Załącznik nr 1 do Zapytania ofertowego

Numer postępowania: 10/2026/NIL

Szczegółowy opis przedmiotu zamówienia

Projekt „Ogólnopolski program rozwoju kompetencji medycznych personelu lekarskiego" w ramach programu Fundusze Europejskie dla Rozwoju Społecznego 2021–2027, współfinansowanego ze środków Europejskiego Funduszu Społecznego Plus

1. Przedmiot i cel zamówienia

Zamówienie obejmuje modernizację lub wdrożenie platformy edukacyjnej NIL realizującej szkolenia asynchroniczne i synchroniczne online, wspierającej wydarzenia stacjonarne i hybrydowe oraz komplementarne aplikacje mobilne, a także uruchomienie, utrzymanie i wsparcie.

Celem jest zapewnienie jednolitego środowiska wspierającego programy dydaktyczne NIL realizowane online i stacjonarnie, a w szczególności:

- Publikacja i wyszukiwanie szkoleń na stronie NIL, identyfikacja, rekrutacja i zapisy uczestników/czek,
- Udział live, stacjonarny, hybrydowy i asynchroniczny,
- Dostęp do e-learningu, multimediów, interakcji, testów, potwierdzenia udziału, certyfikatów, punktów edukacyjnych, a także zapewnienie monitoringu, raportowania i zarządzania użytkownikami/czkami i szkoleniami.

Obowiązkowe kanały dostępu to WWW oraz aplikacje Android i iOS dla uczestników/czek (responsywna strona nie zastępuje aplikacji), zgodne z FUN-24 i TECH-06, dostępne także dla osób z niepełnosprawnościami.

Dla live dopuszcza się usługę zewnętrzną spełniającą FUN-06; nie wymaga się budowy własnego silnika transmisji.

Platforma przetwarza dane identyfikacyjne, numery PWZ, historię kształcenia, dokumenty uczestników/czek i nagrania, a przy dostosowaniach egzaminów także informacje mogące dotyczyć zdrowia. NIL zachowuje kontrolę nad danymi i treściami. Wykonawca przetwarza dane osobowe na udokumentowane polecenie NIL i na warunkach powierzenia.

2. Zakres rzeczowy i granice odpowiedzialności

W ramach wynagrodzenia umownego Wykonawca zrealizuje poniższy zakres prac i usług, zgodnie z wymaganiami OPZ oraz podziałem odpowiedzialności między NIL a Wykonawcę określonym w niniejszym rozdziale.

• Analiza stanu obecnego i potrzeb NIL, analiza ryzyk, danych, treści oraz integracji.

• Projekt funkcjonalny i architektoniczny, prototypy procesów użytkownika/czki, środowiska testowe i produkcyjne.

• Konfiguracja LMS, katalogu szkoleń, zarządzania wydarzeniami, testów, certyfikatów, raportowania i komunikacji.

• Dostarczenie, konfiguracja, publikacja i utrzymanie dedykowanych aplikacji Android i iOS dla uczestników/czek, zgodnie z FUN-24 i TECH-06, wraz z integracją z LMS, testami, dokumentacją i obsługą aktualizacji.

• Integracje z systemami NIL określone w rozdziale 4.

• Testy funkcjonalne, integracyjne, wydajnościowe, dostępności, bezpieczeństwa i odtworzeniowe.

• Dokumentacja, instruktaż administratorów i redaktorów, okres stabilizacji i wsparcia po uruchomieniu.

• Konfiguracja webinarów live, szkoleń hybrydowych i zarządzania salami oraz obiektami; powiązanie harmonogramów, rezerwacji, uczestników/czek i raportów.

• Hosting zarządzany w Europejskim Obszarze Gospodarczym, utrzymanie do 30 czerwca 2029 r., aktualizacje, kopie bezpieczeństwa oraz migracja końcowa.

• Ochrona danych i cyberbezpieczeństwo, w tym wsparcie NIL w ocenie skutków dla ochrony danych i klasyfikacji modułów AI;

- Platforma zostanie uruchomiona bez migracji danych historycznych z dotychczasowych systemów NIL. Zamówienie obejmuje migrację końcową danych zgromadzonych podczas jej eksploatacji oraz przeniesienie Platformy do środowiska NIL lub wskazanego dostawcy, zgodnie z rozdziałem 6 i fazą F8.

2.1. NIL zapewnia dane źródłowe, uprawnienia i dokumentację potrzebną do realizacji zamówienia. Wykonawca odpowiada za adaptery, obsługę błędów, testy, dokumentację i zgłaszanie zależności. Awaria systemu NIL nie zwalnia z obsługi błędów i ponowienia operacji. Za usługi zewnętrzne dobrane do realizacji własnego rozwiązania odpowiada Wykonawca.

2.2. Wykonawca prowadzi rejestr zależności, ryzyk i decyzji. Zmiana zakresu zamówienia wymaga formalnego uzgodnienia na zasadach umowy; sama akceptacja analizy nie zmienia OPZ.

2.3. Wykonawca przygotuje i realizuje plan komunikacji i przekazania wiedzy dla administratorów, zespołu edukacyjnego, prowadzących i użytkowników/czek. Wykonawca podczas realizacji wskaże role, działania, terminy, materiały komunikacyjne, sposób realizowania wsparcia i zbierania informacji zwrotnych.

3. Fazy realizacji i kamienie milowe

Terminy oznaczone jako F0–F6 są terminami granicznymi od zawarcia umowy; prace mogą być równoległe, a każdy etap wymaga przekazania produktów i akceptacji NIL. Akceptacja harmonogramu nie zmienia zakresu ani terminów umowy.

Faza	**Zakres**	Termin graniczny: F0–F6 od zawarcia umowy; F7–F8 według dat kalendarzowych	**Produkt etapu / warunek odbioru**
F0	Inwentaryzacja i kick-off	Do 10 dni	Dostępy do źródeł, rejestr treści i danych, mapa systemów, zależności i ryzyk, uzgodniona lista interesariuszy. Akceptacja planu prac i zasad dostępu do danych. Umowa powierzenia przed dostępem do danych rzeczywistych.
F1	Analiza i projekt rozwiązania	Do końca 3. tygodnia	Projekt funkcjonalny i architektura, mapowanie wymagań na scenariusze użytkownika/czki, integracje, plan testów.
F2	Prototyp (POC) i walidacja UX	Do końca 5. tygodnia	Środowisko demonstracyjne i prototyp katalogu, konta uczestnika/czki, zapisów, kursu, punktów i certyfikatu.

Faza	Zakres	Termin graniczny: F0–F6 od zawarcia umowy; F7–F8 według dat kalendarzowych	Produkt etapu / warunek odbioru
F3	Budowa LMS i modułu live/hybrid	Do końca 10. tygodnia	Kompletna wersja startowa. Wymagana demonstracja pełnej ścieżki publikacji, dostępu, zakończenia i raportowania szkoleń synchronicznych i asynchronicznych. Etap ten obejmuje również kompletne, instalowalne wersje testowe aplikacji Android i iOS, połączone z LMS. Odbiór na podstawie protokołu.
F4	UAT, audyty, wydajność	Do końca 12. tygodnia;	Testy akceptacji użytkowników/czek (UAT) dla kluczowych procesów we wszystkich rolach użytkowników/czek.
F5	Start platformy	Do końca 14. tygodnia; po odbiorze F4	Odbiór obejmuje testy produkcyjne, instruktaż, dokumentację, dostępy NIL, domenę/DNS/certyfikaty i testy. Odroczone są wyłącznie integracje F6. Warunkiem F5 jest również dostępność produkcyjnych aplikacji Android i iOS w Google Play i Apple App Store, instalacja i test kontrolny wersji sklepowych z produkcyjnym LMS, przekazanie dokumentacji oraz potwierdzenie kontroli NIL nad publikacją. Aplikacji nie odracza się do F6.
F6	Integracje	Do końca 24. tygodnia; z możliwością realizacji równolegle z F7	Działające integracje NIL z zatwierdzonej specyfikacji.
F7	Stabilizacja i utrzymanie	Od odbioru startu do 30.06.2029 r.; pierwsze 30 dni: stabilizacja	Raport stabilizacji i miesięczne raporty SLA, bezpieczeństwa, pojemności i działań naprawczych. Utrzymanie trwa również po migracji końcowej do 30 czerwca 2029 r..
F8	Migracja końcowa i przekazanie usługi	Przygotowanie od 1 kwietnia 2029 r.; przełączenie i odbiór najpóźniej 30 czerwca 2029 r., w terminie zatwierdzonym przez NIL.	Plan wyjścia z harmonogramem, parametrami środowiska docelowego i podziałem odpowiedzialności, migracja próbna i końcowa, test odtworzenia, przekazanie danych, kodu i dokumentacji. Odbiór zgodnie z pkt 6.7. Utrzymanie po przełączeniu trwa do daty z pkt 12.1; współdziałanie infrastrukturalne zgodnie z pkt 12.2.

4. Integracje i zarządzanie tożsamością

Specyfikacja określa systemy, właścicieli, funkcje, przepływy i dane, interfejsy, dostępność środowisk, limity i koszty. Szczegóły integracji, takie jak mapowania konkretnych pól, obsługę błędów, logowanie i testy Wykonawca uszczegółowi w F1.

Od F5 do odbioru integracji w F6 obowiązuje tryb przejściowy: NIL ręcznie weryfikuje PWZ i uprawnienia w uprawnionym źródle rejestrowym, zapisując wynik, datę, źródło i autora. Brak lub niejednoznaczność weryfikacji nie uprawnia do szkolenia wymagającego potwierdzenia. W trybie przejściowym konta, role, strukturę i sale obsługuje się lokalnie. W F1 Wykonawca udokumentuje tryb przejściowy i przypisze zamówione połączenia do F5 lub F6; przed F5 przeszkoli odpowiedzialne osoby. Tryb przejściowy nie znosi zamówionych integracji.

INT-01 Identyfikacja i uwierzytelnianie

Platforma obsługuje tworzenie, aktywację, aktualizację, blokadę, dezaktywację i odzyskiwanie kont, role, uprawnienia i rejestr zdarzeń. Wszyscy użytkownicy, w tym uczestnicy i pracownicy NIL, korzystają z kont lokalnych z MFA obejmującym co najmniej dwa niezależne czynniki, od uruchomienia w fazie F5 przez cały okres utrzymania. Jedno konto zapewnia dostęp do WWW i aplikacji mobilnych. Logowanie nie potwierdza PWZ ani uprawnień do szkolenia.

Weryfikacja / odbiór przed F5: utworzenie, aktywacja, aktualizacja, blokada i dezaktywacja konta lokalnego, logowanie i wylogowanie, MFA dla wszystkich ról, odświeżenie i wygaśnięcie sesji, odmowa dostępu oraz odzyskanie konta bez obejścia MFA. Testy obejmują wspólne konto w WWW i obu aplikacjach mobilnych.

INT-02 Weryfikacja PWZ przez CRL

Integracja z API Centralnego Rejestru Lekarzy (CRL) do weryfikacji PWZ jest obowiązkowa i podlega odbiorowi w fazie F6. NIL zapewnia możliwość korzystania z API, dokumentację i uprawniony dostęp na potrzeby realizacji i testów. Do odbioru integracji obowiązuje ręczna weryfikacja opisana we wstępie do rozdziału 4. Awaria CRL nie może być traktowana jako pozytywny wynik weryfikacji.

Weryfikacja / odbiór: Weryfikacja nastąpi po przetestowaniu następujących przypadków: poprawny PWZ, nieistniejący PWZ, konflikt danych, brak łączności, limit zapytań, zmiana statusu prawa, ponowna weryfikacja. Każdy przypadek ma oczekiwany rezultat.

INT-03 Źródło prawdy o danych

Specyfikacja integracyjna wskazuje system referencyjny dla każdego atrybutu, reguły edycji i rozwiązywania konfliktów. Użytkownik/czka nie może nadpisywać danych rejestrowych. Dane kontaktowe mogą być zarządzane w LMS w granicach określonych w specyfikacji.

Weryfikacja / odbiór: Tabela mapowania pól i reguł edycji; test synchronizacji, korekty i rozwiązywania konfliktów.

INT-04 Zarządzanie uprawnieniami

System umożliwi automatyczne przypisywanie kont do grup i kohort oraz udostępnianie i przypisywanie im kursów według konfigurowalnych reguł NIL opartych na zweryfikowanych danych. Administrator włącza i określa te reguły. Niedozwolone treści pozostają niewidoczne i niedostępne także przez bezpośredni link.

Weryfikacja / odbiór: Testy uprawnień między grupami, przy zmianie statusu i przy próbie dostępu bezpośredniego. Logika przydziału jest konfigurowalna.

INT-05 Ewidencja i eksport punktów edukacyjnych

Punkty edukacyjne są ewidencjonowane lokalnie w LMS od fazy F5 zgodnie z FUN-12. Uprawnione osoby mogą eksportować ewidencję punktów zgodnie z wymaganiem FUN-14, z uwzględnieniem nadania, anulowania i korekt oraz danych uczestnika/czki i szkolenia. Eksport nie zmienia stanu naliczeń; jego powtórzenie nie nalicza punktów ponownie ani nie jest potwierdzeniem ich rejestracji poza LMS.

Weryfikacja / odbiór przed fazą F5: lokalne nadanie, anulowanie i korekta punktów, historia operacji, kontrola uprawnień oraz eksport zgodny z ewidencją LMS. Powtórzenie naliczenia lub eksportu nie może powodować podwójnego naliczenia. Nie wymaga się testów transmisji do zewnętrznego systemu punktów.

INT-06 Katalog LMS i ręczna publikacja linków na portalu NIL

Katalog wydarzeń i zapisy są obsługiwane w LMS od fazy F5. Platforma udostępnia adresy stron wydarzeń i zapisów, które NIL ręcznie publikuje i aktualizuje na swoim portalu w miarę potrzeb.

Weryfikacja / odbiór przed F5: utworzenie i aktualizacja wydarzenia w katalogu LMS, udostępnienie linku do jego strony i zapisów oraz poprawne przejście z ręcznie opublikowanego linku na portalu NIL do LMS.

INT-07 Środowisko testowe integracji

Dla usług i połączeń niezbędnych do działania funkcji startowych testy end-to-end i kontrolowana weryfikacja połączeń produkcyjnych muszą być zakończone przed odbiorem F5. Dla integracji z systemami NIL odroczonych do F6 te same warunki muszą być spełnione przed ich uruchomieniem i odbiorem w F6. Zakres obejmuje scenariusze poprawne i błędne, bezpieczeństwo, regresję oraz uzgodnienie danych z okresu przejściowego. Same symulatory nie uprawniają do odbioru żadnej integracji.

Weryfikacja / odbiór: dla każdej integracji raport identyfikuje system i interfejs, zgodność schematów, scenariusze poprawne i błędne, autoryzację, limity, ponowienia, regresję i uzgodnienie danych przejściowych, wyniki i dowody. Wymagany jest podpisany protokół NIL z udziałem właściciela systemu.

INT-08 Usługa katalogowa

Integracja z LDAP/Active Directory nie jest objęta zamówieniem. Kontami, rolami i strukturą organizacyjną zarządza się lokalnie w Platformie zgodnie z INT-01, INT-04 i FUN-21.

Weryfikacja / odbiór: lokalne utworzenie i aktualizacja konta, zmiana jednostki lub opiekuna oraz odebranie dostępu, z zachowaniem historii i weryfikacją uprawnień według INT-04 i FUN-21.

INT-09 Integracje edukacyjne

Zamówienie nie obejmuje integracji z zewnętrznymi platformami edukacyjnymi poza połączeniami wymaganymi do realizacji webinarów (FUN-06) i aplikacji mobilnych (FUN-24). Integracja z CRL pozostaje obowiązkowa zgodnie z INT-02.

