. z 2013 r. poz. 267, ze zm.),
	18. Ustawa z dnia 20 maja 1971- Kodeks Wykroczeń,
	19. Ustawa z dnia 13 września 1996 r. o utrzymaniu czystości i porządku w gminach,
	20. Ustawa z dnia 26 października 1982 r. o wychowaniu w trzeźwości
	 i przeciwdziałaniu alkoholizmowi,
	21. Ustawa z dnia 11 maja 2001 r. - Prawo o miarach,
	22. Ustawa z dnia 10 kwietnia 1974 r. o ewidencji ludności i dowodach osobistych,
	23. Ustawa z dnia 9 listopada 1995 r. o ochronie zdrowia przed następstwami używania tytoniu i wyrobów tytoniowych,
	24. Ustawa z dnia 21 sierpnia 1997 r. o ochronie zwierząt,
	25. Ustawa z dnia 11 marca 2004 r. o ochronie zdrowia zwierząt oraz zwalczaniu chorób zakaźnych zwierząt,
	26. Ustawa z dnia 14 grudnia 2012 r. o odpadach,
	27. Ustawa z dnia 27 kwietnia 2001 r. - Prawo ochrony środowiska,
	28. Ustawa z dnia 18 lipca 2001 r. - Prawo wodne,
	29. Ustawa z dnia 16 kwietnia 2004 r. o ochronie przyrody,
	30. Ustawa z dnia 5 stycznia 2011 r. - Kodeks wyborczy,
	31. Ustawa z dnia 26 czerwca 1974 r. - Przepisy wprowadzające Kodeks pracy,
	32. Ustawa z dnia 6 września 2001 r. o transporcie drogowym,
	33. Ustawa z dnia 16 grudnia 2010 r. o publicznym transporcie zbiorowym,
	34. Ustawa z dnia 23 lipca 2003 r. o ochronie zabytków i opiece nad zabytkami,
	35. Ustawa z dnia 20 stycznia 2005 r. o recyklingu pojazdów wycofanych z eksploatacji,
	36. Ustawa z dnia 29 lipca 2005 r. o zużytym sprzęcie elektrycznym i elektronicznym,
	37. Ustawa z dnia 20 czerwca 1997 r. - Prawo o ruchu drogowym,
	38. Ustawa z dnia 9 sierpnia 1997 r. o strażach gminnych (Dz. U. z 2013 poz.1383 j.t.),
	39. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 12 listopada 2009 r. w sprawie zakresu i sposobu prowadzenia przez straże gminne (miejskie) ewidencji etatów, wyposażenia oraz wyników działań straży,
	40. Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 17 listopada 2003 r., w sprawie wykroczeń za które strażnicy straży gminnych są uprawnieni
	 do nakładania grzywien w drodze mandatu karnego,
	41. Rozporządzenie Rady Ministrów z dnia 9 grudnia 1994 r., w sprawie dokumentacji
	42. i ewidencji grzywien za wykroczenia, ściąganych w postępowaniu mandatowym oraz organów właściwych w sprawach prowadzenia i rozliczania bloczków mandatowych (Dz. U. Nr 131, poz.663),
	43. Rozporządzenie Prezesa Rady Ministrów z dnia 22 lutego 2002 r., w sprawie nakładania grzywien w drodze mandatu karnego (Dz. U. Nr 20, poz.201
	 z późn.zm.),
	44. Rozporządzenie Ministra Spraw Wewnętrznych z dnia 25 kwietnia 2012 r.,
	 w sprawie postępowania z kierowcami naruszającymi przepisy ruchu drogowego (Dz. U. z 2012 r., poz.488.

# Ogólny opis systemu

# Kontekst funkcjonowania

Przedmiotem zamówienia jest zaprojektowanie i wdrożenie Systemu Koordynacji Działań Straży Miejskiej Wrocławia. System będzie działał jako niezależne oprogramowanie służące do rejestrowania i monitorowania zdarzeń, a także usprawnienia i koordynacji działań SMW. System ten ma zoptymalizować proces zarządzania siłami i środkami na terenie obsługiwanym przez straż miejską oraz zapewnić sprawną koordynację zdarzeń odbywających się na terenie miasta. Ponadto system SKD SMW będzie umożliwiał przekazywanie informacji o zdarzeniach bezpośrednio do patroli pieszych lub zmotoryzowanych za pomocą aplikacji mobilnej. Komunikacja szyfrowana pomiędzy stanowiskami dyżurnych Centrum Kierowania a mobilnymi urządzeniami powinna być zrealizowana z wykorzystaniem sieci GSM. System ma umożliwiać wsparcie dla procesów administracyjnych realizowanych przez straż miejską poprzez możliwość generowania, gromadzenia, udostępniania i archiwizowania całości dokumentacji wytwarzanych na potrzeby prowadzenia wyżej wymienionych procesów. System ma umożliwiać wymianę danych pomiędzy systemami dziedzinowymi do zarządzania miastem na potrzeby SM i UMW tj. systemu KSAT (wprowadzone dane dotyczące mandatów winny zostać przekazane do systemu KSAT poprzez szyfrowane połączenie ftp). System powinien także zapewnić możliwość wymiany danych z systemem teleinformatycznym CZK UM Wrocławia.

# Charakterystyka użytkowników

Z systemu SKD będą korzystać :

1. Użytkownik\Strażnik – pracownik\strażnik zatrudnieni w Straży Miejskiej Wrocławia obsługujący aplikację na stanowisku komputerowym (uprawnienia : przeglądanie, wprowadzanie, generowanie raportów i statystyk)
2. Administrator – pracownicy zatrudnieni w Sekcji Informatyki i Łączności Straży Miejskiej Wrocławia (uprawnienia : administracja Systemem, administracja serwerem baz danych, tworzenie i generowanie raportów),
3. Kierownik – pracownicy na stanowisku kierownika referatu/naczelnika Oddziału zatrudnieni w Straży Miejskiej Wrocławia (uprawnienia : przeglądanie, wprowadzanie, edycja, generowanie raportów i statystyk),
4. Użytkownik mobilny - strażnicy zatrudnieni w Straży Miejskiej Wrocławia obsługujący aplikację mobilną na telefonie typu smartphone, tablecie (uprawnienia : przeglądanie, wprowadzanie, edycja).
5. CZK – funkcjonujący w strukturze Wydziału Bezpieczeństwa i Zarządzania Kryzysowego. Działalność CKZ obejmuje m.in. jest realizację zadań z zakresu ustawy o zarządzaniu kryzysowym oraz koordynacja działań ratowniczych i porządkowo ochronnych na terenie Wrocławia i prowadzona jest ona w ścisłej współpracy ze SMW.
6. Wydział Podatków i (Opłat), którego głównym zadaniem jest ustalanie wymiaru podatków i opłat lokalnych, podatku rolnego, leśnego, opłaty skarbowej oraz opłaty za gospodarowanie odpadami komunalnymi. Współpraca ze SMW występuje w zakresie wymiany informacji nt. podpisanych umów śmieciowych oraz składowisk odpadów niebezpiecznych i dzikich wysypisk.
7. Wydział Zarządzania Należnościami (WZN)-podstawową rolą WZN jest prowadzenie postępowań upominawczych oraz działań z zakresu windykacji w celu odzyskiwania należności pieniężnych Gminy i Skarbu Państwa, w tym mandatów/grzywien wystawionych przez SMW.
8. Interesariusze zewnętrzni – grupa docelowa, do której kierowane są e-usługi publiczne (A2B, A2C)

a. mieszkańcy Wrocławia oraz osoby przebywające na terenie Wrocławia korzystający lub mogący korzystać z działań.

b. przedsiębiorcy prowadzący działalność na terenie Wrocławia.

c. turyści odwiedzający Wrocław.

Istotną grupą docelową nie będącą ani interesariuszami zewnętrznymi, ani wewnętrznymi jest:

- Policja – organ państwowy współpracujący ze SMW w zakresie przekazywania zgłoszeń właściwych kompetencyjnie, wymiany informacji na temat zaistniałych zdarzeń, podjętych w związku z nimi interwencji i czynności, oraz osób biorących w nich udział.

- Sąd - organ państwowy współpracujący ze SMW w zakresie przekazywania dokumentacji o zdarzeniach oraz podjętych w związku z nimi działaniach, a kończących się wnioskiem do sądu o ukaranie.

# Główne funkcje systemu

Dostarczony system musi umożliwiać :

1. przyjmowanie, rejestrowanie i monitorowanie zgłoszeń o zdarzeniach SM,
2. gromadzenie danych o służbach miejskich i instytucjach oraz siłach i środkach potrzebnych do codziennej służby SM,
3. prezentowanie danych na mapach cyfrowych Wrocławia,

**Uwaga: Zamawiający udostępni (w terminie 30 dni od podpisania umowy) mapę Wrocławia oraz protokół wymiany danych.**

1. wymianę danych pomiędzy systemami dziedzinowymi do zarządzania miastem na potrzeby Straży Miejskiej tj. systemu KSAT, dane dot. Mandatów karnych (export),
2. udostępnianie danych [wewnątrz systemu (aplikacja mobilna, aplikacja główna) powierzonych na potrzeby operacyjne SM dla użytkowników tj. danych z ewidencji ludności Żródło, Rejestr Dowodów Osobistych i danych z systemu CEPIK,
3. Dwustronna wymiana danych z CZK UM Wrocławia,
4. Wykorzystywać w systemie API portalu Open Data Wrocław celem bezpośredniego upowszechniania wybranych danych z systemu,
5. prowadzenie w formie elektronicznej wszystkich rejestrów w zakresie działań operacyjnych, co do których straż miejska zobowiązana jest do ich prowadzenia,
6. udostępnianie danych [wewnątrz systemu(Aplikacja mobilna)] powierzonych na potrzeby operacyjne strażników,
7. aplikacja mobilna do obsługi pracy w terenie strażników wg. założonych kryteriów (dot. Pkt 3.5.),
8. e-usługi publiczne : dokonanie zgłoszenia drogą elektroniczną, złożenie prośby o usunięcie urządzenia blokującego drogą elektroniczną, zgłoszenie skargi/wniosku.

# Założenia i zależności

Zaproponowane rozwiązanie SKD musi być kompletne i umożliwiające prawidłowe funkcjonowanie systemu. Zamawiający wymaga aby system wykorzystywał zasoby infrastruktury informatycznej tj. serwerów oraz sieci teleinformatycznej posiadanej przez Zamawiającego. Kalkulacja cenowa winna zawierać wykorzystanie w/w elementów. Wszelkie koszty z realizacja przedmiotu zamówienia ponosi Wykonawca.

# Wymagania funkcjonalne i poza funkcjonalne

# Ogólne

1. Obsługa systemu SKD poprzez przeglądarki internetowe tj. Mozilla Firefox 68 ESR, Microsoft Edge ver. 84, Google Chrome ver. 84 oraz dedykowaną aplikację mobilną w określonym zakresie,
2. System powinien mieć budowę modułową. Moduły mogą być wspólne dla wszystkich lub oddzielne dla wybranych użytkowników,
3. System powinien być tak zaprojektowany, wykonany oraz wdrożony aby umożliwiać dalszy jego rozwój, pozwalając na jego elastyczne dostosowanie do wymogów prawnych jak i funkcjonalnych,
4. W Systemie musi być zawarta pomoc kontekstowa. Wszystkie funkcje, komunikaty, polecenia zawarte w aplikacji, a także instrukcje powinny być dostępne w języku polskim,
5. Aktualizacje Systemu powinny być automatyczne bez konieczności ingerencji na stacjach roboczych jak i bez konieczności posiadania uprawnień administracyjnych użytkownika,
6. Wymagane pola do wprowadzania danych powinny być oznaczone w sposób wyraźny i jednolity dla całego Systemu,
7. System musi posiadać zabezpieczenia przed przypadkowym usunięciem danych,
8. System powinien zapewniać automatyczną archiwizację danych zgodnie z zaplanowanym harmonogramem czasowym: kopie całościowe (dot. bazy danych), kopie przyrostowe.

# Wymogi w zakresie interoperacyjności

Proponowany System Koordynacji Działań Straży Miejskiej Wrocławia musi spełniać wymagania operacyjności wskazane w Rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w *sprawie Krajowych Ram interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz wymagań dla systemów teleinformatycznych -z późn. zm.*

Wdrażanie, eksploatowanie, monitorowanie, przeglądanie, utrzymanie i udoskonalanie zarządzania usługą odbywać się będzie z uwzględnieniem Polskich Norm: PN-ISO/IEC 20000-1 i PN-ISO/IEC 20000-2.

Kodowanie znaków w systemie i dokumentach z niego wysyłanych odbywać się będzie według standardu Unicode UTF-8 określonego przez normę ISO/IEC 10646 wraz z późniejszymi zmianami.

Jednym z najważniejszych aspektów w kontekście planowanych do uruchomienia w ramach projektu e-usług oraz funkcjonalności jest zapewnienie odpowiedniego poziomu ich użyteczności. Na potrzeby opracowania interfejsu użytkownika wykorzystane będą metody projektowania zorientowanego na użytkownika. Podstawowym założeniem metod projektowania zorientowanego na użytkownika jest w pierwszej kolejności określenie potrzeb, zainteresowań i zachowań użytkownika, które stanowią podstawowe założenia do realizacji celów biznesowych, funkcjonalnych i technicznych planowanego rozwiązania.

Zakłada się, że dla interesanta, interfejsem systemu będzie responsywna strona WWW. Aby zapewnić właściwą interakcję użytkowników z systemem, prace projektowe uwzględniać będą zalecenia normy PN-EN ISO 9241-210:2011. W szczególności planuje się w ramach kolejnych etapów projektowania uruchamianie testów i badań z udziałem głównych grup użytkowników projektu, które obejmą:

* określenie kontekstu użycia funkcjonalności,
* sprecyzowanie wymagań,
* wytworzenie makiety,
* weryfikację przygotowanych projektów

W celu zapewnienia wysokiej dostępności usług interfejs będzie zgodny ze standardami WCAG 2.1 z uwzględnieniem poziomu AA, zgodnie z Ustawą z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych.

W zakresie nawigacji system będzie wykonany z uwzględnieniem następujących zasad:

1. obsługa interfejsu w układzie pionowym jak i poziomym
2. intuicyjne odnajdywanie menu i linków,
3. łatwość powrotu do strony głównej i stron poprzednich,
4. przejrzystość układu graficznego strony,
5. stosowanie raz przyjętego układu struktury graficznej konsekwentnie na wszystkich stronach,
6. grupowanie informacji na ten sam temat,
7. stosowanie nagłówków i etykiet,
8. stosowanie kolorystyki w rozróżnianiu stałych elementów struktury strony,
9. stosowanie dużych ikon służących do nawigacji i kolorów sugerujących obecność przycisków nawigacji,
10. widoczny fokus

W zakresie kolorów i kontrastów nawigacji system będzie wykonany z uwzględnieniem następujących zasad:

1. dobieranie kolorów i odcieni łatwo rozróżnialnych,
2. stosowanie kontrastów kolorystycznych między elementami graficznymi oraz pomiędzy nimi i tłem,
3. unikanie tła w postaci obrazów i wzorów (ze względu na trudności w odczytaniu tekstu na takim tle).

W zakresie tworzenia i wprowadzania treści system będzie wykonany z uwzględnieniem następujących zasad:

* 1. Poprawne zawijanie i powiększanie tekstu
	2. Możliwość zmiany rozmiaru tekstu
	3. poprawianie wprowadzanych danych o ile to tylko możliwe
	4. Wysokość linii (odstęp między wierszami) do co najmniej 1,5-krotności rozmiaru czcionki;
	5. Rozstaw następujących akapitów co najmniej 2 razy większy od rozmiaru czcionki;
	6. Odstępy między literami (tracking) do co najmniej 0,12-krotności rozmiaru czcionki;
	7. Odstępy między wyrazami do co najmniej 0,16 wielkości czcionki.
	8. Odrzucanie lub wskazywanie treści spod kursora lub fokusa

Dodatkowo, zgodnie z WCAG 2.1 poziom AAA - przy wypełnianiu formularzy, użytkownicy będą ostrzegani o limicie czasu bezczynności użytkownika, którego przekroczenie może spowodować utratę danych. Podczas tworzenia interfejsów graficznych zostaną przeprowadzone badania UX i zostaną przygotowane stosowne projekty graficzne. Prace będą realizowane zasobami mającymi stosowne kompetencje z zakresu UX. Testy zgodności z WCAG zostaną przeprowadzone w ramach testów akceptacyjnych systemu. Zgodność z WCAG 2.1 jest jednym z wymagań niefunkcjonalnych, jakie postawione zostaną wykonawcy systemu. W zakresie komunikacji z innymi systemami zastosowane zostaną otwarte formaty danych oparte o XML, a wymiana danych zostanie oparta o usługi sieciowe zgodne ze standardem WSDL. Wnioskodawca posiada system zarządzania bezpieczeństwem informacji opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001, zgodnie z którym, ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą, w tym:

* 1. PN-ISO/IEC 27002 - w odniesieniu do ustanawiania zabezpieczeń;
	2. PN-ISO/IEC 27005 - w odniesieniu do zarządzania ryzykiem;
	3. PN-ISO/IEC 24762 - w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania. System zapewnia poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

Wymagania Krajowych Ram Interoperacyjności spełnione będą w wymaganiach dla Systemu:

1. Wymienność - poprzez ustalenie w wewnętrznych procesach biznesowych SMW zasad przetwarzania dokumentacji przez system oraz ustalenie stałych interfejsów wymiany danych z innymi systemami i opisanie ich w taki sposób, aby możliwe było podpięcie się nowej aplikacji do istniejących już interfejsów API w systemie.
2. Wymaganie dotyczące udostępnienia zasobów informacyjnych w co najmniej jednym z formatów podanych w załączniku nr 2 do rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.
3. System będzie posiadał formularz do wprowadzania zgłoszeń dla mieszkańca Wrocławia posadowiony na zewnętrznej stronie www. Formularz będzie musiał spełniać wymagania WCAG 2.1 z uwzględnieniem poziomu AAA, określonego w załączniku nr 4 do rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.
4. Systemu będzie zapewniał środki uniemożliwiające nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji (w tym aplikacji mobilnej).
5. Wymaganiem dla Systemu będzie rozliczalność poprzez odnotowanie w dziennikach Systemu (logach) działanie użytkowników lub obiektów w zakresie dostępu do Systemu z uprawnieniami administracyjnymi, uprawnieniami z dostępem do danych osobowych, zapytań do SRP, konfiguracji Systemu (w tym konfiguracji zabezpieczeń), będzie możliwość przechowywania dzienników Systemu (logów) przez okres 2 lat.

