# Definition of Done dla portalu internetowego

Test Użyteczności:

Przeprowadzenie testów użyteczności (usability tests), aby upewnić się, że interfejs jest intuicyjny i łatwy w obsłudze dla końcowego użytkownika.

Sprawdzenie Poprawności Technicznej:

Kontrola poprawności kodu (np. HTML, CSS, JavaScript) pod kątem błędów i zgodności ze standardami webowymi.

Recenzja Kodu:

Przeprowadzenie recenzji kodu przez co najmniej jednego innego programistę, w celu upewnienia się, że kod jest zgodny z najlepszymi praktykami i standardami projektu.

Przygotowanie Środowiska:

Konfiguracja środowiska testowego, w którym można przeprowadzić wszystkie testy przed wypuszczeniem portalu na żywo.

Testy Funkcjonalne:

Przeprowadzenie testów funkcjonalnych, aby sprawdzić, czy wszystkie funkcje działają zgodnie z oczekiwaniami i założeniami projektu.

Spełnienie Kryteriów Akceptacji:

Upewnienie się, że wszystkie kryteria akceptacji określone przez klienta lub Product Ownera zostały spełnione.

Testy Bezpieczeństwa:

Przeprowadzenie testów bezpieczeństwa, aby zapewnić, że dane użytkownika są bezpiecznie przechowywane i chronione.

Responsywność i Kompatybilność:

Testowanie kompatybilności z różnymi przeglądarkami oraz urządzeniami, aby upewnić się, że portal jest responsywny i dostępny dla szerokiej gamy użytkowników.

Optymalizacja SEO:

Przeprowadzenie optymalizacji pod kątem wyszukiwarek internetowych (SEO), aby ułatwić znajdowanie portalu przez potencjalnych użytkowników.

Przygotowanie Do Produkcji:

Przygotowanie wersji produkcyjnej portalu, w tym minifikacja zasobów, optymalizacja wydajności i konfiguracja cache.

Monitorowanie:

Skonfigurowanie narzędzi do monitorowania i logowania błędów, które będą aktywne po wdrożeniu portalu.

Dokumentacja:

Zaktualizowanie dokumentacji projektu, w tym opis funkcji, instrukcji wdrożenia i utrzymania portalu.

Przegląd i Akceptacja Klienta:

Demonstracja portalu dla klienta/Product Ownera i uzyskanie formalnej akceptacji.

Wdrożenie na Środowisko Produkcyjne:

Pomyślne wdrożenie portalu na środowisko produkcyjne.

# Definition of Done dla Epic Rejestracja/Logowanie/Zapomniane Hasło

Funkcjonalność Rejestracji:

Użytkownik może utworzyć nowe konto z walidacją danych wejściowych.

Wdrożono mechanizmy weryfikacji e-mail.

Przeprowadzono testy w celu zapewnienia, że tylko silne hasła są akceptowane.

Funkcjonalność Logowania:

Użytkownik może zalogować się za pomocą adresu e-mail i hasła.

Zaimplementowano ograniczenia na nieudane próby logowania.

Wprowadzono opcjonalne dodatkowe metody uwierzytelniania, np. dwuskładnikowe uwierzytelnianie (2FA).

Funkcjonalność Odzyskiwania Hasła:

Użytkownik może zresetować zapomniane hasło przez e-mail.

Proces odzyskiwania hasła jest bezpieczny i zawiera etapy weryfikacji tożsamości użytkownika.

Walidacja i Testy:

Przeprowadzono walidację frontendu i backendu dla wszystkich pól formularza.

Wszystkie scenariusze rejestracji, logowania i odzyskiwania hasła są pokryte testami automatycznymi (jednostkowe, integracyjne).

Bezpieczeństwo:

Przeprowadzono audyt bezpieczeństwa dla wszystkich trzech funkcjonalności.

Użyto bezpiecznego przechowywania hasła.

Wdrożono odpowiednie środki przeciwko atakom typu CSRF i XSS.

User Experience (UX):

Interfejs użytkownika dla rejestracji, logowania i odzyskiwania hasła jest intuicyjny i zgodny z wytycznymi UX.

Przeprowadzono testy użyteczności z rzeczywistymi użytkownikami, aby upewnić się, że proces jest prosty i zrozumiały.

Dokumentacja:

Zaktualizowano dokumentację projektu, w tym opis nowych funkcjonalności i przepływów użytkownika.

Utworzono i udostępniono dokumentację API związane z autentykacją użytkownika.

Kompatybilność:

Przetestowano funkcjonalności na różnych przeglądarkach i urządzeniach.