5. Wymagania funkcjonalne i procesy edukacyjne

Poniżej określono wymagania funkcjonalne Platformy, obejmujące obsługę użytkowników/czek, organizację i realizację procesów edukacyjnych, zarządzanie treściami, komunikację, raportowanie oraz wykorzystanie sztucznej inteligencji, wraz ze sposobami weryfikacji ich spełnienia na potrzeby odbioru.

FUN-01 Konta, role i grupy

Platforma zapewni role: uczestnik/czka, redaktor/trener, administrator merytoryczny, administrator techniczny, analityk/raportujący oraz opiekun/przełożony. Uprawnienia do jednostek, danych, kursów i raportów są konfigurowalne. Określenie „uczestnik” obejmuje uczestniczki i uczestników, a „użytkownik” wszystkie osoby korzystające z Platformy.

Weryfikacja / odbiór: Zestaw przetestowanych 10 scenariuszy kontroli dostępu opartej na rolach, w tym blokada dostępu do raportów i danych uczestników/czek innych jednostek; matryca ról w dokumentacji.

FUN-02 Katalog i wyszukiwarka

Katalog obejmuje wyszukiwanie i łączenie filtrów według tematu, specjalizacji, terminu, prowadzącego, rodzaju, dostępności i grupy docelowej. Wymagane są przełączane widoki listy i kafli, kategorie z wieloma kursami, sortowanie według nazwy lub ostatniej aktywności oraz oznaczanie kursów gwiazdką. Filtry obejmują wszystkie, aktualne, nadchodzące, zakończone i ulubione szkolenia oraz ukończone, nieukończone, przypisane, dostępne do zapisu, obowiązkowe i wygasające. Kurs z terminem realizacji krótszym niż 7 dni jest oznaczany jako wygasający, a uczestnik/czka otrzymuje informację.

Weryfikacja / odbiór: Kombinowanie filtrów, stan pusty, dostęp publiczny i zalogowany; dostępność na telefonie przez przeglądarkę.

FUN-03 Formularze rejestracji i zgody

Administrator konfiguruje pola zapisów, załączniki oraz wersjonowane zgody, oświadczenia i akceptacje regulaminów. System rozróżnia ich rodzaje i podstawy; nie traktuje każdego oświadczenia jako zgody na przetwarzanie danych. Formularze prezentują i wersjonują klauzule informacyjne zgodnie z RODO-09.

Weryfikacja / odbiór: Przykładowe formularze z warunkami wymaganych pól, rejestrem akceptacji i identyfikatorem wersji dokumentu.

FUN-04 Zapisy na wydarzenia

Obsługa webinaru, kursu asynchronicznego, wydarzenia stacjonarnego i hybrydowego obejmie limit miejsc, listę rezerwową włączaną przez administratora, anulowanie zapisu, potwierdzenia, odwołanie i zmianę terminu.

Weryfikacja / odbiór: Scenariusz pełnego cyklu dla opisanych wyżej typów wydarzeń; brak podwójnego zapisu oraz prawidłowe komunikaty.

FUN-05 Powiadomienia

Administrator konfiguruje dla każdego kursu treść, rodzaj, termin, godzinę i odbiorców automatycznych komunikatów: przed rozpoczęciem, w dniu rozpoczęcia, cyklicznie co wybraną liczbę dni, przed zakończeniem, w ostatnim dniu przed zakończeniem i w dowolnie wskazanym dniu. Może wykluczyć osoby, które ukończyły kurs. System obsługuje także komunikaty o koncie, zapisie, zmianie terminu, anulowaniu, certyfikacie, nowym szkoleniu i nowym lub zmienionym materiale bazy wiedzy. Ogłoszenia są dostępne w platformie oraz jako wiadomości e-mail kierowane do wskazanych odbiorców.

Weryfikacja / odbiór: Szablony w języku polskim, poprawny personalizowany link, rejestr wysyłek, obsługa nieudanego doręczenia; możliwość dołączenia pliku ICS.

FUN-06 Webinary i transmisje

Moduł realizujący webinary / kształcenie synchroniczne będzie powiązany z kontami, wydarzeniami i raportami. Administrator określa termin, prowadzącego, uczestników/czek i uprawnienia; udział jest możliwy z przeglądarki. Wymagane są interakcja z prowadzącym, rejestr wejść i wyjść, obsługa przerw połączenia oraz nagrywanie i publikacja nagrań po włączeniu przez organizatora. Moduł zapewni co najmniej 2 webinary równolegle, po 250 uczestników/czek każdy, łącznie 500 uczestników/czek live jednocześnie. Wymagana pojemność, niezbędne licencje i zasoby są objęte ceną od uruchomienia w F5 przez cały okres utrzymania.

Weryfikacja / odbiór: utworzenie wydarzenia, zapis, powiadomienie i link, udział prowadzącego i uczestnika/czki, interakcja, wyjście i powrót, raport czasu obecności i status uczestnictwa; po włączeniu nagrywania także zapis nagrania i kontrola dostępu.

Odbiór pojemności przed F5: jednoczesny test 2 webinarów po 250 uczestników/czek każdy, z weryfikacją udziału, interakcji, rejestru obecności oraz nagrywania po jego włączeniu. Raport potwierdzi osiągnięcie wymaganej liczby uczestników/czek na każdym webinarze i działanie tych funkcji przy równoległym obciążeniu. Test live nie zastępuje odrębnego testu 1000 sesji LMS z TECH-01.

FUN-07 Tworzenie i dystrybucja kursów

Redaktorzy tworzą kursy z sekcji, lekcji, plików, wideo, prezentacji, PDF, tekstów, e-booków, SCORM i testów. Wbudowane edytory bez programowania obsługują testy, ankiety, lekcje interaktywne (np. H5P), ćwiczenia, zadania, projekty i gry memory. Kursy mają warunki dostępu, zależności, harmonogram, obowiązkowość i ważność. Instruktor zarządza uczestnikami/czkami, ocenami, certyfikatami, raportami, egzaminami, zadaniami praktycznymi, udostępnionymi symulacjami, terminami walidacji i uprawnieniami innych instruktorów.

Weryfikacja / odbiór: Kurs referencyjny z co najmniej dwiema sekcjami, modułem SCORM, testem końcowym, ograniczeniami i certyfikatem.

FUN-08 Obsługa SCORM i xAPI

Platforma obowiązkowo obsługuje SCORM 1.2, SCORM 2004 oraz xAPI. Obsługa xAPI obejmuje rejestrowanie i odczyt zdarzeń aktywności edukacyjnych w repozytorium LRS (Learning Record Store) zapewnionym w ramach rozwiązania, z identyfikacją uczestnika/czki i aktywności oraz zapisem wyników i ukończeń. Niezbędne komponenty, licencje, konfiguracja i utrzymanie LRS są objęte ceną zamówienia. Przesyłanie dużych pakietów danych (powyżej 500MB) odbywa się przez bezpieczne repozytorium.

Weryfikacja / odbiór przed F5: osobne testy SCORM 1.2 i SCORM 2004 na rzeczywistych pakietach NIL obejmują start, wznowienie, zapis postępu, ponowne podejście, ukończenie i eksport raportu. Test treści xAPI obejmuje przesłanie i odczyt zdarzeń w LRS, prawidłową identyfikację uczestnika/czki i aktywności oraz zgodność wyników i ukończeń z raportami Platformy. Odbiór wymaga zaliczenia wszystkich trzech standardów; test jednego nie zastępuje testów pozostałych.

FUN-09 Zasady ukończenia

Ukończenie jest definiowane na poziomie kursu i aktywności: wykonanie określonych zadań, uzyskanie wyniku testu, potwierdzona obecność lub inne zatwierdzone kryterium. Sam czas otwarcia strony nie jest dowodem opanowania treści.

Weryfikacja / odbiór: Wynik pozytywny/negatywny oraz wznowienie, wiele prób i poprawne wyświetlenie certyfikatu; brak możliwości obejścia warunku przez zmianę adresu URL.

FUN-10 Testy i bank pytań

Konfigurowalne quizy: jednokrotny/wielokrotny wybór, prawda/fałsz, dopasowania, pytania otwarte; pule, losowanie, limity czasu i prób, próg zaliczenia.

Weryfikacja / odbiór: Demonstracja banku pytań, losowego testu, podsumowania wyników i ręcznej oceny pytań otwartych.

FUN-11 Certyfikaty i zaświadczenia

Konfigurowalne wzory dokumentów PDF w zależności od typu wydarzenia, organizatora i podstawy przyznania; numer/identyfikator, data, dane lekarza, lekarki, liczba punktów (jeśli dotyczy), archiwum i pobieranie.

Weryfikacja / odbiór: Przykładowe dwa różne wzory, brak wystawienia przed spełnieniem warunku, odtworzenie wersji historycznej i obsługa korekty/anulowania.

FUN-12 Punkty edukacyjne

Administrator może przypisać do wydarzenia regułę i liczbę punktów zgodną z zatwierdzonym modelem NIL. Platforma prowadzi lokalną historię naliczeń, korekt, aneksów i anulowań oraz umożliwia jej eksport na zasadach INT-05 i FUN-14. Nie wymaga się statusów przekazania ani integracji punktów z systemami zewnętrznymi.

Weryfikacja / odbiór: Weryfikacja zdarzenia, naliczenia, cofnięcia i eksportu bez dublowania punktów.

FUN-13 Ankiety i ocena jakości

Administrator tworzy ankiety satysfakcji, anonimowe lub identyfikowalne, i wiąże je z kursem. Może ustawić wypełnienie ankiety jako warunek wydania certyfikatu. Raport anonimowy nie ujawnia odpowiedzi konkretnej osoby.

Weryfikacja / odbiór: anonimowa i identyfikowalna ankieta testowa, raport zbiorczy oraz eksport CSV, XLS i XLSX, bez ujawniania danych poza zakresem roli.

FUN-14 Raporty i wskaźniki projektu

Raporty obejmą wszystkie kursy, pojedyncze szkolenie i historię uczestnika/czki: postępy, wyniki, czasy SCORM, zaliczone i niezaliczone aktywności, status, punkty i dokumenty. Filtry: imię, nazwisko, kurs, jednostka/wydział, data, województwo, wydarzenie i specjalizacja. Wymagane są CSV, oba formaty arkuszy XLS i XLSX oraz PDF i tworzenie kolejnych raportów.

Weryfikacja / odbiór: Odbiór na zatwierdzonym wzorze raportu NIL, słownik definicji danych i kontrola uprawnień do eksportu.

FUN-15 Panel uczestnika/uczestniczki

Panel uczestnika/czki prezentuje na jednej karcie zbiorczej statystyki ostatnich kursów, ostatnio zaliczone aktywności, kontynuowanie ostatniego podejścia, wszystkie zapisy w widoku listy i kafli, status ukończony/w trakcie, procent postępu lub pozostały zakres i wynik końcowy. Obejmuje certyfikaty, punkty i historię wydarzeń. Platforma wspiera indywidualne tempo nauki, śledzenie postępów i rekomendacje kursów zgodnie z uprawnieniami. Dostęp do materiałów wygasa według reguł nadanych uczestnikowi/czce.

Weryfikacja / odbiór: Scenariusze użytkownika/czki nowego, aktywnego, po ukończeniu i z utraconym prawem dostępu.

FUN-16 Praca wielu dostawców treści

Platforma pozwala nadać wykonawcom kursów odrębne uprawnienia redakcyjne i dostęp testowy uczestnika/czki, tak aby nie mogli zmieniać cudzych kursów ani materiałów.

Weryfikacja / odbiór: test rozdzielenia uprawnień dwóch zespołów produkcyjnych oraz publikacja i podmiana dużej paczki SCORM z zachowaniem postępów, jeśli umożliwia to pakiet.

FUN-17 Samokształcenie i biblioteka materiałów

Baza wiedzy jest odrębnym komponentem z katalogami i podkatalogami, nie kursem o tej nazwie. Obsługuje Word, PDF, PPT, MP4, audio i moduły interaktywne, tagi, wyszukiwanie i filtry, wersje, audyt zmian, archiwizację oraz historię korzystania i postępów. Uprawnienia do pojedynczego pliku nadaje się użytkownikom/czkom i grupom. Administrator określa publikację i ważność oraz wysyła ogłoszenia i e-maile o zmianach. Samokształcenie dopuszcza samodzielny zapis według regulaminu; nagrania live podlegają uprawnieniom i ochronie wizerunku.

Weryfikacja / odbiór: osobna baza z katalogami i podkatalogami, plikami Word/PDF/PPT/MP4, wyszukiwaniem po tagach, dwiema wersjami pliku, historią zmian, archiwizacją, powiadomieniem i ograniczeniem dostępu do pliku także przez bezpośredni URL. Dodatkowo zapis na kurs, wznowienie, wygaśnięcie dostępu i raport ukończenia.

FUN-18 Wydarzenia hybrydowe i zasoby fizyczne

Wydarzenia stacjonarne i hybrydowe obejmą rejestrację, listy obecności, limity miejsc, kalendarz sal i obiektów, przypisywanie zasobów i blokadę kolizji rezerwacji. Funkcja jest obowiązkowa. Jej realizacja przez system NIL wymaga wskazania integracji w specyfikacji; w przeciwnym razie Wykonawca zapewnia ją w Platformie.

Weryfikacja / odbiór: Utworzenie wydarzenia hybrydowego z dwiema formami udziału, potwierdzenie odpowiednich list obecności i wygenerowanie raportu łącznego; dla rezerwacji zasobów — przypadek kolizji terminów.

FUN-19 Dowody uczestnictwa i dokumentowanie projektu

System umożliwia dokumentowanie procesu edukacyjnego w ramach projektu: status zapisów, forma udziału, potwierdzenia obecności, zaliczenia modułów, wyniki weryfikacji efektów uczenia się, daty wydania dokumentów i odpowiednie eksporty. Definicje wskaźników, wzory raportów i okresy retencji zatwierdza NIL.

Weryfikacja / odbiór: Zgodność raportu z zatwierdzonym wzorem NIL dla szkolenia live, asynchronicznego i hybrydowego; weryfikacja kompletności, możliwości eksportu i audytowalności korekt.

FUN-20 Onboarding uczestników i uczestniczek szkoleń i automatyczna analiza dokumentów

Administrator określa wymagane dokumenty uczestnika/czki i reguły ich akceptacji. Uczestnik/czka przesyła dokumenty przez bezpieczny mechanizm Platformy. OCR odczytuje imię i nazwisko, zakres szkolenia, liczbę godzin oraz daty wystawienia i ważności, jeżeli występują w dokumencie. Dla każdego pola system prezentuje odczytaną wartość i poziom pewności. Ocena dokumentu i rejestrowanie decyzji odbywają się zgodnie z RODO-05. Wolumen przetwarzania określa TECH-02.

Platforma obsługuje dokumenty PDF, JPG i PNG, do 10 stron i 20 MB każdy. Wykrywanie obrazu podpisu służy ocenie kompletności dokumentu i nie obejmuje potwierdzania jego autentyczności ani technicznej weryfikacji podpisów elektronicznych. Braki, nieczytelność i wyniki niepewne kierowane są do ręcznej oceny.

FUN-21 Panel opiekuna/opiekunki

Panel opiekuna obejmie uczestników/czki przypisanych jednostek oraz powiadomienia o wygasających dokumentach, nierozpoczętych lub nieukończonych kursach i dokumentach do oceny. NIL konfiguruje terminy, np. 30, 14 i 7 dni przed wygaśnięciem, oraz eskalację do wskazanej osoby uprawnionej po upływie terminu działania. Reguła eskalacji określa zdarzenie, termin, odbiorcę i warunek zakończenia. Zmiana jednostki lub przełożonego aktualizuje dostępy, szkolenia i przypisania według INT-04, z zachowaniem historii i odebraniem poprzedniemu opiekunowi nieaktualnych uprawnień.