# Administracja systemem

1. Proponowany System musi spełniać normy bezpieczeństwa dotyczące przetwarzania danych wrażliwych w systemach teleinformatycznych w tym danych osobowych,
2. System musi posiadać moduł administracyjny umożliwiający zarządzanie użytkownikami, uprawnieniami, słownikami, raportami a w tym :
	1. Dodawanie, edycję i usuwanie użytkowników/grup użytkowników,
	2. Nadawanie haseł wraz z nadawaniem i odbieraniem uprawnień do poszczególnych funkcji systemu, modułów, ról dla poszczególnych użytkowników,
	3. Edycję wbudowanych słowników systemowych,
	4. Modyfikowanie ustawień konfiguracyjnych systemu,
	5. Tworzenie i edytowanie raportów w całym systemie,
	6. Wyświetlanie, odbieranie i wysyłanie komunikatów systemowych,
	7. Definiowanie i modyfikowanie :
		1. Liczba przechowywanych haseł historycznych,
		2. Okres przechowywanych haseł historycznych,
		3. Okres ważności hasła,
		4. Złożoność hasła,
	8. Obsługa logów systemowych (informacja o wszystkich czynnościach wykonywanych w systemie, filtrowanie po dacie, godzinie, użytkowniku):
		1. Data i godzina logowania,
		2. Login użytkownika
		3. Nazwa komputera
		4. Adres IP
		5. Data i godzina odnotowanej czynności na rekordach
		6. Rodzaj czynności (np. wprowadzenie, edycja, usunięcie)
		7. Treść przed zmianą
		8. Treść po zmianie
	9. Szyfrowanie danych zgodnie z wymogami RODO
	10. Możliwość wysłania hasła jednorazowego za pomocą wiadomości e-mail.

# Dziennik obsługujący zgłoszenia i interwencje dyżurnego SMW

1. System musi posiadać możliwość rejestracji, zakończenia, aktualizacji i przebiegu służby dyżurnego SMW,
2. System musi posiadać możliwość wprowadzania danych o zgłoszeniu, w tym co najmniej :
	1. Imię i nazwisko, adres, numer telefonu osoby zgłaszającej,
	2. Forma zgłoszenia z wyszczególnieniem na : telefon, radiowo, e-mail, osobiście, pisemnie,
	3. Data i czas przyjęcia interwencji wygenerowane automatycznie na podstawie aktualnego czasu systemowego,
	4. Opis interwencji,
	5. Miejsce interwencji (miejscowość, dzielnica, ulica, numer domu, numer lokalu).

Wymagania:

* Minimalna klikalność, ergonomia formatki, słownikowość, autouzupełnianie,
* Automatyczne wyszukiwanie wcześniej zgłaszanych interwencji wpisanego numeru telefonu,
* Szczegółowy widok okna do wprowadzania zgłoszenia zawiera załącznik nr 1 do OPZ.
1. Pozostałe funkcjonalności :
	1. Możliwość zaznaczenia miejsca interwencji na mapie cyfrowej,
	2. Możliwość wielopoziomowej kategoryzacji interwencji – dane pobierane ze słownika systemowego,
	3. Możliwość szybkiego podglądu w nowym oknie zgłoszeń zarejestrowanych dla konkretnego numeru,
	4. Możliwość przypisywania i odwoływania do obsługi interwencji dowolnej ilości patroli. Prezentacja patroli na podstawie dyslokacji. Statusy oraz czynności wraz ze zdjęciami podejmowane przez patrol winny być widoczne w systemie,
	5. Sortowanie patroli według odległości od miejsca zgłoszonych interwencji,
	6. Możliwość definiowania (słowników) instytucji, do których przekazano lub poinformowano o interwencji,
	7. Możliwość wysłania informacji o zdarzeniu w systemie SKD innemu podmiotowi poprzez e-mail wraz ze statusem „przekazano przez e-mail”,
	8. Możliwość wprowadzenia opisu sposobu realizacji zdarzenia,
	9. Wskazanie daty i godziny zakończenia interwencji z możliwością korekty opisu jako uwagi interwencji,
	10. Możliwość nadawania priorytetu oraz statusu zgłoszonej interwencji. Priorytetyzacja na podstawie podświetlenia odpowiednim kolorem w zależności od aktualnego statusu,
	11. Możliwość automatycznego przyjmowania zgłoszenia/interwencji z aplikacji mobilnej SKD PATROL SMW,
	12. Możliwość definiowania zasad numeracji zdarzenia – numeracja domyślna oraz numeracja własna dla każdego oddzielnego Oddziału/referatu SMW np. ZO-0000/2021,
	13. Możliwość wyświetlania czasu oczekiwania zgłoszenia na podjęcie interwencji, na podstawie statystyki z danych gromadzonych w SKD pozyskanej z różnic pomiędzy czasem wprowadzenia interwencji do systemu, przekazania do obsługi przez patrol SMW i podjęcia interwencji do realizacji w zdefiniowanym okresie,
	14. Możliwość wyświetlania zgłoszeń/interwencji wg. priorytetu, daty i czasu przyjęcia, dla poszczególnych patroli, funkcjonariuszy i globalnie (dynamiczny podgląd danych np. w nowym oknie przeglądarki),
	15. Możliwość wizualizacji miejsca zgłoszenia na mapie. Prezentacja zdarzeń w oparciu o wybrane kategorie w określonym przedziale czasowym.
	16. Automatyczne sygnalizowanie przyjmującemu zgłoszenie o podobnych zgłoszeniach (już zarejestrowanych) pod numerem telefonu zgłaszającego, miejscu i rodzaju zdarzenia oraz umożliwienie podpięcia zgłoszenia do istniejącego pierwotnego zgłoszenia interwencji,
	17. System musi posiadać możliwość prowadzenia statystyki : ilościowej, według kategorii zgłoszenia, rodzaju zgłoszenia, typu zgłoszenia, przekazanego do innej instytucji, według dzielnicy i osiedla, ulic, według wprowadzającego, średniego czasu realizacji interwencji,
	18. możliwość generowania automatycznych meldunków ze służby dyżurnych SMW w formacie PDF z informacją o zarejestrowanych zdarzeniach podczas służby. Możliwość przesłania meldunku na zdefiniowane adresy e-mail w systemie SKD. Wszystkie wygenerowanie meldunki powinny być ewidencjonowane w SKD z informacją o dacie jego sporządzenia, numerze meldunku, osobie sporządzającej, oraz mieć możliwość podłączenia załączników pod meldunki. System powinien mieć możliwość edycji wzoru meldunku,
	19. możliwość generowania raportów z wybranych interwencji z wpisami czynności podejmowanymi w ramach danej interwencji,
	20. system SKD powinien mieć tabelarycznie zorganizowaną listę zgłoszeń z możliwością zarządzania kolumnami oraz eksportu zdarzeń do plików CSV, XLS, PDF.
	21. system musi mieć zaawansowaną wyszukiwarkę na liście zgłoszeń umożliwiającą wyszukiwanie złożone np. po: kategorii, podkategorii, dacie, czasie, obszarze, użytkownikach, zgłaszającym, formie kontaktu, miejscu zdarzenia, dacie dodania, priorytecie, statusie,
	22. system musi posiadać możliwość dodania załącznika do sprawy, (co najmniej pliki DOC, DOCX, PDF, JPG oraz plików wideo itp.) z możliwością zdefiniowania rozmiaru pojedynczego pliku (z poziomu administratora), możliwość współpracy systemu SKD z serwerem poczty elektronicznej, dzięki czemu przesłanie zgłoszenia interwencji do SMW drogą elektroniczną będą prezentowane na liście interwencji oczekujących a po przeprowadzeniu weryfikacji zgłoszenia pojawi się na liście zgłoszeń do realizacji (interwencji), możliwość przeglądu historii zarchiwizowanych i zakończonych zgłoszeń.

# Aplikacja Mobilna SKD PATROL SM – Wymagania

Aplikacja mobilna SKD PATROL SMW powinna być opracowana na platformę mobilną systemu Android w wersji 4.0 lub wyższej. Odnosząc się do poufności danych powinna być dedykowana kadrze zarządzającej (komendanci, kierownicy referatów) i kadrze operacyjnej (strażnicy w patrolach). Aplikacja powinna mieć możliwość definiowania dostępu do wybranych baz danych systemu SKD, aby realizować wymienione niżej czynności:

1. Aplikacja dla kadry zarządzającej powinna posiadać następujące funkcjonalności:
	1. Autoryzacja użytkownika z wykorzystaniem haseł zmienianych w trybie dziennym,
	2. Wysyłanie zgłoszeń do dziennika SMW z wykorzystaniem mechanizmu *push notifications*,
	3. Podgląd miejsca zdarzenia na mapie cyfrowej,
	4. możliwość dodawania zdjęć do dokumentacji podjętych interwencji,
	5. Podgląd listy zgłoszeń w dzienniku dyżurnego SM systemu SKD,
	6. Podgląd archiwum interwencji,
	7. Możliwość pracy offline a po osiągnięciu trybu online możliwość przesłania i synchronizacji danych z systemem SKD,
	8. Weryfikacja sprawców zdarzeń w wewnętrznej bazie danych,
2. Aplikacja dla patrolu powinna posiadać następujące funkcjonalności:
	1. Autoryzacja użytkownika z wykorzystaniem haseł zmienianych w trybie dziennym,
	2. Wysyłanie zgłoszeń do dziennika SMW z wykorzystaniem mechanizmu *push notifications*,
	3. Podgląd miejsca zdarzenia na mapie cyfrowej,
	4. Lista oczekujących interwencji do wykonania,
	5. Opis podejmowanych czynności i załatwienia sprawy w ramach przyjętej interwencji,
	6. Możliwość dodawania zdjęć do dokumentacji podjętych interwencji,
	7. Podgląd listy i archiwum zgłoszeń oraz możliwość dodawania do nich informacji,
	8. Weryfikacja sprawców zdarzeń w wewnętrznej bazie danych ,
	9. Możliwość pracy offline a po osiągnięciu trybu online możliwość przesłania i synchronizacji danych z systemem SKD,
	10. Nawigacja do miejsca zdarzenia z wykorzystaniem GPS,
	11. możliwość wprowadzania danych osób ukaranych wymaganych na potrzeby sporządzenia dokumentacji wymaganej do procedowania MK. Strażnik w aplikacji mobilnej wprowadza informacje o sposobie zakończenia interwencji, numer mandatu a dane osoby ukaranej wprowadza na stanowisku operatora w siedzibie oddziału,
	12. Obsługa kodów QR - wypożyczanie sprzętu służbowego (wydawanie i przyjmowanie wybranych składników wyposażenia: radiostacje, pojazdy, aparaty cyfrowe, itp.),
	13. wykaz danych właścicieli pojazdów będących w bazie SKD SMW,
	14. Podział funkcjonalny pulpitu aplikacji wg m.in. n/w schematu:
		1. Interwencje do realizacji – funkcjonalność powiązana z centralnym rejestrem zgłoszeń. Strażnik otrzymuje zgłoszenia do realizacji (wyświetla mu się czas zgłoszenia i temat oraz planowane przerwy) posortowane wg priorytetu z rozróżnieniem kolorystycznym (najwyżej znajdują się zgłoszenia do realizacji w pierwszej). Funkcjonariusz winien mieć możliwość podgląd miejsca zdarzenia na mapie cyfrowej po kliknięciu na odnośnik. Powinna też być opcja nawigacji z wykorzystaniem GPS. W

W przypadku gdy interwencja nie potwierdza się Funkcjonariusz klika przycisk „Nie potwierdza się” co powoduje automatyczne przesłanie właściwego statusu do dziennika. W przypadku potwierdzenia interwencji Funkcjonariusz ma do dyspozycji ekran właściwy do danej kategorii zgłoszenia, możliwość udokumentowania zdarzenia wbudowanym w urządzenie mobilne aparatem cyfrowym. W kolejności funkcjonariusz zaznacza rodzaj podjętych czynności (pouczono, MK, Sąd/notatka służbowa, odstąpiono, zgłoszenie) i w przypadku zwielokrotnienia wykroczenia (np. kilka osób podlegających sankcjonowaniu) ma do wyboru możliwość ponownego wyboru rodzaju podjętych czynności. Szczegółowe dane o rodzaju podjętych czynności winny podlegać uzupełnieniu w systemie (system winien wymuszać konieczność uzupełnienia tych danych przez strażnika po zalogowaniu w aplikacji na komputerze).

* + 1. Odholowanie pojazdu - **Funkcjonariusz podejmujący decyzję o odholowaniu** ma w aplikacji mobilnej dostępne n/w pola:
* zdjęcie tablicy rejestracyjnej
* zdjęcie sytuacji drogowej
* zdjęcie przedniej szyby pojazdu
* zdjęcie znaku drogowego
* nr rejestracyjny
* nr służbowy
* nr dyspozycji [bloczka]
* ulica
* przyczyna wywozu
* lista rozwijana [wykaz pomocy drogowych]
* lista rozwijana [parkingi na które usuwany jest pojazd]
* data i godzina

Dodatkowe funkcjonalności:

* nr dyspozycji z ostatnio odholowanego pojazdu [przez strażnika]
* kopiuj dane z poprzedniego odholowania
* historia odholowanych pojazdów [przez strażnika ]
* historia pojazdu

Pracownik ma możliwość po wybraniu pojazdu [np. z historii odholowanych pojazdów] zmiany statusu pojazdu z listy wyboru.

**Uwagi:**

Przyciski do wykonywania zdjęć-opis funkcji:

* krótkie naciśnięcie przycisku uruchomi aparat fotograficzny umożliwiający wykonanie zdjęcia na miejscu wykroczenia.
* dłuższe przytrzymanie przycisku spowoduje otwarcie galerii zdjęć wykonanych wcześniej na telefonie, można wówczas wybrać zdjęcie zarejestrowane wcześniej.

Pasek statusu sygnału GPS: kolor czerwony oznacza, że nie ustalono pozycji na mapie na podstawie sygnału GPS.

* + 1. Blokady - **Funkcjonariusz zakładając blokadę** klika przycisk „Założenie blokady” jeśli jest kod NFC to go sczytuje a jeśli go nie ma to z listy rozwijanej wybiera przypisaną do pojazdu blokadę dodatkowo wykonuje zdjęcia pojazdu z założoną blokadą, uzupełnia pola: wykroczenie, nr rejestracyjny pojazdu, czas założenia (domyślnie bieżący czas). Po kliknięciu przycisku np. „Wyślij założenie blokady” do systemu przesyłane są w/w dane oraz dane lokalizacyjne.

Dostępne pola:

* zdjęcie tablicy rejestracyjnej
* zdjęcie sytuacji drogowej
* zdjęcie z założoną blokadą
* zdjęcie znaku drogowego
* rejestracja
* nr służbowy
* nr blokady
* ulica
* opis wykroczenia

Dodatkowe funkcjonalności:

* nr ostatnio założonej blokady
* kopiuj dane z poprzedniej blokady
* historia założonych przez strażnika blokad
* historia pojazdu

**Funkcjonariusz zdejmując blokadę** klika przycisk „Zdjęcie blokady” i wybiera z listy rozwijanej założonych blokad (posortowane: najpierw przypisane do pojazdu użytkowanego przez pracownika). W kolejności funkcjonariusz zaznacza rodzaj podjętych czynności (pouczono, MK, Sąd/notatka służbowa, odstąpiono, zgłoszenie) podaje czas zdjęcia blokady(domyślnie bieżący czas) oraz opcjonalnie winien mieć możliwość wykonania zdjęć (np. w przypadku uszkodzenia blokady). Po kliknięciu przycisku np. „Prześlij” do systemu przesyłane są w/w dane.

**Uwagi:**

Przyciski do wykonywania zdjęć-opis funkcji:

* krótkie naciśnięcie przycisku uruchomi aparat fotograficzny umożliwiający wykonanie zdjęcia na miejscu wykroczenia.
* dłuższe przytrzymanie przycisku spowoduje otwarcie galerii zdjęć wykonanych wcześniej na telefonie, można wówczas wybrać zdjęcie zarejestrowane wcześniej. Pasek statusu sygnału GPS: kolor czerwony oznacza, że nie ustalono pozycji na mapie na podstawie sygnału GPS.
	+ 1. Wezwania - **Pracownik wysyłając wezwanie** najpierw wykonuje dokumentację zdjęciową, następnie uzupełnia dostępne pola (Rejestracja, Nr służbowy(automatycznie), Nr wezwania pap., ulica, opis wykroczenia) .

Dostępne pola:

* zdjęcie tablicy rejestracyjnej
* zdjęcie sytuacji drogowej
* zdjęcie przedniej szyby
* zdjęcie znaku drogowego
* rejestracja
* nr służbowy
* nr blokady
* ulica
* opis wykroczenia

Dodatkowe funkcjonalności:

* nr ostatniego zgłoszenia
* kopiuj dane z poprzedniego zgłoszenia
* historia zgłoszeń strażnika
* historia pojazdu

**Uwagi:**

Przyciski do wykonywania zdjęć-opis funkcji:

* krótkie naciśnięcie przycisku uruchomi aparat fotograficzny umożliwiający wykonanie zdjęcia na miejscu wykroczenia.
* dłuższe przytrzymanie przycisku spowoduje otwarcie galerii zdjęć wykonanych wcześniej na telefonie, można wówczas wybrać zdjęcie zarejestrowane wcześniej.

