Załącznik 1

Standardy środowiska teleinformatycznego UMK

1. Analiza Przedwdrożeniowa

Wykonawca przeprowadzi Analizę Przedwdrożeniową dla wdrażanego Modułu:

1) Celem Analizy Przedwdrożeniowej jest:

a) uszczegółowienie jednoznacznej interpretacji wymagań Zamawiającego i sposobu ich realizacji,
b) uszczegółowienie procesów, które będzie wspierał Moduł,
c) określenie zasad konfiguracji Modułu,
d) rozpoznanie wymaganej integracji z istniejącymi systemami,
e) określenie Platformy Serwerowej oraz Oprogramowania Systemowego niezbędnego do działania Modułu.

2) W wyniku przeprowadzonej Analizy Przedwdrożeniowej musi zostać dostarczony Dokument Analizy zawierający co najmniej:

a) jednoznaczną i zamkniętą listę wymagań wraz z określeniem sposobu ich realizacji oraz kryteria akceptacji dla wymagania,
b) listę słowników i parametrów Modułu,
c) listę potrzebnych raportów wraz z opisem,
d) jednoznacznie ustalone zasady konfiguracji Modułu,
e) jednoznacznie określony sposób i założenia integracji z innymi Modułami,
f) diagram architektury wewnętrznej Modułu (DARWA) - diagram prezentuje elementy składowe Modułu – wraz z opisem,
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 Modułu. Każdy scenariusz powinien być odzwierciedleniem dokładnie określonej funkcjonalności. Każdy scenariusz testowy powinien posiadać identyfikator, nazwę, opis, warunki wstępne, wykaz przypadków testowych. Scenariusze i przepadki testowe muszą zostać uzupełnione o niezbędne kroki do wykonania przed rozpoczęciem testów.
i) zakres Instruktażu,
j) plan testów zawierający elementy, o których będzie mowa w dalszej części dokumentu.

2. Dokumentacja Modułu

1) Dokumentacja Modułu sporządzona na potrzeby zamówienia musi być zgodna ze stanem prawnym aktualnym na dzień przedstawienia jej do odbioru Zamawiającemu.

2) Dostarczona Dokumentacja Modułu 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 Modułu 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 pisania,
c) poprawnością ortograficzną,
d) aktualnymi odnośnikami do innych dokumentów, rozdziałów lub fragmentów Dokumentacji Modułu,
e) musi w całości opisywać funkcjonalności Modułu,
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 umożliwiać administrowanie Modułem.

Wykonawca przygotuje, dostarczy Dokumentację i będzie ją aktualizował tak, aby zawierała co najmniej wymagania określone poniżej:

1) Opis konfiguracji Modułu, w tym wykaz wdrożonych elementów, powiązania pomiędzy nimi, opis ich konfiguracji, implementacja w środowisku Zamawiającego (integracja).

2) Instrukcje start/stop dla całego środowiska (infrastruktura – systemy operacyjne, wspomagające, bazy danych itp.).

3) Instrukcje eksploatacyjne dla Administratorów.

4) Instrukcje instalacji i konfiguracji.

Wymagania dotyczące Dokumentacji Modułu w zakresie instrukcji eksploatacyjnej i dokumentacji technicznej:

1) Instrukcja eksploatacyjna użytkowania Modułu musi zawierać:

a) opis zastosowania, działania i sposobu wykonania (opis krok po kroku) każdej udostępnionej funkcjonalności Modułu z dokładnością do pojedynczej funkcji,
b) opis zastosowania wszystkich użytych słowników,
c) opis wszystkich parametrów Modułu związanych z jej ustawieniami i funkcjonalnościami,
d) wykaz możliwych do przyznania uprawnień do Modułu wraz z ich opisem,
e) listę i opis ikon, przycisków i skrótów klawiaturowych,
f) instrukcja użytkowania musi być wyposażona w wyszukiwarkę i indeks.

2) Dokumentacja techniczna musi zawierać:

a) wymagania techniczne dotyczące sprzętu i środowiska (z dokładnością do wersji środowiska),
b) ustawienia konfiguracyjne środowiska, w którym pracuje Moduł, w tym również opis implementacji w środowisku SI UMK wraz z procedurami start/stop dla wszystkich elementów Modułu,
c) opis parametrów konfiguracji Modułu i sposób ich wykorzystania.
d) musi zostać dostarczony diagram architektury wewnętrznej Aplikacji (DARWA) - diagram prezentuje elementy składowe modułu,
e) opis techniczny rodzajów i zastosowanych protokołów komunikacji (w tym certyfikatów),
f) sposób wykonania instalacji Modułu, instalacji poprawek i kolejnych wersji,
g) procedura odtworzenia danych i konfiguracji,
h) schemat baz danych wraz z opisem struktury uwzględniający powiązania i zależności między obiektami w bazie danych,
i) listę wykorzystywanych słowników danych oraz ich opis,
j) wykaz danych podlegający kontroli poprawności wraz z informacją o sposobie kontroli poprawności,
k) wykaz komunikatów diagnostycznych i standardowych błędów (opis błędu, warunki jego powstania).