Weryfikacja i odbiór: Test wielopoziomowej struktury, dwóch relacji przełożonych, przeniesienia użytkownika/czki, automatycznych zapisów, eskalacji i utraty dostępu przez poprzedniego opiekuna.

FUN-22 Materiały wideo i komunikacja

Platforma umożliwi wgrywanie wideo i osadzanie YouTube/Vimeo. Dla własnego odtwarzacza administrator ustawia próg zaliczenia procentowy lub w minutach z krokiem 5 minut oraz blokadę przewijania do nieobejrzanego fragmentu.

Weryfikacja i odbiór: Test osadzenia, progów i wznowienia, blokady przewijania oraz poprawnego zapisu ukończenia; demonstracja każdego kanału komunikacji i ograniczeń dostępu.

FUN-23 Analiza raportów i potrzeb szkoleniowych

Platforma wspiera analizę potrzeb szkoleniowych poprzez ankiety, wyniki testów, historię ukończeń i raporty luk wskazanych przez NIL. Zapewnia wsparcie AI do podsumowania raportu, opisania trendów i rekomendacji oraz wykonania własnego prompta uprawnionego użytkownika/czki.

Wynik AI jest oznaczony jako wygenerowany i pozostaje powiązany z raportem źródłowym. Nie zastępuje danych liczbowych ani decyzji o zaliczeniu lub przyznaniu punktów. Dostęp do danych jest ograniczony rolą; dostawca AI, lokalizacja przetwarzania, retencja i dopuszczalny zakres danych wymagają akceptacji NIL przed uruchomieniem.

Weryfikacja i odbiór: Porównanie podsumowania z raportem źródłowym, test własnego zapytania, braku dostępu do cudzych jednostek oraz raportu potrzeb szkoleniowych.

FUN-24 Aplikacje mobilne Android i iOS dla uczestników i uczestniczek

Obie aplikacje w języku polskim zapewnią uczestnikowi/czce: wspólne konto WWW z MFA i odzyskiwaniem dostępu (INT-01), katalog i wyszukiwanie, zapisy i przypisane szkolenia, panel postępów i historii, materiały tekstowe/PDF/audio/wideo i SCORM (FUN-08), testy, ankiety, wyniki, ukończenia, punkty i certyfikaty. Obsłużą formularze, akceptacje, bezpieczne przesyłanie wymaganych dokumentów i ich statusy. Uprawnienia, warunki dostępu i ukończenia, próby i terminy są takie same jak w WWW; panel oceny dokumentów dla administratora nie jest wymagany.

Wspólny LMS zapewni kontynuację nauki między WWW i aplikacjami bez utraty zapisanych postępów, wyników, historii i uprawnień oraz bez duplikowania ukończeń i punktów. Aplikacje obsłużą live i nagrania; dla live dopuszcza się przejście do aplikacji lub mobilnej przeglądarki dostawcy z zachowaniem autoryzacji, interakcji, obecności i powrotu do szkolenia. Kursy asynchroniczne realizuje się w aplikacji; dopuszcza się bezpieczne i dostępne osadzone komponenty WWW. Nie wymaga się administracji, tworzenia kursów.

Aplikacje umożliwią pobranie materiałów tekstowych, PDF, audio, wideo i pakietów SCORM do nauki offline oraz lokalny zapis postępów. Po odzyskaniu połączenia postępy zostaną zsynchronizowane z LMS bez utraty danych i podwójnego naliczania ukończeń. Testy końcowe, przesyłanie dokumentów i wydawanie certyfikatów wymagają połączenia z internetem. Aplikacja wyraźnie wskazuje tryb offline i stan synchronizacji.

Weryfikacja / odbiór: Weryfikacja na obu systemach obejmuje instalację wersji sklepowej, logowanie z MFA, zapis na szkolenie, przesłanie dokumentu, realizację materiałów i SCORM, test, ankietę, ukończenie oraz pobranie certyfikatu. Sprawdzeniu podlegają synchronizacja WWW–aplikacja–WWW, zgodność wyników i punktów z LMS, wygaśnięcie sesji, blokada konta i odebranie uprawnień. Test obejmuje również udział live z przerwą połączenia, raport obecności i odtworzenie nagrania. Test na Android i iOS obejmie pobranie materiałów i pakietu SCORM, naukę bez połączenia z internetem, zamknięcie i ponowne uruchomienie aplikacji oraz synchronizację po odzyskaniu połączenia. Postępy muszą zostać zachowane i prawidłowo odwzorowane w LMS, bez duplikowania ukończeń.

AI-01 Moduły wykorzystujące sztuczną inteligencję

Wymaganie to obejmuje wszystkie zastosowania AI, w szczególności FUN-20 i FUN-23. Wykonawca zapewni zgodność z rozporządzeniem (UE) 2024/1689 (AI Act) właściwą dla zastosowania i terminów obowiązywania przepisów. W F1 przedstawi klasyfikację, obowiązki i środki, a przed dostępem do danych rzeczywistych udokumentuje ich spełnienie. Obowiązują także RODO-04 i RODO-05. Wynik AI nie zastępuje decyzji NIL ani uprawnionej osoby; dopuszczalna automatyczna akceptacja dokumentu wykonuje wyłącznie reguły zatwierdzone przez NIL na zasadach FUN-20 i RODO-05.

Dane NIL nie mogą być wykorzystywane do trenowania ani doskonalenia modeli dostawcy. Dostawca modelu, lokalizacja przetwarzania (wyłącznie w Europejskim Obszarze Gospodarczym) i okres retencji zapytań są wskazane w F1. Wykonawca stosuje zabezpieczenia przed wstrzyknięciem poleceń (prompt injection) i ujawnieniem danych spoza uprawnień użytkownika/czki oraz rejestruje zapytania kierowane do modułów AI.

Weryfikacja / odbiór: dokument klasyfikacji AI; oświadczenie dostawcy modelu o braku trenowania na danych NIL; test próby uzyskania danych innej jednostki przez własne zapytanie.

6. Hosting, architektura, wydajność

6.1. Projekt architektury obejmie co najmniej: warstwę aplikacyjną i bazę danych, pamięć podręczną, repozytorium plików, usługę poczty, mechanizm kolejek, monitoring, kopie zapasowe, odseparowane środowisko testowe, kontrolę dostępu i logowanie operacji. Architektura musi umożliwiać przeniesienie Platformy i danych do infrastruktury NIL lub innego dostawcy hostingu.

6.2. Wykonawca zapewni zarządzany hosting produkcyjny i odseparowane środowisko testowe w EOG do odbioru migracji końcowej, z zachowaniem ciągłości utrzymania do 30 czerwca 2029 r. Środowisko będzie jednodzierżawcze, przeznaczone wyłącznie dla NIL, z redundancją zasilania, chłodzenia i łączy. Zarządzanie bezpieczeństwem usług centrum danych i hostingu musi być objęte certyfikatem ISO/IEC 27001 lub wykazanymi równoważnymi środkami na zasadach CYB-04. Hosting obejmie WAF, ochronę DDoS, monitoring 24/7/365, kopie bezpieczeństwa i skalowanie.

6.3. NIL zachowa własność wszystkich danych, kontrolę nad domeną, DNS i certyfikatami, imienne konto administratora technicznego oraz prawo uzyskania pełnej kopii danych i plików w terminie do 5 dni roboczych od żądania. Wykonawca wykona pełną instalację, konfigurację, optymalizację bazy danych i serwera WWW oraz dostosowanie logo, kolorów i domeny NIL.

6.4. W ramach umowy Wykonawca przeprowadzi migrację końcową do środowiska NIL lub wskazanego dostawcy: przeniesie aplikację, bazę, pliki, konta, uprawnienia, konfigurację, historię aktywności, logi i integracje. Przekaże dokumentację, skrypty wdrożeniowe oraz zależności i licencje.

6.5. Plan migracji obejmie terminy, odpowiedzialność, kopię zabezpieczającą, próbę migracji, synchronizację przed przełączeniem, testy i procedurę powrotu. Wykonawca odpowiada za kompletność, integralność danych i zachowanie funkcji.

6.6. Odbiór hostingu obejmuje dokumentację infrastruktury, potwierdzenie spełnienia wymagań certyfikacji lub równoważności według CYB-04 oraz test uzyskania przez NIL pełnej kopii danych i plików przed odbiorem uruchomienia.

6.7. Weryfikacja / odbiór migracji: potwierdzenie kompletności i integralności danych, poprawności kont i uprawnień, działania funkcji i integracji oraz spełnienia wymagań bezpieczeństwa i wydajności w środowisku docelowym. Odbiór obejmie również przekazanie dokumentacji i dostępów administracyjnych. Wyłączenie środowiska źródłowego i usunięcie przechowywanych w nim danych nastąpią dopiero po odbiorze migracji i pisemnym poleceniu NIL, z uwzględnieniem zasad retencji.

TECH-01 Wydajność pod obciążeniem

Platforma obsłuży co najmniej 5500 kont oraz test obciążenia 1000 jednoczesnych sesji wskazany w tabeli odbiorowej. Test obejmie logowanie, zasoby, SCORM, quizy, ukończenia i certyfikaty.

Weryfikacja / odbiór: 60 minut stałego obciążenia; p95 czasu odpowiedzi podstawowych operacji ≤ 3 s, bez transferu strumieniowego; błędy techniczne ≤ 1%. Raport zawiera metryki CPU/RAM/I/O i konfigurację środowiska.

TECH-02 Skalowanie i pojemność

Wykonawca zapewni zasoby i skalowanie dla parametrów TECH-01 oraz pełnego profilu obciążenia i pojemności. Profil stanowi wspólną podstawę wyceny i odbioru: obejmuje konta i sesje, kursy, pliki, wideo, transmisje live, transfer, OCR, zapytania AI i prognozę przyrostu do końca utrzymania. F0, F1 i testy służą doborowi i weryfikacji infrastruktury w tych granicach, a nie ustalaniu po wyborze oferty nowych limitów obowiązkowego zakresu. Sama liczba kont i sesji z TECH-01 nie zastępuje pozostałych parametrów pojemności.

Wszystkie parametry i limity wskazane w poniższej tabeli, wraz z niezbędnymi zasobami, licencjami i usługami zewnętrznymi, są objęte ceną zamówienia od uruchomienia w F5 do 30 czerwca 2029 r.

Parametr	Wymagany zakres
Konta i sesje	Co najmniej 5500 kont i 1000 jednoczesnych sesji LMS.
Przestrzeń na dane	Co najmniej 1 TB przy uruchomieniu, z możliwością zwiększenia do 3 TB na żądanie NIL, w ramach ceny. Przestrzeń obejmuje materiały, dokumenty, nagrania i dane Platformy. Kopie zapasowe, środowisko testowe i logi nie pomniejszają tej puli.
Transfer danych	Co najmniej 5 TB wychodzącego transferu miesięcznie. Transfer przychodzący, wykonywanie kopii i migracja końcowa nie pomniejszają tego limitu. Transmisje live są zapewniane odrębnie zgodnie z FUN-06.
Webinary i nagrania	Dwa równoległe webinary po 250 uczestników/czek oraz do 40 godzin nowych nagrań miesięcznie, zgodnie z FUN-06.
Przechowywanie nagrań	Pojemność umożliwiająca przechowywanie każdego nagrania przez 12 miesięcy. NIL może ustawić krótszy okres retencji. Nagrania podlegają migracji końcowej, jeżeli ich okres retencji nie upłynął.
OCR	Do 500 dokumentów miesięcznie, każdy do 10 stron i 20 MB, zgodnie z FUN-20.
Analiza raportów przez AI	Do 1000 zapytań miesięcznie w FUN-23. Jedno zapytanie obejmuje polecenie użytkownika/czki i dane raportu o łącznej długości do 50 000 znaków ze spacjami oraz odpowiedź do 10 000 znaków. Techniczny podział przetwarzania na kilka wywołań nie zwiększa wykorzystania limitu.

Wykonawca monitoruje wykorzystanie zasobów i powiadamia NIL po osiągnięciu 70%, 85% i 95% każdego limitu. Zwiększenie przestrzeni w zakresie do 3 TB następuje przed jej wyczerpaniem, najpóźniej w ciągu 5 dni roboczych od zlecenia NIL. Zasoby niezbędne do spełnienia pozostałych

wymagań OPZ, w szczególności przechowywania nagrań, kopii i logów, zapewnia Wykonawca niezależnie od wskazanej minimalnej przestrzeni.

Przekroczenie limitu nie powoduje automatycznych dopłat ani usunięcia danych. Wykonawca przedstawia NIL prognozę wykorzystania i propozycję dalszego działania; rozszerzenie zakresu wymaga uprzedniego uzgodnienia na zasadach umowy. Niewykorzystane limity miesięczne nie przechodzą na kolejne miesiące.

Weryfikacja / odbiór: zestawienie przydzielonych zasobów i limitów, test zwiększenia przestrzeni, test progów alarmowych oraz potwierdzenie dostępności wymaganych limitów usług. Raport miesięczny zawiera wykorzystanie zasobów i prognozę ich wyczerpania. Testy wydajności i pojemności live przeprowadza się zgodnie z TECH-01 i FUN-06.

TECH-03 Środowiska

Wykonawca zapewnia środowisko testowe/odbiorowe odseparowane od produkcyjnego i aktualizuje je przed zmianami mającymi wpływ na integralność działania. Dane z produkcji w testach podlegają anonimizacji/pseudonimizacji. Środowisko testowe zawierające dane osobowe spełnia te same wymagania bezpieczeństwa co środowisko produkcyjne.

Weryfikacja / odbiór: Test wdrożenia na staging, regresji, backupu i kontrolowanego wdrożenia na produkcję; lista odseparowanych dostępów.

TECH-04 Dostępność i przeglądarki

Interfejs w języku polskim, obsługa polskich znaków i aktualnych wspieranych wersji Chrome, Edge, Firefox, Opera i Safari. Układ responsywny, bez wtyczek i bez wyłączania domyślnych zabezpieczeń przeglądarki.

Weryfikacja / odbiór: Lista urządzeń i przeglądarek testowych (w tym smartfon/tablet w przeglądarce); scenariusze kluczowych ekranów i formularzy.

Dostępność WWW musi obejmować interfejs udziału w zajęciach live oraz treści asynchroniczne; testy uwzględnią klawiaturę, dostępność czatu i materiałów do samokształcenia oraz możliwość korzystania z napisów/transkrypcji, jeśli mają zastosowanie i są wymagane dla dostarczonych treści.

TECH-05 Infrastruktura i licencjonowanie rdzenia

Rdzeń LMS może być oparty na otwartym kodzie źródłowym objętym uznaną bezpłatną licencją wolnego oprogramowania, np. GNU GPL, MIT lub Apache 2.0. Rozwiązanie jest kompletne, modularne i skalowalne; nowe moduły nie mogą zakłócać istniejących funkcji.

Weryfikacja i odbiór: Dokumentacja architektury i licencji, konfiguracja WAF/monitoringu, raport testu obciążenia i możliwość odtworzenia systemu poza środowiskiem Wykonawcy.

TECH-06 Publikacja, zgodność i utrzymanie aplikacji mobilnych

Aplikacje NIL będą dostępne w Google Play i Apple App Store, bez opłat dla uczestników/czek. Dopuszcza się produkt natywny, wieloplatformowy lub dostosowany, spełniający cały OPZ. Projekt F1 obejmie ścieżki, połączenie z LMS, macierz urządzeń i systemów, testy, publikację, aktualizacje i współdziałanie NIL. Wsparcie obejmie bieżącą oraz dwie poprzednie główne wersje Android i iOS nadal objęte aktualizacjami bezpieczeństwa producenta; macierz jest aktualizowana w utrzymaniu. Testy przeglądarkowe FUN-02 i TECH-04 nie zastępują testów aplikacji.

