

Wymagania dla Aplikacji eRPU

Spis treści

1 Spis treści

2	Wprowadzenie	4
2.1	Cel wdrożenia	4
2.2	Uwarunkowania prawne, normy i systemy.....	4
3	Wymagania dotyczące architektury	5
3.1	Planowana architektura logiczna.....	5
3.2	Wymagania dotyczące Platformy Serwerowej	6
3.2.1	System operacyjny:	7
3.2.2	Wykorzystanie baz danych:	7
3.2.3	Wykorzystanie serwerów WWW:.....	7
4	Wymagania funkcjonalne	7
4.1	Zestawienie funkcjonalności	7
5	Wymagania pozafunkcjonalne.....	15
5.1	Zestawienie wymagań pozafunkcjonalnych.....	15
6	Integracje.....	17
6.1	Active Directory.....	17
6.2	EZD PUW	17
6.3	System BIP MK	18
6.4	System CMS UMK	19
6.5	System CSS.....	19
6.6	System GSI	19
6.7	System KADRY	20
6.8	System SEZAM	21
7	Administracja i zarządzanie uprawnieniami	21
7.1	Zarządzanie uprawnieniami.....	21
7.2	Role Użytkowników Aplikacji.....	22
8	Migracja danych.....	22
9	Dokumentacja.....	23
9.1	Wymagana dokumentacja dla zarządzania Platformą Serwerową.....	23
9.2	Wymagana dokumentacji użytkownika i technicznej dla Aplikacji.....	23
10	Analiza Przedwdrożeniowa	25

11	Kody Źródłowe.....	26
12	Standardy dla usług integracyjnych w UMK	27
13	Harmonogram Wdrożenia	28
14	Administrowanie Platformą Serwerową przez Wykonawcę	29
15	Testy.....	31
15.1	Plan Testów	31
15.2	Wymagania dotyczące wykonania testów bezpieczeństwa Aplikacji.....	31
16	Kopia Zapasowa.....	32

Definicje i skróty:

Active Directory (AD) - usługa katalogowa wdrożona w SI UMK.

Akt Kierowania – Pełnomocnictwo i Upoważnienie PMK.

ATiK – usługi asysty technicznej i konserwacji dla Aplikacji świadczone na zasadach określonych w § X.

Analiza Przedwdrożeniowa – dokument będący wynikiem procesu, podczas którego Wykonawca przeprowadzi szczegółowe uzgodnienia z Zamawiającym dotyczące wdrożenia eRPU w UMK zgodnie z wymaganiami Umowy.

Dokument analizy - Dokumentacja dostarczona w wyniku przeprowadzonej Analizy przedwdrożeniowej, o której mowa w rozdziale 10

Dokumentacja – Dokumentacja szczegółowo opisana w rozdziale 9

eRPU (Aplikacja) – Aplikacja służąca do rejestrowania aktów kierowania (pełnomocnictwa i upoważnienia PMK).

System EZD PUW (EZD PUW) – system elektronicznego zarządzania dokumentacją wdrożony w SI UMK.

Harmonogram Wdrożenia – Harmonogram o którym mowa w rozdziale 13

Jednostka - jednostka organizacyjna Gminy Miejskiej Kraków, komunalna osoba prawna lub inny podmiot realizujący zadania GMK

Komórka - komórka organizacyjna Urzędu Miasta Krakowa

Koszulka – widok w EZD PUW, który umożliwia grupowanie dokumentów, rejestrowanie i prowadzenie Sprawy. Wszystkie operacje na dokumentach (aktualizacja, usuwanie, przekazywanie, udostępnianie) odbywają się zawsze z poziomu koszulki.

Konto Integracyjne – Konto Techniczne dedykowane dla integracji EZD PUW z eRPU, do którego eRPU posiada stosowne uprawnienia w tym do wykonywania WS.

Konto Techniczne - konto użytkownika w systemie EZD PUW wdrożonym w UMK, którego login oraz przeznaczenie nie odnoszą się do fizycznego użytkownika systemu

PMK – Prezydent Miasta Krakowa.

Plan testów – Plan testów, o którym mowa w rozdziale 15

SI UMK – System Informatyczny Urzędu Miasta Krakowa.

Oprogramowanie Systemowe – oprogramowanie niezbędne do prawidłowego działania Aplikacji, w tym w szczególności: sterowniki, systemy operacyjne, oprogramowanie bazodanowe.

Platforma Serwerowa (Platforma) – rozwiązania sprzętowo-programowe stanowiące fundament dla budowy i uruchamiania usług informatycznych w SI UMK. Platforma może przyjmować postać zasobów udostępnionych z wirtualizatora Vmware (mocy obliczeniowej i przestrzeni dyskowej wraz z licencjami na systemy operacyjny lub bazodanowy), albo zasobów fizycznych (serwerów fizycznych wraz z licencjami na system operacyjny) w zależności od wyboru modelu wdrożenia.

Serwis UMK (System CMS UMK) – Serwis Informacyjny Urzędu Miasta Krakowa (intranet) wraz z systemem zarządzania treścią

Single Sign-On (SSO) – zalogowanie do komputera umożliwia dostęp do Aplikacji bez konieczności logowania do Aplikacji.

SOA UMK – wdrożone w UMK rozwiązanie informatyczne oparte o koncepcję modelu usługowego (SOA – Service-Oriented Architecture), zakładające integrację poszczególnych systemów poprzez centralną Szynę Danych.

Sprawa – zdarzenie lub stan rzeczy, w tym z zakresu postępowania administracyjnego, wymagające rozpatrzenia i podjęcia czynności służbowych lub przyjęcia do wiadomości. Założenie sprawy odbywa się z poziomu koszulki, gdzie do tego celu używamy przycisku "Założ sprawę".

System BIP MK (BIP MK)- Platforma Biuletyn Informacji Publicznej Miasta Krakowa

System CSS (CSS) - Centralny System Słowników wdrożony w SI UMK.

System GSI (GSI) - Gminny Serwis Informacyjny (ekstranet).

System KADRY (Kadry) – System dziedziny, służący do zarządzania zasobami ludzkimi i powiązanymi procesami przez cały cykl życia pracownika UMK.

System SEZAM (Sezam) – System dziedziny, służący do zarządzania kontami i uprawnieniami Użytkowników w SI UMK.

Szyna Danych - Szyna danych wykonana w technologii ESB WSO2, udostępniająca interfejsy aplikacjom poprzez WS (Web Service)

UMK – Urząd Miasta Krakowa.

Użytkownik – Użytkownik Aplikacji eRPU.

Web Service (WS) – Usługa sieciowa udostępniona w celu integracji z innymi systemami oraz eksportu/importu danych do/ze źródeł zewnętrznych

Wykonawca – Wykonawca Aplikacji eRPU.

Zamawiający - Gmina Miejska Kraków UMK.

2 Wprowadzenie

Pojęcia zapisane z wielkiej litery zostały zdefiniowane w § 1 wzoru umowy.

W UMK prowadzone są obecnie rejestry Aktów Kierowania poprzez tworzenie arkuszy kalkulacyjnych. Aby ułatwić prowadzenie rejestru konieczna jest budowa aplikacji webowej, która będzie agregowała wszystkie Akty Kierowania.

Aplikacja ma służyć do rejestracji i uzupełniania o określone metadane Aktów Kierowania, które pochodzą z systemu EZD PUW bądź wyjątkowo będą dodawane manualnie.

Uzupełnione i zarejestrowane Akty Kierowania będą publikowane poprzez integrację z Systemem GSI i Serwisem UMK.

2.1 Cel wdrożenia

Wdrożenie ma na celu uporządkowanie prowadzenia rejestrów Aktów Kierowania.

Celem wdrożenia jest wykonanie eRPU oraz integracja z poszczególnymi systemami zgodnie z wytycznymi niniejszego dokumentu. Wykonawca przy wsparciu Zamawiającego dokona również migracji obecnych rejestrów prowadzonych w formie arkuszy kalkulacyjnych do eRPU.

2.2 Uwarunkowania prawne, normy i systemy

Aplikacja musi być zgodna z następującymi aktami prawnymi:

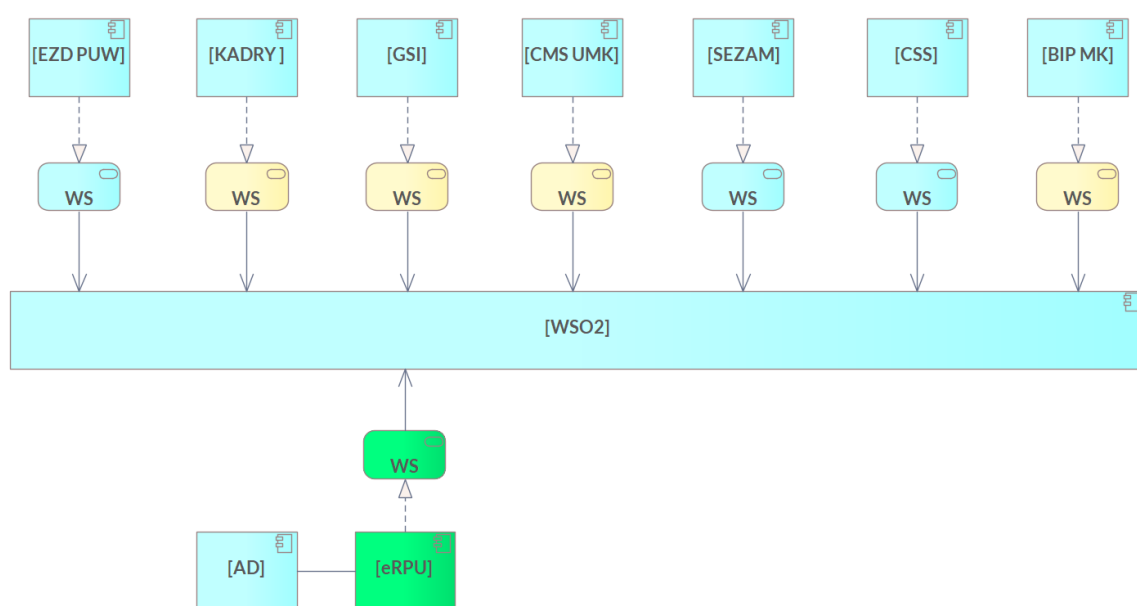
1. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), zwanym dalej „RODO”.
2. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. 2017 poz. 2247).
3. Zarządzenie nr 958/2010 Prezydenta Miasta Krakowa z dnia 30 kwietnia 2010 r. w sprawie wprowadzenia Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Krakowa
4. Ustawa z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i Aplikacji mobilnych podmiotów publicznych (Dz. U. 2019, poz. 848).