Pasek statusu sygnału GPS: kolor czerwony oznacza, że nie ustalono pozycji na mapie na podstawie sygnału GPS.

* + 1. Zgłoszenie wykroczenia

Funkcjonalność winna umożliwiać zgłoszenie interwencji do Dziennika zgłoszeń przez funkcjonariusza. Funkcjonariusz ma dostępne pole opisowe, możliwość udokumentowania zdarzenia wbudowanym w urządzenie mobilne aparatem cyfrowym. O dalszych czynnościach decyduje operator systemu.

* + 1. Podjęcie czynności własnych - Funkcjonalność winna umożliwiać zgłoszenie interwencji do Dziennika zgłoszeń przez funkcjonariusza. Funkcjonariusz ma dostępne pole opisowe, pola kategorii możliwość udokumentowania zdarzenia wbudowanym w urządzenie mobilne aparatem cyfrowym. Zdarzenie automatycznie przypisywane jest do funkcjonariusza. W kolejności funkcjonariusz zaznacza rodzaj podjętych czynności (pouczono, MK, Sąd/notatka służbowa, odstąpiono, zgłoszenie) i w przypadku zwielokrotnienia wykroczenia (np. kilka osób podlegających sankcjonowaniu) ma do wyboru możliwość ponownego wyboru rodzaju podjętych czynności. Szczegółowe dane o rodzaju podjętych czynności winny podlegać uzupełnieniu w systemie (system winien wymuszać konieczność uzupełnienia tych danych).
		2. Raportowanie działań stałych - Funkcjonalność winna umożliwiać przełożonemu:

wprowadzenie w systemie (na stanowisku operatora) zadania stałego:

* temat zgłoszenia
* kategoria zgłoszenia
* czas obowiązywania „od do” lub bezterminowo
* określenie grupy docelowej ( Wszystkie patrole, Referat, Patrol, pracownik)

Zadanie stałe jest zamykane po upływie terminu jego ważności. Funkcjonalność może być powiązana z dziennikiem zgłoszeń przy czym w takim przypadku winno się wyróżniać (np. kolorystyka, dodatkowy status).

Funkcjonalność winna umożliwić pracownikowi:

oznaczenie podjęcia czynności kontrolnej poprzez kliknięcie zadania stałego i wybrania przycisku:

* Przycisk „Raport” . Po kliknięciu przycisku do systemu przesyłane są dane lokalizacyjne i czasowe powiązane z zadaniem stałym wraz z opisem. Czynność może być wielokrotna.
	+ 1. Pobieranie sprzętu i wyposażenia - Funkcjonariusz przy pomocy urządzenia mobilnego winien mieć możliwość pobrania wyposażenia.

**Pobierając sprzęt** klika przycisk „Pobierz” z listy rozwijanej wybiera właściwą kategorię ( np. radiotelefony, czytniki psów, aparaty cyfrowe, itp.) a następnie wybiera sprzęt bądź wyposażenie, które pobiera oraz winno być pole opisowe formularza na ewentualne uwagi (np. o stanie sprzętu, przebiegu) oraz lista statusów (domyślnie „pobrany niedostępny” jako opcja „zabrany do naprawy”, „odebrany”) .

**Dostępne kolorowe statusy:**

- pobrany niedostępny

- zdany dostępny

- zdany niesprawny

- przekazany do naprawy

- w naprawie

- do odbioru z naprawy

- odebrany

Po kliknięciu przycisku „Zarejestruj pobranie” do systemu winny być przesłane dane o dacie i czasie pobrania sprzętu, pracowniku pobierającym, uwagach, statusie sprzętu .

**Pracownik zdając sprzęt** klika przycisk „Zdaj wszystko”(jeśli bez uwag) lub „Zdaj” ( w przypadku uwag) i w tym z listy rozwijanej wybiera właściwą kategorię ( np. radiotelefony, czytniki psów, aparaty cyfrowe, itp.) a następnie wybiera sprzęt bądź wyposażenie, które pobiera oraz winno być pole opisowe formularza na ewentualne uwagi (np. o stanie sprzętu, przebiegu) oraz lista statusów (domyślnie „zdany dostępny” jako opcja „zdany niesprawny”, „w naprawie”) .

Po kliknięciu przycisku „Zarejestruj zdanie” do systemu winny być przesłane dane o dacie i czasie zdania sprzętu, pracowniku zdającym, uwagach, statusie sprzętu.

# Udostępnianie danych do portalu OPEN DATA WROCŁAW

U podstaw analizy danych, które zostaną wystawione jako informacja publiczna leży zatem analiza prawodawstwa, jak również wieloletnia praktyka w udostępnianiu informacji publicznej, zarówno tej która umieszczana jest na BIP Wnioskodawcy, jak i przekazywana indywidualnie – na wniosek zainteresowanych stron. Zakres danych został natomiast określony na podstawie zasobów przetwarzanych w niniejszym projekcie. ułatwienie w postaci bez wnioskowego pozyskania niezbędnych informacji. Analiza danych, jak i szeroka wiedza na temat utrzymania porządku publicznego na terenie Wrocławia wykazują, że Zamawiający w ramach usług systemu będzie ze względu na użyteczność, do udostępnienia na portalu Open Data Wrocław, wyodrębniał następujące zbiory danych:

* ilość ujawnionych wykroczeń wraz z ilością zakończeń, czyli ilość mandatów,
* ilość pouczeń, ilość wniosków do sądu,
* ilość pojazdów odholowanych,
* ilość pojazdów zablokowanych,
* ilość usuniętych wraków pojazdów,
* ilość przyjętych zgłoszeń w tym ilość zgłoszeń telefonicznych, ilość zgłoszeń via e-mail, ilość zgłoszeń via formularz elektroniczny.

Zbiory danych udostępnione zostaną w otwartym i ustrukturyzowanym formacie CSV (Poziom 3\*\*\*) w okresach kwartalnych na portalu Open Data Wrocław:

* plik posiada nagłówek z tytułami kolumn;
* nazwa pliku nie ma znaczenia
* plik ma formę tabelaryczną
* zachowana jest ciągłość rekordów w tabeli
* poszczególne rekordy powinny być jednorodne (w tym sensie, że nie powinny być przedzielane podsumowaniami, grupowaniami, itp)
* poszczególne kolumny oddzielone są separatorem (najlepiej średnikiem)
* plik jest zakodowany w UTF-8
* plik jest umieszczany w lokalizacji, do której jest dostęp protokołem ftp

# e-Usługi publiczne

W wyniku realizacji zamówienia przez Wykonawcę będą uruchomione cztery usługi publiczne na czwartym poziomie dojrzałości (u:

1. udostępnienie e-usługi publicznej pozwalającej na dokonanie zgłoszenia (interwencji, wykroczenia) drogą elektroniczną – spowoduje utworzenie nowego kanału do zgłaszania zdarzeń dostępnego 365 dni 24h, umożliwiającym otrzymywanie informacji o podejmowanych w sprawie czynnościach i ich wynikach drogą elektroniczną.
2. udostępnienie e-usługi publicznej pozwalającej na sprawdzenie statusu sprawy – umożliwi sprawdzenie aktualnego stanu prowadzonej sprawy przez SMW całkowicie drogą elektroniczną
3. udostepnienie e-usługi publicznej pozwalającej na złożenie skargi drogą elektroniczną – udostępni możliwość złożenia skargi na działania SMW przez 365 dni 24h, oraz otrzymania informacji zwrotnej o podjętych działaniach drogą elektroniczną
4. udostępnienie e-usługi publicznej pozwalającej na złożenie prośby o usunięcie blokady drogą elektroniczną – umożliwi zgłoszenie drogą elektroniczną gotowości do zdjęcia blokady oraz otrzymanie przewidywanego czasu oczekiwania na patrol.

**Uwaga: Zamawiający udostępni (w terminie 30 dni od podpisania umowy) szczegółowe dane odnośnie wyglądu i funkcjonalności formularzy internetowy.**

# Wymiana danych z CZK UM Wrocławia

System powinien posiadać funkcjonalność dwustronnej wymiany danych z Centrum Zarządzania Kryzysowego Urzędu Miejskiego Wrocławia. Zamawiający przekaże szczegóły wymiany danych na etapie wdrożenia.

# Wymiana danych z WPiO

System powinien posiadać funkcjonalność dwustronnej wymiany danych z Wydziałem Podatków i Opłat Urzędu Miejskiego Wrocławia. Zamawiający przekaże szczegóły wymiany danych na etapie wdrożenia.

# Wymiana danych z WZN

System powinien posiadać funkcjonalność dwustronnej wymiany danych z Wydziałem Zarządzania Należnościami Urzędu Miejskiego Wrocławia. Zamawiający przekaże szczegóły wymiany danych na etapie wdrożenia.

# Straż Miejska

# Funkcjonariusze

System powinien posiadać co najmniej następujące funkcjonalności:

1. lista pracowników SM wraz z informacjami o: numerze służbowym, imieniu
i nazwisku, numer telefonu, przypisanym referacie, stopniu i stanowisku służbowym, dacie zatrudnienia i zwolnienia, uprawnienia do aplikacji mobilnej dla kadry zarządczej lub służby patrolowej, uprawnienia naczelnika,
2. rejestracja nowych pracowników SM,
3. edycja pracownika, historia zatrudnienia z informacja o przejściach między referatami, oddziałami,
4. powiązanie pracownika z referatem,
5. powiązanie pracownika z oddziałem.

# Centralny rejestr zgłoszeń

System powinien realizować co najmniej następujące funkcjonalności (graficznie przedstawione w załączniku nr 7 – kanały przyjmowania zgłoszeń):

1. Możliwość rejestracji, zakończenia, aktualizacji dyżuru dyżurnego,
2. Możliwość wprowadzania danych o zgłoszeniu, w tym co najmniej:
	1. Data i czas rejestracji zgłoszenia wygenerowana automatycznie na podstawie czasu systemowego,
	2. Opis zdarzenia, miejsce zdarzenia (w tym: osiedle, ulica, numer domu, numer mieszkania),
	3. Zaznaczenie miejsca zdarzenia na mapie cyfrowej,
	4. Kategoria i podkategoria zdarzenia. Dane pobierane ze słownika,
	5. Powiązanie zdarzenia z numerem kamery rejestrującej,
	6. Wskazanie daty i godziny zakończenia obsługi zgłoszenia z możliwością korekty opisu zdarzenia po jego zakończeniu,
	7. Nadawanie priorytetu oraz statusu zgłoszenia zdarzenia. Dane pobieranie ze słownika systemowego. Różne kolory zdarzeń w zależności od aktualnego statusu.
3. System ma mieć możliwość automatycznego nadania zapisanemu zdarzeniu unikatowego numeru,
4. System musi mieć możliwość wyświetlania czasu oczekiwania zgłoszenia na podjęcie interwencji,
5. System musi mieć możliwość wizualizacji miejsca zgłoszenia na mapie. Prezentacja zdarzeń w oparciu o wybrane kategorie w dowolnym przedziale czasowym.
6. System musi mieć możliwość automatycznego sygnalizowania przyjmującemu zgłoszenie informacji o zdarzeniach podobnych (już zarejestrowanych), miejscu i rodzaju zdarzenia oraz umożliwienie powiązania zgłoszenia do istniejącego pierwotnego zgłoszenia;
7. System musi posiadać statystyki: ilościowa, według kategorii, rodzaju zgłoszenia, według ulic, według wprowadzającego, w rozbiciu na numery kamer;
8. System musi mieć możliwość generowania automatycznych meldunków ze służby dyżurnych Centrum Monitoringu. Meldunek w formacie PDF z informacją o zarejestrowanych zdarzeniach podczas dyżuru. Możliwość przesyłania z poziomu modułu wygenerowanego meldunku na zdefiniowane w systemie adresy mailowe;
9. Wszystkie wygenerowane meldunki powinny być zarejestrowane z informacja o dacie sporządzenia, numerze meldunku, osobie sporządzającej. Możliwość podpinania załączników pod meldunki.
10. System musi mieć możliwość generowania na żądanie kart zdarzenia z wpisami czynności podejmowanymi w ramach podejmowanego zdarzenia;
11. System musi posiadać Listę zdarzeń z możliwością zarządzania kolumnami oraz eksportu zdarzeń do plików (PDF oraz CSV). Lista zdarzeń musi być wyposażona w zaawansowana wyszukiwarkę umożliwiającą wyszukiwanie złożone w tym po: kategorii, podkategorii, miejscu zdarzenia, dacie dodania, priorytecie, statusie;
12. System musi mieć możliwość dodania załącznika do sprawy (co najmniej pliki DOC, JPG, PDF);
13. System musi posiadać archiwum zgłoszeń. Możliwość przeglądu historii obsługi zdarzeń zakończonych. Parametr wyszukiwania danych archiwalnych stanowią istotne parametry możliwe do zarejestrowania w zdarzeniu, między innymi data, miejsce, kategoria zdarzenia,
14. Centralny rejestr zgłoszeń obsługują dyżurni Centrum Kierowania, operatorzy monitoringu oraz uprawnieni funkcjonariusze/pracownicy pozostałych komórek SMW,
15. Program zapewnia wizualną identyfikację zgłoszenia, umożliwiając odróżnienie zgłoszeń przyjmowanych przez poszczególne komórki,
16. Zgłoszenie jest realizowane przez komórkę przyjmującą dane zgłoszenie jednakże nie obowiązuje to operatorów monitoringu, których uprawnienia pozwalają na przekazanie danego zgłoszenia dyżurnemu,
17. Dyżurni posiadają uprawnienia do rejestrowania zgłoszeń przekazywanych za pośrednictwem wszystkich dostępnych kanałów komunikacji (telefon, e-mail, sms, inne – np. przekazane ustnie przez przełożonego) oraz do przekazywania ich:
18. patrolom poprzez aplikację mobilną,
19. innym komórkom Straży właściwym pod względem terytorialnym lub merytorycznym (zgłoszenia, które nie wymagają niezwłocznej realizacji), **przy czym przekazywanie zgłoszeń do innej komórki nie wymaga akceptacji ze strony przyjmującego**,
20. decydentowi (Komendant lub Naczelnik),
21. dyżurnym Centrum Zarządzania Kryzysowego.
22. Uprawnione osoby w innych komórkach organizacyjnych, realizujących ustawowe zadania straży, posiadają uprawnienia do rejestrowania zgłoszeń przekazywanych za pośrednictwem telefonów, poczty tradycyjnej, oraz przekazywanych za pośrednictwem innych kanałów komunikacji – np. przekazane ustnie przez przełożonego, przez przechodnia itp.) oraz do przekazywania ich:
23. patrolom poprzez aplikację mobilną,
24. innym komórkom Straży właściwym pod względem terytorialnym lub merytorycznym (zgłoszenia, które nie wymagają niezwłocznej realizacji), **przy czym w przypadku przekazywanie zgłoszeń do innej komórki (w tym również do dyżurnego) wymagana jest akceptacja przez przyjmującego**,
25. decydentowi (Komendant lub Naczelnik).
26. Operatorzy monitoringu posiadają uprawnienia w centralnym rejestrze zgłoszeń do :
	1. Rejestrowania zgłoszeń przyjmowanych telefonicznie,
	2. Rejestrowania zgłoszeń zauważonych w wyniku obserwacji kamer monitoringu miejskiego.

# Siły i środki

Moduł przeznaczony do zarządzania personelem oraz środkami trwałymi będącymi na wyposażeniu odpowiedniej komórki organizacyjnej SMW. System powinien realizować co najmniej następujące funkcjonalności:

1. dyslokacja strażników – patrole. Tworzenie patroli z podziałem na zmiany oraz wskazaniem referatu i osoby odpowiedzialnej. Możliwość wybierania
z listy strażników, pojazdów oraz kryptonimów dla patroli. Zaznaczanie na mapie rejonu działania oraz możliwość definiowania zadań stałych i przerw strażników. Przy czym o zarejestrowanej przerwie oraz wyjściu patrolu z rejonu musi być powiadomiony dyżurny SM. Funkcja przeglądania aktualnych i archiwalnych informacji dotyczących patroli, zapisywanie do pliku PDF oraz drukowanie raportu za wskazany okres dyslokacji,
2. samochody i inne pojazdy Straży Miejskiej. Lista samochodów. Dodawanie nowych pojazdów z określeniem: numeru rejestracyjnego, marki pojazdu, modelu, ilości miejsc, roku produkcji, typ pojazdu, statusu pojazdu, wyposażenia,
3. zarządzanie radiotelefonami/lokalizatorami/urządzeniami mobilnymi. Rejestracja w systemie urządzeń z określeniem; kodu urządzenia, IMEI urządzenia, numeru seryjnego, modelu urządzenia, typu urządzenia, numeru telefonu, limitu danych, adresu IP urządzania, statusu aktywny/nieaktywny. Zarządzanie urządzeniami w tym przypisanie radiotelefonu/lokalizatora/urządzenia mobilnego do patrolu/pojazdu, wydawanie i zwrot urządzeń strażnikom oraz historia wydanych
i zwracanych urządzeń(powinna być możliwość zdefiniowanych dowolnych statusów dla urządzeń, np.:

- pobrany,

- zdany,

- niesprawny,

- przekazany do naprawy,

- w naprawie,

- do odbioru po naprawie.

1. zarządzanie blokadami w tym przypisanie blokady do pojazdu, możliwość przypisania unikalnego identyfikatora oraz roboczego oznaczenia, wydanie i zwrot urządzeń blokujących, historia wydawanych i zwracanych urządzeń wraz z przypisanym statusem (np. w użytkowaniu, skradziona, itp).

# Blokady na koła

Moduł musi umożliwiać rejestrowanie blokad założonych na koła, tworzyć listę założonych blokad. Po zdjęciu blokady i zapisaniu tego w systemie, zdarzenie zostaje przeniesione do archiwum. Komponent musi być zintegrowany z mapą cyfrową w zakresie prezentacji aktywnych blokad. Moduł blokad musi być powiązany z ewidencją sił i środków oraz aplikacją mobilną w zakresie założenia, zdjęcia, rozliczenia blokady.