NIL jest właścicielem kont wydawcy i kontroluje wpisy, identyfikatory oraz publikację aktualizacji. Wykonawca przygotuje pakiety, opisy, grafiki, informacje o prywatności i deklaracje, obsłuży zgłoszenia oraz uwagi sklepów i opublikuje obie aplikacje do F5. NIL zapewni formalne potwierdzenia i upoważnienia wskazane z terminami w F1. Plan uwzględni recenzję sklepową, poprawki i ponowne zgłoszenia; wersja testowa ani samo zgłoszenie nie stanowią odbioru. Koszty kont, publikacji, komponentów i aktualizacji są objęte ceną.

7. Bezpieczeństwo, prywatność, dostępność cyfrowa

• Przetwarzanie danych zgodnie z RODO, na ustalonych podstawach i warunkach powierzenia przed dostępem do danych rzeczywistych.

• TLS/HTTPS, bezpieczne przechowywanie haseł, RBAC i MFA dla wszystkich kont zgodnie z INT-01 oraz autoryzacja, walidacja, limitowanie wywołań i rejestrowanie zdarzeń API.

• Ochrona aplikacyjna przed typowymi zagrożeniami OWASP Top 10, hardening, skan podatności, procedura incydentów, monitoring i aktualizacja komponentów.

• Szyfrowane kopie bezpieczeństwa i odseparowane uprawnienia backupowe; logi operacyjne z retencją zgodną z uzgodnioną polityką i zasadą minimalizacji.

• Interfejsy Platformy muszą spełniać co najmniej WCAG 2.1 na poziomie AA oraz standardy dostępności właściwe dla projektu FERS. Zgodność dotyczy rozwiązania dostarczanego i konfigurowanego dla NIL; podlega audytowi i retestom określonym w SEC-05 oraz rozdziale 10, a dla aplikacji mobilnych również TECH-06.

• Test dostępności obejmuje klawiaturę, czytnik ekranowy, kontrast, opis błędów formularzy, napisy/transkrypcje tam, gdzie dotyczą dostarczonych treści, i reprezentatywne ekrany LMS oraz katalogu wydarzeń.

SEC-01 Audyt i zarządzanie podatnościami

Przed uruchomieniem produkcyjnym Wykonawca zapewni, w ramach wynagrodzenia umownego, przeprowadzenie testów bezpieczeństwa przez niezależny podmiot zewnętrzny, nieuczestniczący w projektowaniu ani wytwarzaniu Platformy i posiadający udokumentowane doświadczenie w testowaniu bezpieczeństwa aplikacji internetowych.

Testy obejmą weryfikację wymagań OWASP ASVS 4.0.3 na poziomie 2 (L2), mających zastosowanie do Platformy, analizę podatności oraz testy penetracyjne aplikacji i jej interfejsów API. Zakres obejmie wszystkie role użytkowników/czek, panel administracyjny, mechanizmy uwierzytelniania i autoryzacji, zarządzanie sesjami, przesyłanie plików oraz zabezpieczenia danych. Wyłączenie wymagania jako niemającego zastosowania wymaga uzasadnienia w raporcie.

Wykonawca przekaże NIL raport zawierający zakres, metodykę i ograniczenia testów, wyniki weryfikacji wymagań oraz wykaz podatności wraz z klasyfikacją ryzyka, dowodami i zaleceniami naprawczymi.

Warunkiem uruchomienia produkcyjnego jest usunięcie podatności krytycznych i wysokich oraz potwierdzenie skuteczności poprawek przez podmiot przeprowadzający testy. Wyjątek wymaga wdrożenia środka kompensacyjnego, potwierdzenia jego skuteczności w ponownych testach oraz pisemnej akceptacji ryzyka przez NIL, określającej uzasadnienie, okres obowiązywania wyjątku i termin docelowego usunięcia podatności. Koszty poprawek i ponownych testów ponosi Wykonawca.

Weryfikacja / odbiór: Raport z niezależnych testów bezpieczeństwa, raport z ponownej weryfikacji wykrytych podatności oraz rejestr wyjątków zaakceptowanych przez NIL. Dokumentacja musi potwierdzać brak otwartych podatności krytycznych i wysokich poza wyjątkami spełniającymi powyższe warunki. Wymaganie dotyczy wykazania spełnienia określonych kryteriów bezpieczeństwa; nie stanowi gwarancji odporności na wszystkie możliwe ataki.

SEC-02 Kopie i odtworzenie

Wymagane są codzienne szyfrowane kopie danych i plików poza głównym środowiskiem oraz odseparowane uprawnienia. Rodzaj i częstotliwość kopii, dzienników transakcyjnych lub replikacji muszą spełniać CYB-08; minimum dobowe nie zastępuje RPO. Harmonogram i procedury podlegają dokumentowaniu i testom według CYB-08.

Weryfikacja / odbiór: rzeczywiste odtworzenie danych i aplikacji, pomiar RPO/RTO, potwierdzenie integralności i kompletności oraz dokumentacja procedury i retencji.

SEC-03 Incydenty i zgodność

Wykonawca zgłasza NIL incydenty bezpieczeństwa w terminach i na zasadach określonych w CYB-10. Naruszenia ochrony danych osobowych podlegają RODO-06. Zmiany wynikające z nowych przepisów podlegają analizie zakresu, terminów i odpowiedzialności na zasadach umowy.

Weryfikacja / odbiór: Plan komunikacji awaryjnej, rejestr zdarzeń, raport przyczynowy dla incydentu krytycznego i kontrola terminów działań naprawczych.

SEC-04 Logi i ochrona danych

Platforma rejestruje logowania, działania administracyjne, zmiany treści i dokumentów, operacje na danych osobowych oraz decyzje OCR. Logi są dostępne uprawnionym administratorom, zabezpieczone przed nieuprawnioną zmianą i przechowywane co najmniej 12 miesięcy (CYB-09). Nie zapisuje się w logach haseł ani zbędnych treści dokumentów.

System wspiera prawa osób zgodnie z RODO-11 i obowiązującą retencją. Dane i kopie są szyfrowane i chronione kontrolą dostępu. Naruszenia ochrony danych osobowych zgłasza się w terminach i na zasadach określonych w RODO-06.

Weryfikacja i odbiór: Test eksportu i korekty danych, retencji, ograniczenia dostępu, kompletności logów i próbnego zgłoszenia incydentu.

SEC-05 Dostępne kursy i egzaminy

Wymagane są zgodność z co najmniej WCAG 2.1 AA, współpraca z czytnikami ekranu, powiększenie tekstu i zmiana kontrastu. Platforma i dostarczane przez Wykonawcę materiały audio/wideo zapewnią wymagane napisy lub transkrypcje.

Egzaminy umożliwiają konfigurację alternatywnych form odpowiedzi, np. nagrania głosowego lub odpowiedzi pisemnej, i indywidualnego wydłużenia czasu. Wykonawca opracuje procedury równego dostępu. Podstawą odbioru są audyt i retesty rozwiązania po konfiguracji dla NIL zgodnie z rozdziałem 10; wcześniejsze raporty dotyczące produktu, jeżeli zostały przedstawione, ich nie zastępują. Informacje o dostosowaniach podlegają ochronie zgodnie z RODO-08.

Weryfikacja i odbiór: Audyt ścieżek logowania, nawigacji w kursie, quizu, przesyłania zadania i pobierania certyfikatu; test klawiaturą, czytnikiem oraz próbny egzamin z dostosowaniem.

8. Ochrona danych osobowych

Wymagania RODO-01–RODO-12 obowiązują we wszystkich fazach realizacji i utrzymania oraz uszczegóławiają rozdział 7. Umowa powierzenia zostanie zawarta przed udostępnieniem danych rzeczywistych.

RODO-01 Powierzenie przetwarzania danych

Wykonawca przetwarza dane osobowe wyłącznie jako podmiot przetwarzający, na podstawie umowy powierzenia zgodnej z art. 28 RODO, stanowiącej załącznik do umowy. Umowa powierzenia zostanie

zawarta przed udostępnieniem Wykonawcy jakichkolwiek danych rzeczywistych, w tym danych do migracji.

Jeżeli NIL przetwarza dane uczestników/czek projektu jako podmiot przetwarzający na podstawie umowy o dofinansowanie, Wykonawca działa jako dalszy podmiot przetwarzający i stosuje obowiązki wynikające z tej umowy w zakresie przekazanym przez NIL.

Weryfikacja / odbiór: podpisana umowa powierzenia przed dostępem do danych rzeczywistych w F0; potwierdzenie zgody instytucji właściwej, jeżeli jest wymagana. Do spełnienia tych warunków czynności w F0 mogą być wykonywane wyłącznie bez udostępniania Wykonawcy danych rzeczywistych. Weryfikacja obejmuje datę zawarcia umowy i nadania dostępów; wymóg dotyczy również każdego wcześniejszego udostępnienia danych koniecznego do rozpoczęcia prac.

RODO-02 Dalsze podmioty przetwarzające

Wykonawca, na etapie analizy i projektowania rozwiązania (F1), przedstawi Zamawiającemu wykaz planowanych dalszych podmiotów przetwarzających dane osobowe, w szczególności dostawców usług hostingu, poczty elektronicznej, transmisji live i wideokonferencji, OCR, AI, przechowywania i udostępniania materiałów wideo oraz obsługi zgłoszeń technicznych (help desk), o ile podmioty te będą przetwarzać dane osobowe w związku z realizacją zamówienia.

Wykaz będzie obejmował co najmniej nazwę podmiotu, zakres i cel przetwarzania danych oraz lokalizację ich przetwarzania.

Powierzenie przetwarzania danych osobowych dalszemu podmiotowi wymaga uprzedniej pisemnej zgody NIL, na zasadach określonych w umowie powierzenia przetwarzania danych osobowych. Wykonawca zobowiązany jest zgłosić planowane dodanie lub zmianę dalszego podmiotu przetwarzającego z co najmniej 14-dniowym wyprzedzeniem, umożliwiającym NIL weryfikację i podjęcie decyzji.

Wykonawca zapewni nałożenie na dalsze podmioty przetwarzające obowiązków ochrony danych osobowych nie mniej rygorystycznych niż obowiązki wynikające z umowy zawartej z NIL oraz ponosi odpowiedzialność za działania i zaniechania tych podmiotów w zakresie powierzonych im czynności.

Weryfikacja / odbiór: przedstawienie wykazu dalszych podmiotów przetwarzających w fazie F1, uzyskanie wymaganych zgód NIL przed rozpoczęciem przetwarzania danych oraz aktualizacja wykazu przy każdym odbiorze i w raportach kwartalnych.

RODO-03 Lokalizacja danych i przekazywanie poza EOG

Dane osobowe, w tym kopie zapasowe, logi, nagrania i dane OCR/AI, są przechowywane i przetwarzane w EOG. Dostęp administracyjny do infrastruktury i baz danych odbywa się wyłącznie z EOG, zgodnie z CYB-05.

Wyjątek od przetwarzania w EOG wymaga uprzedniej pisemnej zgody NIL, mechanizmu z rozdziału V RODO i oceny skutków transferu. Nie obejmuje dostępu administracyjnego (CYB-05), hostingu (pkt 6.2), modeli AI (AI-01) ani usługi live i jej nagrań (FUN-06, RODO-10), dla których EOG jest obowiązkowe. Osadzane odtwarzacze i pozostałe integracje wymagają wskazania przekazywanych danych i ich minimalizacji.

Weryfikacja / odbiór: oświadczenie o lokalizacji centrów danych; mapa przepływów danych w projekcie technicznym (F1).

RODO-04 Ocena skutków dla ochrony danych

Wykonawca przekaże NIL w fazie F1 informacje niezbędne do przeprowadzenia oceny skutków dla ochrony danych (art. 35 RODO): opis operacji przetwarzania, przepływów danych, środków

bezpieczeństwa, modułów OCR/AI i podmiotów trzecich. Wykonawca uwzględni w projekcie środki wynikające z oceny. Uruchomienie modułów FUN-20 i FUN-23 na danych rzeczywistych następuje po zatwierdzeniu oceny przez NIL.

Weryfikacja / odbiór: dokumentacja wejściowa do oceny skutków zaakceptowana przez Inspektora Ochrony Danych NIL; lista środków z oceny powiązana z wymaganiami.

RODO-05 Decyzje automatyczne w module dokumentów

Automatyczna akceptacja w FUN-20 jest dopuszczalna wyłącznie przez wykonanie reguł i progów zatwierdzonych oraz skonfigurowanych przez NIL. Wynik AI nie jest samodzielną podstawą decyzji o uprawnieniu uczestnika/czki

. Wynik niepewny, odrzucenie, zwrot lub uznanie nieważności wymagają weryfikacji przez osobę uprawnioną przed wywołaniem negatywnego skutku dla uczestnika/czki.

Uczestnik/czka jest informowany o wykorzystaniu automatycznego odczytu i może zażądać rozpatrzenia dokumentu przez człowieka. System zapisuje podstawę decyzji, poziom pewności i osobę weryfikującą.

Weryfikacja / odbiór: test, w którym dokument niespełniający kryteriów trafia do kolejki ręcznej, a nie jest odrzucony automatycznie; test żądania weryfikacji przez człowieka.

RODO-06 Naruszenia ochrony danych

Wykonawca zgłasza NIL każde stwierdzone lub podejrzewane naruszenie ochrony danych osobowych bez zbędnej zwłoki, nie później niż w ciągu 24 godzin od jego wykrycia, na wskazane adresy Inspektora Ochrony Danych i administratora bezpieczeństwa NIL. Zgłoszenie zawiera co najmniej informacje z art. 33 ust. 3 RODO; informacje niedostępne w chwili zgłoszenia Wykonawca uzupełnia niezwłocznie.

Wykonawca wspiera NIL w zgłoszeniu do Prezesa UODO i zawiadomieniu osób, których dane dotyczą, oraz prowadzi rejestr naruszeń.

Weryfikacja / odbiór: procedura zgłaszania naruszeń w dokumentacji; ćwiczenie próbnego zgłoszenia przed uruchomieniem i co 12 miesięcy.

RODO-07 Retencja, usuwanie i zwrot danych

Platforma umożliwia konfigurację okresów przechowywania dla poszczególnych kategorii danych (konta nieaktywne, dokumenty z FUN-20, nagrania, logi, ankiety, dane migracyjne) oraz automatyczne usunięcie lub anonimizację po ich upływie, z zachowaniem dowodów uczestnictwa wymaganych w projekcie FERS.

Po przekazaniu danych w planie wyjścia i zakończeniu ich przetwarzania na danym środowisku Wykonawca, na polecenie NIL, usuwa je także u dalszych podmiotów i potwierdza to pisemnie. Wyłączenie źródła podlega pkt 6.7 i nie przerywa utrzymania do daty z pkt 12.1. Kopie usuwa się po cyklu retencji, najpóźniej 90 dni od zakończenia danego przetwarzania i przekazania. Gwarancja nie uzasadnia zachowania danych produkcyjnych. Dostęp do konkretnej naprawy NIL nadaje ponownie w niezbędnym zakresie według RODO-01; po naprawie obowiązuje ten sam zwrot lub usunięcie.

Weryfikacja / odbiór: test reguł retencji na danych testowych oraz protokół zwrotu lub usunięcia danych po zakończeniu danego przetwarzania, z wykazem środowisk i dalszych podmiotów oraz terminem wygaśnięcia kopii. Dla F8 protokół wskazuje również dane niezbędne do pozostałych czynności utrzymania i termin ich usunięcia; samo dalsze obowiązywanie gwarancji nie odracza tego terminu.