3 Wymagania dotyczące architektury

3.1 Planowana architektura logiczna

Architektura musi być oparta o architekturę zorientowaną na usługi, zgodną z wdrażanym modelem SOA UMK. Integracja poszczególnych usług oparta jest o szynę danych ESB WSO2, zapewniającą wymianę danych oraz usług pomiędzy zintegrowanymi elementami modelu.

Projektowana koncepcja architektury obejmuje szereg zintegrowanych komponentów pozwalających na osiągnięcie wymaganej funkcjonalności. Na poniższym diagramie pokazano wszystkie elementy planowanej architektury. Zielonym kolorem zaznaczono komponenty, które muszą zostać dostarczone w ramach opisywanego zamówienia, szczegóły opisane poniżej.






Rysunek 1 Koncepcja Architektury

Poszczególne elementy z podziałem na rodzaje obiektów opisano w tabeli poniżej.

Legenda:

Obiekt	Opis obiektu
	Komponent oznaczający daną aplikację bądź system. <ul style="list-style-type: none">Kolorem niebieskim oznaczono aplikacje/systemy istniejące.Kolorem zielonym oznaczono aplikacje/systemy do wykonania przez Wykonawcę
	Usługa realizowana poprzez dany komponent połączony relacją realizacji. <ul style="list-style-type: none">Kolorem niebieskim oznaczono usługi istniejąceKolorem zielonym oznaczono usługi do wykonania przez Wykonawcę

	<ul style="list-style-type: none"> Kolorem kremowym oznaczono usługi planowane do wdrożenia lub w trakcie wdrożenia w SI UMK
	Linia oznaczająca relację opisującą korzystanie z usługi przez dany komponent.
	Linia oznaczająca relację opisującą realizację usługi przez dany komponent.
	Linia oznaczająca relację opisującą bezpośrednią integrację komponentów.

Lista wszystkich systemów koncepcji Architektury:

1. będące częścią zamówienia, na które składa się:
 - a) eRPU
2. systemy istniejące do integrowania z Aplikacją w ramach zamówienia:
 - a) Active Directory
 - b) System EZD PUW
 - c) System BIP MK
 - d) System CMS UMK
 - e) System CSS
 - f) System GSI
 - g) System KADRY
 - h) System SEZAM

3.2 Wymagania dotyczące Platformy Serwerowej

Zamawiający zapewni elementy Oprogramowania Systemowego obejmujące: systemy operacyjne, oprogramowanie bazodanowe oraz sterowniki wymagane do ich poprawnego działania.

Dopuszcza się stosowanie tylko określonych poniżej systemów operacyjnych oraz oprogramowania dodatkowego (tj. bazy danych, serwerów aplikacyjnych itp.) w wersji wspieranej przez producenta nie krócej niż 3 lata od daty odebrania Aplikacji.

Aplikacja musi zostać zainstalowana na udostępnionej przez Zamawiającego Platformie Serwerowej opartej o jeden ze wskazanych w niniejszym dokumencie systemów operacyjnych, baz danych, serwerów aplikacyjnych.

3.2.1 System operacyjny:

Stosować można alternatywnie następujące rodzaje systemu operacyjnego:

- a) Od Windows Server 2019 (w ramach posiadanych licencji)
- b) RedHat Enterprise Linux

3.2.2 Wykorzystanie baz danych:

Stosować można alternatywnie następujące rodzaje baz danych:

- a) PostgreSQL
- b) Microsoft SQL Server STD

3.2.3 Wykorzystanie serwerów WWW:

Stosować można alternatywnie następujące serwery aplikacyjne:

- a) WildFly
- b) Apache/Tomcat
- c) IIS Microsoft
- d) Nginx

4 Wymagania funkcjonalne

4.1 Zestawienie funkcjonalności

ID	Grupa wymagań
F1	Rejestr Aktów Kierowania
F1.1	Aplikacja musi umożliwiać Użytkownikom przeglądanie rejestrów Aktów Kierowania.
F1.2	Rejestr Aktów Kierowania musi być prowadzony i wyodrębniony dla każdego z rodzajów (osobno dla Pełnomocnictw i osobno dla Upoważnień)
F1.3	Aplikacja musi mieć możliwość chronologicznego generowania numeru rejestru w eRPU dla nowych Aktów Kierowania pochodzących z EZD PUW, przy czym numery muszą być generowane osobno dla Pełnomocnictw i Upoważnień.
F1.4	Aplikacja nie może dublować numerów rejestrów w eRPU już nadanych w Aplikacji w ramach rejestrów dla poszczególnych rodzajów Aktów Kierowania
F1.5	Aplikacja musi rezerwować numery dla Aktów Kierowania, które zostały zainicjowane poprzez EZD PUW.
F1.6	Akty Kierowania muszą mieć nadawane odpowiednie statusy ustalone z Wykonawcą na etapie Analizy Przedwdrożeniowej.
F1.7	Rejestr Pełnomocnictw musi być prezentowany przez kolumny co najmniej:

	<ul style="list-style-type: none"> a) Rodzaj aktu b) Nr chronologiczny Aktu Kierowania c) Nr Sprawy z EZD PUW d) Rok e) Osoba lub osoby umocowane f) Osoba lub osoby – zastępca g) Jednostka h) Jednostka realizująca i) Pełnomocnictwo łączne tak/nie j) Zakres Pełnomocnictwa. k) "Status rejestracji" (propozycja Zamawiającego to: nowe, w toku, w trakcie korekty, zarejestrowane, opublikowane, wycofane z publikacji jednak muszą zostać one omówione i ustalone z Wykonawcą na etapie Analizy Przedwdrożeniowej) l) Status aktu (obowiązujące, archiwalne) m) Operator n) Wyłączenie jawności tak/nie o) Data podpisania p) Data obowiązywania od q) Data obowiązywania do r) Kategoria (zarządzana słownikiem w Aplikacji) s) Źródło danych (EZD PUW, ręczne dodanie w Aplikacji, dane zmigrowane) t) Tryb ważności (zarządzany słownikiem w Aplikacji) <p>Kolejność poszczególnych kolumn zostanie ustalona na etapie Analizy Przedwdrożeniowej</p>
F1.8	<p>Rejestr Upoważnień musi być prezentowany przez kolumny co najmniej:</p> <ul style="list-style-type: none"> a) Rodzaj aktu b) Nr chronologiczny Aktu Kierowania c) Nr Sprawy z EZD PUW d) Rok e) Osoba lub osoby upoważnione f) Osoba lub osoby – zastępca g) Jednostka h) Jednostka realizująca i) Upoważnienie do wydawania decyzji tak/nie j) Tytuł Upoważnienia k) "Status rejestracji" (propozycja Zamawiającego to: nowe, w toku, w trakcie korekty, zarejestrowane, opublikowane, wycofane z publikacji jednak muszą zostać one omówione i ustalone z Wykonawcą na etapie Analizy Przedwdrożeniowej) l) Status aktu (obowiązujące, archiwalne) m) Operator n) Wyłączenie jawności tak/nie

	<ul style="list-style-type: none"> o) Data podpisania p) Data obowiązywania od q) Data obowiązywania do r) Kategoria (zarządzana słownikiem w Aplikacji) s) Źródło danych (EZD PUW, ręczne dodanie w Aplikacji, dane migrowana) t) Tryb ważności (zarządzany słownikiem w Aplikacji) <p>Kolejność poszczególnych kolumn musi zostać omówiona i ustalona na etapie Analizy Przedwdrożeniowej</p>
F1.9	W Aplikacji musi być możliwość odesłania wybranego Aktu Kierowania do EZD PUW w celu korekty danych wraz z koniecznością dodania komentarza przez Użytkownika.
F1.10	W Aplikacji musi być możliwość edycji Aktów Kierowania procedowanych przed wdrożeniem procedowania w EZD PUW.
F1.11	W Aplikacji musi być możliwość edycji Aktów Kierowania (przez Gospodarza Aplikacji) z poziomu wybranego rejestru (procedowanych poprzez EZD PUW)
F1.12	Wyszukiwanie
F1.13	Zarówno w rejestrze Pełnomocnictw jak i Upoważnień musi być możliwość wyszukiwania na podstawie co najmniej danych z F1.7 i F.1.8
F1.14	Sortowanie, wyszukiwanie, filtrowanie musi być dostępne po wszystkich polach dostępnych w rejestrach.
F1.15	Wyniki wyszukiwania muszą mieć możliwość pobrania do pliku m.in. arkusza kalkulacyjnego.
F1.16	Dodawanie Aktów Kierowania do rejestru
F1.17	Dany Akt Kierowania musi być dodawany automatycznie do rejestru z EZD PUW zgodnie z opisem z rozdziału EZD PUW
F1.18	W Aplikacji musi być możliwość ręcznego dodania Aktu Kierowania do Aktów procedowanych przed wdrożeniem procedowania w EZD PUW.
F1.19	W Aplikacji musi być możliwość ręcznego usunięcia Aktu Kierowania z dodanych do rejestrów Aktów Kierowania, które były procedowane przed wdrożeniem procedowania w EZD PUW.
F1.20	Moduł Uzupełniania Aktów Kierowania o dane
F1.21	Uzupełnianie musi mieć możliwość prezentacji danych pochodzących z EZD PUW (per Sprawa). Niektóre z pochodzących danych muszą mieć zablokowaną możliwość edycji danych przez Użytkownika. Szczegóły zostaną ustalone na etapie Analizy Przedwdrożeniowej.