# Ewidencja druków

Moduł ewidencji druków musi umożliwiać pracę z dokumentami na poziomie uprawnień referatu oraz całej straży miejskiej.

1. ewidencja przyjmowania i zdawania bloczków z Izby Skarbowej, ewidencja bloczków wezwań, przekazywanie ich kierownikom referatów
i strażnikom SM. Rozliczenie bloczków. Bloczek musi być w każdej chwili wycofany lub przekazany innemu funkcjonariuszowi. Ewidencja ma przechowywać dane o wszystkich przyjętych, wydanych, rozliczonych bloczkach, blankietach wykorzystanych, blankietach niewykorzystanych;
2. notatniki służbowe. Ewidencja wydawania i rozliczania notatników służbowych strażnikom SM z uwzględnieniem daty archiwizacji.
3. raporty bloczków. Raporty za wybrany okres w zakresie: zbiorczego rozliczenia bloczków, zestawień bloczków do rozliczenia, bloczki w pełni wykorzystane, bloczki częściowo wykorzystane.
4. inwentaryzacja bloczków mandatowych.
5. ewidencja mandatów karnych:
6. możliwość wprowadzenia wszystkich danych widniejących na odcinkach
mandatowych oraz danych dodatkowych np. wymagalność karty MRD5/1, nr rej. pojazdu, marka pojazdu, rozróżnienie dat: data wystawienia mandatu(data ukarania), data wymagalności(data ukarania + 7dni), data rozliczenia mandatu, data księgowania, przy mandatach wysyłkowych – data doręczenia mandatu oraz data zwrotu potwierdzenia doręczenia mandatu do jednostki SM; oraz możliwość dokonywania korekty i uzupełnienia wprowadzonych danych w każdym momencie,
7. możliwość automatycznego przyporządkowania na podstawie kodu pocztowego w adresie ukaranego danych dotyczących danej miejscowości, czyli ulicy, gminy, powiatu, województwa lub możliwość tworzenia takiej bazy,
8. możliwość tworzenia bazy osób ukaranych przez Straż Miejską – kartoteka osobowa,
9. możliwość wykorzystania danych osób już istniejących w bazie przy ponownym wprowadzaniu mandatu takiej osoby po numerze PESEL,
10. dopisywanie kolejnych mandatów dla istniejącego w bazie ukaranego
i automatyczna informacja o ukaranym istniejącym w bazie po numerze PESEL,
11. sprawdzanie formalne przy wprowadzaniu danych np. poprawności numeru PESEL, poprawne dekodowanie numeru PESEL od roku 2000, sprawdzenie czy osoba ukarana ukończyła 17 lat na podstawie numeru PESEL,
12. możliwość wprowadzania obcokrajowców bez numeru PESEL (po zaznaczeniu odpowiedniego okienka generowanie unikalnego ciągu znaków imitującego numer PESEL, np.: 11111111111),
13. możliwość dodawania kolejnych adresów ukaranych z funkcją wybierania tego aktualnego (to samo dot. dowodu osobistego czy prawa jazdy),
14. system powinien posiadać wykaz przepisów ze szczegółowym opisem,
na podstawie których nakładane są grzywny oraz możliwość ich edycji, dokonywania poprawek czy dopisywania nowych,
15. ewidencja mandatów powinna zawierać podział na paczki tzn. - zbiorcze wykazy z każdego oddziału/wydziału Straży Miejskiej celem przekazania do Wydz. Finansowego UMW, z możliwością wydruku takiej paczki ułożonej serią i nr mandatu. Wykaz taki powinien zawierać dane osobowe tzn. imię, nazwisko ukaranego, pesel, adres zameldowania, nr mandatu, kwotę mandatu, rodzaj mandatu,
16. ewidencja mandatów gotówkowych, kredytowanych i zaocznych z odpowiednim oznaczeniem umożliwiającym rozróżnienie ww. mandatów; raport taki powinien zawierać ilość ogółem nałożonych mandatów z podziałem na rodzaj mandatu: gotówkowy, kredytowany, wraz z kwotami,
17. wyszukiwanie mandatów wg nr mandatu, danych osobowo-adresowych osoby ukaranej mandatem, danych z wykroczenia np. po numerze rejestracyjnym pojazdu, rodzaju wykroczenia, typie wykroczenia, miejscu wykroczenia itp.,
18. możliwość dopisania dowolnej informacji do wprowadzonego mandatu karnego tzn. uwag od strony danych osobowych, czy danych dot. mandatu,
19. możliwość tworzenia raportu karalności osób ukaranych(ukaranych mandatem, wnioskiem do sądu),
20. możliwość tworzenia bazy osób upoważnionych do nakładania mandatów i możliwość generowania raportów z nałożonych mandatów przez danego funkcjonariusza (zbiorczo przez wszystkich funkcjonariuszy z wyróżnieniem zarówno numeru strażnika jak i jego nazwiska) z podziałem na mandaty nałożone za odpowiedni rodzaj
wykroczenia, z wyróżnieniem kwot grzywien, rodzaju nałożonego mandatu, daty wystawienia mandatu,
21. możliwość generowania formularzy statystycznych; raportów umożliwiających wyszukiwanie w założonych przedziałach czasowych wg dowolnie zadanych parametrów: danych osobowo adresowych, danych funkcjonariuszy nakładających mandat, kwalifikacji prawnej wykroczenia, miejscu wykroczenia, rodzaju mandatu, ilościowo i listowanie.

Przykładowe wymagane raporty – załącznik nr 8 do OPZ

1. możliwość generowania raportów dot. mandatów drogowych, do których wymagana jest karta rejestracyjna - MRD 5/1,
2. możliwość eksportu danych o mandatach z bazy do plików w formacie KSAT 2000 zgodnie z przekazaną dokumentacją importu do KSAT.

# Rejestr zapytań CEPIK

W tym module powinny być realizowane zapytania do systemu CEPIK (zapytania o właściciela/użytkownika, zapytanie o pojazdy zarejestrowane na daną osobę, szczegółowe dane dotyczące posiadanych przez osobę dokumentów/uprawnień). Możliwość wygenerowania zapytania o kierowcą na podstawie imienia, nazwiska, numeru PESEL. Wygenerowana odpowiedz z Systemu CEPIK musi być wczytywana do systemu SKD w miejscu powstania zapytania.

# Rejestr zapytań ŹRÓDŁO

W tym module powinny być realizowane zapytania do systemów ŹRÓDŁO i Rejestr Dowodów Osobistych(zapytania o dane osoby, wizerunki). Możliwość wygenerowania zapytania o osobę na podstawie imienia, nazwiska, numeru PESEL. Wygenerowana odpowiedz z Systemu ŹRÓDŁO oraz RDO musi być wczytywana do systemu SKD w miejscu powstania zapytania.

# Formularze działań i interwencji

Lista formularzy :

1. System powinien mieć możliwość wprowadzania do systemu na odrębnych dedykowanych formularzach: mandatów, pouczeń, wezwań/zawiadomień, notatek na wniosek/urzędowych, spraw w toku, spraw przekazanych do RSOW, spraw przekazanych innemu organowi lub instytucji, spraw bez znamion wykroczenia, sprawy załatwionych na miejscu. Lista formularzy powinna posiadać możliwość filtrowania wpisów, co najmniej po: dacie wykroczenia, dacie wystawienia w dowolnym przedziale czasowym dla wybranych referatów, ukaranym.
2. Każdy wpis na liście powinien dać możliwość jego edycji, wprowadzania załączników, podglądu, powiązania z dziennikiem zdarzeń SM lub innym formularzem, określenia dodatkowych parametrów (słownik systemowy), powielenia formularza,
3. Dostępna musi być funkcja eksportu karty formularza w postaci pliku PDF,
4. Dostępna musi być wyszukiwarka formularzy, co najmniej po parametrach:
5. typ formularza,
6. personalia strażnika SM,
7. dowolna fraza,
8. data z uwzględnieniem daty wystawienia, wykroczenia, wprowadzenia,
9. System powinien mieć:
10. możliwość dokonania zbiorczego przedawnienia na podstawie zakresu dat ukarania,
11. umożliwić zapisywanie na karcie kontowej mandatu m. in. informacji
o wystawionych upomnieniach, tytułach wykonawczych, zmianach w zakresie danych adresowych,
12. rejestrować i zachować historię zmian, ze wskazaniem na dokument zmieniający, jeśli taki istnieje, daty zmiany, zakresu zmiany, użytkownika dokonującego zmiany.

# Dziennik RSOW

System SKD musi tworzyć oddzielne zestawienia na potrzeby RSOW (dziennik RSOW). Formularze zarejestrowane w dzienniku RSOW powinny mieć co najmniej możliwość:

1. edycji spraw,
2. wprowadzenia personaliów osób w sprawie sprawcy  /  podejrzani  /  osoby pokrzywdzone  /  świadkowie do zdarzenia,
3. ewidencja czynności podejmowanych w ramach prowadzonej sprawy  /  formularza. Lista czynności (słownik systemowy) powinna być powiązana z generatorem szablonów dokumentów,
4. dodawania załączników,
5. wpisywania dat wokand, miejsc rozpraw, przypomnień terminów,
6. dziennik RSOW musi mieć możliwość przeszukiwania, co najmniej
po parametrach: data przekazania do RSOW oraz personaliach strażnika SM prowadzącego sprawę.
7. Predefiniowane formularz tj. notatki służbowe, protokoły przesłuchań z możliwością ich edycji i dostosowania do własnych potrzeb.

System SKD SMW musi zachować zgodność z załączonym „Diagram ZKW” stanowiącym załącznik nr do OPZ.

# Kartoteka sprawców

Podczas wprowadzania wykroczeń system powinien automatycznie zapisywać sprawcę pod unikalnym ID (najlepiej numer PESEL) oraz numery rejestracyjne pojazdów z wykroczeń. Powstała w ten sposób kartoteka sprawców powinna prezentować liczbę mandatów, pouczeń, spraw RSOW dla osoby ujętej w kartotece. Jeżeli dana osoba popełni wykroczenie po raz kolejny jego dane, po wpisaniu numeru PESEL, powinny być automatycznie wczytywane przy wprowadzaniu kolejnych formularzy. Kartoteka sprawców powinna być wyposażony w funkcje wyszukiwarki sprawców zdarzeń oraz tworzenia zestawień w formatach PDF i CSV. Informacja o próbach doręczenia korespondencji. Kartoteka powinna być dostępna w aplikacji mobilnej z możliwością : wyszukiwania po numerze PESEL, imieniu i nazwisku, nr rejestracyjnym (informacja zwrotna mówiąca: czy osoba była karana i w jaki sposób oraz czy istnieje informacja o próbie doręczenia korespondencji). Na potrzeby SMW kartoteka powinna umożliwiać wyszukiwanie po wszystkich polach wprowadzonych do bazy danych.

# Karty MRD-5

Na podstawie wprowadzonych danych do formularzy system ma umożliwiać zbiorcze generowanie kart rejestracyjnych MRD-5. System powinien posiadać historię przesłania kart MRD-5 do wydruku (statusy: wygenerowano, wydrukowano, wydrukowano duplikat)

# Statystyki

System SKD powinien mieć możliwość tworzenia i drukowania :

1. zestawień\statystyk wg. Daty w tym wystawienia,
2. zestawień według : wykroczeń, wprowadzania, personaliów strażników SM, typu formularzy, zakończone lub w toku, kategorii wykroczeń, artykułów wykroczeń, informacji statystycznych, ulicy wykroczenia, osobach, dodatkowych parametrach zarejestrowanych w dzienniku i powiązanych z formularzem,
3. zestawień z formularzy powiązanych z informacjami statystycznymi. Możliwość filtrowania po wybranej informacji statystycznej.
4. ewidencji wyników działań. Zestawienia wyników działań dla wybranego strażnika SM lub referatu lub oddziału. Możliwość filtrowania po dacie,
5. sprawozdania z działalności SM. Tworzenie zestawienia z działalności SM zgodnego z Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 12 listopada 2009 r. w sprawie zakresu i sposobu prowadzenia przez straże gminne (miejskie) ewidencji etatów, wyposażenia oraz wyników działań straży.
6. formularzy według artykułów. Tworzenie zestawień za wybrany okres z podziałem na artykuły kodeksu wykroczeń z uwzględnieniem liczby i kwot mandatów oraz innych formularzy powiązanych z właściwym artykułem
7. Wykaz niezbędnych statystyk stanowi załącznik nr 7 do OPZ.

# Odholowane pojazdy

Moduł ten powinien być powiązany z aplikacją mobilną SKD Patrol oraz umożliwiać wprowadzanie dokumentacji fotograficznej bezpośrednio z aplikacji.

Moduł Odholowane pojazdy musi umożliwiać :

1. Rejestrowanie i tworzenie listy odholowanych pojazdów,
2. Integrację z mapą cyfrową w zakresie prezentacji odholowań,
3. Nadawanie indywidualnych statusów (np. zgłoszono do odholowania, odholowany, do odbioru, odebrany, archiwum),
4. Nadawanie ról w systemie według odpowiedniego zakresu wykonywanych czynności:
	1. Patrol podejmujący działania lub dyżurny CK wprowadza (funkcjonalność dostępna w aplikacji mobilnej oraz desktopowej):
		1. Data, godzina, miejsce, powód usunięcia pojazdu,
		2. Kto wydał dyspozycję usunięcia pojazdu,
		3. Numer rejestracyjny, marka oraz model usuwanego pojazdu,
		4. Określenie firmy usuwającej, parking na który pojazd zostanie usunięty,
		5. Numer dyspozycji
		6. Dokumentacja fotograficzna
	2. Funkcjonariusz w referacie wykroczeń podczas czynności wyjaśniających oraz wydawania pozwolenia na odbiór pojazdu wprowadza brakujące dane do sprawy wraz z numerem i kwotą mandatu,
	3. Raportowanie – system winien generować raporty statystyczne i dane merytoryczne na podstawie wybranego zakresu z niżej wymienionych dostępnych pól systemowych.

Układ funkcjonalny aplikacji przeglądarkowej w wersji desktopowej powinien być zbliżony do n/w przykładu i musi zawierać n/w zakresy pól poszerzone o dostęp do dokumentacji fotograficznej:

* Numer z książki dyżurnego CZK [pole tekstowe],
* Numer z książki dyżurnego KM Policji [pole tekstowe],
* Data dyspozycji\*,
* Godzina dyspozycji\*,
* Miejsce usunięcia\*[słownik ulic]+[pole tekstowe] do uszczegółowienia,
* Wydał dyspozycję\* [słownik – wyszukanie po numerze strażnika],
* Marka pojazdu\*[ słownik – lista wyboru]
* Model pojazdu\*[pole tekstowe],
* Numer rejestracyjny\*[pole tekstowe],
* Usunięcie wykonuje\*[pole tekstowe],
* Lokalizacja parkingu\*[pole tekstowe],
* Sprawę zakończył(a)\* [słownik – wyszukanie po numerze strażnika],
* Numer zezwolenia\*[pole tekstowe],
* Data zakończenia\*,
* Godzina zakończenia\*,
* Sposób zakończenia\*[lista wyboru],
* Numer wezwania [pole tekstowe]
* Seria i nr mandatu\* [pole tekstowe];
* Kwota mandatu [pole tekstowe]
* Uwagi [pole opisowe] ,
* Wprowadził(a) [autouzupełnianie po zalogowanym użytkowniku],
* Edytował(a) [autouzupełnianie po strażniku, który edytował],
* Przyczyna usunięcia\*[lista wyboru + wyszukiwanie],
* Dokumentacja [Załączniki jpg, pdf, doc, zip, png, itp.] możliwość dodania kilku załączników,
* Zdjęcia,
* Status\* [lista wyboru] : zgłoszono do odholowania, odwołano odholowanie, odwołano odholowanie-holownik w drodze; odwołano odholowanie-holownik na miejscu; odwołano odholowanie-pojazd na lawecie; odholowany; do odbioru; odebrany; archiwum

# Obsługa wykroczeń drogowych

System musi wspierać wszystkie czynności realizowane na potrzeby referatu wykroczeń w szczególności:

1. przyjmowanie zgłoszeń dot. wykroczeń drogowych wraz z dokumentacją zdjęciową zarówno za pośrednictwem urządzeń mobilnych jak i komputera stacjonarnego [stanowisko operatora] w przypadku udokumentowania wykroczenia za pomocą aparatu fotograficznego,
2. zgłoszenie powinno zawierać dodatkowo informację o naruszanym przepisie, oznaczeniem geolokalizacyjnym miejsca popełnienia wykroczenia możliwym do uwidoczniania na mapie, możliwość przejścia do miejsca wykroczenia w aplikacji streetview,
3. dodawane wykroczenie powinno mieć min. 4 zdjęcia prezentujące – pojazd popełniający wykroczenie, zdjęcie kontekstowe miejsca popełnienia wykroczenia wraz z oznakowaniem, przednią szybę pojazdu, zdjęcie tablicy rejestracyjnej,
4. informacją zwrotną z systemu na etapie zgłaszania wykroczenia powinien być numer wykroczenia ewidencjonowany w systemie, informacja o ilości postępowań prowadzonych wobec ww. pojazdu oraz informacja o tym czy korespondencja doręczana jest bez przeszkód, w aplikacji Mobilnej (przed rej. Zgłoszenia aby strażnik mógł zadecydować czy zakłada blokadę czy wystawia wezwanie (w aplikacji internetowej jako opcja na liście zgłoszeń)
5. wykroczenia powinny mieć możliwość nadawania informacji o aktualnym statusie, statusy nadawane ręcznie.
6. do wykroczenia powinna być możliwość przypisywania informacji o strażniku wykonującym czynności w miejscu zdarzenia jak i informacje o osobie odpowiedzialnej za prowadzenie postępowania administracyjnego,
7. system powinien informować o zdarzeniach którym upływa określony parametrycznie czas od dnia popełnienia wykroczenia,
8. system powinien umożliwiać generowanie kompletnej dokumentacji dot. postępowania z rozróżnieniem na dokumentację przesyłaną do firm i instytucji, firm leasingowych i osób fizycznych tj.:
* wezwań,
* pism przewodnich wraz z dokumentacją zdjęciową,
* oświadczenia do wypełnia przez odbiorcę wraz z pouczeniami.
* kart MRD/PRD5
* innej dokumentacji wytworzonej w czasie trwania postępowania.
	+ Wezwania zgodnie z załączonym wzorem (3 rodzaje na bazie szablonów dostarczonych przez zamawiającego) Pismo przewodnie (predefiniowany szablon korespondencji -ok. 40 wersji formatek do generowania dokumentacji) Nie wynikają z ustawy, prowadzona na potrzeby postepowania. Koperty i zwrotki (ok. 3 rodzajów). Inna dokumentacja: protokół przesłuchania świadka, notatka służbowa, protokół przesłuchania sprawcy, wniosek do sądu, dobrowolne poddanie się karze, pismo informacyjne dla sprawcy wykroczenia.

