System informatyczny wspomagający zarządzanie w obszarach: RODO, ryzyko, kompetencje pracowników, kontrola zarządcza, dostępu do aplikacji, zasobów i kluczy.

Zamawiający dopuszcza realizację zamówienia w oparciu o kilka produktów pochodzących od różnych wykonawców jak również złożenie oferty częściowej w zakresie jednego lub kilku wyspecyfikowanych modułów funkcjonalnych.

System będzie użytkowany przez ok 1.000 pracowników w 100 komórkach organizacyjnych (wydziały, referaty, biura) Urzędu.

1. Wymagania ogólne:

1.1. Aplikacja musi umożliwiać działanie na serwerach pracujących pod kontrolą systemu operacyjnego Windows lub Linux uruchomionych w infrastrukturze Zamawiającego;

1.2. Aplikacja musi zapewniać jednoczesny dostęp dla wielu użytkowników za pomocą przeglądarki internetowej;

1.3. Wymagane jest prawidłowe działanie aplikacji w przeglądarkach Chrome, Firefox, Edge bez konieczności instalowania dodatkowych komponentów;

1.4. Aplikacja musi zapewniać uwierzytelnianie zarówno na podstawie przypisanych do użytkowników loginów i haseł jak i w oparciu o konta domenowe Active Directory.

1.5. Uwierzytelnienie rozumiane jako zapewnienie dostępu do danych i funkcji aplikacji musi być realizowane na podstawie przypisywanych do użytkowników ról systemowych z uwzględnieniem ich miejsca w strukturze organizacyjnej. Wymagane jest umożliwienie zarówno centralnego zarządzania przydzielaniem ról jak i możliwość delegowania zarządzania rolami osobom zarządzającym komórkami organizacyjnymi w zakresie podległych im pracowników.

1.6. System musi posiadać interfejsy komunikacyjne API pozwalające na dwukierunkową synchronizację danych z innymi systemami w technologii REST API w zakresie:

1.6.1. w ramach każdej jednostki pobieranie danych o strukturze organizacyjnej i użytkownikach z bazy danych użytkowników w domenie ActiveDirectory tej jednostki lub odwrotnie zasilanie ActiveDirectory danymi o strukturze organizacyjnej (zakres min.: imię, nazwisko, id pracownika, PESEL, zdjęcie, jednostka organizacyjna, komórka organizacyjna, komórki podległe (min 3 poziomy zagnieżdżenia w ramach jednostki), stanowisko, przełożony, lokalizacja, telefony, e-mail (w przypadku synchronizacji „system wybrany -> domena", wskazana jest możliwość zakładania nowych użytkowników we wskazanym OU dla jednostek i przypisanych do nich domen)

1.6.2. przekazywanie zgłoszeń do systemu ITSM w zakresie min. tytułu, treści, zgłaszającego, odpowiedzialnej osoby/grupy osób, atrybutów zgłoszenia wraz z możliwością określenia odpowiedzialności za dany zasób/dotyczące go zgłoszenie i ustaleniem słowników przekodowań w zakresie typów zgłoszeń w systemach oraz odbierania informacji o statusach realizacji zgłoszeń wraz z opisem

1.6.3. zasilanie i aktualizacja bazy CMDB systemu ITSM w zakresie określonych zasobów przypisanych do użytkownika wraz z możliwością określenia słowników przekodowań dla zasobów oraz ich kategorii minimum w zakresie uprawnień do zasobów takich, jak aplikacji, upoważnienia, klucze, itp.

2. Wymagania funkcjonalne:

2.1. **Zarządzanie strukturą organizacyjną:**

2.1.1. Możliwość zarządzania strukturą organizacyjną złożoną z urzędu miasta i podległych jednostek organizacyjnych;

2.1.2. Dla urzędu miejskiego możliwość zdefiniowania wielopoziomowej struktury komórek organizacyjnych;

2.1.3. Dla każdej z jednostek organizacyjnych możliwość zdefiniowania wielopoziomowej struktury komórek organizacyjnych.

2.2. **Zarządzanie budynkami i pomieszczeniami:**

2.2.1. Możliwość prowadzenia rejestru budynków oraz powiązanych z nimi pomieszczeń;

2.2.2. Możliwość dowolnego definiowania (słownik) typów pomieszczeń;

2.2.3. Możliwość podglądu powiązanych z pomieszczeniem zasobów i pracowników.

2.3. **Zarządzanie pracownikami:**

2.3.1. Ewidencja pracowników z uwzględnieniem ich miejsca pracy w konkretnych pomieszczeniach i komórkach organizacyjnych;