F1.22	<p>Dany rejestr Aktu Kierowania musi mieć możliwość manualnego uzupełnienia wybranego Aktu Kierowania o statusie „nowy” oraz „w trakcie korekty” w Aplikacji, pochodzącego z EZD PUW o dane:</p> <ul style="list-style-type: none"> a) Numer rejestrowy Aktu Kierowania (tylko wyświetlany) b) Osoba (umocowana, zastępca) c) Jednostka d) Jednostka realizująca e) Pełnomocnictwo łączne tak/nie f) Upoważnienie do wydawania decyzji tak/nie g) Tytuł Upoważnienia /zakres Pełnomocnictwa h) “Status rejestracji” nadawany automatycznie (proponując Zamawiającego to: nowe, w toku, w trakcie korekty, zarejestrowane, opublikowane, wycofane z publikacji jednak muszą zostać one omówione i ustalone z Wykonawcą na etapie Analizy Przedwdrożeniowej) i) Status aktu (obowiązujący/archiwalny) j) Data obowiązywania od k) Data obowiązywania do l) Tryb ważności (zarządzany słownikiem w Aplikacji)
F1.23	W module musi być możliwość przypisania Operatora do prowadzenia danego Aktu Kierowania. Domyślnie przypisanie ma nastąpić automatycznie.
F1.24	Publikacja danych Aktów Kierowania w Systemie CMS UMK i Systemie GSI
F1.25	<p>W Aplikacji musi być możliwość publikowania danych Aktów Kierowania z poziomu wybranego rejestru Aktu Kierowania. Przekazywane mają być dane opisane zgodnie z rozdziałem System CMS UMK oraz System GSI</p> <p>Publikowanie musi odbywać się za pomocą ręcznej akcji Użytkownika.</p>
F1.26	W Aplikacji publikacja musi mieć możliwość prezentacji publikowanych danych przed opublikowaniem (podgląd).
F1.27	W Aplikacji, z poziomu wybranego rejestru Aktu Kierowania musi być możliwość wycofania wybranego Aktu Kierowania z publikacji. Użytkownik musi mieć możliwość wpisania powodu wycofania. Przeglądanie powodu wycofania danego Aktu Kierowania musi być dostępne do wglądu z poziomu danego rejestru Aktu Kierowania.
F2	Moduł akceptacji zmiany statusu Aktu Kierowania
F2.1	W Aplikacji musi być moduł do akceptacji/odrzućenia zmiany statusu danego Aktu Kierowania na podstawie zmian w danych, które zostaną pobrane poprzez WS. Zakres pobieranych danych znajduje się w rozdziale System KADRY oraz danych z Systemu BIP MK zgodnie z rozdziałem System BIP MK
F2.2	W miejscu akceptacji musi pojawić się lista wszystkich Aktów Kierowania powiązanych z pracownikiem UMK, u którego zmienił się tryb pracy zgodnie z

	rozdziałem System KADRY oraz dany Akt Kierowania został uchylony zgodnie z System BIP MK
F2.3	W Aplikacji musi być możliwość akceptacji/odrzućenia przez Użytkownika zmiany statusu danego Aktu Kierowania na podstawie danych z Systemu KADRY zgodnie z rozdziałem System KADRY oraz danych z Systemu BIP MK zgodnie z rozdziałem System BIP MK
F2.4	Przy akceptacji/odrzućeniu musi być możliwość wprowadzenia powodu (pole opisowe).
F2.5	W Aplikacji musi być możliwość przeglądania historii akceptacji wraz z opisem powodu akceptacji bądź odrzućenia. Historia musi być również widoczna z poziomu danego Aktu Kierowania (czynności jakie użytkownik Aplikacji eRPU wykonał).
F3	Powiadomienia
F3.1	Aplikacja musi mieć możliwość automatycznego powiadomienia Użytkownika na jego adres e-mail (możliwość wskazania jednego bądź wielu adresów e-mail) o pojawieniu się nowej pozycji do akceptacji z Systemu KADRY lub Systemu BIP MK zgodnie z opisem w rozdziałem System KADRY oraz w rozdziałem System BIP MK
F3.2	W powiadomieniu mailowym musi znaleźć się link prowadzący do miejsca akceptacji zmiany statusu Aktu Kierowania zgodnie z F3.
F4	Słowniki
F4.1	Słowniki muszą umożliwiać podpowiadanie i walidację danych.
F4.2	Funkcje dostępne na słownikach: <ul style="list-style-type: none"> a) Przeglądanie listy dostępnych słowników, b) Przeglądanie słownika, c) Dodanie i modyfikacja wartości w słowniku, d) Usunięcie wartości ze słownika, e) Podpowiadanie wartości ze słownika.
P4.3	Wszystkie operacje na słownikach muszą być logowane (kto i kiedy daną wartość zmienił, dodał lub usunął). Log ten ma być dostępny dla Administratora Technicznego aplikacji. Usuwanie wartości ze słownika, zmiany wartości w słownikach nie mogą wpływać na wprowadzone i zatwierdzone już w systemie dane (nie mogą zmieniać danych już wprowadzonych a muszą być widoczne dopiero w nowych dokumentach). Zmiany wartości słowników muszą być oznaczone z podaniem okresu obowiązywania. Historyczna wartość słownika musi być możliwa do sprawdzenia przy wskazaniu odpowiedniego statusu wartości słownikowej nie tylko na podstawie logów. Usuwanie wartości ze słownika nie powoduje faktycznego usunięcia a jedynie ustawienia na status archiwalny oraz zmiany okresu, w którym wartość była dostępna.

F5	Monitorowanie Użytkowników (logi)
F5.1	W związku z przetwarzaniem danych osobowych Aplikacja musi spełnić wymagania:
F5.1.2	Zapis daty i godziny wprowadzenia danych do Aplikacji, określenia operatora, który dane wprowadził i zakresu tych danych.
F5.1.3	Zapis źródła pozyskania danych osobowych w przypadku, gdy dane pozyskano z innego źródła niż osoba, której dane dotyczą.
F5.1.4	Zapis informacji o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały przekazane, wraz z określeniem daty i zakresu udostępnianych danych.
F5.1.6	Zapis eksportu do edytowalnego pliku treści danych osobowych.
F5.1.7	Zapis daty i godziny zmiany danych w Aplikacji i określenia operatora, który zmiany wprowadził.
F5.1.8	Zapis usunięcia danych z Aplikacji.
F5.1.9	Zapis oznaczenia wraz z odnotowaniem daty danych, których przetwarzanie zostało ograniczone.
F5.1.10	Zapis oznaczenia wraz z odnotowaniem daty danych, wobec przetwarzania których wniesiono sprzeciw.
F5.1.11	Zapis wygenerowania i wydrukowania raportu zawierającego informacje, o których mowa w wymaganiach F5.12-F5.10 w dowolnym określonym przez żądającego raport układzie i zakresie.
F5.2	Aplikacja musi posiadać odpowiednie rejestry, umożliwiać ich przeglądanie, sortowanie, filtrowanie, wyszukiwanie danych po dowolnych polach. Z rejestrów tych musi być możliwość generowania raportów w zakresie:
F5.2.1	Historii zmian uprawnień Użytkowników (z dokładnością do roli): login, nazwisko, imię, jednostka, komórka organizacyjna, rola, data nadania roli, data odebrania roli.
F5.2.2	Historii Lista sesji Użytkowników: musi zawierać listę wszystkich sesji Użytkowników, wraz z informacjami: login, nazwisko, imię, jednostka, komórka organizacyjna, data i godzina początku sesji, data i godzina zakończenia sesji (jeśli sesja już została zakończona), adresie IP komputera, na którym powstała sesja.
F5.2.3	Listy otwartych sesji: Login, nazwisko, imię, jednostka, komórka organizacyjna, data /godzina początku sesji (musi być możliwość wylogowania wszystkich Użytkowników).
F5.2.4	Historii logowań: login, nazwisko, imię, jednostka, komórka organizacyjna, data i godzina zalogowania, data i godzina wylogowania, czas logowania.
F5.2.5	Kont Użytkowników w Aplikacji: login, nazwisko, imię, jednostka, komórka organizacyjna, data założenia konta, data dezaktywacji/blokady konta, czy

	aktywne, do kiedy ważne, data zmiany hasła, data ostatniego logowania, status konta.
F5.2.6	Historii zmian dotyczących kont Użytkowników: zawiera wszystkie atrybuty konta Użytkownika (login, nazwisko, imię, jednostka, komórka organizacyjna, data założenia konta, data zablokowania konta, czy aktywne, do kiedy ważne, data zmiany hasła) oraz powiązań konta Użytkownika z innymi obiektami (np. uprawnienia, sesje), wraz z datą i godziną zmiany oraz informacją o tym kto zmianę wykonał.
F5.2.7	Listy aktywnych Użytkowników wraz z przypisanymi rolami (imię, nazwisko, login, komórka organizacyjna, referat, role). Lista osób zawierać następujące informacje: login, nazwisko, imię, jednostka, komórka organizacyjna, data nadania uprawnienia, data odebrania uprawnienia.
F5.2.8	Listy osób, które w zadanym okresie miały nadane uprawnienia, przy czym musi być możliwość wyszukiwania po parametrach: <ul style="list-style-type: none"> a) okres (od, do) wraz z możliwością wyszukania listy osób, które miały nadane uprawnienia przez cały okres jak i w jego fragmencie, b) rola (możliwe zaznaczenie kilku).
F5.2.9	Historia wywołań WS
F5.2.10	Wszystkie raporty wskazane w F5.2.1-F5.2.9 muszą posiadać: <ul style="list-style-type: none"> a) nagłówek zawierający tytuł raportu, b) zadane parametry wyszukiwania dla których został wygenerowany raport, c) informację kto i kiedy wygenerował raport, d) część zasadniczą z wygenerowanymi danymi wraz z nagłówkami kolumn.
F5.2.11	W Aplikacji muszą być logowane zdarzenia z dokładnością do każdego parametru określonego w F5.2.1-F5.2.9. Komunikaty zdarzeń muszą być opisane w sposób czytelny dla Użytkownika.
F5.2.12	W Aplikacji muszą być rejestrowane działania Użytkowników oraz zdarzenia związane z bezpieczeństwem informacji. Logi muszą zawierać rejestrację wszystkich działań Użytkownika w Aplikacji wraz z datą, godziną, minutą i sekundą wykonania tych działań. Dane te muszą być przechowywane przez określony przez Zamawiającego czas dla potrzeb przyszłych postępowań wyjaśniających oraz monitorowania kontroli dostępu. Logi bieżące mają być przechowywane w Aplikacji natomiast reguły związane z przechowywaniem logów archiwalnych zostaną uzgodnione na etapie Analizy Przedwdrożeniowej.
F5.2.13	Aplikacja musi zawierać mechanizm do przeglądania logów bieżących (wstępnie wszystkie do 24 miesięcy; okres ustawiany parametrem) i archiwalnych