Proces obsługi zdjęciowej wykroczeń przedstawia **Załącznik nr 5 do OPZ – RSOW – Diagram ZKW.**

# Pozostałe wymagania

# Architektura systemu

1. System powinien być zbudowany w trójwarstwowej architekturze obejmującej :
	1. Warstwa aplikacji obejmująca serwer systemu SKD,
	2. Warstwa danych obejmująca serwer baz danych MS SQL SERVER 2019,
	3. Warstwa prezentacji obejmująca interfejs użytkownika – klient WWW.
2. System SKD nie może pracować jako połączenie do serwera terminali,
3. Repozytorium plików/materiałów musi być zapisywane bezpośrednio na serwerze aplikacji,
4. Struktura plików serwera aplikacji, w której będzie przechowywane repozytorium musi być tak zaprojektowane, aby dostęp do tych plików był wyłącznie z poziomu serwera aplikacyjnego a użytkownik nie miał uprawnień do tych plików.

# Wymagania wydajnościowe

1. Wykonany System przez Wykonawcę umożliwi pracę co najmniej 100 użytkownikom jednocześnie przy założeniu wydajności tj. wyświetlanie grafiki, animowanych plików gif, zdjęć, odtwarzanie plików wideo i audio poprzez wbudowany/zintegrowany odtwarzacz z przesyłaniem strumieniowym plików, a także włączanie i wyświetlanie map.
2. W przypadku gdy wydajność systemu spadnie poniżej oczekiwanego poziomu wskazanego powyżej, system musi wygenerować komunikat o braku dostępności do zasobów systemu.
3. Zaproponowany system przez Wykonawcę musi zapewnić następujące czasy odpowiedzi :
	1. Średni czas odpowiedzi przy transakcjach bez zapisu informacji do bazy danych nie może przekraczać 5 sek., czas maksymalny 25 sek.,
	2. Średni czas odpowiedzi przy transakcjach z zapisem informacji do bazy danych nie może przekraczać 10 sek., czas maksymalny 40 sek.,
	3. Przez czas odpowiedzi rozumie się czas upływający od momentu wykonania przez użytkownika na stacji roboczej czynności wyzwalającej określone zachowanie systemu (naciśnięcie odpowiedniego przycisku lub kontrolki w oknie system w zależności od sytuacji itp.) do momentu uzyskania oczekiwanych wyników tej akcji na stacji roboczej użytkownika, pomniejszony o czas transportu komunikatów w elementach infrastruktury nie będących przedmiotem dostaw od Wykonawcy.

# Wymagania bezpieczeństwa

Standardy bezpieczeństwa zastosowane w ramach zintegrowanego systemu zapewniającego koordynację działań Straży Miejskiej, który zostanie wdrożony w ramach postępowania będą zapewniały bezpieczeństwo przetwarzania danych zgodnie z obowiązującym prawem.

W ramach tworzenia systemu teleinformatycznego uwzględnione zostaną:

* 1. wytyczne w zakresie bezpieczeństwa informacji zawarte w Rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych – opisano w ramach kryterium nr 1,
	2. podejście „Security by Design” poprzez dobranie i implementację właściwych mechanizmów bezpieczeństwa, adresujących wymagania funkcjonalne i niefunkcjonalne oraz minimalizujących skutki lub eliminujących możliwość wystąpienia znanych zagrożeń, wg. zidentyfikowanych przez OWASP 10 zasad bezpieczeństwa, do których należą:
		1. Minimalizowanie powierzchni ataku – każda funkcjonalność dotycząca wymiany informacji z otoczeniem (interfejs użytkownika, interfejs komunikacji z zewnętrznym systemem, ładowanie plików) niesie za sobą ryzyko wystąpienia błędu skutkującego możliwością zaistnienia podatności systemu. W celu zapewnienie bezpieczeństwa już na etapie wytwarzania istotnym jest ograniczanie tego ryzyka.
		2. Stosowanie domyślnego poziomu bezpieczeństwa (ang. security by default) – Zastosowane mechanizmy bezpieczeństwa powinny mieć domyślnie ustaloną politykę działania na włączoną, np. weryfikacja złożoności hasła użytkownika, wymuszanie zmiany hasła po N dniach.
		3. Nadawanie minimalnych uprawnień (ang. least privileges) – każde z kont dla użytkownika lub usługi powinno posiadać minimalny zestaw uprawnień do zasobów, niezbędny do realizowania założonej funkcjonalności, np. usługa powinna być uruchamiana z uprawnieniami dedykowanego dla niej konta nieposiadającego uprawnień root/admin, o ile nie jest to niezbędne.
		4. Ochrona w głąb – w systemach zbudowanych w oparciu o tę zasadę stosowane są mechanizmy bezpieczeństwa na kilku warstwach, co znacząco utrudnia ich przełamanie/kompromitację. Wynika to z faktu, że zidentyfikowanie wielu różnych podatności na różnych warstwach jest dużo trudniejsze i bardziej czasochłonne niż na jednej.
		5. Kontrolowane działanie w przypadku wystąpienia błędu (ang. fail securely) – w przypadku wystąpienia błędu, wyjątku system powinien w sposób kontrolowany przejmować ich obsługę, informując o wystąpieniu błędu lub w sytuacjach krytycznych kończąc swoje działanie po zalogowaniu informacji o zaistniałym zdarzeniu.
		6. Brak zaufania do zewnętrznych usług – w wielu przypadkach elementem systemu są usługi dostarczane przez zewnętrzne podmioty, które mogą mieć zupełnie odmienne podejście do polityki bezpieczeństwa czy też ochrony danych. W związku z tym we wszystkich przypadkach zwracane dane powinny być weryfikowane oraz powinna być weryfikowana poprawność działania usługi (o ile to możliwe).
		7. Rozdział obowiązków (ang. separation of duties) – w organizacji występują różne role, które powinny mieć swoje odzwierciedlenie w systemie. Dla przykładu użytkownik rejestrujący umowy w systemie nie powinien mieć uprawnień do zarządzania listą pracowników w organizacji czy też administracją całego rozwiązania.
		8. Unikanie bezpieczeństwa przez niejawność (ang. security by obscurity) – opieranie bezpieczeństwa systemu na utajnieniu całego rozwiązania: technologii, architektury, kodu źródłowego, użytych komponentach czy też zastosowanych algorytmach kryptograficznych prowadzi często do odwrotnej niż zakładano sytuacji. Bezpieczeństwo systemu powinno opierać się na wielu różnych ściśle określonych czynnikach, do których na przykład zaliczyć można polityki haseł, limity liczby transakcji, segmentacja sieci, prowadzenie audytu.
		9. Zaprojektowanie mechanizmów w sposób prosty i przejrzysty – stosowanie złożonych mechanizmów w systemach, jak i komplikowanie architektury niesie większe ryzyko wystąpienia błędu skutkującego podatnością i w efekcie możliwym nieuprawnionym dostępem do danych lub kompromitacją całego systemu.
		10. Prawidłowe usuwanie błędów związanych z bezpieczeństwem – W przypadku usuwania błędów związanych z mechanizmami bezpieczeństwa czy też z bezpieczeństwem całego systemu istotnym jest przeprowadzenie stosownych testów w celu prawidłowe zidentyfikowanie przyczyny wystąpienia błędu.
		11. System zapewni możliwość rozróżniania danych osobowych na następujące kategorie: zgłaszający, świadek, pokrzywdzony, obwiniony, ukarany oraz rozróżnienie na dane potwierdzone i dane prawdopodobne.

# Bezpieczeństwo danych

Bezpieczeństwo danych zostanie zapewnione na kilku poziomach:

Uwierzytelnienie i autoryzacja

1. Uwierzytelnienie użytkowników w interfejsie graficznym będzie odbywało się co najmniej za pomocą loginu i hasła użytkownika lub środków identyfikacji elektronicznej pochodzących z Węzła Krajowego Identyfikacji Elektronicznej. Autoryzacja użytkowników będzie odbywała się zgodnie z przyznanymi uprawnieniami. Zakres danych i dostęp do określonych funkcjonalności będzie ograniczony do przypisanych ról. Administratorzy systemu posiadać będą dostęp do zakresu danych (np. logi) i funkcjonalności (np. konfiguracje), zgodnie z zapotrzebowaniem wynikającym z pełnionej roli. Komunikacja użytkowników z aplikacją będzie odbywała się z wykorzystaniem szyfrowanego połączenia TLS w wersji 1.2 lub nowszej (starsze wersje SSL 2.0 i 3.0 nie będą używane).
2. Bezpieczeństwo warstwy transportowej przy zestawianiu połączeń między Systemem a systemami trzecimi będzie wymagało uwierzytelnienia zarówno po stronie klienta jak i serwera za pomocą certyfikatów (tzw. „Two-way TLS authentication”).

Bezpieczeństwo komunikacji

Transmisja danych pomiędzy przeglądarką użytkownika a Platformą będzie realizowana poprzez szyfrowany kanał transmisyjny SSL. Próba nawiązania połączenia nieszyfrowanego HTTP będzie automatycznie przekierowywana do połączenia szyfrowanego HTTPS. Również połączenia z innymi systemami będą realizowane poprzez kanał szyfrowany SSL lub w razie konieczności poprzez kanał VPN. Połączenie aplikacji mobilnej SKD PATROL SMW z systemem będzie realizowane poprzez kanał VPN.

Bezpieczeństwo składowania dokumentów

Przychodzące wiadomości będą odbierane, a następnie powinny być składowane w bazie danych. Wszystkie załączniki powinny być zapisane jako binarne pliki na dedykowanym zasobie dyskowym, a metadane załączników wraz z lokalizacją powinny trafić do bazy danych. W metadanych powinien znaleźć się wyliczony skrót (hash) z zawartości pliku. Wyliczany skrót powinien być wykonany za pomocą algorytmu SHA-256, ponieważ należy on do bezpiecznych algorytmów rodziny SHA-2. Składowane pliki będą w postaci zaszyfrowanej, tak jak zostały dostarczone przy wykorzystaniu protokołu AS4.

# Bezpieczeństwo Danych Osobowych (RODO)

W systemie będą przechowywane zwykłe dane osobowe użytkowników systemu, oraz dane wrażliwe osób biorących udział w interwencjach, jedynie w zakresie niezbędnym do realizacji zdefiniowanych procesów. System zapewni przestrzegania podstawowych zasad przetwarzania danych osobowych zgodnie z treścią RODO:

1. Zasada zgodności z prawem, rzetelności przejrzystości – dane osobowe muszą być przetwarzane zgodnie z prawem, tj. musi istnieć podstawa prawna przetwarzania tych danych, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą, tzn. informacje dotyczące zbierania, wykorzystywania lub wszelkich innych sposobów przetwarzania danych oraz zakresu, w jakim te dane są lub będą przetwarzane przez administratora systemu, muszą być znane i zrozumiałe dla tych osób;
2. Zasada ograniczonego celu – dane muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
3. Zasada minimalizacji danych – dane mogą być przetwarzane w zakresie adekwatnym, stosownym i ograniczonym do celu, w którym zostały zebrane;
4. Zasada prawidłowości – dane muszą być prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe były prawidłowe i w razie potrzeby uaktualniane, a dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane;
5. Zasada ograniczonego przechowywania – dane muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez czas ograniczony do ścisłego minimum, nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane (retencja danych);
6. Zasada integralności i poufności – przetwarzanie danych musi odbywać się w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, poprzez stosowanie odpowiednich środków technicznych lub organizacyjnych;
7. Zasada rozliczalności – administrator danych musi być w stanie wykazać przestrzeganie wszystkich powyższych zasad (prowadzenie odpowiedniej dokumentacji oraz zapewnienie dowodów stosowania powyższych zasad)

# Bezpieczeństwo serwerów aplikacyjnych

Bezpieczeństwo serwera aplikacji – w celu wykonania zabezpieczenia serwera aplikacyjnego zostaną wykonane następujące czynności:

1. wprowadzenie konfiguracji warstwy transportowej: SSL/TLS
2. wprowadzenie zabezpieczeń zgodnych z zaleceniami Open Web Application Security Project (OWASP) dotyczącymi warstwy transportowej (https://www.owasp.org/index.php/Transport\_Layer\_Protection\_Cheat\_Sheet)
3. zostaną wyłączone konfiguracje umożliwiające pobranie informacji o typie serwera i wersji, zostaną zablokowane żądania pobrania listy katalogów, zostaną zablokowane żądania typu HTTP TRACE i HTTP OPTIONS
4. zostaną zmienione standardowe hasła dostępowe administratora oraz zostanie zablokowany dostęp do konsoli administracyjnej serwera
5. zostanie wprowadzona kontrola dostępu zgodna z wcześniejszymi definicjami

# Serwer baz danych wymagania

Proponowany system musi współpracować z silnikiem bazodanowym opartym o rozwiązanie Microsoft SQL Server 2019 gdyż takim serwerem bazodanowym dysponuje Zamawiający.

* 1. Pozostałe wymagania dotyczące systemu
1. System powinien umożliwiać wymuszanie złożoności hasła Użytkownika, czasu życia hasła, sprawdzanie historii haseł, blokowanie konta przez administratora bądź w przypadku przekroczenia limitu nieudanych logowań.
2. System musi zapewniać zmiany własnego hasła dla Użytkownika poprzez podanie hasła bieżącego i podaniu dwukrotnie nowego hasła.
3. Przywileje użytkowników Systemu powinny być określane za pomocą ról systemowych.
4. Wykonawca zapewnia mechanizm automatycznego wykonywania kopii zapasowych danych.
5. Serwer aplikacyjny musi posiadać funkcjonalność wykonywania kopii całego serwera aplikacji. Kopia musi zawierać wszystkie elementy niezbędne do jego funkcjonowania tak, aby po zainstalowaniu sytemu operacyjnego od początku i odtworzeniu serwera aplikacyjnego z kopii zapasowej, będzie on w pełni funkcjonalny. Kopie zapasowe będą wykonywane na dysk wskazany przez Zamawiającego.
6. System musi zapewniać, że funkcjonalność wykonywania kopii zapasowych będzie odrębną polityką wykonywania kopii repozytorium plików od polityki wykonywania kopii pozostałych elementów Systemu.
7. Każde konto (login) w systemie powinno być indywidualne (przydzielany tylko dla jednego użytkownika) oraz unikatowe (nie może się powtarzać, nie może być kontem tzw. Współdzielonym) Raz wykorzystane loginy nie mogą się powtarzać (nawet w przypadku, gdy login jest nieaktywny lub został usunięty).
8. System powinien „wymuszać" tworzenie haseł o odpowiedniej konstrukcji tzn. hasło składające się z dużych i małych liter, cyfr, znaków specjalnych, oraz odpowiedniej długości (minimalna ilość znaków w haśle). Po wprowadzeniu hasła system powinien pokazywać siłę hasła w odpowiedniej skali.
9. System powinien wymuszać okresową zmianę hasła, np. co 30 dni. Hasła muszą być przechowywane w postaci zaszyfrowanej.
10. System powinien mieć możliwość blokowania konta po określonej liczbie nieudanych prób logowania do systemu. Administrator systemu powinien otrzymać automatyczną informację o zablokowaniu konta z powodu kilkukrotnego błędnego wpisania loginu lub hasła.
11. System musi zapewniać integrację z Microsoft Active Directory w celu synchronizacji kont użytkowników Systemu.
12. System musi zapewniać autentykację Użytkowników z wykorzystaniem Active Directory, który funkcjonuje w infrastrukturze Zamawiającego.

# Elementy infrastruktury informatycznej, którą Zamawiający zamierza udostępnić do realizacji zamówienia

Do celów realizacji niniejszego zamówienia Zamawiający zamierza udostępnić następujące elementy infrastruktury informatyczne:

1. Serwer wirtualny w infrastrukturze Zamawiającego bez systemu operacyjnego. Wybór systemu należy do Wykonawcy i jego instalacja wraz z niezbędnymi komponentami jest przedmiotem niniejszego Zamówienia,
2. Serwer wirtualny na potrzeby systemu SKD wraz z bazą danych będzie miał przydzielone następujące minimalne zasoby :
	1. CPU – 4 rdzenie
	2. RAM – 32 GB
	3. HDD – 500GB
3. Serwer wirtualny na potrzeby replikacji bazy danych będzie miał przydzielone następujące minimalne zasoby :
	1. CPU – 2 rdzenie,
	2. RAM – 16 GB
	3. HDD – 500 GB

# Warunki realizacji umowy

# Warunki dostawy i odbioru

1. Odbiór dostarczonych Produktów i wymaganej funkcjonalności przeprowadzony będzie przez Zamawiającego w oparciu o scenariusze testowe, także ścieżki negatywne przygotowane przez Wykonawcę, a zatwierdzone przez Zamawiającego przed rozpoczęciem Odbioru, chyba że umowa stanowi inaczej.
2. Dodatkowo Zamawiający ma prawo do opracowania własnych scenariuszy testowych, w oparciu o które będzie dokonywał Odbioru.
3. W trakcie testów i odbioru pracownikom Zamawiającego asystować będą pracownicy Wykonawcy.
4. Odbiorowi podlegają Produkty dostarczane w ramach realizacji niniejszej umowy.
5. Odbioru dokonuje wyznaczony przedstawiciel Zamawiającego oraz upoważniony przedstawiciel Wykonawcy.
6. Odbiór ma formę pisemną, w postaci Protokołu Odbioru podpisanego przez obie strony umowy, pod rygorem nieważności.
7. Protokół Odbioru zawierać będzie co najmniej:

a) opis Produktu podlegający odbiorowi,

b) miejsce i datę,

c) imiona i nazwiska Przedstawicieli Stron podpisujących protokół.