Podczas integrowania systemów dodatkowo:

Instrukcja integracji, w wersji do udostępniania osobom trzecim w celu właściwego zintegrowania się z Modułem powinna zawierać:

a) opis usługi, interfejsów i wytyczne umożliwiające integrację Modułu z innymi aplikacjami.
b) pliki ze schematami (WSDL, GML, Swagger/OpenApi, itp.)
c) opis metod i struktur danych interfejsów.
d) Charakterystykę katalogów i plików kodu źródłowego,
e) Diagram klas,
f) Komentarze w kodzie źródłowym pozwalające na automatyczne wygenerowanie dokumentacji w formacie HTML lub PDF przy użyciu dedykowanego narzędzia (np. Javadoc)

3) Instrukcja Użytkownika ma zostać przekazana w języku polskim.

3. Harmonogram wdrożenia

Harmonogram wdrożenia zostanie ustalony z Zamawiającym w oparciu o zapisy oraz terminy wskazane w Umowie.

Harmonogram wdrożenia musi zawierać następujące etapy:

1) Analiza Przedwdrożeniowa zakończona protokołem odbioru
2) wykonanie Modułu przez Wykonawcę,
3) instalacja w środowisku testowym,
4) opracowanie scenariuszy testowych i planu testów,
5) wypełnienie systemu danymi (konfiguracja, zasilenie słowników),
6) przeprowadzenie testów,
7) wdrożenie koniecznych zmian przez Wykonawcę,
8) testy rozwiązania po zmianach,
9) zatwierdzenie rozwiązania do wdrożenia w produkcji,
10) uruchomienie rozwiązania w środowisku produkcyjnym,
11) instruktaż dla Administratorów i Użytkowników,
12) odbiór Modułu,
13) eksploatacja próbna,
14) usuwanie usterek,
15) odbiór eksploatacji próbnej,
16) wykonanie i dostarczenie dokumentacji,
17) przygotowanie raportów i sprawozdania końcowego,
18) przekazanie Modułu w zarządzanie Zamawiającemu.

4. Monitorowanie zdarzeń i Użytkowników

Monitorowanie Użytkowników (logi)

1) Moduł, musi spełniać następujące wymagania:

a) zapis daty i godziny wprowadzenia danych do Modułu, określenia operatora, który dane wprowadził i zakresu tych danych,
b) zapis źródła pozyskania danych osobowych w przypadku, gdy dane pozyskano z innego źródła niż osoba, której dane dotyczą,
c) zapis informacji o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały przekazane, wraz z określeniem daty i zakresu udostępnianych danych,
d) zapis eksportu do edytowalnego pliku treści danych osobowych,
e) zapis daty i godziny zmiany danych w Module i określenia operatora, który zmiany wprowadził,
f) zapis usunięcia danych z Modułu,
g) zapis oznaczenia wraz z odnotowaniem daty danych, których przetwarzanie zostało ograniczone,
h) zapis oznaczenia wraz z odnotowaniem daty danych, wobec przetwarzania których wniesiono sprzeciw,
i) zapis wygenerowania i wydrukowania raportu zawierającego informacje, o których mowa w lit. a–h w dowolnym określonym przez żądającego raport układzie i zakresie.

2) Moduł musi posiadać odpowiednie rejestry, umożliwiać ich przeglądanie, sortowanie, filtrowanie, wyszukiwanie danych po dowolnych polach. Z rejestrów tych musi być możliwość generowania raportów w zakresie:

a) historii zmian uprawnień Użytkowników (z dokładnością do roli): login, nazwisko, imię, jednostka, komórka organizacyjna, rola, data nadania roli, data odebrania roli,
b) historia lista sesji Użytkowników: zawierać będzie listę wszystkich sesji Użytkowników, wraz z informacjami: login, nazwisko, imię, jednostka, komórka organizacyjna, data i godzina początku sesji, data i godzina zakończenia sesji (jeżeli sesja już została zakończona), adresie IP komputera, na którym powstała sesja,
c) listy otwartych sesji: Login, nazwisko, imię, jednostka, komórka organizacyjna, data /godzina początku sesji (musi być możliwość wylogowania wszystkich Użytkowników),
d) historii logowań: login, nazwisko, imię, jednostka, komórka organizacyjna, data i godzina zalogowania, data i godzina wylogowania, czas logowania,
e) kont Użytkowników w Module: 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,
f) 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,
g) listy aktywnych Użytkowników wraz z przypisanymi rolami (imię, nazwisko, login, komórka organizacyjna, referat, role),
h) listy osób, które w zadanym okresie miały nadane uprawnienia, przy czym powinna być możliwość wyszukiwania po parametrach:
    - okres (od, do) wraz z możliwością wyszukania listy osób, które miały nadane uprawnienia przez cały okres jak i w jego fragmencie,
    - rola (możliwe zaznaczenie kilku).