Wydanie i Wdrożenie:

Funkcjonalności są w pełni zintegrowane z głównym kodem aplikacji i działają na środowisku testowym.

Przeprowadzono pełne regresyjne testy systemu po integracji nowych funkcji.

Akceptacja:

Uzyskano formalną akceptację Product Ownera lub klienta po demonstracji działania funkcjonalności.

Monitoring i Logowanie:

Skonfigurowano systemy monitorujące i logujące, które wykrywają i rejestrują problemy związane z procesem logowania i odzyskiwania hasła.

# kryteria akceptacji dla "Jako użytkownik chcę przesłać plik na serwer”

Możliwość wybrania pliku do przesłania:

Użytkownik może wybrać plik z lokalnego dysku za pomocą standardowego okna dialogowego systemu operacyjnego.

Obsługiwane formaty plików to: JPG, PNG dla zdjęć restauracji i PDF dla menu restauracji.

Maksymalny rozmiar pliku to 5MB.

Walidacja pliku przed przesłaniem:

System weryfikuje, czy wybrany plik spełnia kryteria dotyczące formatu i rozmiaru.

Jeśli plik nie spełnia wymagań, użytkownik otrzymuje czytelny komunikat o błędzie z informacją, jakie warunki nie zostały spełnione.

Postęp przesyłania:

Podczas przesyłania pliku użytkownik widzi wskaźnik postępu lub inny graficzny element wskazujący na trwający proces przesyłania.

Użytkownik otrzymuje informację zwrotną po pomyślnym przesłaniu pliku lub w przypadku wystąpienia błędu podczas przesyłania.

Przypisanie przesłanego pliku do odpowiedniej restauracji:

Przesłany plik jest automatycznie przypisywany do profilu restauracji, z której pochodzi, na podstawie danych zawartych w pliku lub wybranych przez użytkownika opcji.

Zachowanie bezpieczeństwa i prywatności:

Wszystkie przesyłane pliki są skanowane w poszukiwaniu złośliwego oprogramowania.

Dane użytkowników i zawartość przesyłanych plików są chronione zgodnie z obowiązującymi przepisami o ochronie danych osobowych.

Dostępność i wydajność:

Funkcjonalność przesyłania plików jest dostępna 24/7, z wyjątkiem planowanych przerw technicznych.

Czas przesyłania pliku nie przekracza 30 sekund dla użytkowników z przeciętnym połączeniem internetowym.

Interfejs użytkownika:

Interfejs przesyłania plików jest intuicyjny i zgodny z ogólnym projektem aplikacji.

Po przesłaniu pliku użytkownik ma możliwość jego podglądu oraz usunięcia lub zastąpienia pliku, jeśli to konieczne.

# kryteria akceptacji dla "Jako użytkownik chcę zmienić swoje hasło"

Dostępność opcji zmiany hasła:

Użytkownik ma możliwość łatwego znalezienia opcji zmiany hasła w ustawieniach konta.

Weryfikacja tożsamości przed zmianą hasła:

Przed zmianą hasła użytkownik musi potwierdzić swoją tożsamość, np. przez wprowadzenie aktualnego hasła lub kliknięcie w link weryfikacyjny wysłany na jego adres email.

Wymagania dotyczące nowego hasła:

System przedstawia jasne wymagania dotyczące nowego hasła (np. minimalna długość, konieczność użycia liter, cyfr i znaków specjalnych).

Nowe hasło musi różnić się od poprzednich haseł używanych przez użytkownika.

Wprowadzenie i potwierdzenie nowego hasła:

Użytkownik musi wprowadzić nowe hasło oraz potwierdzić je, wpisując ponownie w osobnym polu, aby zminimalizować ryzyko błędu.

Walidacja i informacja zwrotna:

System weryfikuje zgodność nowego hasła z wymaganiami i informuje użytkownika o ewentualnych błędach w sposób zrozumiały i konstruktywny.

W przypadku powodzenia, użytkownik otrzymuje potwierdzenie zmiany hasła.

Bezpieczeństwo procesu:

Wszystkie dane przesyłane w procesie zmiany hasła są szyfrowane.

Po zmianie hasła użytkownik otrzymuje powiadomienie e-mail z informacją o zmianie hasła dla celów bezpieczeństwa.

Logowanie po zmianie hasła:

Po zmianie hasła, wszystkie inne sesje (na innych urządzeniach) zostają wylogowane, a użytkownik musi ponownie się zalogować używając nowego hasła.

Odzyskiwanie dostępu w przypadku zapomnienia hasła:

W procesie zmiany hasła dostępna jest opcja odzyskania dostępu dla użytkowników, którzy zapomnieli swojego aktualnego hasła.