2.3.2. Rejestrowanie danych o pracownikach w zakresie: imienia, nazwiska, stanowiska, komórki organizacyjnej, adresu e-mail, nr telefonu, datach początku i końca zatrudnienia, wymiaru etatu;

2.3.3. Możliwość generowania raportów (w formacie .xml, .csv) zawierających informację o sumie etatów przypisanych do poszczególnych budynków, lokalizacjach;

2.3.4. Możliwość grupowego przenoszenia pracowników pomiędzy komórkami organizacyjnymi;

2.3.5. Możliwość wydruku kart obiegowych w oparciu o zdefiniowane szablony;

2.3.6. Rejestracja rozwiązania stosunku pracy musi generować zadania odebrania zasobów posiadanych przez zwalnianego pracownika;

2.3.7. Możliwość dołączania zdjęć profilowych pracowników;

2.3.8. Możliwość wyszukiwania pracowników na podstawie dowolnych kryteriów;

2.3.9. Karta pracownika – widok agregujący informacje o pracowniku w zakresie: danych kontaktowych, wizerunku, dokumentów pracowniczych, przypisanych zadań, dostępnych usług i złożonych wniosków;

2.3.10. Widok dedykowany dla osób zarządzających komórkami organizacyjnymi umożliwiający dostęp do kart podległych pracowników.

2.4. **Rejestry dokumentów pracowniczych:**

2.4.1. Definiowanie dowolnej ilości kategorii dokumentów pracowniczych;

2.4.2. Możliwość przypisania odrębnych zarządzających dla kategorii dokumentów pracowniczych;

2.4.3. Możliwość określenia dla każdej kategorii dokumentów pracowniczych okresu ważności;

2.4.4. Możliwość tworzenia listy pracowników zobowiązanych do złożenia dokumentu na podstawie reguł, w oparciu o komórkę organizacyjną i stanowisko;

2.4.5. Możliwość automatycznej weryfikacji posiadania przez pracownika wymaganych dokumentów w procesie nadawania upoważnienia;

2.4.6. Generowanie zadań i notyfikacji mailowych dla pracowników zobowiązanych do złożenia dokumentu.

2.5. **Testy kompetencji:**

2.5.1. Możliwość powiązania testu kompetencji z kategorią dokumentów pracowniczych;

2.5.2. Możliwość zdefiniowania dowolnej ilości pytań testowych;

2.5.3. Możliwość określenia czasu trwania testu i ilości losowanych pytań;

2.5.4. Możliwość generowania zadań i notyfikacji mailowych dla pracowników zobowiązanych do realizacji testu;

2.6. **Baza wiedzy:**

2.6.1. Zapewnienie wszystkim pracownikom dostępu aktualnych wersji dokumentów zgromadzonych w bazie wiedzy;

2.6.2. Możliwość ograniczenia dostępu do dokumentów zawartych w określonych katalogach wyłącznie do pracowników wskazanej komórki organizacyjnej

2.6.3. Przechowywanie historycznych wersji dokumentów

2.6.4. Wielopoziomowa struktura katalogów dokumentów;

2.6.5. Możliwość przypisania do każdego katalogu dokumentów lub linków do stron internetowych;

2.6.6. Możliwość tworzenia listy pracowników zobowiązanych do zapoznania się z dokumentem na podstawie reguł, w oparciu o komórkę organizacyjną i stanowisko;

2.6.7. Możliwość generowania zadań i notyfikacji mailowych dla pracowników zobowiązanych do zapoznania się z dokumentem.

2.7. **Zarządzanie zasobami:**

2.7.1. Możliwość definiowania kategorii zasobów;

2.7.2. Możliwość określania jednostek organizacyjnych odpowiedzialnych za zarządzanie kategoriami zasobów i zasobami;

2.7.3. Wsparcie dla zarządzania centrum usług wspólnych poprzez umożliwienie definiowania odrębnych kontraktów/umów dla jednostek organizacyjnych będących odbiorcami zasobów;