1. Po przeprowadzeniu odbiorów poszczególnych Produktów Strony dokonają końcowego odbioru przedmiotu zamówienia potwierdzonego Końcowym Protokołem Odbioru.

# Scenariusze testowe

Przed produkcyjnym uruchomieniem wdrażanego systemu, w celu zapewnienia wysokiego poziomu bezpieczeństwa, Wykonawca przeprowadzi testy penetracyjne, których celem jest zidentyfikowanie w systemie podatności umożliwiających naruszenie integralności, poufności i dostępności przetwarzanych danych. Testy penetracyjne będą przeprowadzone zarówno w warstwie aplikacyjnej jaki i warstwie sprzętowej:

1. Testy warstwy aplikacyjnej przeprowadzane zostaną w środowisku zbieżnym z produkcyjnym i będą miały na celu zidentyfikowanie podatności możliwych do wykorzystania w trakcie użytkowania aplikacji. Testy przeprowadzone zostaną w oparciu o OWASP Testing Guide, przy uwzględnieniu listy najpopularniejszych zagrożeń OWASP Top 10 oraz CWE/SANS Top 25 Weaknesses. W testach zostaną wykorzystane elementy metodyki PTES (Penetration Testing Execution Standard) oraz OSSTMM (Open Source Security Testing Methodology Manual). Wykonanie testów będzie zgodne z podejściem „Gray Box” (na podstawie dostarczonej dokumentacji projektowej), w środowisku testowym.
2. Testy infrastruktury sprzętowej – w zakresie adekwatnym do sposobu realizacji projektu - przeprowadzane na środowisku produkcyjnym mające na celu zweryfikowanie poprawności instalacji i konfiguracji mechanizmów bezpieczeństwa infrastruktury sprzętowo-programowej, w tym:
3. urządzeń sieciowych,
4. serwerów,
5. systemów operacyjnych,
6. usług sieciowych,
7. aplikacji serwerowych np. serwerów aplikacji,
8. baz danych.

# Przygotowanie danych

Przed przystąpieniem do testów Wykonawca wprowadzi do Systemu dane testowe, na podstawie których, Zamawiający będzie mógł przetestować wymagane funkcjonalności Systemu.

# Odbiór Systemu (w tym poszczególnych Aplikacji)

1. Co najmniej 3 dni przed terminem rozpoczęcia testów (procedury odbioru) Wykonawca zgłosi na piśmie gotowość Systemu do odbioru.
2. Przedstawiciele Zamawiającego rozpoczną testy w terminie nie dłuższym niż 3 Dni od daty zgłoszenia gotowości do przeprowadzenia testów.
3. Przedstawiciele Zamawiającego dostarczą raport z testów w terminie 2 Dni od dnia zakończenia testów. Raport z testowania wykaże ewentualne błędy lub braki.
4. Wykonawca zobowiązany jest do bezpłatnego usunięcia wskazanych w raporcie z testów błędów lub braków w terminach ustalonych przez Strony. Jeśli Strony nie ustalą inaczej, błędy i braki muszą zostać usunięte w terminie 5 Dni od daty przekazania raportu z testowania. W przypadku przekroczenia wyznaczonych terminów usunięcia błędów i braków Zamawiający ma prawo zastosować odpowiednie sankcje wynikające z umowy.
5. Po usunięciu wszystkich błędów lub braków wskazanych w raporcie Wykonawca ponownie przekaże poprawiony System do testowania zgodnie z podaną wyżej procedurą.
6. Po pozytywnym wyniku testów, zostanie podpisany Protokół Odbioru.
7. Jeżeli po dwukrotnym testowaniu, przy tym samym zakresie danych, według ww. procedury, System nadal zawierać będzie te same błędy lub błędy wynikające z usunięcia błędów w wyniku pierwszego testowania, Zamawiający ma prawo odmówić odbioru Systemu oraz zastosować odpowiednie sankcje wynikające z umowy.
8. Po pozytywnym wyniku testów i podpisaniu Protokołu Odbioru, Wykonawca przekaże
9. Zamawiającemu, wymaganą Dokumentację. Zamawiający odbiera Dokumentację zgodnie z procedurą odbioru Dokumentacji. Do terminu uruchomienia i wdrożenia Systemu wlicza się czas niezbędny na czynności odbioru Systemu.

# Odbiór dokumentacji

Dokumentacja będąca przedmiotem niniejszej umowy zostanie odebrana wg następującej procedury:

1. W terminie 7 Dni od daty przekazania Zamawiający powinien dokonać merytorycznej oceny przedłożonej Dokumentacji i podpisać Protokół Odbioru lub jeśli zawiera ona wady (merytoryczne, jest niekompletna, niespójna, sprzeczna z obowiązującymi przepisami prawa lub niezgodna z wymaganiami umowy) przekazać Wykonawcy w formie pisemnej Uwagi do Dokumentacji.
2. Brak zgłoszenia, w wyżej wymienionym terminie, pisemnych uwag przez Zamawiającego jest równoznaczne z akceptacją Dokumentacji.
3. W przypadku zgłoszenia uwag Wykonawca zobowiązany jest dokonać poprawek w Dokumentacji w terminie 5 Dni i przekazać Dokumentację do odbioru ostatecznego.
4. Do poprawionej wersji Dokumentacji stosuje się opisaną powyżej procedurę odbioru Dokumentacji.
5. Ostateczny odbiór Dokumentacji potwierdzony będzie podpisanym Protokołem Odbioru.
6. Jeżeli zgłoszone uprzednio uwagi nie zostały uwzględnione w poprawionej wersji Dokumentacji, Zamawiający może odmówić odbioru poprawionej wersji Dokumentacji i zastosować odpowiednie sankcje wynikające z umowy, aż do momentu uwzględnienia wszystkich uwag.
7. Do terminu uruchomienia i wdrożenia Systemu wlicza się czas niezbędny na czynności odbioru Dokumentacji.

# Szkolenia

1. Zamawiający wymaga, aby szkolenia zostały przeprowadzone na infrastrukturze i sprzęcie jak również lokalizacji będących w jego dyspozycji. Sprzęt i lokalizację, o których mowa w zdaniu poprzednim zapewnia Zamawiający.
2. Na 14 dni przed planowanym rozpoczęciem szkoleń, chyba, że Strony ustalą inaczej, Wykonawca przygotuje „Szczegółowy Plan Szkoleń” zawierający:

a. harmonogram szkoleń,

b. zakres szkolenia,

c. wielkość grupy,

d. minimalne wymagania wobec przystępujących do szkoleń,

e. materiały szkoleniowe.

1. Przedstawiciele Zamawiającego zatwierdzą przedstawiony „Szczegółowy Plan Szkoleń” w ciągu 3 Dni od jego otrzymania. Po zatwierdzeniu ww. planu, jakiekolwiek zmiany terminów, bądź innych istotnych warunków szkoleń, są dopuszczalne jedynie za zgodą obu Stron.
2. W dniu rozpoczęcia szkolenia każdy jego uczestnik otrzymuje materiały szkoleniowe.
3. W przypadku zastrzeżeń, co do sposobu i zakresu prowadzonych szkoleń Wykonawca uzgodni z Zamawiającym wprowadzenie odpowiednich modyfikacji programu szkoleniowego.
4. W przypadku, gdy z winy Wykonawcy szkolenie nie odbyło się w wyznaczonym terminie Zamawiający ma prawo zastosować odpowiednie kary umowne.

# Modyfikacje

1. W przypadku konieczności wykonania modyfikacji, Zamawiający zobowiązany jest do zgłoszenia konieczności modyfikacji na piśmie lub w formie elektronicznej.
2. W terminie 5 Dni od daty zgłoszenia Wykonawca zobowiązany jest do przedstawienia Zamawiającemu, wyceny pracochłonności wykonania modyfikacji wraz z orientacyjnym terminem oraz proponowanym sposobem realizacji zgłoszenia.
3. Po ustaleniu warunków realizacji modyfikacji dotyczących, co najmniej:
	1. pracochłonności, terminu i sposobu realizacji (wraz ze wskazaniem ewentualnych skutków ubocznych), Wykonawca przystąpi do jej wykonania.
	2. Odbiór modyfikacji nastąpi zgodnie z procedurą, opisaną dla odbioru Systemu.
	3. W przypadku, gdy wprowadzenie modyfikacji wywoła skutki uboczne, o których Wykonawca nie poinformował Zamawiającego przy ustalaniu warunków realizacji, Wykonawca ma obowiązek usunięcia skutków ubocznych,
	4. na swój koszt w ustalonym przez Strony terminie.
4. Zamawiający zweryfikuje spełnienie wymagań, zgodnie z procedurą opisaną dla odbioru Systemu.

# Wprowadzanie zmian (Usuwania błędów)

1. Wykonawca wykona i wprowadzi Zmiany, wynikające ze zgłoszonych błędów.
2. Wykonawca zapewnia dla każdej Wersji generowanie komunikatów umożliwiających zidentyfikowanie błędów.
3. Za błąd (zwany w Umowie Błędem) Strony uznają brak działania Oprogramowania lub Oprogramowania Aplikacyjnego, brak działania lub nieprawidłowe działanie udokumentowanej jego funkcji.
4. Za Błąd uważa się także brak działania lub nieprawidłowe działanie Oprogramowania Aplikacyjnego wynikające z braku kompatybilności z poszczególnymi wersjami środowiska.
5. Za Błąd nie uznaje się jednak nieprawidłowości wynikających z działania sprzętu, urządzeń peryferyjnych, systemu operacyjnego i jego ustawień, oprogramowania narzędziowego, bazy danych oraz wirusów komputerowych, nieautoryzowanego dostępu oraz użytkowania niezgodnego z dokumentacją.
6. Za Błąd nie uznaje się też nieprawidłowości wynikających ze stanu parametrów konfiguracyjnych Oprogramowania i środowiska, na którym oprogramowanie funkcjonuje chyba, że wartości parametrów konfiguracyjnych zostały wprowadzone przez Wykonawcę lub zgodnie z zaleceniami Wykonawcy, albo wynikają z Dokumentacji.
7. Rodzaje Błędów - W zależności od tego, w jaki sposób Błąd wpływa na realizację zadań Zamawiającego, Zamawiający może zakwalifikować Błędy do następujących kategorii:
	1. **Błąd Krytyczny** - Błąd uniemożliwiający eksploatację Oprogramowania lub Oprogramowania Aplikacyjnego lub powodujący utratę, lub uszkodzenie danych i jednocześnie niepozwalający na znalezienie takiego sposobu używania Oprogramowania, aby obejść skutki jego wystąpienia, bez istotnego wydłużenia czasu wykonywanych operacji. Za błąd krytyczny uważane są także problemy z wydajnością Oprogramowania w przypadku, gdy spadek wydajności Oprogramowania powoduje zagrożenie realizacji ustawowych obowiązków Zamawiającego.
	2. **Błąd Istotny** - Błąd uniemożliwiający eksploatację Oprogramowania lub powodujący utratę danych, lub powodujący uszkodzenie danych i jednocześnie pozwalający na znalezienie takiego sposobu używania Oprogramowanie, aby obejść skutki jego wystąpienia, bez istotnego wydłużenia czasu wykonywanych operacji.
	3. **Błąd Zwykły** - Błąd, który w danym okresie utrudnia realizację zadań Zamawiającego na tyle, że nie jest zasadna jego realizacja w terminach dla Błędów Pozostałych.
8. Wykonanie Zmiany (usunięcie Błędu) i jej dostarczenie nastąpi w następujących

terminach:

* **Błąd Krytyczny** - w ciągu 1 dnia od zgłoszenia przez Zamawiającego oraz wprowadzenie do najbliższej Wersji (chyba, że Strony postanowią inaczej),
* **Błąd Istotny** - w ciągu 2 dni roboczych od dnia zgłoszenia przez Zamawiającego oraz wprowadzenie do najbliższej Wersji (chyba, że Strony postanowią inaczej),
* **Błąd Zwykły** - w ciągu 10 dni roboczych od dnia zgłoszenia przez Zamawiającego oraz wprowadzenie do najbliższej Wersji (chyba, że Strony postanowią inaczej),
1. Czas reakcji Wykonawcy na Błędy wynosi:
	1. 1 (jedną) godzinę dla błędów krytycznych.
	2. 1 (jeden) dzień roboczy dla błędów pozostałych.

Brak w tym czasie reakcji po stronie Wykonawcy oznacza, że Wykonawca zaakceptował klasyfikację zgłoszenia.

1. Wykonawca zobowiązuje się usunąć Błędy w terminach określonych powyżej, chyba że Strony ustalą inaczej.
2. Strony uznają ww. termin wykonania Zmiany (usunięcia Błędu) za dotrzymany, jeżeli w ww. terminie Wykonawca zastosuje tymczasowe obejście, umożliwiające korzystanie z funkcji Oprogramowania bez istotnego, z punktu widzenia działalności Zamawiającego, wydłużenia czasu wykonywanych operacji i bez utraty danych. Zastosowanie obejścia nie zwalnia Wykonawcy z obowiązku wykonania Zmiany (usunięcia Błędu) w uzgodnionym przez Strony dodatkowym terminie, który Strony są zobowiązane ustalić w ciągu 2 dni od daty zgłoszenia. W przeciwnym przypadku termin wykonania Zmiany upływa 10 dnia od daty zgłoszenia.

# Dostosowanie, Instalacja Systemu, Konfiguracja

1. Wykonawca zobowiązany jest do Dostawy Systemu, Instalacji Systemu i Konfiguracji wszystkich niezbędnych komponentów środowiska w terminach uzgodnionych z Zamawiającym.
2. Wykonawca po Instalacji Systemu wykona Konfigurację i dokona dostosowań do prawidłowego i optymalnego działania Systemu, a także przetestuje wszystkie operacje systemowe i funkcje Systemu.
3. W szczególnych przypadkach dostosowanie dotyczyć będzie integracji z oprogramowaniem funkcjonującym u Zamawiającego.
4. Wykonawca dokona także uzupełnienia słowników.
5. Wszelkie prace w środowisku Zamawiającego Wykonawca zaplanuje i przeprowadziw uzgodnieniu z Zamawiającym.
6. Wykonawca zobowiązany jest do zapewnienia w siedzibie Zamawiającego wsparcia technicznego oraz usług serwisowych w ciągu całego procesu testowania i wdrażania, w zakresie nie mniejszym niż przewidziany w okresie gwarancji i wsparcia technicznego opisanego w OPZ.