RODO-08 Ochrona danych w fazie projektowania i domyślna ochrona

Domyślne ustawienia platformy zapewniają minimalny zakres przetwarzania i widoczności danych: profile, listy uczestników/czek, wpisy na forum i obecności są widoczne wyłącznie dla ról, które tego potrzebują. Formularze zbierają wyłącznie pola zatwierdzone przez NIL.

Informacje o dostosowaniach egzaminów i potrzebach związanych z niepełnosprawnością są przechowywane oddzielnie, dostępne wyłącznie dla wskazanych ról i nie trafiają do raportów ogólnych ani eksportów.

Weryfikacja / odbiór: przegląd ustawień domyślnych z Inspektorem Ochrony Danych NIL; test dostępu do danych o dostosowaniach z ról nieuprawnionych.

RODO-09 Informacje dla użytkowników, użytkowniczek i pliki cookies

Platforma umożliwia publikację i wersjonowanie klauzul informacyjnych (art. 13 i 14 RODO), regulaminu i polityki prywatności przygotowanych przez NIL oraz ich prezentację w miejscu zbierania danych.

Pliki cookies i podobne technologie inne niż niezbędne są stosowane wyłącznie po uzyskaniu zgody użytkownika/czki, za pomocą mechanizmu umożliwiającego jej wycofanie. Wykonawca dostarczy wykaz stosowanych plików cookies i narzędzi analitycznych oraz informacje potrzebne NIL do przygotowania dokumentów.

Weryfikacja / odbiór: test banera zgody (odmowa, zgoda, wycofanie); wykaz plików cookies w dokumentacji.

RODO-10 Nagrania zajęć live

Nagrywanie zajęć jest domyślnie wyłączone. Przed rozpoczęciem nagrania platforma informuje uczestników/czki i prowadzących w sposób widoczny oraz umożliwia udział bez włączonej kamery i mikrofonu. Nagrania są przechowywane w EOG, dostępne zgodnie z uprawnieniami i usuwane po okresie ustalonym przez NIL.

Weryfikacja / odbiór: test komunikatu o nagraniu, uprawnień i reguły usunięcia.

RODO-11 Realizacja praw osób

Platforma umożliwia administratorowi NIL realizację praw z art. 15–21 RODO, w tym eksport danych osoby w formacie ustrukturyzowanym i nadającym się do odczytu maszynowego, sprostowanie, ograniczenie i usunięcie, z uwzględnieniem obowiązków retencji. Wykonawca wykonuje czynności techniczne, których nie można wykonać z panelu, w ciągu 5 dni roboczych od zlecenia NIL.

Weryfikacja / odbiór: test eksportu, sprostowania, ograniczenia i usunięcia danych przykładowej osoby.

RODO-12 Rejestr i audyt

Wykonawca prowadzi rejestr kategorii czynności przetwarzania (art. 30 ust. 2 RODO) i udostępnia go NIL na żądanie. NIL lub upoważniony audytor może przeprowadzić audyt przetwarzania danych i bezpieczeństwa, w tym u dalszych podmiotów przetwarzających, po zawiadomieniu z 10-dniowym wyprzedzeniem, a w przypadku naruszenia – bez wyprzedzenia. Wykonawca usuwa stwierdzone niezgodności w uzgodnionym terminie.

Weryfikacja / odbiór: udostępnienie rejestru przy odbiorze uruchomienia; plan działań po audycie.

9. Cyberbezpieczeństwo

Wymagania CYB-01–CYB-12 obowiązują we wszystkich fazach realizacji i utrzymania oraz uszczegóławiają rozdział 7 i SEC-01–SEC-04. Stosuje się je niezależnie od statusu NIL na gruncie

ustawy o krajowym systemie cyberbezpieczeństwa; jeżeli obowiązki ustawowe mają zastosowanie, Wykonawca wspiera NIL w ich realizacji.

CYB-01 Weryfikacja bezpieczeństwa aplikacji i testy penetracyjne

Platforma, w tym moduł live, API i integracje, spełnia wymagania OWASP ASVS 4.0.3 na poziomie 2. Niezależny podmiot zewnętrzny spełniający warunki SEC-01 przeprowadzi test penetracyjny aplikacji i infrastruktury: przed uruchomieniem produkcyjnym w F5 dla całego zakresu startowego, przed uruchomieniem integracji odroczonych do F6 dla nowych interfejsów i zmienionych mechanizmów zgodnie z pkt 10.2, następnie co 12 miesięcy oraz po każdej istotnej zmianie architektury lub aktualizacji wersji głównej. Zakres i metodykę testu (np. OWASP WSTG, PTES) zatwierdza NIL. Retesty są wykonywane na koszt Wykonawcy. Przed każdym z tych uruchomień obowiązują warunki usunięcia podatności i dopuszczania wyjątków z SEC-01.

Weryfikacja / odbiór: raport z testu i retestu z klasyfikacją CVSS; usunięcie podatności krytycznych i wysokich, z wyjątkami dopuszczonymi wyłącznie na warunkach SEC-01.

CYB-02 Zarządzanie podatnościami

Wykonawca monitoruje podatności wszystkich komponentów: systemu operacyjnego, bazy, rdzenia LMS, wtyczek, bibliotek i usług zewnętrznych. Od wykrycia podatności obowiązują terminy: krytyczne (CVSS ≥ 9,0) — usunięcie do 72 godzin i ograniczenie ryzyka do 24 godzin; wysokie — do 14 dni; średnie — do 60 dni; niskie — w planowanej aktualizacji. Brak poprawki producenta nie zwalnia z ograniczenia ryzyka; Wykonawca wdraża środek kompensacyjny i przedstawia NIL plan usunięcia, a odstępstwo od terminu wymaga udokumentowanej akceptacji NIL.

Aktywnie wykorzystywaną podatność należy obsługiwać jak krytyczną. Skan podatności infrastruktury i aplikacji wykonuje się co najmniej raz w miesiącu.

Weryfikacja / odbiór: rejestr podatności z datami wykrycia i usunięcia w raporcie miesięcznym.

CYB-03 Bezpieczny proces wytwórczy

Kod dedykowany dla NIL jest wytwarzany zgodnie z udokumentowanym bezpiecznym cyklem wytwórczym: przegląd kodu, statyczna analiza kodu (SAST), skanowanie zależności (SCA), dynamiczne testy bezpieczeństwa (DAST) przed wdrożeniem na produkcję, zarządzanie sekretami poza repozytorium. Wykonawca przekazuje i aktualizuje wykaz komponentów oprogramowania (SBOM) w formacie CycloneDX lub SPDX.

Weryfikacja / odbiór: opis procesu w projekcie technicznym; SBOM przy każdym odbiorze i po aktualizacji wersji.

CYB-04 Bezpieczeństwo organizacji Wykonawcy i łańcucha dostaw

Zarządzanie bezpieczeństwem usług centrum danych i hostingu wykazuje się ważnym certyfikatem ISO/IEC 27001 dostawcy lub operatora centrum danych, którego zakres obejmuje infrastrukturę i usługi wykorzystywane dla NIL. Sam certyfikat organizacji, nieobejmujący tych usług, nie wystarcza. Równoważność wymaga udokumentowanego systemu zarządzania bezpieczeństwem obejmującego ten sam zakres: ocenę ryzyka, polityki i odpowiedzialności, kontrole bezpieczeństwa fizycznego i operacyjnego, zarządzanie dostępem, dostawcami, incydentami i ciągłością, audyty oraz działania korygujące. Wykonawca przedstawi niezależne potwierdzenie stosowania tych środków i mapowanie do wymagań ISO/IEC 27001; samo oświadczenie nie stanowi dowodu równoważności.

Wykonawca stosuje wobec podwykonawców i dostawców usług wymagania bezpieczeństwa nie niższe niż określone w OPZ i na żądanie NIL przedstawia dowody ich spełnienia. Wykonawca wspiera NIL w realizacji obowiązków wynikających z ustawy o krajowym systemie cyberbezpieczeństwa, jeżeli mają zastosowanie, w tym w szacowaniu ryzyka i audycie.

Przy odbiorze hostingu należy potwierdzić ważność dowodów i objęcie nimi rzeczywistej infrastruktury i usług NIL.

CYB-05 Kontrola dostępu

Dostęp administracyjny do infrastruktury i bazy danych odbywa się wyłącznie z imiennych kont, z uwierzytelnianiem wieloskładnikowym i wyłącznie z terytorium EOG.

MFA jest obowiązkowe dla wszystkich kont Platformy zgodnie z INT-01. Platforma zapewnia ochronę logowania (blokadę lub opóźnienie, wykrywanie wykradzionych haseł) i bezpieczne zarządzanie sesją. Wykonawca przegląda uprawnienia personelu co kwartał i odbiera je niezwłocznie po zakończeniu udziału osoby w usłudze.

Weryfikacja / odbiór: test uwierzytelniania wieloskładnikowego dla ról; lista osób z dostępem uprzywilejowanym w raporcie kwartalnym.

CYB-06 Bezpieczeństwo przesyłanych plików i treści

Każdy plik przesyłany do platformy (dokumenty z FUN-20, materiały bazy wiedzy, zadania, pakiety SCORM/H5P) jest weryfikowany pod kątem typu, rozmiaru i złośliwego oprogramowania przed udostępnieniem. Treści interaktywne (SCORM, H5P) są serwowane w sposób ograniczający dostęp skryptów do sesji użytkownika/czki, np. z odrębnej domeny lub w izolowanej ramce. Platforma stosuje nagłówki bezpieczeństwa, w tym Content Security Policy i HSTS.

Weryfikacja / odbiór: test przesłania pliku testowego EICAR i pliku o niedozwolonym typie; skan nagłówków bezpieczeństwa.

CYB-07 Szyfrowanie

Dane w bazie, repozytorium plików, nagraniach i kopiach zapasowych są szyfrowane algorytmem co najmniej AES-256 lub równoważnym. Transmisja odbywa się wyłącznie z użyciem TLS 1.2 lub nowszego, z wyłączeniem słabych szyfrów. Klucze kryptograficzne są przechowywane oddzielnie od danych, z kontrolą dostępu i procedurą rotacji.

Weryfikacja / odbiór: opis szyfrowania i zarządzania kluczami w dokumentacji; test konfiguracji TLS.

CYB-08 Kopie zapasowe i ciągłość działania

Kopie spełniają regułę 3-2-1, w tym kopię niezmienialną/offline w fizycznie odrębnej lokalizacji w EOG. RPO: ≤ 4 h dla awarii i ≤ 24 h dla katastrofy centrum danych. RTO wynosi ≤ 6 godzin zegarowych dla zwykłej awarii oraz ≤ 24 godziny zegarowe przy utracie głównego centrum danych wymagającej odtworzenia w środowisku zapasowym. RTO liczy się od zakłócenia do zweryfikowanego odtworzenia produkcji i dotkniętych funkcji kluczowych (pkt 12.4), z bezpieczeństwem i integralnością danych. RPO określa wiek punktu odtworzenia, nie przestój. Odtwarzanie działa 24/7; opóźnienie wykrycia, decyzji lub przełączenia nie przesuwa RTO. Architektura, kopie i zasoby zapasowe zapewnią te parametry. Dla katastrofy stosuje się odrębny termin P1 z tabeli w pkt 12.3, bez wyłączenia przestoju z SLA. RPO/RTO, pkt 12.3 i 12.4 obowiązują łącznie; dotrzymanie RTO 24 h nie oznacza dotrzymania miesięcznej dostępności 99%.

Wykonawca opracuje i utrzymuje plan ciągłości działania i odtwarzania po awarii; test odtworzenia wykonuje przed uruchomieniem i co 6 miesięcy, a test planu odtwarzania po awarii – co 12 miesięcy.

Odbiór: plan odtwarzania zatwierdzony przez NIL i raport potwierdzający RPO/RTO oraz procesy kluczowe. Przed startem testuje się awarię i symulowaną utratę centrum danych; później według częstotliwości powyżej. Raport podaje czasy zakłócenia, wykrycia, działań i przywrócenia, punkt danych oraz wyniki weryfikacji funkcji.

CYB-09 Rejestrowanie zdarzeń

Logi bezpieczeństwa (logowania, błędy uwierzytelnienia, zmiany uprawnień, operacje administracyjne, dostęp do danych osobowych, eksporty, zdarzenia WAF) są przechowywane przez co najmniej 12 miesięcy, zabezpieczone przed modyfikacją i opatrzone zsynchronizowanym czasem. Wykonawca zapewni eksport logów w standardowym formacie (np. syslog lub przez API).

Weryfikacja / odbiór: test kompletności logów dla wybranych zdarzeń; test eksportu logów.

CYB-10 Obsługa incydentów bezpieczeństwa

Wykonawca zgłasza NIL incydent bezpieczeństwa wpływający lub mogący wpłynąć na poufność, integralność lub dostępność platformy: wstępnie w ciągu 4 godzin od wykrycia (24/7), z raportem zawierającym ocenę skutków w ciągu 24 godzin i raportem końcowym z analizą przyczyn w ciągu 30 dni.

Wykonawca zabezpiecza dowody, współpracuje z NIL i właściwym zespołem CSIRT oraz wdraża działania naprawcze. Obowiązek ten nie zastępuje RODO-06.

Weryfikacja / odbiór: procedura obsługi incydentów z kontaktami 24/7; ćwiczenie próbne przed uruchomieniem.

CYB-11 Domena i poczta

Platforma działa w domenie NIL. Domena, rekordy DNS i certyfikaty pozostają pod kontrolą NIL lub są jej przekazywane na każde żądanie. Wiadomości wysyłane z platformy są uwierzytelnione SPF, DKIM i DMARC w polityce uzgodnionej z NIL.

Weryfikacja / odbiór: test nagłówków wiadomości; potwierdzenie własności domeny.

CYB-12 Raportowanie bezpieczeństwa

Wykonawca dołącza do raportu miesięcznego część dotyczącą bezpieczeństwa: wykryte i usunięte podatności, wdrożone poprawki, incydenty, zdarzenia WAF/DDoS, wyniki testów kopii i zmiany dostępów.

Weryfikacja / odbiór: raport miesięczny zaakceptowany przez NIL.

10. Testy odbiorowe i zasady akceptacji

10.1. Macierz odbiorowa obejmuje wszystkie wymagania OPZ. Każdy jej wpis wskazuje identyfikator wymagania, a dla postanowień bez osobnego identyfikatora — numer punktu lub rozdziału z jednoznacznym opisem wymagania, oraz scenariusz, dane testowe, wynik, dowód i status: zaliczony albo niezaliczony. Wpis określa również właściwy etap odbioru, tak aby wymagania F5, F6 i F8 oraz czynności okresowe nie były mylone. Wyjątek wymaga wyraźnej podstawy w OPZ lub umowie i pisemnej decyzji NIL; nie może służyć pominięciu wymagania minimalnego. Scenariusze użytkownika/czki opracowane w F1 uszczegóławiają weryfikację, nie zmieniając zakresu zamówienia.

10.2. F5 wymaga zaliczenia testów funkcji i ról, kont/MFA, usług startowych, rzeczywistych paczek SCORM, wydajności, niezależnego pentestu, WCAG, RPO/RTO i regresji; ścieżki zapis–certyfikat i trybu przejściowego; pełnej kopii, retencji i ćwiczeń naruszeń/incydentów. Wymagane są właściwe dowody RODO-01–RODO-12 i CYB-01–CYB-12. F6 obejmuje testy INT-07, w tym awarie CRL, oraz uzupełnienie oceny ochrony danych, bezpieczeństwa, dostępności i wydajności. Niezależne testy i retesty obejmą nowe interfejsy oraz zmienione uwierzytelnianie i autoryzację tych interfejsów; nie obejmuje to wyłączonych w INT-01 i INT-08 integracji tożsamości. Poprawki i retesty obowiązują zgodnie z OPZ. F8 testuje się według pkt 6.7.