2.7.4. Prowadzenie rejestrów użytkowników zasobów;

2.7.5. Zarządzanie pojemnością zasobów;

2.7.6. Możliwość rejestrowania zależności pomiędzy zasobami;

2.7.7. Możliwość definiowania przyszłych związanych z zasobem zadań

2.7.8. Możliwość prowadzenia rejestru istotnych dla utrzymania zasobu zdarzeń (dziennik)

2.7.9. Możliwość składania przez kierowników komórek organizacyjnych wniosków o udostępnienie zasobu pracownikom tych komórek;

2.7.10. Rejestracja rozwiązania stosunku pracy musi generować zadania odbierania uprawnień do systemów informatycznych i innych zasobów posiadanych przez zwalnianych pracowników;

2.7.11. Możliwość dowolnego definiowania poziomów dostępu do zasobów (np. role w aplikacji, uprawnienia do systemów itp.);

2.7.12. Weryfikacja możliwości udzielenia dostępu do zasobu w kontekście wymaganych dokumentów pracowniczych i posiadanego zakresu upoważnienia do przetwarzania danych osobowych;

2.7.13. Możliwość zgłaszania incydentów związanych z użytkowanymi zasobami;

2.7.14. Możliwość definiowania obiegów dla wniosków o udostępnienie zasobów oraz zgłoszeń. Definicja obiegu musi pozwalać na określenie dowolnej ilości przypisanych do poszczególnych komórek organizacyjnych kroków takich jak: inicjowanie, opiniowanie, zatwierdzanie, realizacja.

2.8. **Rejestr czynności przetwarzania / kategorii czynności przetwarzania:**

2.8.1. Możliwość utworzenia rejestru czynności przetwarzania (procesów) realizowanych w jednostce organizacyjnej;

2.8.2. Opis czynności przetwarzania musi obejmować przynajmniej:

2.8.2.1. Oznaczenie administratora danych

2.8.2.2. Cel przetwarzania

2.8.2.3. Podstawę prawną legalizującą przetwarzanie;

2.8.2.4. Określenie kategorii osób, których dane są przetwarzane;

2.8.2.5. Określenia kategorii danych

2.8.2.6. Wskazanie odbiorców danych.

2.8.3. Możliwość dokumentowania przekazania (udostępnienia) i pozyskania danych;

2.8.4. Możliwość powiązania i wyświetlenia listy pracowników posiadających upoważnienia do przetwarzania danych w ramach czynności;

2.8.5. Możliwość powiązania zasobów wykorzystywanych do przetwarzania danych w ramach czynności;

2.8.6. Możliwość powiązania kategorii dokumentów pracowniczych wymaganych dla uzyskania upoważnienia do przetwarzania danych w ramach czynności;

2.8.7. Możliwość generowania klauzuli informacyjnej;

2.8.8. Możliwość powiązania umów związanych z realizacją czynności w szczególności umów powierzenia przetwarzania danych osobowych.

2.9. **Rejestr upoważnień do przetwarzania danych osobowych;**

2.9.1. Możliwość składania wniosków o nadanie upoważnienia do przetwarzania danych osobowych;

2.9.2. Automatyczne generowanie wniosku o nadanie upoważnienia na podstawie wniosku o dostęp do zasobu;

2.9.3. Proces zarządzania upoważnieniami musi realizować zasadę jednego ważnego upoważnienia – każdy pracownik posiada jedno ważne upoważnienie;

2.9.4. Utrzymanie rejestru aktualnych i odwołanych upoważnień.

2.10. **Zarządzanie ryzykiem, cele i mierniki:**

2.10.1. Możliwość definiowania celów organizacji, możliwość grupowania celów

2.10.2. Możliwość przypisywania właścicieli celów

2.10.3. Możliwość definiowania dla każdej grupy celów odrębnych słowników: kryteriów oceny ryzyk oraz zagrożeń;

2.10.4. Możliwość prowadzenia rejestru niezgodności zawierającego: opis niezgodności, wskazanie wymagań których niezgodność dotyczy oraz listę podejmowanych i planowanych działań