# Warunki i zakres licencji

* 1. W ramach wynagrodzenia, dla dostarczanego Oprogramowania Wykonawca przekazuje lub udziela Zamawiającemu licencji lub sublicencji na warunkach określonych przez producenta, które to licencje lub sublicencje będą wymienione i szczegółowo opisane w dokumentacji powykonawczej.
	2. Na czas wdrożenia i testów Systemu Wykonawca przekazuje i udziela Zamawiającemu na Oprogramowanie Aplikacyjne lub na poszczególne, wyodrębnione części Oprogramowania Aplikacyjnego, stanowiące odrębny przedmiot licencjonowania, niewyłącznej, przenaszalnej licencji lub sublicencji na polach eksploatacji wymienionych w ust. 6 obowiązującej na terytorium Rzeczypospolitej Polskiej.
	3. Począwszy od dnia odbioru Systemu Wykonawca przekazuje i udziela Zamawiającemu, na Oprogramowanie Aplikacyjne lub na poszczególne, wyodrębnione części Oprogramowania Aplikacyjnego, stanowiące odrębny przedmiot licencjonowania, niewyłącznej, przenaszalnej licencji lub sublicencji na korzystanie z Oprogramowania Aplikacyjnego, na terenie Rzeczypospolitej Polskiej na nieograniczonej liczbie stanowisk, licencje nie są przypisane do komputera/stanowiska/pracownika. Ilekroć w postanowieniach Umowy lub OPZ mowa jest o Oprogramowaniu Aplikacyjnym postanowienia te odnoszą się również do poszczególnych, wyodrębnionych części Oprogramowania Aplikacyjnego, stanowiących odrębny przedmiot licencjonowania. Wykaz udzielonych licencji - Załącznik nr. 3
	4. Licencji, o której mowa w ust. 3 udziela się na okres 30 lat z 5 letnim terminem wypowiedzenia, ze skutkiem na koniec następnego roku kalendarzowego.
	5. Licencja, o której mowa w ust. 3, obejmuje automatycznie kolejne aktualizacje, modyfikacje i rozszerzenia Systemu wprowadzone zarówno przez samego Wykonawcę, jak i zamówione przez Zamawiającego, na polach eksploatacji wskazanych w ust. 6.
	6. Licencja, o której mowa w ust. 3, udzielona jest na polach eksploatacji obejmujących:
		1. prawo do trwałego lub czasowego zwielokrotnienia Oprogramowania Aplikacyjnego w całości lub w części, w sposób określony Dokumentacją, w celu wprowadzania do pamięci komputera, uruchamiania, stosowania lub przechowywania i wyświetlania oprogramowania;
		2. prawo do łączenia z innym oprogramowaniem komputerowym;
		3. przystosowywania, zmiany układu wykonania lub jakichkolwiek innych zmian w programie komputerowym, Zamawiającemu przysługuje prawo do sporządzania niezbędnej liczby kopii Oprogramowania Aplikacyjnego jako kopii zapasowej;
		4. wielokrotne użycie jednego obrazu nośnika w procesie Instalacji Systemu i tworzenia kopii zapasowych;
		5. obserwowanie, używanie i testowanie funkcjonowania Oprogramowania Aplikacyjnego w celu poznania jego idei zasad funkcjonowania, również przez podmioty trzecie, w celu osiągnięcia współdziałania (interoperacyjności) z niezależnie wytworzonym oprogramowaniem.
	7. Przekazanie praw, o których mowa w ust. f, obejmuje wszystkie wersje Oprogramowania Aplikacyjnego, jakie muszą być dostarczone Zamawiającemu przez Wykonawcę w ramach niniejszej umowy.
	8. Wykonawca może wypowiedzieć Zamawiającemu prawo do korzystania z Systemu bez zachowania terminu określonego w ust. 4 wyłącznie w przypadkach określonych w ust. 9, z zastrzeżeniem postanowień ust. 10 oraz bezwzględnie obowiązujących przepisów prawa.
	9. Wykonawca może wypowiedzieć licencję po uzyskaniu prawomocnego wyroku sądowego, gdy Zamawiający:
		1. narusza warunki licencyjne w odniesieniu do miejsca, zakresu lub sposobu korzystania z Systemu lub jego części;
		2. w inny sposób narusza prawa autorskie do Systemu lub warunki licencji określone w niniejszej Umowie.
	10. Przed skorzystaniem z prawa wypowiedzenia licencji, zgodnie z ust. i, Wykonawca wezwie Zamawiającego do zaniechania wskazanych przez Wykonawcę naruszeń ww. warunków, wyznaczając na to 7 dniowy termin. Po bezskutecznym upływie terminu, Wykonawca może wypowiedzieć licencję z zachowaniem terminu wypowiedzenia określonego w ust. 4.
	11. Wykonawca nie ma prawa do wypowiedzenia licencji, nawet w przypadkuuzyskania wyroku sądowego, o którym mowa w ust 9, jeśli Zamawiający zaniechał naruszeń i usunął skutki naruszeń.
	12. Wykonawca jest odpowiedzialny względem Zamawiającego za wszelkie wady prawne Systemu, a w szczególności za ewentualne roszczenia osób trzecich wynikające z naruszenia praw własności intelektualnej, w tym za nieprzestrzeganie przepisów ustawy z dnia 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych -j.t.Dz.U.2006r. Nr 90, poz. 631, z późn. zm. Uprawnienia z tytułu rękojmi za wady prawne Systemu wygasają z upływem dwóch lat od chwili, kiedy Zamawiający dowiedział się o istnieniu wady. Strony zgodnie oświadczają, iż wydłużają okres rękojmi za wady fizyczne Systemu na okres 2 lat, który biegnie od daty podpisania Protokołu Odbioru Systemu.
	13. Wykonawca gwarantuje, że System będący przedmiotem Umowy nie jestobciążony prawami osób trzecich i że w razie udzielenia licencji lub sublicencji na ten System, Zamawiający korzystając z tego Systemu nie naruszy w jakikolwiek sposób praw autorskich osób trzecich.
	14. W przypadku wystąpienia przez osoby trzecie z roszczeniami wobecZamawiającego wynikającymi z ewentualnych naruszeń praw własności intelektualnej i powstałymi w wyniku korzystania przez Zamawiającego z przedmiotów umowy, Wykonawca zobowiązuje się do podjęcia na swój koszt wszelkich kroków prawnych zapewniających Zamawiającemu należytą ochronę przed takimi roszczeniami, a w szczególności zobowiązuje się wystąpić w miejsce Zamawiającego, lub w przypadku braku takiej możliwości – przystąpić po stronie Zamawiającego, do wszelkich postępowań toczących się przeciwko Zamawiającemu. W przypadku wydania orzeczenia sądowego czasowego, lub ostatecznego, zakazującego korzystania z utworów dostarczonych Zamawiającemu w ramach wykonywania niniejszej Umowy, Wykonawca nie później, niż w terminie 14 dni od daty wydania takiego orzeczenia na własny koszt dostarczy i zainstaluje u Zamawiającego utwory o funkcjach zamiennych (równoważnych) do utworów, których dotyczy orzeczenie i zapewni Zamawiającemu swobodne korzystanie z tych utworów na podstawie licencji, sublicencji, cesji praw, najmu itp. Wykonawca pokryje wszelkie szkody i koszty zasądzone od Zamawiającego w takich procesach lub postępowaniach. Jeżeli dostarczone Produkty zostaną uznane za naruszające patenty, inne prawa własności przemysłowej czy prawa autorskie, Wykonawca na swój koszt i według swojego wyboru:
		1. uzyska dla Zamawiającego prawo do kontynuowania używania takiego Sprzętu lub Oprogramowania, lub dokona wymianę Sprzętu lub Oprogramowania Licencjonowanego na nie naruszające patentów i innych praw własności przemysłowej, praw autorskich, lub zmodyfikuje go w taki sposób, aby naruszenia nie miały miejsca, lub dostarczy inne rozwiązanie funkcjonalne pozwalające Zamawiającemu na nieprzerwane świadczenie usług w tym samym zakresie i co najmniej takiej samej jakości.
	15. Wykonawca, w ramach wynagrodzenia, o którym mowa w § 7 ust.1 Umowy,po odbiorze Dokumentacji, udziela Zamawiającemu wyłącznej licencji do Dokumentacji powykonawczej, na niżej wymienionych polach eksploatacji, zaś dla Dokumentacji Użytkownika, Administratora i szkoleniowej udziela Zamawiającemu niewyłącznej licencji lub ewentualnie sublicencji na następujących polach eksploatacji:
		1. wprowadzanie/zapisywanie w pamięci komputerów,
		2. trwałego lub czasowego zwielokrotniania Dokumentacji w całości lub części,
		3. odtwarzanie,
		4. przechowywanie,
		5. sporządzanie niezbędnej liczby kopii zapasowych (kopii bezpieczeństwa) nośników
		6. instalacyjnych i nośników z zainstalowanym oprogramowaniem,
		7. wyświetlanie,
		8. użytkowanie,
		9. stosowanie,
		10. przystosowywanie, zmiany układu wykonania, innych zmian,
		11. polach eksploatacji wymienionych w art. 75 ustawy z dnia 4 lutego 1994 r. o prawie
		12. autorskim i prawach pokrewnych;
		13. przekazanie w części lub całości i wykorzystywanie przez podmioty trzecie w celu osiągnięcia współdziałania niezależnie stworzonego programu komputerowego.
		14. prawo do wykonywania zależnego prawa autorskiego na polach eksploatacji wymienionych powyżej,
		15. prawo zezwalania na wykonywanie zależnego prawa autorskiego na polach eksploatacji wymienionych powyżej.
	16. Udzielenie Zamawiającemu licencji do Dokumentacji następuje z chwilą podpisaniaprzez Strony Protokołu Odbioru.
	17. Wraz z przekazaniem nośnika Wykonawca przenosi na Zamawiającego prawa własności do nośnika.

# Dokumentacja

1. Wykonawca w ramach realizacji umowy dostarczy Zamawiającemu Dokumentację:
	1. Użytkownika;
	2. Administratora;
	3. Szkoleniową;
	4. Powykonawczą.
2. Wykonawca zobowiązany jest do utrzymywania dostarczonej Dokumentacji w aktualności.
3. Aktualizacja Dokumentacji następuje każdorazowo po wprowadzeniu przez Wykonawcęzmian w Systemie. W przypadku wprowadzenia zmian do Systemu wymagających odzwierciedlenia w Dokumentacji, zarówno wskutek pojawienia się aktualizacji Systemu, jak i poprawy błędów lub zmiany konfiguracji, Wykonawca dostarczy zaktualizowaną Dokumentację (lub tę jej część, której zmiana dotyczy) w terminie nieprzekraczającym 15 dni od daty dokonania zmian w Systemie chyba, że Strony ustalą inaczej.
4. Dostarczenie zaktualizowanej przez Wykonawcę Dokumentacji jest warunkiem koniecznym dla podpisania przez Zamawiającego Końcowego Protokołu Odbioru.
5. Dokumentacja musi być sporządzona w języku polskim, chyba że dotyczy oprogramowania narzędziowego obcego pochodzenia, wykorzystywanego w Systemie, dla którego nie ma dokumentacji w języku polskim, w takim przypadku Dokumentacja może zostać przekazana w języku angielskim.
6. Dokumentacja musi być dostarczona w formie papierowej i elektronicznej na nośniku CD/DVD, w postaci umożliwiającej uzyskanie jej wydruku przy pomocy powszechnie używanych narzędzi.
7. Wykonawca zobowiązany jest do dostarczenia Dokumentacji, o której mowa w pkt 1 niniejszego paragrafu, w formie papierowej w 1 egzemplarzu oraz elektronicznej w pliku PDF.

# Dokumentacja szkoleniowa

Dokumentacja szkoleniowa musi zawierać ścieżki postępowania.

# Dokumentacja Administratora

1. Wykonawca dostarczy dokumentację administratora.
2. Dokumentacja Administratora aplikacji musi opisywać kolejność czynności i zakres możliwych danych do wprowadzenia oraz sposób postępowania w sytuacjach szczególnych i awaryjnych.
3. Dokumentacja Administratora powinna być dostępna w postaci elektronicznej umożliwiającej przeszukiwanie oraz odnajdowanie konkretnych tematów, zarówno z poziomu aplikacji oraz w postaci umożliwiającej jej wydruk.
4. Dokumentacja Administratora obejmować będzie, co najmniej:
	1. instrukcję instalacji i konfiguracji Oprogramowania i Oprogramowania Aplikacyjnego,
	2. opis parametrów instalacyjnych i konfiguracyjnych Oprogramowania i Oprogramowania Aplikacyjnego wraz z opisem dopuszczalnych wartości i ich wpływem na działanie Oprogramowania i Oprogramowania Aplikacyjnego obejmujący także wartości zalecanych ustawień,
	3. opis możliwych do zastosowania możliwych ról i uprawnień wraz z ich wpływem na działania Oprogramowania i Oprogramowania Aplikacyjnego,
	4. opis nadawania ról i uprawnień,

# Dokumentacja użytkownika

1. Dokumentacja użytkownika musi zawierać opis pełnej funkcjonalności oprogramowania w sposób umożliwiający samodzielne użytkowanie Oprogramowania,
2. W zakresie kluczowych funkcji użytkowych dokumentacja użytkownika zawieraćbędzie „ścieżki postępowania”,
3. Dostarczona przez Wykonawcę Dokumentacja użytkownika, w tym „ścieżki postępowania”, zostaną przygotowane w sposób umożliwiający Zamawiającemu dodanie ich, jako odrębnych artykułów do bazy wiedzy.

# Dokumentacja powykonawcza

1. Dokumentacja powykonawcza zawierać będzie zestaw parametrów systemowych i bazodanowych, niezbędnych dla prawidłowej i efektywnej pracy Systemu. Wykonawca zobowiązany jest do utrzymywania dokumentacji konfiguracyjnej w aktualności,
2. Dokumentacja powykonawcza m.in. musi dotyczyć:
	1. dostarczonego Systemu (usług, oprogramowania narzędziowego – o ile jest wymagane), wraz z opisem uruchomionego środowiska na dzień przekazania dokumentacji;
	2. procedury odtworzeniowej środowiska aplikacyjnego i bazodanowego.
3. Dokumentacja Powykonawcza musi obejmować, dokumentację Użytkownika oraz Administratora aplikacji.
4. Dokumentacja Powykonawcza musi zawierać, co najmniej:
	1. spis treści.
	2. Ogólny opis Systemu wraz z elementami składowymi;
	3. schematy graficzne przedstawiające ogólną budowę Systemu,
	4. szczegółowy opis poszczególnych komponentów Systemu,
	5. opis każdego z WebService’ów lub plików wymiany wraz ze wskazaniem danych wejściowych oraz danych wyjściowych,
	6. instrukcję dla użytkownika i administratora systemu,
	7. sposób wykonywania kopii zapasowej serwera aplikacyjnego oraz sposób odtwarzania systemu po awarii całego serwera,
	8. spis parametrów Oprogramowania, które mają wpływ na poprawne i wydajne funkcjonowanie Systemu,
	9. zrzuty konfiguracyjne Systemu z wyłączeniem serwera baz danych, który Zamawiający posiada i udostępnia do realizacji zadania.
5. Wykonawca zobowiązany jest do dostarczenia Dokumentacji Użytkownika, Administratora, Szkoleniowej i Powykonawczej, sporządzonej w języku polskim w formie papierowej w 1 egzemplarzu oraz elektronicznej w pliku PDF.

# Licencja na kody źródłowe

1. Zamawiający na warunkach określonych w umowie otrzyma licencje do kodów źródłowych do systemu wraz z wydaniem tych kodów źródłowych.
2. W terminie wskazanym w §7 ust. 6 Umowy Wykonawca przekaże Zamawiającemu Kod Źródłowy Systemu wraz z dokumentacją techniczną. Kod źródłowy będzie opatrzony komentarzami zawierającymi krótki opis jego działania, definicje użytych zmiennych oraz numer Wersji Systemu, w której dokonano ostatnich Modyfikacji. Kod Źródłowy obejmował będzie zbiór plików źródłowych, elementów tworzących interface użytkownika, zainstalowanej u Zamawiającego Wersji Systemu. W skład tego zbioru wchodzą:
	1. formularze, menu,
	2. raporty,
	3. biblioteki,
	4. ikony,
	5. szablony dokumentów,
	6. inne jednostki programowe
	7. skrypty tworzące strukturę baz danych, czyli:
		* 1. tabele,
			2. perspektywy,
			3. wyzwalacze,
			4. indeksy,
			5. role bazodanowe,
	8. migawki,
	9. a także tę część kodu aplikacji, która jest składowana w bazie danych w postaci pakietów, funkcji i procedur.

W razie potrzeby przekształcenia danych (zawartych w tabelach baz danych przed

modyfikacją) tak, by spełnione były wymogi aktualnej aplikacji, Wykonawca jest

zobowiązany przygotować i przekazać Zamawiającemu odpowiednie skrypty w ramach dostarczanego Kodu Źródłowego. Kod Źródłowy Systemu wraz z opisem struktur katalogów kodów źródłowych oraz opisem standardu nazewnictwa plików źródłowych i wynikowych (nagłówek kodu źródłowego składający się z: nazwy pliku, daty powstania Wersji); opis obejmuje wszystkie definicje zmiennych i stałych, opis nagłówków procedur i metod zawierający listy i opis argumentów, danych wynikowych oraz skondensowanego opisu działania; Kod Źródłowy i kod wynikowy musi być zgodny z dostarczoną Wersją Systemu; wymagane przez Zamawiającego dokumenty muszą być dostarczone w wersji polskojęzycznej. Skomentowane muszą być kluczowe instrukcje sterujące – warunki, wyniki.