	<p>(wstępnie wszystkie powyżej 24 miesięcy; okres ustawiany parametrem) w tym zapewniający możliwość:</p> <ul style="list-style-type: none"> a) wyszukiwania b) filtrowania po wybranych przez Użytkownika typach zdarzeń i ich cechach c) sortowania po wybranych przez Użytkownika typach zdarzeń i ich cechach
F5.2.14	Aplikacja musi zapewniać mechanizm eksportu pliku logów do serwera zewnętrznego przy użyciu standardowych protokołów i mieć możliwość synchronizacji z serwerem czasu (protokół NTP).
F5.2.15	Aplikacja musi zapisywać działania związane z uruchamianiem funkcji interfejsu integracyjnego wraz z możliwością włączenia powiadamiania mailowego o błędach.
F5.2.16	Generowane raporty muszą być eksportowane do plików innego formatu w szczególności XLSX, CSV, w zależności od zapotrzebowania Użytkownika.
F6	Moduł raportów
F6.1	<p>Aplikacja musi mieć możliwość wygenerowania raportów dotyczących upoważnień w oparciu o dane:</p> <ul style="list-style-type: none"> a) Okres wydania upoważnienia (od, do) b) Imię c) Nazwisko d) Wydział e) Komórka f) Jednostka g) Daty obowiązywania upoważnienia h) Do czego i) Upoważnienie do wydawania decyzji
F6.2	Przy generowaniu powyższych raportów musi istnieć możliwość wyboru informacji, które taki wykaz będzie zawierał
F6.3	Generowane raporty muszą być eksportowane do plików innego formatu w szczególności XLSX, CSV, w zależności od zapotrzebowania Użytkownika.
F7	Inne
F7.1	W Aplikacji musi być możliwość podpięcia raportów przygotowanych w zewnętrznych narzędziach np.: POWER BI. Raporty podpinane są przy pomocy linkowania do nich bez udziału mechanizmu integrującego
F7.2	Sortowanie, wyszukiwanie, filtrowanie musi być dostępne po wszystkich polach dostępnych w Aplikacji.

5 Wymagania pozafunkcjonalne

5.1 Zestawienie wymagań pozafunkcjonalnych

ID	Grupa wymagań
P1	Wymagania ogólne
P1.1	Aplikacja musi uwzględniać warunki środowiskowe SI UMK, czyli musi uwzględniać wymagania dotyczące Platformy Serwerowej wraz z licencjami, które posiada UMK, zgodnie z zapisami zawartymi w niniejszym dokumencie.
P1.1.2	Aplikacja musi pracować w technologii warstwowej rozumianej jako architektura typu klient-serwer, zakładająca co najmniej separowanie interfejsu Użytkownika, logiki biznesowej oraz danych, przy czym każda z powyższych warstw może mieć własny podział warstwowy. Architektura tego typu pozwala aktualizować lub zastępować poszczególne moduły niezależnie od siebie, w miarę jak zmieniają się warunki techniczne - przykładowo, zmiana systemu operacyjnego na komputerze użytkownika (np. z Windows na Linux lub odwrotnie), wpływa jedynie na warstwę interfejsu użytkownika, ale nie na przetwarzanie i składowanie.
P1.1.3	Aplikacja musi umożliwiać integrację z zewnętrznymi narzędziami monitorującymi. Zamawiający będzie stosował system Orion SolarWinds do monitorowania parametrów działania Aplikacji.
P1.1.4	Technologia musi umożliwić integrację z innymi aplikacjami/systemami SI UMK poprzez Web Service.
P1.1.5	Aplikacja musi być skalowalna pod względem ilości Użytkowników, wielkości bazy danych.
P2	Interfejs Użytkownika
P2.1	Dostępność
P2.1.1	Aplikacja musi być dostępna przez przeglądarkę www (co najmniej EDGE, Mozilla Firefox, Google Chrome do 3 wersji wstecz) przez szyfrowane połączenie (https) i umożliwiać pracę wielu Użytkowników jednocześnie. Oznacza to, że wszystkie wskazane w wymaganiach funkcjonalnych funkcje Aplikacji mają być dostępne przez interfejs WWW.
P2.1.2	Aplikacja stosuje mechanizmy responsywności w celu umożliwienia prawidłowego korzystania z wszystkich funkcjonalności i treści na różnych rozdzielczościach.
P2.1.3	Aplikacja umożliwia pracę na komputerach z użyciem rozdzielczości od 1366x768px.
P2.1.4	Aplikacja musi posiadać interfejs Użytkownika w polskiej wersji językowej.
P2.1.5	Aplikacja musi uwzględniać komfort pracy Użytkowników z dysfunkcjami (WCAG 2.1. AA) minimum w zakresie: a) Postrzegalności: 1.4- Możliwość rozróżnienia - ułatwienia percepcji treści, 1.3 Możliwość adaptacji odpowiednia (zrozumiała) prezentacja zawartości,

	b) Funkcjonalności: 2.2 Wystarczająca ilość czasu, 2.3 Ataki padaczki – migotanie, 2.4 Możliwości nawigacji, 2.5 Sposoby wprowadzania danych c) Zrozumiałości: 3.2 Przewidywalność, 3.3 Pomoc przy wprowadzaniu informacji d) Kompatybilności - 4.1 Kompatybilność
P2.2	Wydajność
P2.2.1	Czas pobrania danych i odświeżania/odbudowy ekranu po czynności wykonanej przez Użytkownika nie może być dłuższy niż 4 sekundy dla 95% żądań (przy obciążeniu 10 żądań na sekundę) przy czym w czas ten nie wlicza się czasu pobierania informacji z systemów zewnętrznych, spowolnień spowodowanych ograniczeniami łącz internetowych po stronie dostawców tych łącz oraz czasu przesyłania plików powyżej 1,2 MB.
P2.2.2	Z Aplikacji jednocześnie może korzystać co najmniej 200 Użytkowników.
P2.2.3	<p>Przyjmuje się następujące założenia dotyczące prędkości odszukiwania i wyświetlania rekordów danych wyszczególnione poniżej (dla 95% żądań przy obciążeniu 10 żądań na sekundę):</p> <ul style="list-style-type: none"> – wyszukiwanie po dowolnych kryteriach w czasie: do 3 sekund, – generowanie raportów w czasie: do 30 sekund, – zatwierdzenie zmian przez Użytkownika w czasie: do 3 sekund, <p>Powyższe wymagania dotyczą działania w przypadku braku konieczności pobierania danych ze źródeł zewnętrznych.</p>
P3	Zarządzanie Użytkownikami
P3.1	Aplikacje dla Użytkowników są pogrupowane w role.
P3.2	Dostępne są mechanizmy nadawania ról i definiowania uprawnień dla ról.
P3.3	Możliwość pracy w Aplikacji z uprawnieniami AT ma być na podstawie nadanej roli (login Użytkownika, a nie login np.: administrator).
P3.4	Aplikacja musi zawierać odseparowane funkcje administracyjne (moduł zarządzania uprawnieniami, logi i konfiguracji, szablony raportów) od funkcji związanych z pracą merytoryczną w Aplikacji.
P3.5	Aplikacja musi umożliwiać definiowanie czynności w grupy ról
P4	Bezpieczeństwo i niezawodność
P4.1	Wszystkie usługi konieczne do poprawnego działania Aplikacji muszą być uruchamiane automatycznie w procesie uruchamiania serwera/serwerów.
P4.2	Aplikacja musi spełniać wymogi bezpieczeństwa zgodne z OWASP top 10.
P4.3	Zastosowane lub dostarczone komponenty Aplikacji i elementy środowiska systemowo-programowego muszą być w wersjach stabilnych i najbardziej aktualnych

	lub takich, dla których producent zapewnia wsparcie przez następnych 3 lat (na dzień odbioru Aplikacji).
P4.4	Dane w bazie muszą być zapisywane według standardu Unicode UTF-8.
P4.5	<p>1) Aplikacja musi spełniać wymagania Polityki Bezpieczeństwa Informacji w zakresie stosowania hasła, które:</p> <ul style="list-style-type: none"> ○ nie może zawierać nazwy konta Użytkownika ani części jego pełnej nazwy dłuższej niż dwa kolejne znaki, ○ musi być zmieniane nie rzadziej niż raz na 90 dni, ○ jest inne niż 10 ostatnio wprowadzonych haseł, ○ składa się z minimum 12 znaków, ○ musi zawierać 3 rodzaje znaków spośród następujących czterech kategorii: <ul style="list-style-type: none"> ▪ zawiera małe litery alfabetu łacińskiego (od a do z), ▪ zawiera duże litery alfabetu łacińskiego (od A do Z), ▪ zawiera cyfry systemu dziesiętnego (od 0 do 9), ▪ zawiera znaki specjalne, niealfabetyczne (na przykład !, \$, #, %).
P4.6	Aplikacja musi posiadać wydzielony interfejs zarządzania (w sytuacji technicznie i ekonomicznie uzasadnionej), który nie jest udostępniony w Internecie. Dostęp do tych interfejsów zarządzania musi być (jako minimum) ograniczony do wyselekcjonowanych adresów IP, chroniony przed próbami ataków przełamujących hasła i realizowany poprzez szyfrowane protokoły SSH, HTTPS (z ważnymi certyfikatami). Dostęp do nich mogą posiadać jedynie uprawnieni Użytkownicy.
P4.7	Aplikacja musi umożliwiać pracę w różnych podsieciach IP w obrębie jednej sieci LAN.
P4.8	Środowisko sieciowe dla Aplikacji musi korzystać z protokołu TCP/IP ver. 4.

6 Integracje

W niniejszym rozdziale została wymieniona enumeratywna lista integracji, które musi zapewnić Wykonawca Aplikacji. Dla każdej z integracji został dodany opis informujący o tym jakich przepływów danych oczekuje Zamawiający pomiędzy poszczególnymi systemami/aplikacjami integrującymi się z Aplikacją.

6.1 Active Directory

Wykonawca zintegruje Aplikację z Active Directory w SI UMK zgodnie z opisem rozdziału 7 [Administracja i Zarządzanie Uprawnieniami](#).