10.3. Wady odbiorowe dzieli się na: A — blokujące uruchomienie lub naruszające bezpieczeństwo albo integralność danych; B — istotnie ograniczające proces, z dostępnym obejściem; C — niekrytyczne. Odbiór wymaga braku wad A; wady B i C wymagają pisemnego planu usunięcia i decyzji NIL. Dla podatności bezpieczeństwa stosuje się szczególne warunki SEC-01, w tym dopuszczone tam środki kompensacyjne. Klasy A/B/C stosuje się do odbiorów, w tym zmian rozwojowych z pkt 12.9; priorytety P1–P4 z pkt 12.3 służą obsłudze zgłoszeń w utrzymaniu oraz wad gwarancyjnych na zasadach pkt 12.8.2. Klasyfikacja odbiorowa nie zastępuje priorytetu zgłoszenia ani odwrotnie.

10.4. Odbiór F5 wymaga spełnienia testów z pkt 10.2, dokumentacji startowej według DOK-08, uprawnień administracyjnych, procedury wycofania, szablonów certyfikatów i danych do utrzymania. F6 wymaga odbioru integracji według INT-07, aktualnej dokumentacji i instruktażu oraz procedury powrotu. Obowiązuje pkt 10.3; F5 nie stanowi odbioru integracji odroczonych. F8 podlega pkt 6.7.

Dowód odbioru	Wymagany produkt
Ścieżki użytkowników/czek	Zapis na wydarzenie → udział/SCORM → test/ankieta → punkty → dwa wzory certyfikatu.
Integracje	Raport i podpisany protokół zgodnie z INT-07: usługi startowe w F5, integracje odroczone w F6.
Migracja końcowa (F8)	Dla migracji końcowej w F8: rejestr źródeł i celów, zgodność ilościowa, wyjątki, podpisany raport dry-run i cut-over zgodnie z pkt 6.7.
Bezpieczeństwo/WCAG	Raporty, retesty i zamknięcie niezgodności; wyjątki wyłącznie na zasadach SEC-01 i pkt 10.3. Weryfikacja RODO-01–RODO-12 i CYB-01–CYB-12: umowa powierzenia, wykaz podmiotów, mapa przepływów, ocena skutków dla FUN-20/FUN-23, testy retencji, praw osób, cookies, nagrań i ręcznej weryfikacji OCR, procedury naruszeń, SBOM i plan odtworzenia.
Wydajność	Profil testu 1000 sesji, metryki p95 i błędów, zasoby, wyniki testu szczytowego.
Dokumentacja i szkolenia	Aktualne instrukcje w języku polskim, materiały redaktora i administratora; protokoły warsztatów.

10.5. Wykonawca przeprowadzi pilotaż obejmujący reprezentatywne role i formy szkoleń, zbierze informacje zwrotne i usunie uzgodnione błędy przed uruchomieniem. Raport pilotażu zawiera scenariusze, uczestniczące role, wyniki, listę problemów, decyzje i retesty. Scenariusze UAT muszą objąć także FUN-20–23, zarządzanie salami, strukturę organizacyjną, bazę wiedzy, automatyczne wiadomości i progi zaliczenia wideo.

10.6. Odbiór F4/F5 wymaga osobnych raportów Android i iOS, identyfikujących aplikację, LMS, wersje systemów, urządzenia, scenariusze FUN-24, dowody, wyniki i retesty. Testy obejmują wszystkie systemy z macierzy TECH-06 na rzeczywistych urządzeniach; emulatory ich nie zastępują. Wymagane są audyt dostępności i niezależne testy bezpieczeństwa wraz z retestami według TECH-06 i SEC-01. Regresja F6 obejmuje aplikacje, zwłaszcza logowanie, uprawnienia i punkty. Obowiązuje pkt 10.3. Odbiór WWW nie zastępuje raportów aplikacji ani ich produkcyjnej publikacji do F5.

11. Instruktaż i przekazanie wiedzy

11.1. Wykonawca przeprowadzi min. 30 godzin szkoleniowych (30 x 45 minut) dla administratorów i redaktorów, w tym do 8 godzin stacjonarnie. Zakres obejmie administrację techniczną, merytoryczną, raportowanie i tworzenie kursów oraz wydarzeń.

11.2. Program obejmuje użytkowników/czki, strukturę, kursy, kategorie, bazę wiedzy, edytory treści, SCORM, live/hybrydę, sale, OCR i dokumenty, testy, certyfikaty, raporty, dostępność, integracje, kopie i eskalację incydentów. Wykonawca dostarczy podręczniki, instrukcje, procedury i materiały szybkiego startu oraz zweryfikuje umiejętności i przeprowadzi certyfikację uczestników/czek szkolenia na zasadach pkt 11.3.

11.3. Odbiór: program i ewidencja 30 godzin, listy obecności, materiały w języku polskim, wykonane zadania praktyczne, wyniki weryfikacji umiejętności i potwierdzenia ukończenia. Certyfikacja dotyczy szkolenia z obsługi systemu i nie jest deklaracją zewnętrznej akredytacji. Działania komunikacyjne i przygotowanie do ról należy udokumentować zgodnie z pkt 2.3.

12. Utrzymanie i wsparcie po wdrożeniu

12.1. Utrzymanie trwa nieprzerwanie od odbioru uruchomienia produkcyjnego w F5 do 30 czerwca 2029 r. włącznie.

Pierwsze 30 dni utrzymania stanowi stabilizację: monitoring, obsługę zgłoszeń i usuwanie błędów zgodnie z SLA.

12.2. Utrzymanie obejmuje hosting zgodnie z pkt 6.2, LMS, moduł live i integracje, monitoring, kopie, aktualizacje, naprawę wad, administrację, wsparcie użytkowników/czek i raporty SLA. Po migracji końcowej obowiązki utrzymaniowe Wykonawcy trwają do daty z pkt 12.1. NIL lub wskazany dostawca udostępnia środowisko docelowe spełniające udokumentowane wymagania rozwiązania i uzgodnione dostępy; Wykonawca odpowiada za przeniesienie, konfigurację oraz ciągłość obsługi Platformy w tym środowisku do końca utrzymania. Plan F8 wskazuje wykonawców czynności infrastrukturalnych, kopii, monitoringu, aktualizacji i reagowania na awarie, kanały eskalacji oraz sposób weryfikacji parametrów SLA, RPO i RTO. Podział czynności nie może pozostawiać luk w utrzymaniu ani automatycznie znosić zobowiązań Wykonawcy. Rozwój poza zakresem OPZ nie zastępuje obowiązku usuwania wad.

Utrzymanie do 30 czerwca 2029 r., także po migracji, obejmuje obie aplikacje i połączenie z LMS (TECH-06). Ich kluczowe funkcje na obsługiwanych systemach podlegają monitoringowi, D i priorytetom P1–P4; dostęp do WWW nie oznacza automatycznie naprawy kanału mobilnego. W F8 należy potwierdzić działanie aplikacji ze środowiskiem docelowym i przekazać konfigurację, kontrolę publikacji oraz materiały do aktualizacji zgodnie z rozdziałem 13.

12.3. Wsparcie I i II linii obejmuje e-mail i telefon dla administratorów oraz help desk z e-mailem i infolinią z poczekalnią dla użytkowników/czek. Rejestracja zgłoszeń i alarmów działa całodobowo; P1 jest obsługiwany 24/7/365 w godzinach zegarowych. P2–P4 rozlicza się w godzinach obsługi: poniedziałek–piątek, 8:00–16:00 czasu polskiego, z wyłączeniem świąt ustawowych w Polsce. Rejestr zawiera numer, kategorię, status i historię czasów. Reakcja oznacza rozpoczęcie diagnozy przez właściwą osobę i pierwszą merytoryczną odpowiedź e-mail z priorytetem i działaniami; automat nie wystarcza. Termin reakcji i termin rezultatu z tabeli biegną równolegle od wcześniejszego wykrycia przez monitoring lub otrzymania zgłoszenia; dla P2–P4 wyłącznie w oknie obsługi. Dla P1 i P3 przywrócenie oznacza zweryfikowane działanie procesu lub bezpieczne obejście zachowujące rezultat, uprawnienia i integralność danych, nie samą instrukcję, częściową naprawę ani start serwera. Dla P2 wymagane jest usunięcie istotnego ograniczenia i przywrócenie pełnego działania dotkniętej funkcji; istniejące obejście nie kończy tego terminu. Dla P4 obowiązuje rezultat wskazany w tabeli. Jeżeli zastosowano obejście, przyczynę należy usunąć według planu zaakceptowanego

przez NIL. Priorytet wynika z wpływu; spór, zmiana priorytetu ani ponowna rejestracja nie zerują czasu. Po zmianie priorytetu stosuje się właściwy termin liczony od pierwotnego początku zgłoszenia.

Klasa	**Przykład**	Reakcja i pierwsza odpowiedź	Wymagany rezultat i termin
P1 krytyczna	Platforma niedostępna; brak logowania dla wszystkich; utrata integralności danych; niedostępność funkcji kluczowej określonej w pkt 12.4 bez skutecznego, bezpiecznego obejścia, uniemożliwiająca realizację danego procesu przez grupę uprawnionych użytkowników/czek.	≤ 1 godzina zegarowa; obsługa 24/7/365	Przywrócenie lub bezpieczne obejście: ≤ 6 godzin zegarowych; przy utracie głównego centrum danych: ≤ 24 godziny zegarowe zgodnie z CYB-08.
P2 wysoka	Istotne ograniczenie procesu dla grupy użytkowników/czek, z bezpiecznym obejściem pozwalającym osiągnąć wymagany rezultat; bez przesłanek P1. Niedostępność funkcji kluczowej bez takiego obejścia jest P1, nie P2.	≤ 4 godziny obsługi	Usunięcie istotnego ograniczenia i przywrócenie pełnego działania dotkniętej funkcji: ≤ 24 godziny obsługi (3 dni robocze po 8 godzin). Samo istniejące obejście nie spełnia tego rezultatu.
P3 średnia	Problem pojedynczej funkcji o ograniczonym wpływie, przy dostępnej bezpiecznej alternatywie; bez przesłanek P1 i P2.	≤ 3 godziny obsługi	≤ 40 godzin obsługi
P4 niska	Błąd kosmetyczny, pytanie, sugestia	≤ 3 godziny obsługi	Błąd: usunięcie ≤ 160 godzin obsługi. Pytanie lub sugestia: pełna odpowiedź lub ocena ≤ 8 godzin obsługi; wdrożenie zmiany poza OPZ wymaga odrębnego zatwierdzenia.

12.4. Dostępność wynosi ≥ 99% miesięcznie, 24/7. SLA = 100% × (T − D) / T: T to minuty świadczenia usługi w miesiącu, także niepełnym, a D — łączny czas niedostępności co najmniej jednej funkcji kluczowej, bez wielokrotnego liczenia nakładających się przerw. Limit D wynosi 1% T, czyli 432 minuty (7 h 12 min) w pełnym miesiącu 30-dniowym. Dostępność, terminy P1–P4 i RPO/RTO obowiązują łącznie; spełnienie jednego nie zastępuje pozostałych ani nie wyłącza przerwy z D. Wyczerpanie limitu nie zwalnia z przywracania. Prace planowe, migracja, awarie i katastrofa centrum danych nie podlegają automatycznemu wyłączeniu z pomiaru.

Funkcje kluczowe: logowanie/MFA i autoryzowany dostęp; katalog i zapisy; materiały/SCORM ze wznowieniem i zapisem postępu; testy/egzaminy, wyniki i ukończenia; prowadzenie i udział w zaplanowanym live z obecnością; należne certyfikaty, lokalne punkty i historia; przesyłanie i ocena wymaganych dokumentów. Ręczna ocena zastępuje OCR/AI tylko przy rzeczywistej obsłudze w wymaganym terminie. Pomiar obejmuje zakres produkcyjny od F5, a od F6 także integracje warunkujące te procesy. Niedostępność to techniczna niemożność bezpiecznego wykonania procesu, także dla grupy uprawnionych osób; nie obejmuje prawidłowej odmowy uprawnień ani błędu urządzenia lub łącza pojedynczego użytkownika/czki. Tryb przejściowy lub obejście musi zapewnić wymagany rezultat; przerwa kończy się po weryfikacji działania, nie po zmianie priorytetu.

Monitoring 24/7/365 sprawdza reprezentatywne procesy, nie tylko serwer: funkcje stałe co najwyżej co 5 minut, live dodatkowo podczas zajęć. NIL ma dostęp do wyników i historii. W F1 Wykonawca określi scenariusze, konta, zewnętrzne punkty pomiaru i weryfikację alarmów; konfigurację sprawdza się przed F5 i aktualizuje przed integracjami F6 bez zawężania zakresu SLA. Pomiar opiera się na monitoringu, logach i zgłoszeniach: od najwcześniej udokumentowanego początku do zweryfikowanego przywrócenia. Brak pomiaru nie dowodzi dostępności; udokumentowane zgłoszenia NIL uwzględnia się w raporcie. Raport miesięczny zawiera T, D, SLA, chronologię przerw z funkcjami i dowodami, czasy P1–P4 i każde przekroczenie osobno.

12.5. Wykonawca ogranicza ryzyko podatności krytycznych, wdraża poprawki i raportuje postęp zgodnie z terminami CYB-02. Brak poprawki producenta wymaga środka kompensacyjnego i planu naprawy. Aktualizacje przechodzą testy regresji kursów i integracji.

Terminy usuwania i ograniczania ryzyka podatności z CYB-02 nie zastępują terminów obsługi zdarzeń z pkt 12.3. Jeżeli podatność powoduje awarię lub niedostępność funkcji, stosuje się równolegle właściwy priorytet P1–P4 i odpowiadający mu czas przywrócenia oraz wymagania pkt 12.4 i CYB-08, gdy mają zastosowanie. Terminy zawiadomień i raportów z CYB-10 oraz RODO-06 są odrębnymi obowiązkami i nie wydłużają czasu reakcji ani przywrócenia.

12.6. Prace rozwojowe podlegają pkt 12.9.1–12.9.6.

12.7. Monitoring działa 24/7/365; skany i testy podlegają CYB-01–CYB-02, a audyty RODO-12. Co najmniej raz na 6 miesięcy Wykonawca przegląda i wdraża dostępne, wspierane aktualizacje wersji istniejących komponentów, po testach regresji. Jeśli aktualizacji nie wydano, dokumentuje przegląd i potwierdza wsparcie wersji. Nie jest to obowiązek tworzenia nowych funkcji dedykowanych, rozliczanych według pkt 12.9. Aktualizacje bezpieczeństwa zachowują krótsze terminy CYB-02. Raport miesięczny obejmuje SLA, pojemność, integracje, live, bezpieczeństwo (CYB-12), działania naprawcze i rozliczenie rozwoju (pkt 12.9.6).

12.8. Gwarancja obejmuje odebrane produkty od odbioru, przez utrzymanie i 12 miesięcy po jego zakończeniu — do 30 czerwca 2030 r. włącznie. Migracja F8 ani przekazanie innemu dostawcy jej nie ograniczają. Pełne warunki określają pkt 12.8.1–12.8.3; gwarancja jest odrębna od utrzymania.

12.8.1. Gwarancja obejmuje usuwanie wad i niezgodności z OPZ: LMS, modyfikacji, integracji, aplikacji, konfiguracji, dokumentacji i prac migracyjnych Wykonawcy. Cena obejmuje diagnozę, naprawy i niezbędne aktualizacje, testy/retesty, aktualizacje kodu, SBOM i dokumentacji oraz publikację poprawek mobilnych wraz z narzędziami, środowiskami testowymi i uprawnieniami. Nie obciąża to puli rozwoju ani nie wymaga zakupu dalszego wsparcia, utrzymania lub hostingu. Zgłoszenia dokonane przed końcem gwarancji podlegają pełnej obsłudze i naprawie także po tej dacie.