Lista osób, o której mowa w pkt g) powinna zawierać następujące informacje: login, nazwisko, imię, jednostka, komórka organizacyjna, data nadania uprawnienia, data odebrania uprawnienia.

Zakres powyższych raportów musi zostać ostatecznie uzgodniony na etapie Analizy Przedwdrożeniowej.

Wszystkie raporty wskazane w pkt 2) muszą posiadać:

- nagłówek zawierający tytuł raportu,
- zadane parametry wyszukiwania dla których został wygenerowany raport,
- informację kto i kiedy wygenerował raport,
- część zasadniczą z wygenerowanymi danymi wraz z nagłówkami kolumn.

3) W Module muszą być logowane zdarzenia z dokładnością do każdego parametru określonego w pkt 2). Komunikaty zdarzeń muszą być opisane w sposób czytelny dla Użytkownika.

4) W Module muszą być rejestrowane działania Użytkowników oraz zdarzenia związane z bezpieczeństwem informacji. Logi musza zawierać rejestracje wszystkich działań Użytkownika w Module 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 Module natomiast reguły związane z przechowywania logów archiwalnych zostaną uzgodnione na etapie Analizy Przedwdrożeniowej.

Moduł musi zawierać mechanizm do przeglądania logów bieżących (wstępnie wszystkie do 24 miesięcy; okres ustawiany parametrem) i archiwalnych (wstępnie wszystkie powyżej 24 miesięcy; okres ustawiany parametrem) w tym zapewniający możliwość:

- - wyszukiwania,
- - filtrowania po wybranych przez Użytkownika typach zdarzeń i ich cechach,
- - sortowania po wybranych przez Użytkownika typach zdarzeń i ich cechach.

5) Moduł musi zapewniać mechanizm eksportu pliku logów do serwera zewnętrznego przy użyciu standardowych protokołów i mieć możliwość synchronizacji z serwerem czasu (protokół NTP).

6) Generowane raporty muszą być eksportowane do plików innego formatu w szczególności XLSX, CSV, w zależności od zapotrzebowania Użytkownika.

5. Testy dla wdrażanego Modułu

Testy są obowiązkowym elementem wdrożenia Modułu i zmian Aplikacji/Modułu. Mają być przeprowadzane zgodnie z poniższymi zasadami:

1) Plan testów zawiera scenariusze testowe właściwe do realizacji testów Modułu.
2) Plan testów w zakresie wdrożenia Modułu musi zawierać co najmniej:
   a) testy funkcjonalne,
   b) testy wydajności,
   c) testy bezpieczeństwa,
   d) testy akceptacyjne.
3) Plan testów zawiera listę funkcjonalności Modułu, które mają zostać poddane testom.
4) Wyłączenia – Zamawiający dopuszcza, aby testy nie obejmowały poszczególnych zakresów (obszarów/elementów). Wymaga to pisemnego uzasadnienia z podaniem przyczyny, dla której następuje wyłączenie. Wyłączenia muszą być zatwierdzone przez Zamawiającego. Brak zgody Zamawiającego skutkuje koniecznością przeprowadzenia testów w tym zakresie.
5) Plan testów określa warunki, których spełnienie pozwala na rozpoczęcie testów. Zapis tych warunków musi być odzwierciedlony w harmonogramie realizacji wdrożenia.
6) Plan testów zawiera zestaw kryteriów pozwalających uznać testy za zakończone z wynikiem pozytywnym. Zestaw kryteriów podlega akceptacji Zamawiającego.
7) 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).
8) Plan testów zawiera spis środowisk przeznaczonych do wykorzystania w trakcie testów.
9) Plan testów zostanie opracowany przez Wykonawcę.
10) Plan testów musi zostać zaakceptowany przez Zmawiającego w zakresie zgodności z wymogami wskazanymi w Umowie.

Wymagania dotyczące wykonania testów bezpieczeństwa Modułu

1) Wykonanie testów bezpieczeństwa jest niezbędne dla uruchomienia produkcyjnego Modułu 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 Modułu,
   b) testy konfiguracji Modułu, sprawdzenie błędów generowanych przez Moduł i jej komponenty oraz wykonanie testów mających na celu wykrycie podatności,
   c) testy walidacji danych wejściowych,
   d) testy logiki biznesowej Modułu
   e) testy dodatkowe (Web Services, test CMS, SSL itp).
4) Po przeprowadzeniu testów bezpieczeństwa Modułu, a przed wdrożeniem produkcyjnym, Wykonawca prześle, na adres mailto: 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 Moduł, poddaje się on dobrowolnie testom bezpieczeństwa informatycznego Modułu 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.