6.2 EZD PUW

Integracja eRPU (dedykowane dla eRPU konto w EZD PUW - eRPU posiada dane autoryzacyjne tego konta (login) i używa ich w ramach wykorzystania API EZD PUW)

Integracja w zakresie pobierania danych z EZD PUW do Aplikacji (inicjatorem jest zawsze Aplikacja, EZD PUW nie ma możliwości inicjacji przekazania danych):

1. Pobierania danych dotyczących Aktów Kierowania do Aplikacji co najmniej w zakresie:
 - a) pobierania identyfikatora Koszulki wraz z identyfikatorami powiązanych Koszulek,
 - b) pobierania dokumentów zawartych w Koszulce (wraz z dokumentami w powiązanych Koszulkach),
 - c) pobierania znaku Sprawy w założonej Koszulce,
 - d) aktualizowania (pobierania danych) Aktów Kierowania w zakresie nowych dokumentów pochodzących z EZD PUW,
 - e) pobrania identyfikatora Konta Integracyjnego dla Aplikacji (Aplikacja ma uprawnienia do tego konta) oraz identyfikatora Konta Technicznego, na które Aplikacja ma przekazywać Koszulki z Konta Integracyjnego,
 - f) przekazywania metadanych Koszulki w tym metadanych załączników zawartych w Koszulce,
2. Integracja w zakresie przekazywania danych z Aplikacji do EZD PUW co najmniej:
 - a) W zakresie zmiany statusu ważności lub innej sytuacji wymagającej komunikacji z eRPU do EZD PUW Aktu Kierowania poprzez założenie nowej Koszulki i dołączenie do niej metadanych identyfikujących Sprawę prowadzoną po stronie EZD PUW (Znak Sprawy oraz identyfikator Koszulki dla tej Sprawy) oraz dodatkowych informacji zawartych w obiektach możliwych do dodania do koszulki poprzez API EZD (notatka),
 - b) przekazywania dokumentów zawartych w Koszulce (wraz z dokumentami w powiązanych Koszulkach),
 - c) związanych z walidacją poprawności metadanych w Koszulkach znajdujących się na Koncie Integracyjnym Aplikacji.

Wszystkie Sprawy w eRPU muszą mieć możliwość aktualizowania na dwa sposoby (aktualizowanie Sprawy z EZD PUW):

- a) Automatyczny przy każdorazowym odpytywaniu o Sprawę,
- b) Ręczny poprzez manualną aktualizację wszystkich Spraw (przykładowo przycisk „aktualizuj wszystkie”).

Koszulka do której eRPU chce dokonać aktualizacji i wysłać aktualizację do EZD PUW, nie znajduje się na Koncie Integracyjnym. eRPU tworzy nową Koszulkę i łączy do niej informację w formie tekstowej ale ze wskazaniem w tym tekście na idKoszulki której dotyczy aktualizacja; Nową koszulkę eRPU przekazuje na konto wpływu eRPU z odpowiednim komentarzem przekazania.

6.3 System BIP MK

W BIP MK przechowywane są obowiązujące ZPMK, gdzie dane ZPMK może uchylać Pełnomocnictwo lub Upoważnienie PMK.

Aplikacja musi zostać zintegrowana z Systemem BIP MK w zakresie pobierania danych:

- Akt kierowania, który jest uchylany (nr Aktu Kierowania, Imię i Nazwisko, jednostka, data podpisania Aktu Kierowania)

- Informacja o nr ZPMK, roku ZPMK, data podpisania ZPMK, tytuł
- Informacja o linku

6.4 System CMS UMK

Aplikacja musi przekazywać następujące dane do Systemu CMS UMK:

- Rodzaj aktu
- Numer Aktu Kierowania
- Rok
- Imię Nazwisko (osoby wraz z informacją czy upoważniony czy zastępujący)
- Data podpisania Aktu Kierowania
- Obowiązuje od
- Obowiązuje do
- Tytuł Upoważnienia/zakres Pełnomocnictwa.
- Status aktu (obowiązujący, archiwalny)
- Plik do pobrania z Aktem Kierowania
- Rozmiar pliku
- Informacje o wyłączeniu jawności
- Wszystkie powiązane Akty Kierowania
- Upoważnienia do wydawania decyzji [tak/nie]
- Pełnomocnictwo łączne [tak/nie]

Metka:

Jednostka odpowiedzialna - Wydział operatora

Osoba publikująca - Operator dokonujący publikacji/aktualizacji aktu kierowania

Data publikacji - data pierwszej publikacji aktu

Data aktualizacji - data kolejnej publikacji aktu lub zmiany aktu spowodowanego zmianą statusu (uchylenie, wygaśnięcie, utrata mocy itp.)

6.5 System CSS

Aplikacja musi zostać zintegrowana w zakresie pobierania Komórek na prawach wydziału (symbol i nazwa) oraz główne nazwy MJO (symbol i nazwa). Komórki oraz główne nazwy MJO muszą być pobierane do miejsca wprowadzania danych dot. Aktów Kierowania w Module Uzupełniania Aktów Kierowania o dane.

6.6 System GSI

Aplikacja musi przekazywać następujące dane do System GSI w związku z wymaganiami funkcjonalnymi dotyczącymi publikacji danych:

- Rodzaj aktu
- Numer Aktu Kierowania
- Rok
- Imię Nazwisko (osoba lub osoby wraz z informacją czy upoważniony czy zastępujący)
- Data podpisania Aktu Kierowania
- Obowiązuje od
- Obowiązuje do
- Tytuł Upoważnienia/zakres Pełnomocnictwa.
- Status aktu (obowiązujący, archiwalny)
- Plik do pobrania z Aktem Kierowania
- Rozmiar pliku
- Informacje o wyłączeniu jawności
- Wszystkie powiązane Akty Kierowania
- Metka (jednostka odpowiedzialna - Wydział operatora
- Osoba publikująca - Operator dokonujący publikacji/aktualizacji aktu kierowania
- Data publikacji - data pierwszej publikacji aktu
- Data aktualizacji - data kolejnej publikacji aktu lub zmiany aktu spowodowanego zmianą statusu (uchylenie, wygaśnięcie, utrata mocy itp.)

6.7 System KADRY

Integracja jest konieczna ze względu na możliwe zmiany kadrowe pracownika UMK (zakończenie zatrudnienia, zmiana funkcji itd.)

Niektóre Akty Kierowania obowiązują w okresie zatrudnienia na danym stanowisku, w danej Komórce Organizacyjnej. W momencie, gdy pracownik UMK przestanie pełnić daną funkcję lub następuje wygaśnięcie stosunku pracy pomiędzy pracownikiem UMK a UMK, to dany Akt Kierowania traci moc.

Integracja w zakresie pobierania danych z Systemu KADRY do Aplikacji.

Pobieranie danych dotyczących zatrudnienia pracowników UMK w Aplikacji co najmniej w zakresie:

- a) Imię i nazwisko
- b) Zmiana Komórki bądź jednostki
- c) Zmiany Stanowiska kadry kierowniczej wyższego szczebla na inne
- d) Data końca zatrudnienia
- e) Data końca angażu wynikająca ze zmian z lit. b) i c)
- f) Symbol Komórki lub jednostki

6.8 System SEZAM

Integracja z SEZAM odbywa się poprzez szynę danych WSO2. Konieczna jest integracja w dwóch zakresach opisanych w pkt 1 i 2 poniżej.

1. Integracja w zakresie automatycznego nadawania uprawnień Użytkownikom:
 - a) Implementacja uniwersalnego interfejsu ma na celu zunifikowanie mechanizmu nadawania uprawnień. Idea bazuje na założeniu że dla większości aplikacji nadawanie uprawnień mają charakter hierarchiczny, gdzie na szczycie hierarchii znajduje się lista ról, które mogą być przydzielone, a na kolejnych poziomach uszczegółowiane są uprawnienia związane z daną rolą. Zunifikowany sposób nadawania uprawnień, pozwala na zdefiniowanie uniwersalnego interfejsu graficznego, służącego nadawaniu uprawnień, jak również interfejsów typu web-service, pozwalających na pobranie definicji dostępnych uprawnień, oraz przekazywania do systemów skonfigurowanych dla konkretnych pracowników uprawnień.
 - b) Uprawnienia nadawane pracownikom do danego systemu konfigurowane w oparciu o plik XML konfiguracji uprawnień.
2. System SEZAM:
 - a) pobiera plik konfiguracji uprawnień z systemu zewnętrznego,
 - b) pozwala na zdefiniowanie w oparciu o pobrany plik uprawnień w procesie nadawania lub modyfikacji uprawnień,
 - c) przekazuje zdefiniowane uprawnienia do systemu zewnętrznego.

7 Administracja i zarządzanie uprawnieniami

7.1 Zarządzanie uprawnieniami

Dla Użytkowników będących pracownikami UMK Aplikacja musi zostać zintegrowana z Active Directory w celu i zakresie służącym zapewnieniu funkcji tzw. jednokrotnego logowania SSO.

Konta Użytkowników, którzy nie zalogowali się do aplikacji w ciągu 92 dni muszą być automatycznie blokowane w Aplikacji i otrzymywać status „brak aktywności przez 92 dni”. Blokada musi uniemożliwiać zalogowanie się do Aplikacji Użytkowników lokalnych oraz pochodzących z Active Directory. Administrator Techniczny musi mieć możliwości oznaczenia kont technicznych, konta tego typu konta nie mogą być blokowane i otrzymać status „konto techniczne”.

Wykonawca musi zapewnić dodatkowo mechanizmy:

budowy lokalnej bazy Użytkowników, w przypadku budowy bazy lokalnej konieczne jest zastosowanie logowania dwuskładnikowego (musi być poprzez e-mail i telefon w zależności od tego posiadanego narzędzia przez Użytkownika Aplikacji) oraz wprowadzenie parametru, który

pozwoli na określenie liczby nieudanych prób logowań po których będzie blokowany dostęp do Aplikacji. Każda Aplikacja musi pozwalać na ręczną zmianę hasła przez Użytkownika.

Zarządzanie uprawnieniami Użytkowników odbywa się w Aplikacji.