12.8.2. Po utrzymaniu pozostają zgłoszenia gwarancyjne e-mail i telefonem od NIL lub upoważnionego dostawcy, rejestr, dowody napraw/testów oraz klasyfikacja i terminy pkt 12.3, w tym całodobowe P1 oraz P2–P4 w godzinach obsługi. Gwarant współpracuje z administratorem środowiska, dostarczając poprawkę, instrukcje wdrożenia/wycofania i wsparcie. Brak niezbędnego dostępu lub czynności NIL/nowego dostawcy wstrzymuje wyłącznie czas zależnej czynności, od zarejestrowania konkretnej przeszkody, wymaganej czynności i wpływu na termin. Nie wstrzymuje reakcji, możliwej diagnozy ani prac testowych. Po usunięciu przeszkody licznik biegnie dalej bez zerowania; braki zasobów Wykonawcy nie uzasadniają wstrzymania.

12.8.3. Po 30 czerwca 2029 r. NIL lub nowy dostawca przejmuje hosting, administrację, monitoring, kopie i odtwarzanie infrastruktury, help desk uczestników/czek, planowe audyty, rozwój oraz koszty bieżącej eksploatacji i licencji (rozdział 13). Gwarant nie prowadzi środowiska według pkt 12.4 i CYB-08, lecz nadal naprawia objęte gwarancją wady powodujące awarie. Gwarancja nie obejmuje nowych funkcji ani dostosowań do późniejszych zmian interfejsów, systemów operacyjnych i prawa, chyba że są niezbędne do naprawy takiej wady. Prawidłowa migracja, administracja i wdrożenia według

dokumentacji nie znoszą ochrony. Wyłączenie zgłoszenia wymaga wykazania związku przyczynowego z działaniem poza odpowiedzialnością Wykonawcy i nie wyłącza pozostałego rozwiązania. Dostęp gwaranta podlega wymaganiom RODO i bezpieczeństwa; ochrony nie uzależnia się od zachowania kopii danych produkcyjnych.

12.9. Tworzenie nowych komponentów i prace rozwojowe

12.9.1. Miesięczny ryczałt od odbioru F5 do 30 czerwca 2029 r. obejmuje całe utrzymanie i wsparcie z rozdziału 12 oraz 10 roboczogodzin rozwoju na zlecenie NIL. Diagnoza i usuwanie wad, awarii i podatności, wymagane aktualizacje i SLA nie wymagają dopłat. Pula nie przedłuża utrzymania ani nie zmienia gwarancji.

12.9.2. Rozwój obejmuje związane z edukacją i organizacją NIL nowe komponenty lub zmiany LMS, paneli, formularzy, raportów/eksportów, certyfikatów, powiadomień, bazy wiedzy i aplikacji, zgodne z architekturą zamówienia. Puli nie obciążają obowiązkowy zakres OPZ (w tym F6, aplikacje i F8), utrzymanie, naprawy wad, awarii, podatności i regresji ani gwarancja, niezależnie od techniki naprawy.

12.9.3. Przed pracami Wykonawca przedstawi rozwiązanie, godziny według czynności, termin, kryteria odbioru, zależności i wpływ na bezpieczeństwo, dostępność, integracje i aplikacje. Estymacja obejmie analizę, projekt, konfigurację/programowanie, testy, wdrożenie i dokumentację. Roboczogodzina to 60 minut jednej osoby; czas zespołu sumuje się. Upoważniona osoba NIL zatwierdza zakres, limit i termin; uprzednio zatwierdza też ich zmiany i przekroczenia, bez automatycznej dopłaty lub obciążania następnych pul. Prace ponad dostępną pulę wymagają zaakceptowanego etapowania albo odrębnej podstawy umownej, bez dorozumianego rozszerzenia zamówienia.

12.9.4. Pula narasta po 10 godzin za pełny miesiąc, do 30 godzin na pełny kwartał świadczenia utrzymania. Przez kwartał rozumie się kwartał kalendarzowy. Za niepełny pierwszy miesiąc ryczałt i pulę nalicza się proporcjonalnie: liczba dni kalendarzowych od odbioru F5 do końca miesiąca, włącznie, podzielona przez liczbę dni tego miesiąca. Kwotę zaokrągla się do grosza, a pulę do 0,01 roboczogodziny. Pula pierwszego kwartału jest sumą tak naliczonych godzin, nie automatycznie 30 godzin. Niewykorzystane godziny przechodzą tylko między miesiącami tego kwartału, bez zwiększania limitu; wygasają z końcem kwartału, najpóźniej 30 czerwca 2029 r. Rezerwacja lub akceptacja estymacji nie zużywa puli — rozlicza się rzeczywiście wykonane, udokumentowane prace. Wykonawca planuje realizację w okresie dostępności godzin; etapowanie i odbiory częściowe wymagają zgody NIL. Formularz cenowy odzwierciedla tę zasadę.

12.9.5. Zmiany spełniają wymagania ochrony danych, bezpieczeństwa, dostępności i CYB-03. Przed wdrożeniem Wykonawca przedstawia wersję testową i wyniki testów funkcji oraz regresji, także aplikacji i integracji objętych zmianą. Obowiązują pkt 10.3, SEC-01 i niezależne testy wymagane w CYB-01. Wdrożenie wymaga zgody NIL, planu wycofania i zachowania SLA; odbiór obejmuje kod, konfigurację, dokumentację, SBOM i licencje według rozdziału 13. Rezultat podlega utrzymaniu i gwarancji; poprawianie jego błędów nie obciąża dodatkowo puli. Nowe opłaty licencyjne lub usługi wymagają uprzedniego ujawnienia i odrębnej zgody NIL, bez automatycznego zwiększenia ryczałtu.

12.9.6. Rejestr zleceń i godzin jest dostępny NIL. Raport miesięczny z pkt 12.7 wykazuje zakresy, estymacje, czynności, rzeczywisty czas, testy i odbiory oraz godziny naliczone, przeniesione, wykorzystane i pozostałe, a na koniec kwartału — wygasające. NIL zatwierdza rozliczenie na podstawie ewidencji i rezultatów; nie rozlicza się niewykonanych prac ani niezaakceptowanych przekroczeń. Niewykorzystanie puli nie rodzi dopłat ani samodzielnego zlecenia Wykonawcy. Rozwój nie ogranicza obsługi awarii i utrzymania.

13. Prawa do rozwiązania, dokumentacja, wyjście z usługi

13.1. Wykonawca przekaże wykaz wszystkich komponentów Platformy i ich licencji. Rdzeń open source pozostaje objęty licencjami jego autorów. W przypadku rdzenia własnościowego warunki licencji muszą umożliwiać dalszą eksploatację Platformy w środowisku NIL lub wskazanego dostawcy oraz jej obsługę przez inny podmiot. W odniesieniu do dedykowanych modyfikacji i kodu NIL otrzyma, na zasadach określonych w umowie, prawa umożliwiające bezterminowe korzystanie, modyfikowanie, rozwijanie i utrzymanie Platformy na własnych serwerach lub w wybranej chmurze, także przy udziale innego podmiotu, bez cyklicznych opłat licencyjnych na rzecz Wykonawcy po zakończeniu umowy.

Cena oferty obejmuje wszystkie koszty licencji, hostingu i usług zewnętrznych niezbędnych do wykonania obowiązków OPZ w okresach właściwych dla tych obowiązków. Bieżącą eksploatację, hosting i utrzymanie wycenia się do 30 czerwca 2029 r., a obsługę gwarancyjną także przez 12 miesięcy po zakończeniu utrzymania, zgodnie z pkt 12.8–12.8.3. Wykonawca nie może uzależniać wykonania zamówionych obowiązków od dodatkowych opłat poza wynagrodzeniem umownym. Gwarancja nie przedłuża finansowania bieżącej eksploatacji środowiska przez Wykonawcę.

13.2. W ramach planu wyjścia Wykonawca przekaże wszystkie dane w otwartym formacie umożliwiającym ponowny import, paczki kursów i repozytoria, konfigurację, schemat integracji i dokumentację API, wykaz komponentów z wersjami, procedury kopii i odtwarzania, instrukcje uruchomienia, kopie kodu należącego do NIL oraz niezbędne dostępy bezpiecznym kanałem. Plan obejmuje kontrolę NIL nad domeną, DNS i certyfikatami (CYB-11), aktualny SBOM (CYB-03) i potwierdzenie usunięcia danych u Wykonawcy i dalszych podmiotów według RODO-07.

13.3. Uruchomienie Platformy poza środowiskiem Wykonawcy musi być możliwe na podstawie przekazanych danych, kodu, konfiguracji, dokumentacji i dostępów określonych w pkt 13.2, zgodnie z udzielonymi licencjami. Samo przekazanie maszyn wirtualnych nie spełnia wymagań przekazania tych produktów ani wykazania przenoszalności, którą weryfikuje się zgodnie z pkt 13.4.

13.4. Wykonawca potwierdzi przenoszalność przez odtworzenie pakietu eksportowego na niezależnym środowisku. Test może stanowić część migracji końcowej, jeżeli obejmie jej pełne kryteria odbioru z pkt 6.7. Dane uczestników/czek muszą pozostać chronione i kompletne.

F8 obejmie procedurę gwarancji dla NIL i nowego dostawcy: kontakty, eskalacje, zgłoszenia i klasyfikację, bezpieczne dane diagnostyczne i dostęp czasowy, testowanie, wdrażanie i wycofywanie poprawek. Protokół wskaże wersje i konfigurację, odpowiedzialności infrastrukturalne/gwarancyjne, otwarte zgłoszenia z planami i koniec ochrony. Nie ogranicza warunków pkt 12.8–12.8.3. Po utrzymaniu nadal przekazuje się kod, SBOM i dokumentację napraw gwarancyjnych.

13.5. Projekt techniczny będzie zawierał dokumentację istniejącego rozwiązania, wykaz komponentów, wersji i licencji oraz parametry infrastruktury. Dla elementów planowanych wystarczy opis zakresu, zależności, licencji i praw NIL. Przy odbiorze Wykonawca przekaże aktualną dokumentację, wykaz komponentów oprogramowania, kod oraz instrukcje budowania, instalacji, konfiguracji i integracji. Dopuszcza się rdzeń otwarty lub własnościowy, spełniający OPZ i wymagania pkt 13.1–13.4.

13.6. Wymagania dla dokumentacji

Cena obejmuje dokumentację utrzymania, administracji technicznej i merytorycznej, redaktora, uczestnika, kodu i interfejsów, aktualizowaną według DOK-08. Ma umożliwiać NIL albo wskazanemu podmiotowi samodzielną obsługę i utrzymanie bez Wykonawcy.

DOK-01 Wymagania ogólne

Dokumentacja jest sporządzona w języku polskim, w formacie edytowalnym (DOCX lub Markdown) oraz w PDF. Dokumentacja użytkownika/czki i redaktora jest dodatkowo dostępna w Platformie jako

pomoc online. Każdy dokument zawiera numer wersji, datę, rejestr zmian i wskazanie wersji Platformy, której dotyczy. Dokumentacja nie zawiera haseł, kluczy ani innych sekretów.

Dokumentacja jest przekazywana do repozytorium wskazanego przez NIL. NIL może ją modyfikować, powielać i udostępniać, w tym podmiotom realizującym utrzymanie lub rozwój Platformy, na zasadach określonych w umowie. Dokumentacja przeznaczona dla użytkowników/czek spełnia wymagania co najmniej WCAG 2.1 AA.

W fazie F1 Wykonawca przedstawi plan dokumentacji: wykaz dokumentów, ich strukturę, odbiorców i terminy przekazania.

Weryfikacja / odbiór: plan dokumentacji zatwierdzony przez NIL w F1.

DOK-02 Dokumentacja utrzymaniowa

Zakres minimalny: architektura i diagramy produkcji, testów i kopii; wersje i licencje komponentów, wtyczek i kodu dedykowanego (SBOM, CYB-03); konfiguracja serwerów, bazy, WWW, pamięci podręcznej, kolejek i poczty; parametry połączeń, błędy i ponowienia INT-01–INT-09; zadania cykliczne i harmonogram kopii.

Procedury krok po kroku: start/zatrzymanie usług; wydanie i wycofanie wersji; aktualizacja rdzenia i wtyczek; backup/restore i odtwarzanie awaryjne; skalowanie; odnawianie certyfikatów; dostępy uprzywilejowane; alarmy monitoringu; incydenty (CYB-10) i naruszenia (RODO-06); rotacja logów; usuwanie po retencji (RODO-07).

Dokumentacja zawiera także wykaz znanych problemów i obejść oraz matrycę kontaktów i eskalacji.

Weryfikacja / odbiór: test odtworzenia z kopii i test wdrożenia nowej wersji wykonane przez osobę wskazaną przez NIL wyłącznie na podstawie dokumentacji.

DOK-03 Dokumentacja administratora technicznego

Zakres: instalacja od podstaw; konfiguracja systemu, wtyczek i wyglądu; konta, role i macierz uprawnień (FUN-01); logowanie, MFA, odzyskiwanie i integracje (INT-01); harmonogramy i poczta; bezpieczeństwo i wydajność; retencja, eksport, sprostowanie, ograniczenie, usuwanie, anonimizacja i akceptacje (RODO-07, RODO-09, RODO-11); logi i raporty techniczne (SEC-04); rozwiązywanie typowych problemów.

Weryfikacja / odbiór: wykonanie przez administratora NIL wybranych zadań wyłącznie na podstawie dokumentacji: nadanie roli, reset MFA użytkownika/czki, konfiguracja reguły retencji, eksport danych osoby.

DOK-04 Dokumentacja administratora merytorycznego

Zakres: katalog i kategorie; kursy, ścieżki i wydarzenia live/stacjonarne/hybrydowe; zapisy, limity i listy rezerwowe; sale i obiekty; powiadomienia; certyfikaty i punkty; panel opiekuna i jednostki; baza wiedzy; reguły dokumentów i ocena ręczna (FUN-20, RODO-05); ankiety; raporty i wskaźniki FERS; typowe zgłoszenia uczestników/czek.

Weryfikacja / odbiór: wykonanie przez administratora merytorycznego NIL, wyłącznie na podstawie dokumentacji, scenariusza obejmującego utworzenie wydarzenia, zapisy, wystawienie certyfikatu i przygotowanie raportu.

DOK-05 Dokumentacja redaktora, redaktorki (trenera, trenerki)

Zakres: kursy, sekcje i lekcje; edytory testów, ankiet, interakcji i zadań; import i aktualizacja SCORM; banki pytań, oceny i informacja zwrotna; live z nagrywaniem i udostępnianiem (RODO-10); dostęp i ukończenie; dostępne materiały (napisy, transkrypcje, opisy alternatywne, kontrast); publikacja i archiwizacja.

Weryfikacja / odbiór: przygotowanie przez redaktora NIL kursu referencyjnego wyłącznie na podstawie dokumentacji.

DOK-06 Dokumentacja użytkownika, użytkowniczki (uczestnika, uczestniczki)

Zakres: rejestracja, logowanie, MFA i odzyskiwanie; katalog i zapisy; live i kursy asynchroniczne; testy; certyfikaty i punkty; dokumenty; baza wiedzy; prywatność i prawa RODO; dostępność; najczęstsze pytania i help desk.

Instrukcja mobilna obejmie instalację ze sklepów, MFA, szkolenia, synchronizację z WWW, łączność, aktualizacje i pomoc; podlega odbiorowi przed F5 (DOK-08). Dokumentacja techniczna i utrzymaniowa opisze połączenie z LMS, systemy, budowanie, podpisywanie, publikację i aktualizacje, zależności, licencje i bezpieczne uprawnienia wydawcy, umożliwiając dalszą obsługę przez NIL lub inny podmiot. Stosuje się pkt 13.1, 13.5 i DOK-07; sekrety przekazuje się oddzielnym bezpiecznym kanałem.