1. Integralną częścią Kodu Źródłowego jest zrzut baz danych (dump) wykonany bez danych. Zrzut ten winien wykonać Zamawiający bezpośrednio po instalacji nowej Wersji Systemu w obecności przedstawiciela Wykonawcy, który podpisze protokół stwierdzający poprawność wykonania zrzutu bazy danych (dump). Powyższy zrzut stanowi część Kodu Źródłowego.
2. Kod Źródłowy i wszystkie dostarczone materiały, o których mowa w ust. 4 będą aktualizowane z zachowaniem zasad ust. 9 oraz będą w stanie umożliwiającym pełną kompilację konsolidację Oprogramowania Aplikacyjnego.
3. Wraz z Kodem źródłowym Wykonawca dostarczy:
	1. specyfikację środowiska sprzętowo-systemowego wymaganego do przeprowadzenia procedury generacji kodu wynikowego,
	2. instrukcję generacji kodu wynikowego (systemu docelowego),
	3. narzędzia do przygotowania wersji instalacyjnych wytworzonego oprogramowania (wersji pełnej, aktualizacji, łat) wraz z odpowiednią dokumentacją opisującą ich użycie (w języku polskim). W przypadku gdy do przygotowania wersji instalacyjnych konieczne będzie użycie narzędzi licencjonowanych, Wykonawca zobowiązany jest w ramach niniejszej umowy i wynagrodzenia, o którym mowa w §6 ust. 1 Umowy dostarczyć Zamawiającemu odpowiednie licencje.
	4. narzędzia do instalacji wytworzonego oprogramowania wraz ze szczegółowym opisem instalacji. W przypadku, gdy do instalacji wytworzonego oprogramowania konieczne będzie użycie narzędzi licencjonowanych, Wykonawca zobowiązany jest w ramach niniejszej umowy i wynagrodzenia, o którym mowa §6 ust. 1 Umowy dostarczyć Zamawiającemu odpowiednie licencje.
4. W terminie uzgodnionym przez Strony Wykonawca zaprezentuje Zamawiającemu proces generowania Systemu z dostarczonych Kodów Źródłowych, zgodnie z regułami i dokumentacją, o których mowa w niniejszym paragrafie.
5. Dostarczony kompletny Kod Źródłowy wraz z dokumentacją techniczną powinien umożliwiać odtworzenie kompletnego Oprogramowania Aplikacyjnego bez konieczności zaangażowania (udziału) Wykonawcy. Strony zgodnie zastrzegają, iż w przypadku, gdy dostarczony Kod źródłowy nie będzie kompletny zastosowanie mają postanowienia – Uzupełnienie Kodów Źródłowych, Dokumentacji niniejszego opisu przedmiotu zamówienia.
6. Wykonawca gwarantuje, że Dostarczony Kod Źródłowy wraz z dokumentacją techniczną i pozostałymi elementami Dokumentacji zawiera wszystkie informacje umożliwiające podmiotom trzecim świadczenie usług nadzoru autorskiego oraz wykonywanie dowolnych Modyfikacji Systemu oraz struktur baz danych. W przypadku niespełnienia powyższego warunku Wykonawca zobowiązany jest do stosownych uzupełnień zgodnie z postanowieniami – Uzupełnienie Kodów Źródłowych, Dokumentacji niniejszego opisu przedmiotu zamówienia.
7. Strony zgodnie oświadczają, iż w celu zapewnienia kompletności i potwierdzenia jakości złożonych Kodów Źródłowych i materiałów, o których mowa w ust. 4 Zamawiający uprawniony będzie do przeprowadzenia z udziałem Wykonawcy próbnej kompilacji i konsolidacji. W tym przypadku Zamawiający zawiadomi Wykonawcę o terminie i miejscu przeprowadzenia próbnej kompilacji i konsolidacji oraz o środowisku, na którym zostanie przeprowadzona próbna kompilacja.
8. Do Kodów Źródłowych Systemu każdorazowo musi zostać dołączona szczegółowa procedura kompilacji i konsolidacji oraz zaktualizowane pozostałe elementy Dokumentacji. Kody Źródłowe i szczegółowa procedura dotycząca przebiegu czynności kompilacji winny być dostarczone w wersji elektronicznej, redundantnie – na dwóch nośnikach o gwarantowanej trwałości (nie krótszej niż 10 lat) w zalakowanych kopertach.
9. Kody źródłowe wraz z całą Dokumentacją stanowią własność Zamawiającego wraz z przekazaniem nośników Wykonawca przenosi na Zamawiającego prawa własności tych nośników.
10. Przekazanie Kodów Źródłowych wraz z Dokumentacją potwierdzone zostanie podpisanym przez Strony Protokołem Przekazania Kodów Źródłowych/ Dokumentacji .
11. Wykonawca upoważnia Zamawiającego do wykorzystania Kodów Źródłowych i Dokumentacji w zakresie wynikającym z niniejszej Umowy i udzielonych licencji.
12. Wykonawca, w ramach wynagrodzenia, o którym mowa w § 6 ust. 18 Umowy, z dniem przekazania Kodów źródłowych udziela Zamawiającemu, obowiązującej na terytorium Rzeczypospolitej Polskiej, niewyłącznej licencji na korzystanie z Kodów Źródłowych na polach eksploatacji opisanych w ust. 12.
13. Licencja, o której mowa w ust. 12, jest udzielona na rzecz Zamawiającego oraz jednostek organizacyjnych i jednostek budżetowych Urzędu Miasta Wrocław wyłącznie w celu utrzymywania i rozwoju Systemu, przez Zamawiającego lub podmioty trzecie mające podpisaną z Zamawiającym umowę na utrzymanie i rozwój Systemu, na własne potrzeby Zamawiającego na następujących polach eksploatacji:
	1. wprowadzanie i zapisywanie w pamięci komputerów;
	2. trwałego zwielokrotniania dokumentacji technicznej w całości lub części;
	3. odtwarzanie, przechowywanie, wyświetlanie, użytkowanie, stosowanie, przystosowywanie oraz zmiany układu wykonania i inne zmiany;
	4. sporządzanie niezbędnej liczby kopii zapasowych (kopii bezpieczeństwa) nośników;
	5. modyfikacje Kodu Źródłowego wynikające z konieczności zmiany Systemu w jego celu dostosowania do zmian w powszechnie obowiązujących przepisach prawa lub przepisach prawa miejscowego, z zastrzeżeniem pozostałych warunków licencyjnych określonych w Umowie,
	6. modyfikacje Kodu Źródłowego wynikające z konieczności zmiany Systemu, w celu jego łączenia z oprogramowaniem komputerowym, przystosowywania, zmiany układu wykonania lub jakichkolwiek innych zmian w Systemie,
	7. prawo do udostępnienia, udzielenia licencji bądź sublicencji do Kodów źródłowych w celu powierzenia czynności związanych z eksploatacją, utrzymaniem (w tym usuwanie błędów), aktualizacją, rozbudową i rozwojem Systemu, łącznie z prawem dekompilacji/użycia/modyfikacji/ wykorzystania Kodu źródłowego i struktur baz danych, podmiotowi trzeciemu, w tym wykonawcy, z którym Zamawiający będzie miał zawartą umowę na utrzymanie i rozwój Systemu na polach eksploatacji wymienionych w ust. 12,
	8. prawo do opublikowania i udostępnienia Kodów źródłowych uczestnikom postępowania o udzielenie zamówienia publicznego na utrzymanie i rozwój Systemu.
14. Przekazanie praw, o których mowa w ust. 15, obejmuje wszystkie Wersje Kodów Źródłowych, jakie muszą być dostarczone Zamawiającemu przez Wykonawcę w ramach niniejszej Umowy w okresie jej obowiązywania.
15. Licencji, o której mowa w ust. 11, udziela się na okres 30 lat z 5 letnim terminem wypowiedzenia, ze skutkiem na koniec następnego roku kalendarzowego.
16. W ramach wynagrodzenia opisanego w §6 ust. 18 Umowy z chwilą wydania Kodów Źródłowych Wykonawca przenosi w całości na Zamawiającego nieograniczone w czasie, niewyłączne prawo do wykonywania praw zależnych do Kodów źródłowych oraz systemu baz danych, w szczególności poprzez wprowadzanie zmian, modyfikacji uzupełniania Kodów Źródłowych oraz baz danych (prawa zależne) oraz niewyłączne, nieograniczone w czasie, prawo do zezwalania na wykonywanie zależnego prawa autorskiego do wszystkich. Produktów i utworów powstałych z związku z wykorzystaniem Kodów Źródłowych oraz baz danych lub nabytych w trakcie obowiązywania Umowy w celu realizacji czynności związanych z eksploatacją, utrzymaniem, aktualizacją, rozbudową i rozwojem Systemu.
17. Wykonawca wyraża zgodę na wykonywanie w jego imieniu przez Zamawiającego autorskich praw osobistych do Kodów źródłowych według potrzeb Zamawiającego wynikających z realizacji czynności związanych z eksploatacja, utrzymaniem, aktualizacją, rozbudową i rozwojem Systemu.
18. Przed skorzystaniem z prawa wypowiedzenia licencji do Kodów Źródłowych lub Dokumentacji, Wykonawca wezwie Zamawiającego do zaniechania wskazanych przez Wykonawcę naruszeń ww. warunków, wyznaczając na to 30 dniowy termin. Po bezskutecznym upływie terminu, Wykonawca może wypowiedzieć licencję z zachowaniem umownego terminu wypowiedzenia właściwego dla Kodów źródłowych lub Dokumentacji. Postanowienia powyższego ustępu nie maja zastosowania przypadku uzyskanie przez Wykonawcę prawomocnego wyroku sądu powszechnego, stwierdzającego naruszania przez Zamawiającego warunków licencji do Kodów Źródłowych lub Dokumentacji.
19. Wykonawca nie ma prawa do wypowiedzenia licencji dla Kodów źródłowych lub Dokumentacji, nawet w przypadku uzyskania wyroku sądowego, jeśli Zamawiający zaniechał naruszeń i usunął skutki naruszeń.
20. Wykonawca jest odpowiedzialny względem Zamawiającego za wszelkie wady prawne Kodów Źródłowych lub Dokumentacji, a w szczególności za ewentualne roszczenia osób trzecich wynikające z naruszenia praw własności intelektualnej, w tym za nieprzestrzeganie przepisów ustawy z dnia 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych - j.t. Dz. U. 2006 r. Nr 90, poz. 631, z późn. zm. Uprawnienia z tytułu rękojmi za wady prawne Kodów źródłowych lub Dokumentacji wygasają z upływem dwóch lat od chwili, kiedy Zamawiający dowiedział się o istnieniu wady.
21. Wykonawca gwarantuje, że Kody Źródłowe i Dokumentacja nie są obciążone prawami osób trzecich i że w razie udzielenia licencji na te kody, Zamawiający korzystając z tych kodów nie naruszy w jakikolwiek sposób praw autorskich osób trzecich.
22. W przypadku wystąpienia przez osoby trzecie z roszczeniami wobec Zamawiającego wynikającymi z ewentualnych naruszeń praw własności intelektualnej i powstałymi w wyniku korzystania przez Zamawiającego z przedmiotów umowy, Wykonawca zobowiązuje się do podjęcia na swój koszt wszelkich kroków prawnych zapewniających Zamawiającemu należytą ochronę przed takimi roszczeniami, a w szczególności zobowiązuje się wystąpić w miejsce Zamawiającego, lub w przypadku braku takiej możliwości – przystąpić po stronie Zamawiającego, do wszelkich postępowań toczących się przeciwko Zamawiającemu. W przypadku wydania orzeczenia sądowego czasowego, lub ostatecznego, zakazującego korzystania z Produktów dostarczonych Zamawiającemu w ramach wykonywania niniejszej Umowy, Wykonawca nie później, niż w terminie 14 dni od daty wydania takiego orzeczenia na własny koszt dostarczy i zainstaluje u Zamawiającego Produkty o funkcjach zamiennych (równoważnych) do Produktów, których dotyczy orzeczenie i zapewni Zamawiającemu swobodne korzystanie z tych Produktów na podstawie licencji, sublicencji, cesji praw, najmu itp. Wykonawca pokryje wszelkie szkody i koszty zasądzone od Zamawiającego w takich procesach lub postępowaniach. Jeżeli dostarczone Produkty zostaną uznane za naruszające patenty, inne prawa własności przemysłowej czy prawa autorskie, Wykonawca na swój koszt i według swojego wyboru uzyska dla Zamawiającego prawo do kontynuowania używania Kodów Źródłowych i Dokumentacji pod rygorem odstąpienia od Umowy z winy Wykonawcy, lub zlecenia przez Zamawiającego usunięcia naruszeń praw podmiotom trzecim na koszt Wykonawcy. W takim przypadku Zamawiający zastrzega sobie prawo potrącenia, kosztów usunięcia naruszenia praw oraz należności zasądzonych od Zamawiającego na rzecz osób trzecich z wynagrodzenia przysługującego Wykonawcy.
23. Wykonawca w ramach wynagrodzenia, o którym mowa w § 7 ust. 1 rozszerzy licencję na System, udzieloną w ramach na Umowy na Dostawę Systemu, do licencji unlimited, licencje nie są przypisane do komputera stanowiska / pracownika.
24. Wykonawca wyraża zgodę na wykonywanie w jego imieniu przez Zamawiającego autorskich praw osobistych do Dokumentacji i Kodu Źródłowego według potrzeb Zamawiającego wynikających z realizacji czynności związanych z eksploatacja, utrzymaniem, aktualizacją, rozbudową i rozwojem Systemu.
25. Powyższe postanowienia znajdą zastosowanie także do wszelkich kolejnych aktualizacji (update i upgrade) Kodów Źródłowych i Dokumentacji.

# Uzupełnianie kodów źródłowych, dokumentacji

1. Wykonawca zobowiązuje się w ramach realizacji przedmiotu Umowy, do uzupełnienia, na każde żądanie Zamawiającego, Kodów źródłowych oraz Dokumentacji, w szczególności w przypadku, gdy jest to niezbędne dla prawidłowego przeprowadzenia postępowania o udzielnie zamówienia publicznego lub świadczenia usług nadzoru autorskiego przez podmioty trzecie w szczególności, gdy:

a. zawarte w nich informacje okażą się niewystarczające dla realizacji uprawnień przysługujących Zamawiającemu z tytułu udzielonych licencji, w szczególności w zakresie świadczenia przez podmioty trzecie usług nadzoru autorskiego obejmujące czynności związanych z eksploatacją, utrzymaniem (w tym usuwanie błędów), aktualizacją, rozbudową i rozwojem Systemu, dekompilacją/użyciem/modyfikacją/ wykorzystaniem Kodu źródłowego i struktur baz danych oraz wykonywanie dowolnych modyfikacji Systemu/Elementów Systemu oraz struktur baz danych;

b. nie są one kompletne lub aktualne;

c. dostarczony kompletny Kod Źródłowy wraz z dokumentacją techniczną nie umożliwia odtworzenia kompletnego Oprogramowania Aplikacyjnego bez konieczności zaangażowania (udziału) Wykonawcy.

1. Wykonawca zobowiązany jest również do udzielania wszelkich niezbędnych wyjaśnień dotyczących Kodów źródłowych i Dokumentacji składanych w toku prowadzonego przez Zamawiającego postępowania o udzielenie zamówienia na świadczenie usług nadzoru autorskiego. Wyjaśnienia Wykonawca zobowiązany jest przekazać Zamawiającemu w terminie maksymalnie trzech dni od daty przekazania przez Zamawiającego wniosku o udzielenie wyjaśnień.
2. Wykonawca na pisemne wezwanie Zamawiającego, dokona uzupełnień w dostarczonym Kodzie źródłowym, Dokumentacji lub udzieli dodatkowych wyjaśnień w terminie określonym przez Zamawiającego.
3. Wykonawca, w ramach umowy zobowiązany jest do dokonywania uzupełnień i udzielania wyjaśnień do dnia r.

# Wsparcie techniczne i gwarancja

1. Wykonawca gwarantuje, że dostarczony System jest rozwiązaniem kompletnym i skalowalnym, spełniającym wymagania Zamawiającego, oraz że System będzie poprawnie i wydajnie pracował w środowisku Zamawiającego przeznaczonym do realizacji Umowy.
2. Na dostarczony System musi być udzielona minimum 12-miesięczna gwarancja Wykonawcy.
3. Wykonawca udzieli w tym okresie minimum 12 miesięcy wsparcia technicznego.
4. Wykonawca udziela gwarancji na wszystkie dostarczone Produkty, System oraz na zrealizowany cały przedmiot Umowy w zakresie usuwania błędów i wad w Oprogramowaniu Aplikacyjnym, w terminach i na zasadach opisanych w punkcie 8.8.
5. Wykonawca w ramach Umowy jest zobowiązany do usunięcia wszystkich Błędów zgłoszonych w okresie obowiązywania Umowy, na zasadach i terminach określonych nawet, jeśli termin usunięcia Błędu wykroczy poza okres obowiązywania Umowy.
6. W ramach wsparcia technicznego Wykonawca zobowiązuje się w ramach wynagrodzenia określonego w §7 ust. 1 Umowy do:
7. bezpośredniej diagnostyki Systemu w docelowych lokalizacjach,
8. konsultacji w zakresie obsługi technicznej i użytkowej Systemu drogą telefoniczną i mailową,
9. aktualizacji dostarczonej Dokumentacji,
10. konfiguracji Systemu,
11. poprawnego funkcjonowanie Systemu,
12. utrzymywania oprogramowania w zgodności z przepisami prawa powszechnie obowiązującego, bez konieczności ich wcześniejszego zgłoszenia przez Zamawiającego,
13. dostosowania oprogramowania do zmian wynikających ze zmian aktów prawa miejscowego oraz uchwał wydawanych przez organy stanowiące Zamawiającego;
14. Dostarczanie nowych Wersji Systemu,
15. Wykonywanie Modyfikacji w ilościach określonych w Umowie.
16. W przypadku ujawnienia się w okresie gwarancji wad lub usterek Zamawiający poinformuje o tym Wykonawcę na piśmie. Wykonawca zobowiązuje się do usunięcia w okresie obowiązywania gwarancji i rękojmi wad i/lub usterek w terminach wyznaczonych przez Zamawiającego. W przypadku nie usunięcia wad lub usterek w wyznaczonym przez Zamawiającego terminie, Zamawiający może naliczyć karę umowną zgodnie z §5 ust. 1 pkt.4 Umowy.
17. Strata lub szkoda w dostawie lub oprogramowaniu w okresie między dniem rozpoczęcia a dniem zakończenia terminu gwarancji lub rękojmi, powinna być naprawiona przez Wykonawcę na jego koszt, jeżeli utrata lub zniszczenie wynika z działań lub zaniedbania Wykonawcy.
18. Gwarantem dostaw wykonywanych przez podwykonawców jest Wykonawca.
19. Wykonawca nie ponosi odpowiedzialności z tytułu rękojmi za wady przedmiotu Umowy i z tytułu gwarancji, jakości po wykazaniu, że wada powstała wskutek działań Zamawiającego, które Wykonawca na piśmie zakwestionował. W przypadku dostarczenia oprogramowania bieg terminu rękojmi rozpoczyna się w dniu następnym po dniu podpisania każdego protokołu odbioru końcowego poszczególnych dostaw.
20. Dokonanie przez Zamawiającego bez zgody Wykonawcy, w okresie trwania gwarancji, zmian w Oprogramowaniu Aplikacyjnym, wyłącza odpowiedzialność Wykonawcy z tytułu wad Oprogramowania Aplikacyjnego, wyłącznie w zakresie, w jakim Zamawiający dokonał tych zmian.
21. Zgłoszenie awarii i usterek będzie możliwe w trybie 24/7/365.
22. Usługa wsparcia technicznego obejmuje również modyfikację systemu, która ma zapewnić prawidłowe obsługiwane przez pojawiające się w okresie świadczenia usługi aktualizacje, co najmniej następujących przeglądarek: Microsoft Edge, Mozilla Firefox; Google Chrome.
23. Aktualizacja Systemu wynikająca z konieczności poprawnej obsługi wydawanych nowych wersji przeglądarek internetowych, musi nastąpić najpóźniej w okresie 1 miesiąca od ukazania się aktualizacji przeglądarki internetowej.
24. Okres gwarancji i wsparcia technicznego rozpoczyna się od dnia podpisania Końcowego Protokołu Odbioru bez zastrzeżeń.
25. Usługa gwarancyjna świadczona ma być w miejscu instalacji Systemu.
26. Wszelkie koszty związane z naprawami gwarancyjnymi, usuwaniem ujawnionych awarii i usterek, itp. ponosi Wykonawca.
27. Okres gwarancyjny zostaje przedłużony o łączną liczbę dni, w których System był wyłączony z eksploatacji, z powodu naprawy podczas trwania okresu gwarancyjnego.
28. Wykonawca zobowiązuje się do zwrotu kosztów naprawy gwarancyjnej zrealizowanej przez Zamawiającego w przypadku, gdy dwukrotnie bezskutecznie wzywał Wykonawcę do jej wykonania.
29. Wykonawca ma obowiązek przyjmowania zgłoszeń serwisowych poprzez telefon, e-mail oraz WWW .
30. Wykonawca zapewni dostęp do systemu wsparcia klienta, za pomocą, którego Zamawiający będzie mógł:

a. uzyskać pomoc poprzez telefon lub e-mail lub WWW w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych rozwiązań,

b. zgłaszać zauważone nieprawidłowości w działaniu Systemu.