7.2 Role Użytkowników Aplikacji

- 1) W Aplikacji muszą zostać opracowane minimum następujące role :
 - a) Administrator Techniczny (AT) Aplikacji – rola umożliwia dostęp do wszystkich funkcji Aplikacji związanych z administrowaniem Aplikacji i zarządzaniem uprawnieniami oraz do związanych z tym słowników i parametrów (np. modyfikacja opisu roli, okresowe raporty kont i przyznanych im ról, dostęp do logów Aplikacji, zarządzanie parametrami Aplikacji, weryfikacja nieautoryzowanych dostępów do Aplikacji).
 - b) Gospodarz Aplikacji - rola dająca dostęp do wszystkich funkcji związanych z merytoryczną obsługą Aplikacji oraz związanymi z tym słownikami i parametrami (w tym kontrola i aktualizacja słowników i parametrów związanych z merytorycznymi funkcjonalnościami Aplikacji). Ma możliwość podglądu przyznanych ról i uprawnień w Aplikacji.
 - c) Pracownik merytoryczny (Operator) – pracuje w Aplikacji wykorzystując dostępne funkcje jednak nie ma dostępu do słowników i parametrów Aplikacji ani do części związanej z zarządzaniem Aplikacją i Użytkownikami.
 - d) Obserwator – Użytkownik mający uprawnienia tylko do podglądu wybranych danych bez możliwości ich edycji (bez słowników).
 - e) Administrator uprawnień - rola ma umożliwiać wyłącznie nadawanie uprawnień do Aplikacji, Użytkownik z tą rolą nie może mieć możliwości zmiany swoich uprawnień oraz nadania roli Administratora Technicznego (AT) Aplikacji.
- 2) Aplikacja musi posiadać możliwość przypisania Użytkownika do dowolnej roli oraz przypisania mu dowolnej liczby ról.

8 Migracja danych

Wykonawca dokona migracji danych, metadanych oraz powiązań między danymi w celu przeniesienia aktualnie przetwarzanych przez Zamawiającego Aktów Kierowania wraz z powiązaniami i metadanymi do Aplikacji.

W niektórych z Aktów Kierowania numery mogą być takie same w danym roku. Jako iż numer danego Aktu Kierowania wraz z rokiem mogą być takie same, to Wykonawca musi rozróżnić je odpowiednią flagą.

Obecne rejestry prowadzone są w formie arkuszy kalkulacyjnych.

Szczegóły dotyczące migracji zostaną ustalone na etapie Analizy Przedwdrożeniowej.

9 Dokumentacja

1. Dokumentacja sporządzona na potrzeby zamówienia musi być zgodna ze stanem prawnym aktualnym na dzień przedstawienia jej do odbioru Zamawiającemu.
2. Dostarczona Dokumentacja musi być w języku polskim, być spójna i nie może zawierać sprzeczności. Wykonawca musi zapewnić wzajemną zgodność pomiędzy wszystkimi rodzajami informacji umieszczonymi w Dokumentacji, brak logicznych sprzeczności oraz spójność pomiędzy informacjami zawartymi w Dokumentacji.
3. Dostarczona Dokumentacja ma charakteryzować się:
 - a) jednolitą strukturą, rozumianą jako podział danego dokumentu na rozdziały, podrozdziały i sekcje w czytelny i zrozumiały sposób,
 - b) jednolitym sposobem opisywania rozumianym jako zachowanie spójnej struktury, formy i sposobu pisanie,
 - c) poprawnością ortograficzną,
 - d) aktualnymi odnośnikami do innych dokumentów, rozdziałów lub fragmentów Dokumentacji,
 - e) musi w całości opisywać funkcjonalności Aplikacji,
 - f) musi zawierać pełne przedstawienie omawianego problemu obejmujące całość rozpatrywanego zakresu zagadnienia i nie zawierać zbędnej treści,
 - g) musi zawierać uzgodnienia poczynione z Zamawiającym w trakcie realizacji przedmiotu Umowy.
4. Dokumentacja musi umożliwić administrowanie Aplikacją

9.1 Wymagana dokumentacja dla zarządzania Platformą Serwerową

Wykonawca jest zobowiązany do wykonania i dostarczenia dokumentacji technicznej zarządzania Platformą Serwerową dla Aplikacji zawierającej co najmniej:

1. Opis konfiguracji systemu, w tym wykaz wdrożonych elementów, powiązania pomiędzy nimi, opis ich konfiguracji, implementacja w środowisku Zamawiającego (integracja) oraz oprogramowania dodatkowego
2. Instrukcje start/stop dla całego środowiska (infrastruktura – systemy operacyjne, wspomagające, bazy danych itp.).
3. Instrukcje eksploatacyjne dla Administratorów Technicznych.
4. Instrukcje wykonywania kopii zapasowych i odtwarzania z kopii.
5. Instrukcje instalacji i konfiguracji.

9.2 Wymagana dokumentacji użytkownika i technicznej dla Aplikacji

1. Instrukcja eksploatacyjna użytkownika Aplikacji musi zawierać:
 - a) Opis zastosowania, działania i sposobu wykonania (opis krok po kroku) każdej udostępnionej funkcjonalności Aplikacji z dokładnością do pojedynczej funkcji.
 - b) Opis zastosowania wszystkich użytych słowników.
 - c) Opis wszystkich parametrów Aplikacji związanych z jej ustawieniami i funkcjonalnościami.
 - d) Wykaz możliwych do przyznania uprawnień do Aplikacji wraz z ich opisem.
 - e) Listę i opis ikon, przycisków i skrótów klawiaturowych.

- f) Instrukcja użytkownika musi być wyposażona w wyszukiwarkę i indeks.
2. Dokumentacja techniczna musi zawierać:
- wymagania techniczne dotyczące sprzętu i środowiska (z dokładnością do wersji środowiska)
 - ustawienia konfiguracyjne środowiska, w którym pracuje Aplikacja, w tym również opis implementacji w środowisku SI UMK wraz z procedurami start/stop dla wszystkich elementów Aplikacji.
 - opis parametrów konfiguracji Aplikacji i sposób ich wykorzystania.
 - Diagramy architektury logicznej i fizycznej Aplikacji. Diagramy architektury muszą zawierać również rozmieszczenia oraz powiązanie jego poszczególnych elementów, na poziomie sprzętowym oraz oprogramowania, z uwzględnieniem wersji produkcyjnej i testowej.
- Muszą zostać dostarczone poniższe diagramy:
- architektury wewnętrznej Aplikacji (DARWA) - diagram prezentuje elementy składowe Aplikacji (moduły),
 - struktury danych (DARSD) - zawiera logiczny lub fizyczny model danych.
 - przepływu komunikacji (DARPK) – diagram zwany również diagramem sekwencji prezentujący szczegółowo realizację wybranych aspektów komunikacji pomiędzy systemami/aplikacjami,
 - procesów biznesowych (DAPB) - opisujący sekwencję kroków prowadzącą do określonego rezultatu biznesowego
- Powyższe diagramy muszą zostać zamodelowane zgodnie ze standardem UMK umieszczonym w załączniku nr 4. „Zasady modelowania architektury rozwiązania w Urzędzie Miasta Krakowa”.
- opis techniczny rodzajów i zastosowanych protokołów komunikacji (w tym certyfikatów).
 - sposób wykonania instalacji Aplikacji, instalacji poprawek i kolejnych wersji.
 - procedura odtworzenia danych i konfiguracji.
 - schemat baz danych wraz z opisem struktury uwzględniający powiązania i zależności między obiektami w bazie danych.
 - listę wykorzystywanych słowników danych oraz ich opis.
 - wykaz danych podlegający kontroli poprawności wraz z informacją o sposobie kontroli poprawności.
 - wykaz komunikatów diagnostycznych i standardowych błędów w tym API integracyjnych (opis błędu, warunki jego powstania).
3. W związku z integracjami (gdzie instrukcja integracji musi być w wersji do udostępniania osobom trzecim w celu właściwego zintegrowania się z Aplikacją; zgodnie z rozdziałem 12 Standardy dla usług integracyjnych w UMK):
- opis usługi, interfejsów i wytyczne umożliwiające integrację Aplikacji z innymi Aplikacjami.
 - pliki ze schematami (WSDL, GML, Swagger/OpenApi, itp.).
 - opis metod i struktur danych interfejsów.
4. W związku z przekazaniem kodów źródłowych (zgodnie z rozdziałem 11 Kody Źródłowe):
- charakterystykę katalogów i plików kodu źródłowego.
 - diagram klas.

- c) komentarze w kodzie źródłowym pozwalające na automatyczne wygenerowanie dokumentacji w formacie HTML lub PDF przy użyciu dedykowanego narzędzia (np. Javadoc).
 - d) repozytorium .git zawierające historię zmian kodu.
 - e) oraz zgodnie z wymaganiem pkt. 13. niniejszego załącznika.
5. Instrukcja Użytkownika ma zostać przekazana w języku polskim.

10 Analiza Przedwdrozeniowa

1. Celem Analizy Przedwdrozeniowej jest:
 - a) uszczegółowienie jednoznacznej interpretacji wymagań Zamawiającego i sposobu ich realizacji
 - b) uszczegółowienie procesów, które będzie wspierała Aplikacja
 - c) określenie zasad konfiguracji Aplikacji
 - d) rozpoznanie wymaganej integracji z istniejącymi systemami
 - e) określenie Platformy Serwerowej oraz Oprogramowania Systemowego niezbędnego do działania Aplikacji.
2. W wyniku przeprowadzonej Analizy Przedwdrozeniowej musi zostać dostarczony Dokument analizy zawierający co najmniej:
 - a) jednoznaczna i zamknięta listę wymagań wraz z określeniem sposobu ich realizacji oraz kryteria akceptacji dla wymagania
 - b) listę słowników i parametrów Aplikacji
 - c) listę potrzebnych raportów wraz z opisem
 - d) jednoznacznie ustalone zasady konfiguracji Aplikacji
 - e) jednoznacznie określony sposób i założenia integracji z innymi Aplikacjami
 - f) diagramy architektury logicznej i fizycznej Aplikacji. Diagramy muszą być również opisane. Diagramy architektury muszą zawierać rozmieszczenia oraz powiązanie jego poszczególnych elementów, na poziomie sprzętowym oraz oprogramowania, z uwzględnieniem wersji produkcyjnej i testowej.

