

WYMAGANIA TECHNICZNE DOTYCZĄCE SERWISÓW INTERNETOWYCH

- 1) Kodowanie stron wg standardów HTML5 oraz CSS3, zakończone poprawną walidacją w narzędziu W3C (<http://validator.w3.org>).
- 2) Kodowanie znaków UTF-8.
- 3) Prosty i przejrzysty interfejs wykonany w całości z uwzględnieniem zasad Responsive Web Design.
- 4) Warstwa prezentacji uwzględniająca wymagania WCAG na poziomie zgodnym z obowiązującymi przepisami prawa (w tym m.in. *Ustawa z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych* oraz *Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności*, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych), przechodząca poprawną walidację przy pomocy narzędzia pod adresem <http://wave.webaim.org>. Zapewnienie dokonywania zmian w przypadku konieczności dostosowania do zmian w wymaganiach prawnych.
- 5) Dynamiczna zawartość oparta na wspieranej i stabilnej technologii, pełna funkcjonalność musi być wytworzona na jednej ze wskazanych technologii: php, python, ruby, erlang, ASP.Net lub OpenJDK. Dopuszcza się realizację części frontend za pomocą JavaScript bez stosowania po stronie klienta technologii (np. Adobe Flash czy Java).
- 6) Zapewnienie integralności danych poprzez transakcyjne przetwarzanie.
- 7) Wszystkie załączniki plikowe wykorzystywane w systemie muszą być przechowywane poza bazą danych, z zastosowaniem odpowiednich zabezpieczeń uniemożliwiających bezpośredni dostęp do plików z poziomu przeglądarki. Wszystkie załączniki plikowe muszą być przechowywane z wykorzystaniem storage obiektowego zgodnego ze standardem S3 udostępnionego przez Zamawiającego.
- 8) Kod dostarczonego rozwiązania musi być jawny i dostarczony w takiej postaci, aby Zamawiający był w stanie prześledzić jego działanie pod kątem bezpieczeństwa. Zabronione jest korzystanie z mechanizmów szyfrujących typu *ioncube*.
- 9) W przypadku wykorzystania narzędzi do minimalizacji kodu wyjściowego (HTML,

CSS, JavaScript) Wykonawca dostarczy także wersję z bazowymi plikami źródłowymi bez minimalizacji.

- 10) Prawidłowe działanie z najnowszymi, stabilnymi wersjami przeglądarek (również w wersji mobilnej), z równoczesnym zachowaniem wsparcia dla minimum 3 poprzednich wersji przeglądarek: Mozilla Firefox, Google Chrome, Microsoft Edge, Safari, Opera.
- 11) Optymalizacja pod kątem pozycjonowania serwisu (m.in. przyjazne linki, itp.).
- 12) Optymalizacja czasu ładowania stron (mała łączna wielkość plików tworzących pojedynczą stronę).
- 13) Funkcjonalność wysyłania poczty elektronicznej z serwisu będzie realizowana przy wykorzystaniu skrzynki pocztowej na serwerze poczty elektronicznej Zamawiającego, za pomocą dedykowanej biblioteki wybranego rozwiązania bez korzystania z funkcji systemowej mail.
- 14) Dane przechowywane w relacyjnej bazie danych, w najnowszej stabilnej wersji, rozwiązanie typu Opensource (np. MySQL, PostgreSQL) lub MS SQL. W przypadku konieczności zakupu licencji Wykonawca dostarczy wszystkie niezbędne licencje obejmujące całość rozwiązania pozwalające na bezproblemowe i wydajne wykorzystywanie przez cały okres trwania umowy.
- 15) Dynamiczne generowanie wersji „do wydruku” w oparciu o CSS, która będzie dostosowana do specyfiki wydruku tj.: bez tła, zredukowana ilość elementów, w tym graficznych.
- 16) System powinien być zoptymalizowany pod względem dostępności dla znacznej liczby jednoczesnych użytkowników.
- 17) System powinien być zoptymalizowany pod względem pozycjonowania (SEO). Wykonawca uwzględni podane przez Zamawiającego opisy stron i słowa kluczowe (sekcja meta).

ZABEZPIECZENIA

- 1) Serwis musi uniemożliwiać dostęp do funkcji i zgromadzonych w nim danych z pominięciem mechanizmów bezpieczeństwa.
- 2) Serwis musi być odporny na znane techniki ataku i włamań, w tym w szczególności podatnościami z aktualnej listy Top 10 wg organizacji OWASP, znajdującymi się w specyfikacji The OWASP Top 10 – 2021.
- 3) W przypadku pojawienia się nowych, nieznanych wcześniej technik włamań, Wykonawca jest zobowiązany do ich analizy oraz dostarczenia niezbędnych poprawek i uaktualnień eliminujących podatności dostarczonego rozwiązania w ramach świadczonej pomocy technicznej.
- 4) Serwis musi filtrować i walidować wszystkie dane wejściowe (np. z formularzy) w celu zminimalizowania ryzyka naruszenia integralności systemu bądź danych.
- 5) Wykonawca ma obowiązek dokonywania poprawek dostarczonego systemu

w oparciu o przedstawione przez Zamawiającego wyniki audytu pod kątem bezpieczeństwa teleinformatycznego w ramach obowiązującego wsparcia technicznego.

- 6) Wykonawca w ramach obowiązującej usługi gwarancyjnej na bieżąco będzie dostosowywał system pod kątem bezpieczeństwa informacji, w szczególności ochrony danych osobowych oraz do najnowszych komponentów serwera – wybrana technologia webowa, baza danych – wydawanych przez producenta jako najnowsze stabilne wersje produkcyjne, przy uwzględnieniu bieżącego hardeningu systemu i jego komponentów. Przy większych zmianach wersji jednego z ww. komponentów Zamawiający udostępni nowe środowisko produkcyjne, na które Wykonawca dokona migracji systemu.
- 7) Strona internetowa serwisu musi zapewniać walidację danych pobieranych z formularzy, danych URL oraz być odporna na popularne zagrożenia (takie jak: ataki semantyczne na adres URL, ataki związane z ładowaniem plików, ataki typu crosssite scripting, ataki typu CSRF, wstrzykiwanie kodu SQL, itp.

Infrastruktura techniczna wersji produkcyjnej oraz testowej będzie uzgodniona z Wykonawcą.

Proces wytwarzania oraz wszystkich modyfikacji będzie przeprowadzany i przechowywany w lokalnym repozytorium Git Zamawiającego, w tym ilość maszyn wirtualnych na potrzeby realizacji Zamówienia.