2.10.5. System powinien wspierać cykliczną ocenę systemu kontroli zarządczej – w szczególności poprzez funkcję samooceny i audytu wewnętrznego;

2.10.6. System powinien pozwalać na generowanie list celów, ryzyk oraz działań naprawczych i korygujących w rozbiciu na komórki organizacyjne;

2.10.7. Możliwość tworzenia i wysyłania list kontrolnych/ankiet;

2.10.8. Możliwość wypełnienia i przesłania oświadczenia o stanie kontroli zarządczej na poziomie komórki organizacyjnej oraz jednostki;

2.10.9. Możliwość rejestrowania i szacowania ryzyk w kontekście: zasobów, grup zasobów, operacji przetwarzania;

2.10.10. Możliwość szacowania ryzyka związanego z przetwarzaniem danych osobowych na poziomie czynności przetwarzania. Ryzyko musi uwzględniać wartości przetwarzanych kategorii danych, skalę przetwarzania oraz kontekst organizacji;

2.10.11. Możliwość agregacji ryzyk zasobów na poziomie procesu (czynności przetwarzania);

2.10.12. Możliwość definiowania mierników na poziomie grupy celów organizacji;

2.10.13. Możliwość powiązania czynności przetwarzania z dowolnymi wskaźnikami;

2.10.14. Możliwość zbierania wartości wskaźników z poziomu czynności przetwarzania i agregowania (np. suma, średnia) na poziomie grupy celów organizacji.

2.10.15. Możliwość prezentacji wyników w dostępnej i przejrzystej formie z możliwością pobrania pliku pdf lub xlsx. (mapa ryzyk)

2.11. **Incydenty, naruszenia i podatności:**

2.11.1. Możliwość rejestracji zgłoszeń incydentów, naruszeń i podatności dostępna dla wszystkich pracowników;

2.11.2. Przypisanie zadań związanych z analizą incydentów, naruszeń i podatności;

2.11.3. Rejestrowanie czynności związanych z analizą incydentów, naruszeń i podatności;

2.11.4. Powiązania naruszenia i podatności z ryzykiem;

2.11.5. Utrzymywanie rejestru incydentów, , naruszeń i podatności dla jednostki z możliwością monitorowania ich statusów.

2.12. **System zgłoszeniowy**

2.12.1. System zgłoszeniowy umożliwia rejestrowanie, śledzenie i zarządzanie wszystkimi zgłoszeniami od momentu ich utworzenia do zamknięcia. Każde zgłoszenie otrzymuje unikalny identyfikator;

2.12.2. Automatyczne przydzielanie zgłoszeń do odpowiednich pracowników lub działów, eskalacja zgłoszeń, automatyczne odpowiedzi, powiadomienia i przypomnienia;

2.12.3. Generowanie raportów i analiz dotyczących m.in. liczby zgłoszeń, czasu reakcji, obciążenia pracowników obsługujących zgłoszenia;

2.12.4. Baza danych klientów z historią ich zgłoszeń i interakcji.

2.13. **Zarządzanie dostępem do pomieszczeń i kontrola obiegu fizycznych kluczy**

2.13.1. System musi umożliwiać prowadzenie ewidencji fizycznych kluczy do pomieszczeń i zarządzanie dostępem do nich zgodnie z zasadami kontroli dostępu.

2.13.2. Każdy klucz lub zestaw kluczy powinien być przypisany do konkretnego pomieszczenia oraz posiadać unikalny identyfikator.

2.13.3. System powinien umożliwiać przypisanie kluczy lub zestawów kluczy do komórek organizacyjnych

2.13.4. System powinien umożliwiać osobom zarządzającym komórkami organizacyjnymi na nadawanie i odbieranie uprawnień do pobierania kluczy w zakresie podległych sobie pracowników i przypisanych pomieszczeń.

2.13.5. System musi rejestrować każde pobranie i zdanie klucza z dokładnym oznaczeniem daty, godziny oraz danych osoby, która klucz pobrała lub zdała.

2.13.6. System powinien umożliwiać generowanie raportów z historii obiegu kluczy, filtrując po osobie, pomieszczeniu, dacie i godzinie.