Muszą zostać dostarczone poniższe diagramy:

 - procesów biznesowych (DAPB) - opisujący sekwencję kroków prowadzącą do określonego rezultatu biznesowego
 - architektury wewnętrznej Aplikacji (DARWA) - diagram prezentuje elementy składowe Aplikacji (moduły),

Powyższe diagramy powinny zostać zamodelowane zgodnie ze standardem UMK umieszczonym w załączniku nr 4. „Zasady modelowania architektury rozwiązania w Urzędzie Miasta Krakowa”
 - g) opis Platformy Serwerowej i Oprogramowania Systemowego. W przypadku wykorzystania komponentów lub oprogramowania firm trzecich, konieczne jest wskazanie tych komponentów oraz informacji o licencji
 - h) scenariusze testowe, które są niezbędne do sprawdzenia poprawności działania Aplikacji. Każdy scenariusz powinien być odzwierciedleniem dokładnie określonej funkcjonalności. Każdy scenariusz testowy powinien posiadać identyfikator, nazwę, opis, warunki wstępne, wykaz przypadków testowych. Scenariusze i przypadki

testowe muszą zostać uzupełnione o niezbędne kroki do wykonania przed rozpoczęciem testów.

i) plan szkoleń.

j) plan testów zawierający elementy, o których mowa w rozdziale 15 Testy

11 Kody Źródłowe

Kody źródłowe muszą być przekazane w formie elektronicznej (przed kompilacją), umożliwiającej analizę i rozbudowę przez zarówno Zamawiającego jak i firmy trzecie działające na potrzeby Zamawiającego. Wykonawca musi przekazać informację o:

1. wszystkich bibliotekach i dodatkach niezbędnych do kompilacji kodu i uruchomienia Aplikacji.
2. rekomendowanym środowisku programistycznym wraz z jego konfiguracją i wskazaniem wymaganych aplikacji dodatkowych.
3. parametrach i zmiennych środowiska produkcyjnego aplikacji, koniecznych do uruchomienia Aplikacji.
4. Instrukcję krok po kroku z opisem czynności i wylistowanymi komendami, której efektem jest uruchomienie Aplikacji w środowisku produkcyjnym z kodów źródłowych Aplikacji (wraz z kompilacją, jeżeli jest potrzebna, ustawieniem zmiennych środowiskowych, instalacją zależności, przygotowaniem bazy produkcyjnej, itd.).
5. w przypadku przekazywania kodu źródłowego Aplikacji, musi być on przekazany w taki sposób, aby było możliwe umieszczenie kodu w lokalnym repozytorium Gitlab Zamawiającego.

Pracownik Centrum Obsługi Informatycznej założy repozytorium kodu w systemie Gitlab, zarządzanym przez COI oraz wklei do niego kod źródłowy Aplikacji. Każdorazowo po przekazaniu aktualizacji kodu źródłowego przez Wykonawcę, pracownik Centrum Obsługi Informatycznej będzie aktualizować kod w repozytorium kodów źródłowych.

Powyższe informacje muszą zawierać wskazanie:

1. wersji i dystrybucji wszystkich niezbędnych komponentów.
2. sposobu instalacji bibliotek i dodatków.
3. sposobu ustawiania parametrów i zmiennych środowiskowych.

W przypadku wykorzystania komponentów lub oprogramowania firm trzecich wymagających osobnych licencji, konieczne jest wskazanie tych komponentów i niezbędnego zakresu licencji.

W szczególnych przypadkach, na potrzeby weryfikacji przekazanych kodów źródłowych oraz instrukcji im towarzyszących, dopuszczone jest stworzenie środowiska do kompilacji, przy czym sam proces kompilacji będzie wykonywany przez pracownika UMK (i/lub w asyście firmy zewnętrznej).

W celu dokonania weryfikacji kompletności i czytelności kodu źródłowego, w obecności Zamawiającego Wykonawca ma dokonać kompilację i sprawdzenie poprawności działania kodu źródłowego lub należy ustalić inny tryb weryfikacji kodu źródłowego.

Kody źródłowe przekazane przez Wykonawców są przechowywane w szafie pancерnej COI UMK oraz w repozytorium Gitlab.

12 Standardy dla usług integracyjnych w UMK

1. Dostarczone rozwiązanie ma bazować na modelu usługowym, czyli wymiany danych poprzez mechanizm serwisów webowych.
2. Integracje muszą odbywać się poprzez jeden z poniższych sposobów:
 - a) Protokół komunikacyjny SOAP
 - b) styl architektury oprogramowania REST
3. W przypadku stosowania SOAP, wymagane jest dostarczenie:
 - a) plików WSDL - definiuje, jakie informacje i w jaki sposób można wydobyć z serwisu (reguły określające sposób komunikacji z serwerem), stosowane zabezpieczenia, adres właściwego serwisu, listę udostępnianych metod wraz z argumentami i zwracanymi typami.
 - b) plików XML ze schematami XSD lub w przypadku danych przestrzennych Geography Markup Language (GML).
 - c) wymagane jest dostarczenie przykładowych payloadów (requestów)/responsów. Co najmniej jeden payload na każdą akcję (operację/metodę) w usłudze.
 - d) wszystkich certyfikatów wykorzystywanych do zabezpieczenia usługi wraz z ich hasłami, opis standardów zabezpieczeń usługi. Opis użytych zabezpieczeń należy zdefiniować za pomocą specyfikacji WS-Policy i dołączyć do udostępnionego WSDL.
 - e) projektu w SoapUI lub Postman przygotowanego w taki sposób, że po uruchomieniu z dowolnego komputera z tej samej podsieci, gdzie znajduje się usługa, będzie działał poprawnie. Projekt będzie zawierał każdy z przykładowych payloadów z punktu c.
4. W przypadku stosowania REST, wymagane jest dostarczenie:
 - a) plików RAML opisującego sposób wywołania usługi (opisywaniu zasobów, metod, parametrów, odpowiedzi, typów mediów i innych konstrukcji HTTP) lub zainstalowany SwaggerUI z definicjami OpenApi lub Swagger i możliwością ich wywołania bezpośrednio z graficznego interfejsu webowego.
 - b) plików JSON lub XML definiujący schemy wejściowe/zwrotne/błędy, a w przypadku danych przestrzennych Geography Markup Language (GML).
 - c) wymagane jest dostarczenie przykładowych payloadów (requestów)/responsów. Co najmniej jeden payload na każdą akcję (operację/metodę) w usłudze.
 - d) opis sposobu zabezpieczenia usługi (opis standardów zabezpieczeń usługi). Opis musi umożliwić integrację nowej Aplikacji z API, również w przypadku wykorzystania standardu JWT lub OAuth.
 - e) projektu w SoapUI lub Postman przygotowanego w taki sposób, że po uruchomieniu z dowolnego komputera z tej samej podsieci, gdzie znajduje się usługa, będzie działał poprawnie. Projekt będzie zawierał każdy z przykładowych payloadów z punktu c.
5. Mechanizm autentykacji oraz szyfrowania komunikatów implementowany ma być w oparciu o standard WS-Security w modelu wykorzystującym certyfikaty X.509 lub w oparciu o serwer KERBEROS; w przypadku REST standardu JWT/OAuth. Dopuszczalne są mechanizmy bazujące na innych technologiach, jednak ich wykorzystanie każdorazowo wymaga konsultacji i uzyskania zgody Kierownika Referatu Architekta Systemu w UMK.
6. Komunikaty przesyłane między dostawcą a odbiorcą usług mają korzystać z protokołu HTTP/HTTPS.

7. Znaki w dokumentach wysyłanych z Aplikacji mają być kodowane według standardu Unicode UTF-8.
8. Usługi sieciowe mają korzystać z mechanizmów zapewniających zachowanie integralności, niezaprzeczalności, poufności i autentyczności danych przesyłanych w komunikatach
9. Usługa musi logować jej wywołania oraz w logach powinna być informacja zawierająca: datę/czas, adres IP z którego było wywołanie, request. Usługa musi mieć możliwość prostego włączania/wyłączania logowania poprzez plik konfiguracyjny.
10. Informacje w logach przechowywane mają być przez okres co najmniej 2 lat od daty ich zapisu. Okres ten może być inny, zgodny ze wskazanym w odrębnych przepisach prawa. Należy ustawić dzienną i miesięczną rotację pliku logów.
11. Przygotowany przez Wykonawcę Interfejs zostanie podłączony przez UMK do Szyny Danych przy współpracy z Wykonawcą. Wykonawca nie otrzyma bezpośredniego dostępu do Szyny Danych. Interfejs ten może być wykorzystany na rzecz innych integracji z dowolnymi Aplikacjami w SI Gminy Miejskiej Kraków. W niektórych przypadkach Zamawiający może umieszczać interfejsy typu REST w narzędziu API Manager.

13 Harmonogram Wdrożenia

1. Musi zawierać kamienie milowe i produkty.
2. Musi zawierać sekwencję zdarzeń.
3. Musi składać się z następujących zadań:
 - a) Analiza Przedwdrożeniowa zakończona protokołem uzgodnień
 - b) instalacja środowiska testowego
 - c) przygotowanie rozwiązania przez Wykonawcę
 - d) dostawa i instalacja Oprogramowania Systemowego w środowisku testowym
 - e) instalacja w środowisku testowym
 - f) opracowanie scenariuszy testowych i planu testów
 - g) wypełnienie Aplikacji danymi
 - h) przeprowadzenie testów
 - i) wdrożenie koniecznych zmian przez Wykonawcę
 - j) testy rozwiązania po zmianach
 - k) zatwierdzenie rozwiązania do wdrożenia w produkcji
 - l) instalacja środowiska produkcyjnego
 - m) uruchomienie rozwiązania w środowisku produkcyjnym
 - n) migracja danych
 - o) szkolenia dla Administratorów Technicznych i Użytkowników
 - p) odbiór Aplikacji
 - q) wykonanie i dostarczenie Dokumentacji
 - r) przygotowanie raportów i sprawozdania końcowego
 - s) przekazanie Platformy Serwerowej, Oprogramowania Systemowego i Aplikacji w zarządzanie przez Zamawiającego.
4. Do czasu zakończenia wdrożenia (podpisania protokołu odbioru) zarządzanie znajduje się po stronie Wykonawcy, zgodnie z zakresem określonym w rozdziale [Administrowanie Platformą Serwerową przez Wykonawcę.](#)

5. Musi zawierać terminy, czas trwania poszczególnych zadań (co najmniej pomiędzy kamieniami milowymi).

14 Administrowanie Platformą Serwerową przez Wykonawcę

1. Platforma Serwerowa będzie w całości zarządzana i administrowana przez Wykonawcę na zasadach zgodnych z Systemem Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Krakowa (Zarządzenie nr 958/2010 Prezydenta Miasta Krakowa z dnia 30 kwietnia 2010 r. w sprawie wprowadzenia Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Krakowa). W tym w szczególności Wykonawca będzie odpowiadał za:
 - a) Właściwą konfigurację i zarządzanie elementami Platformy Serwerowej, w szczególności za zapewnienie bezpieczeństwa Platformy Serwerowej, Oprogramowania Systemowego, Aplikacji i danych w nich przetwarzanych, w tym także za poprawne zabezpieczenie kopii bezpieczeństwa i przygotowanie procedur odtworzeniowych.
 - b) Bieżące monitorowanie elementów Platformy Serwerowej, w szczególności pod kątem prób nieautoryzowanego dostępu do informacji chronionych.
 - c) Przeciwdziałanie próbom włamania, zniszczenia oraz nieautoryzowanego dostępu do Platformy Serwerowej.
 - d) tworzenie i zabezpieczenie kopii zapasowych danych chronionych oraz zasobów lub konfiguracji Platformy Serwerowej, niezbędnych do prawidłowej pracy Aplikacji lub do przetwarzania danych w tych Aplikacjach.
 - e) Uaktualnianie Dokumentacji technicznej Platformy Serwerowej w zakresie co najmniej instrukcji zatrzymania, uruchomienia i weryfikacji poprawności działania serwerów i usług tworzących Platformę Serwerową.
 - f) Podjęcie natychmiastowych działań zabezpieczających w przypadku zagrożenia bezpieczeństwa Platformy Serwerowej.
 - g) Usuwanie błędów baz danych (w tym brak spójności i integralności danych).
 - h) Bieżące nadzorowanie zdrowia i utrzymanie w ruchu Oprogramowania Systemowego i Platformy Serwerowej, w tym instalowanie aktualnych poprawek udostępnianych przez producentów.
 - i) Weryfikacje i konfiguracje poprawności działania Oprogramowania Systemowego i Platformy Serwerowej.
 - j) Zapewnienie współpracy elementów Środowiska testowego (w oparciu o przekazane przez Zamawiającego wskazówki) z:
 - środowiskiem wirtualizacyjnym Zamawiającego poprzez instalacje i konfiguracje pakietu Vmware tools – dotyczy serwerów wirtualnych,
 - systemem Orion SolarWinds Zamawiającego, do monitorowania stanu serwerów – dotyczy wszystkich serwerów.
 - Klientem commvault – na potrzeby realizacji backupu. (Backup może być realizowany z poziomu maszyny wirtualnej lub plikowo po instalacji agenta).

- k) Przygotowanie wykazu aplikacji i usług udostępnianych przez serwery, zarówno do sieci LAN UMK jak i do sieci Internet, wykaz zostanie wykorzystywany do stworzenia polityk firewall UMK.
 - l) Bieżące administrowanie systemem w zakresie czynności związanych ze strojeniem Aplikacji, monitorowaniem wydajności, monitorowaniem zdarzeń systemowych, zarządzaniem zmianami oraz zarządzaniem awariami.
2. Zamawiający jest odpowiedzialny za zarządzanie Użytkownikami Aplikacji oraz za nadzór nad zarządzaniem wszystkimi Użytkownikami, w tym w szczególności Zamawiający posiada uprawnienia i jest odpowiedzialny za:
- a) Techniczne nadawanie, cofnięcie i modyfikację uprawnień Użytkownikom do Aplikacji. Zamawiający prowadzi ewidencję wszystkich Użytkowników Aplikacji.
 - b) Przeprowadzanie okresowych przeglądów kont i uprawnień wszystkich Użytkowników.
3. Wykonawca jest odpowiedzialny za zarządzanie Użytkownikami Platformy Serwerowej (tzw. Użytkownicy systemowi zarządzani poza mechanizmami Aplikacji) w tym w szczególności Wykonawca posiada uprawnienia i jest odpowiedzialny za techniczne nadawanie, cofnięcie i modyfikację uprawnień Użytkownikom do Platformy Serwerowej (tzw. Użytkownicy systemowi zarządzani poza mechanizmami Aplikacji) za akceptacją Zamawiającego. Wykonawca prowadzi ewidencję wszystkich Użytkowników Platformy Serwerowej oraz ich uprawnień.
4. Platforma Serwerowa musi być zarządzana i skonfigurowana przez Wykonawcę w taki sposób, aby:
- a) Zapewnić obsługę określonej w umowie liczbie równoczesnych Użytkowników (zalogowanych i pracujących w Aplikacjach). Powyższe ograniczenie nie dotyczy Użytkowników korzystających z ogólnie dostępnych wyszukiwarek, niewymagających logowania do systemów.
 - b) Pozwalać będą na dostęp do nich z wykorzystaniem mechanizmu autentykacji SSO (Single Sign-On). Zrealizowany on będzie w oparciu o centrum autentykacji Zamawiającego (Active Directory).
 - c) Zagwarantowany został czas dostępu do Aplikacji i transfer danych umożliwiający efektywną pracę w Aplikacjach.
 - d) Dostęp do Aplikacji przez Użytkowników i Administratorów realizowany był z ja tam dopisałem wykorzystaniem protokołu HTTPS i przeglądarki Microsoft Edge w najnowszej wersji wspieranej przez producenta. Przetwarzane Aplikacje muszą być dostępne przez 24 godziny na dobę przez 7 dni w tygodniu z wyłączeniem uzgodnionych z Zamawiającym przerw niezbędnych na dokonanie konserwacji i aktualizacji Platformy Serwerowej.
 - e) Dostęp do Platformy Serwerowej możliwy jest jedynie przez zdefiniowane kanały komunikacyjne oraz kanały przeznaczone do administrowania i monitorowania systemu. Przedstawicielom Zamawiającego udostępniana będzie aktualna lista zabezpieczeń i lista otwartych kanałów komunikacyjnych (lista otwartych portów) na serwerze aplikacyjnym.
 - f) Zapewnić środowisko testowe na potrzeby weryfikacji zmian i nowych wersji Aplikacji.
 - g) Zapewnić wysoką dostępność dla realizowanej usługi.

5. Wykonawca zobowiązany jest do udostępnienia bazy danych dla upoważnionych przedstawicieli Zamawiającego. Dostęp musi być realizowany z wykorzystaniem protokołu SSL.
6. Wykonawca zapewni instrukcję zatrzymania, uruchomienia i weryfikacji poprawności działania serwerów tworzących Środowisko testowe na wypadek sytuacji awaryjnych skutkujących samoczynnym wyłączeniem serwerów lub wymagających szybkiego wyłączenia serwerów.

15 Testy

15.1 Plan Testów

1. Dostarczony przez Wykonawcę Plan Testów musi zawierać scenariusze testowe właściwe do realizacji testów Aplikacji.
2. Plan Testów w zakresie Aplikacji i wdrożenia musi zawierać co najmniej
 - a) testy funkcjonalne,
 - b) testy wydajności,
 - c) testy bezpieczeństwa,
 - d) testy akceptacyjne.
3. Plan Testów musi zawierać listę funkcjonalności Aplikacji, które mają zostać poddane testom.
4. Plan Testów musi określać warunki, których spełnienie pozwala na rozpoczęcie testów. Zapis tych warunków musi być odzwierciedlony w Harmonogramie Wdrożenia.
5. Plan Testów musi zawierać zestaw kryteriów pozwalających uznać testy za zakończone z wynikiem pozytywnym. Zestaw kryteriów podlega akceptacji Zamawiającego.
6. Plan Testów zawiera harmonogram ich realizacji, z podaniem terminu rozpoczęcia i zakończenia zadań testowych oraz informację kto i w którym środowisku wykonuje testy (Wykonawca, Wykonawca z Zamawiającym, Zamawiający).
7. Plan Testów zawiera spis środowisk przeznaczonych do wykorzystania w trakcie testów.
8. Plan Testów zostanie opracowany przez Wykonawcę.
9. Plan Testów musi zostać zaakceptowany przez Zamawiającego w zakresie zgodności z wymogami wskazanymi w Umowie

15.2 Wymagania dotyczące wykonania testów bezpieczeństwa Aplikacji

1. Dostarczony Wykonanie testów bezpieczeństwa jest niezbędne dla uruchomienia produkcyjnego Aplikacji i przeprowadzenie testów leży po stronie Wykonawcy.
2. Testy, o których mowa w pkt 1 muszą zostać przeprowadzone zgodnie z metodyką OWASP, a ich wynik musi być wolny od podatności OWASP TOP 10:2021.
3. Zakres ww. testów musi obejmować co najmniej:
 - a) testy uwierzytelniania, autoryzacji oraz mechanizmów zarządzania sesją Aplikacji,
 - b) testy konfiguracji Aplikacji, sprawdzenie błędów generowanych przez Aplikację i jej komponenty oraz wykonanie testów mających na celu wykrycie podatności,
 - c) testy walidacji danych wejściowych,
 - d) testy logiki biznesowej Aplikacji - jako opcja,

- e) testy dodatkowe (Web Services, SSL itp).
- 4. Po przeprowadzeniu testów bezpieczeństwa Aplikacji, a przed wdrożeniem produkcyjnym, Wykonawca prześle, na adres cyberbezpieczenstwo@um.krakow.pl raport z przeprowadzonych testów zawierający co najmniej informacje na temat metod jakimi testy zostały wykonane, zakresu testów, stwierdzonych podatności lub ich braku.
- 5. Wykonawca zezwala na udostępnianie raportu osobom trzecim oraz prawo do osobnego korzystania z każdego z elementów raportu.
- 6. Wykonawca oświadcza, iż w okresie obowiązywania umowy, w której Wykonawca pozostaje stroną o określonym zakresie odpowiedzialności za Aplikację, poddaje się on dobrowolnie testom bezpieczeństwa informatycznego Aplikacji organizowanym przez Zamawiającego.
- 7. Podatności, zalecenia i rekomendacje powstałe w wyniku testów, o których mowa w pkt 6 oraz podatności, o których mowa w pkt 4, będą zgłaszane Wykonawcy zgodnie z procedurą dotyczącą usuwania błędów, określoną w obowiązującej umowie między stronami.

16 Kopia Zapasowa

- 1) Używany w Urzędzie Miasta Krakowa System Centralnego Backupu posiada następujące cechy:
 - a) Oprogramowanie: Commvault
 - b) Okres przechowywanie kopii zapasowych: 1 tydzień
 - c) Obejmuje wszystkie systemy serwerowe SI UMK, w tym bazy danych. Nie obejmuje stacji roboczych Użytkowników, a jedynie systemy serwerowe.
 - d) Standardowo wszystkie serwery wirtualne obejmowane są backupem z poziomu środowiska VMware.
- 2) Wykonawca wdrażający Aplikację musi skorzystać z Systemu Centralnego Backupu w UMK w ramach standardowego backupu całej maszyny.
- 3) Wykonawca musi współpracować z Zamawiającym w trakcie procesu obejmowania backupem Aplikacji (dodawania do Systemu Centralnego Backupu oraz tworzenia optymalnej polityki backupu).