Dokumentacja jest dostępna w Platformie jako pomoc kontekstowa, jako przewodnik PDF oraz w formie co najmniej 5 filmów instruktażowych, każdy do 3 minut, z napisami.

Weryfikacja / odbiór: test zrozumiałości z udziałem uczestników/czek pilotażu (pkt 10.5); weryfikacja dostępności dokumentacji i filmów.

DOK-07 Dokumentacja techniczna kodu i interfejsów

Dla kodu dedykowanego i integracji: moduły i zależności, instrukcje budowania i instalacji, model danych oraz API (np. OpenAPI) z przykładami wywołań i kodami błędów, zgodnie z pkt 13.5.

Weryfikacja / odbiór: zbudowanie i instalacja kodu dedykowanego na środowisku testowym na podstawie instrukcji; przegląd specyfikacji API przez NIL.

DOK-08 Odbiór i aktualizacja dokumentacji

Robocze DOK-03–DOK-06 należy przekazać przed UAT w F4; ostateczne DOK-02–DOK-07 dla startu, kont lokalnych/MFA i trybu przejściowego — przed odbiorem F5. Dokumentacja integracji, zabezpieczeń i wyjścia z trybu przejściowego wymaga zatwierdzenia przed F6. NIL ma 10 dni roboczych na uwagi, Wykonawca 5 na ich uwzględnienie; plan uwzględni te terminy przed odbiorami, dla startu w F4. Instruktaż startowy poprzedza F5, a integracyjny F6, w wymiarze rozdziału 11.

Dokumentację aktualizuje się do 10 dni roboczych po zmianie wersji, konfiguracji lub funkcji, a gdy jest produktem odbioru lub wdrożenia (F5, F6, pkt 12.9.5) — wraz z tym produktem. Pełny przegląd odbywa się co 12 miesięcy; brak aktualności jest wadą. F8 wymaga wersji dla środowiska docelowego, a naprawy po utrzymaniu — aktualizacji według pkt 12.8.1.

Weryfikacja / odbiór: rejestr wersji dokumentacji w raporcie miesięcznym (pkt 12.7); zgodność dokumentacji z Platformą sprawdzana przy przeglądzie rocznym i teście przenośności (pkt 13.4).

14. Wymagania dotyczące informacji i promocji Projektu

14.1. Wymagania dotyczące informacji i promocji

a) Platforma edukacyjna, w tym jej projekt graficzny, interfejs użytkownika/czki, aplikacje mobilne Android i iOS, poszczególne widoki, komponenty, funkcjonalności oraz materiały opracowywane przez Wykonawcę w ramach realizacji zamówienia, muszą być zgodne z obowiązującymi dla Projektu zasadami informacji i promocji Funduszy Europejskich na lata 2021–2027, wynikającymi w szczególności z właściwych wytycznych, umowy o dofinansowanie Projektu oraz innych dokumentów określających obowiązki informacyjne i promocyjne.

b) Wykonawca zobowiązany jest do uwzględnienia odpowiedniego oznakowania Projektu, w szczególności właściwego zestawienia znaków, logotypów, informacji tekstowych oraz innych wymaganych elementów identyfikacji wizualnej. Oznakowanie powinno zostać umieszczone w odpowiednich miejscach platformy, w tym na stronie głównej, w katalogu szkoleń, panelach użytkowników/czek oraz innych widokach wskazanych przez Zamawiającego, zgodnie z obowiązującymi zasadami informacji i promocji. Wymaganie obejmuje również aplikacje mobilne Android i iOS, w zakresie mającym zastosowanie do ich funkcjonalności i sposobu prezentacji treści.

c) Wymagania dotyczące oznakowania obejmują również szablony certyfikatów, zaświadczeń, dokumentów, powiadomień oraz innych materiałów opracowywanych lub konfigurowanych przez Wykonawcę w ramach zamówienia, w zakresie wynikającym z obowiązujących zasad informacji i promocji. Platforma powinna umożliwiać Zamawiającemu stosowanie odpowiedniego oznakowania w materiałach i dokumentach generowanych przez system.

d) Zamawiający przekaże Wykonawcy wymagane wzory oznakowania, logotypy, zestawienia znaków, elementy graficzne oraz, w razie potrzeby, dodatkowe instrukcje dotyczące sposobu ich stosowania. Wykonawca zobowiązany jest do uwzględnienia przekazanych elementów podczas projektowania, wdrażania i utrzymania platformy oraz aplikacji mobilnych.

e) Wykonawca nie może samodzielnie modyfikować przekazanych przez Zamawiającego znaków, logotypów ani innych elementów identyfikacji wizualnej, w szczególności zmieniać ich proporcji, kolorystyki, układu lub wzajemnego położenia, chyba że Zamawiający wyrazi na to zgodę lub możliwość taka wynika z właściwych zasad informacji i promocji.

f) Sposób umieszczenia oznakowania musi zapewniać jego odpowiednią widoczność, czytelność i prawidłowe wyświetlanie na urządzeniach o różnych rozdzielczościach ekranu, z zachowaniem wymagań dotyczących minimalnych rozmiarów, proporcji, pól ochronnych, kolejności znaków oraz pozostałych zasad ich stosowania.

g) Projekt graficzny platformy i aplikacji mobilnych, w zakresie obejmującym rozmieszczenie i sposób prezentacji oznakowania Projektu, wymaga akceptacji Zamawiającego przed wdrożeniem produkcyjnym. W przypadku stwierdzenia nieprawidłowego lub niepełnego oznakowania Wykonawca zobowiązany jest do dokonania, w ramach wynagrodzenia za realizację zamówienia, wszystkich niezbędnych korekt dotyczących zakresu objętego zamówieniem.

h) W okresie utrzymania platformy, określonym w OPZ do dnia 30 czerwca 2029 r., Wykonawca zobowiązany jest do zachowania prawidłowego oznakowania Projektu, w szczególności podczas aktualizacji oprogramowania, modyfikacji interfejsu, wprowadzania zmian w funkcjonalnościach platformy oraz aktualizacji aplikacji mobilnych. W przypadku zmian wymagań dotyczących informacji i promocji Wykonawca zobowiązany jest do dostosowania oznakowania, zgodnie z informacjami i materiałami przekazanymi przez Zamawiającego, w ramach wynagrodzenia za utrzymanie, o ile dostosowanie nie wymaga istotnej przebudowy systemu lub wdrożenia nowych funkcjonalności nieobjętych zamówieniem.

i) Wymagania dotyczące oznakowania nie obejmują merytorycznej ani graficznej przebudowy istniejących materiałów edukacyjnych przekazanych przez Zamawiającego, chyba że obowiązek taki został wyraźnie określony w OPZ. Wykonawca zobowiązany jest jednak do zapewnienia możliwości prawidłowego oznakowania materiałów publikowanych za pośrednictwem platformy.

j) Platforma edukacyjna, w tym jej oznakowanie oraz wszystkie elementy identyfikacji wizualnej związane z Projektem, musi być zgodna z aktualnie obowiązującymi zasadami informacji i promocji Funduszy Europejskich na lata 2021–2027, w szczególności z:

- Księgą Tożsamości Wizualnej marki Fundusze Europejskie 2021–2027;

- Podręcznikiem wnioskodawcy i beneficjenta Funduszy Europejskich na lata 2021–2027 w zakresie informacji i promocji;
- Kartą wizualizacji dla programu Fundusze Europejskie dla Rozwoju Społecznego;
- postanowieniami umowy o dofinansowanie Projektu oraz dokumentami i zaleceniami przekazanymi przez Zamawiającego.

Wykonawca zobowiązany jest do stosowania powyższych dokumentów w zakresie mającym zastosowanie do przedmiotu zamówienia, z uwzględnieniem ich aktualizacji obowiązujących w okresie realizacji zamówienia, na zasadach określonych w niniejszym OPZ.

Aktualne dokumenty, wzory oznakowania, logotypy, zestawienia znaków oraz pozostałe elementy identyfikacji wizualnej dostępne są na oficjalnej stronie programu Fundusze Europejskie dla Rozwoju Społecznego 2021–2027:

https://rozwojspoleczny.gov.pl/promocja-programu/zasady-promocji-i-oznakowania-programu/

14.2. Projekt graficzny i akceptacja interfejsu użytkownika, użytkowniczki

a) W ramach realizacji zamówienia Wykonawca zobowiązany jest do opracowania kompletnego projektu graficznego interfejsu użytkownika, użytkowniczki platformy edukacyjnej NIL, obejmującego zarówno wersję przeglądarkową (WWW), jak i aplikacje mobilne Android i iOS. Projekt musi uwzględniać wymagania funkcjonalne określone w OPZ, identyfikację wizualną NIL, zasady informacji i promocji Projektu FERS, wymagania dostępności cyfrowej oraz zasady responsywności i użyteczności interfejsu (UX/UI).

b) Wykonawca zobowiązany jest do przedstawienia Zamawiającemu co najmniej dwóch odrębnych wariantów koncepcji graficznej, umożliwiających wybór preferowanego kierunku wizualnego. Każdy wariant powinien obejmować co najmniej stronę główną, katalog szkoleń, panel uczestnika/czki, widok kursu oraz reprezentatywne widoki aplikacji mobilnych. Warianty powinny różnić się w sposób umożliwiający rzeczywisty wybór koncepcji, przy zachowaniu spójności z identyfikacją wizualną NIL.

c) Przygotowanie i przedstawienie wariantów koncepcji graficznej nastąpi w ramach fazy F1 – Analiza i projekt rozwiązania. Wykonawca przedstawi koncepcje w terminie umożliwiającym ich ocenę, zgłoszenie uwag i zatwierdzenie przez Zamawiającego przed zakończeniem tej fazy.

d) Zamawiający ma prawo wyboru jednego z przedstawionych wariantów, wskazania elementów wymagających zmiany lub połączenia rozwiązań zaproponowanych w różnych wariantach. Zamawiający może zgłaszać uwagi dotyczące w szczególności kolorystyki, typografii, układu elementów, nawigacji, sposobu prezentacji treści, ikonografii oraz ogólnej estetyki interfejsu.

e) Wykonawca zobowiązany jest do uwzględnienia uwag Zamawiającego oraz przedstawienia poprawionej koncepcji graficznej. W ramach wynagrodzenia za realizację zamówienia Wykonawca zapewni co najmniej dwie tury poprawek wybranego wariantu. Usunięcie niezgodności z wymaganiami OPZ nie jest wliczane do wskazanego limitu poprawek.

f) Ostateczna koncepcja graficzna wymaga akceptacji Zamawiającego w formie dokumentowej. Wykonawca nie może przystąpić do wdrożenia docelowego interfejsu bez uzyskania tej akceptacji. Brak akceptacji z powodu niespełnienia wymagań OPZ lub nieuwzględnienia uzgodnionych uwag zobowiązuje Wykonawcę do dokonania niezbędnych korekt w ramach wynagrodzenia za realizację zamówienia.

g) Na podstawie zaakceptowanej koncepcji Wykonawca opracuje szczegółowy projekt graficzny interfejsu oraz prototyp w ramach fazy F2 – Prototyp (POC) i walidacja UX. Projekt musi obejmować wszystkie niezbędne widoki, komponenty i stany interfejsu wymagane do realizacji funkcjonalności określonych w OPZ, z zachowaniem spójności wizualnej platformy WWW i aplikacji mobilnych.

h) W przypadku modernizacji istniejącego rozwiązania Wykonawca może wykorzystać dotychczasowe elementy interfejsu, pod warunkiem ich zgodności z zaakceptowaną koncepcją graficzną oraz wymaganiami OPZ. W przypadku wdrożenia nowego rozwiązania Wykonawca zobowiązany jest do zapewnienia kompletnego interfejsu zgodnego z zaakceptowanym projektem.

i) Wszystkie koszty przygotowania wariantów koncepcji graficznej, opracowania szczegółowego projektu interfejsu, prototypów oraz wprowadzenia wymaganych poprawek muszą zostać uwzględnione w cenie oferty. Zamawiający nie przewiduje odrębnego wynagrodzenia z tego tytułu.

14.3. Weryfikacja i odbiór

Weryfikacja spełnienia wymagań dotyczących informacji i promocji nastąpi przed odbiorem produkcyjnym platformy w fazie F5 i obejmie sprawdzenie prawidłowości oznakowania reprezentatywnych widoków platformy, aplikacji mobilnych oraz szablonów dokumentów generowanych przez system. Stwierdzone niezgodności Wykonawca usunie przed odbiorem, w ramach wynagrodzenia za realizację zamówienia.

Weryfikacja projektu graficznego obejmie przedstawienie i ocenę wariantów koncepcji w fazie F1, akceptację wybranego wariantu oraz ocenę szczegółowego projektu i prototypu w fazie F2. Ostateczny odbiór interfejsu nastąpi w ramach testów i odbiorów określonych w rozdziale 10 OPZ. Stwierdzone niezgodności z wymaganiami OPZ lub zaakceptowanym projektem graficznym Wykonawca zobowiązany jest usunąć w ramach wynagrodzenia za realizację zamówienia.

15. Wymagania dotyczące dostępności cyfrowej dla osób z niepełnosprawnościami i osób ze szczególnymi potrzebami

15.1. Wymagania dotyczące dostępności cyfrowej

a) Platforma edukacyjna, w tym jej projekt graficzny, struktura, nawigacja, interfejs użytkownika/czki, aplikacje mobilne Android i iOS, formularze, komponenty, funkcjonalności edukacyjne oraz materiały opracowywane przez Wykonawcę w ramach realizacji zamówienia, muszą spełniać wymagania dostępności cyfrowej dla osób z niepełnosprawnościami oraz osób ze szczególnymi potrzebami.

b) Wykonawca zobowiązany jest do zaprojektowania, wdrożenia i utrzymania platformy zgodnie z wymaganiami standardu co najmniej WCAG 2.1 na poziomie AA oraz standardami dostępności właściwymi dla Projektu FERS, zgodnie z wymaganiami określonymi w rozdziale 7, TECH-04, TECH-06 i SEC-05 OPZ. Wymagania obejmują cztery podstawowe zasady dostępności cyfrowej: postrzegalność, funkcjonalność, zrozumiałość i kompatybilność.

c) W szczególności platforma musi zapewniać:

- możliwość obsługi wszystkich podstawowych funkcjonalności za pomocą klawiatury, bez konieczności korzystania z myszy;
- prawidłową współpracę z technologiami wspomagającymi, w tym czytnikami ekranu;
- odpowiedni kontrast tekstów i elementów interfejsu oraz możliwość powiększania treści bez utraty ich czytelności i funkcjonalności;
- logiczną strukturę nagłówków, czytelną nawigację oraz jednoznaczne oznaczenie elementów interaktywnych;
- alternatywne opisy tekstowe dla grafik i innych elementów nietekstowych, jeżeli są wymagane;
- dostępne cyfrowo formularze rejestracyjne, komunikaty, przyciski, powiadomienia oraz mechanizmy uwierzytelniania, w tym MFA;
- możliwość korzystania z platformy na urządzeniach mobilnych i przy różnych rozdzielczościach ekranu;

- dostępność funkcjonalności związanych z przeglądaniem katalogu szkoleń, zapisami, uczestnictwem w szkoleniach, monitorowaniem postępów, rozwiązywaniem testów i quizów, wypełnianiem ankiet oraz pobieraniem certyfikatów;
- dostępność odtwarzaczy multimedialnych, materiałów audio i wideo oraz elementów interaktywnych, w tym komponentów wykorzystywanych do realizacji treści SCORM i xAPI, w zakresie zapewnianym przez Wykonawcę;
- możliwość korzystania z napisów, transkrypcji oraz innych rozwiązań wspierających dostępność materiałów multimedialnych, zgodnie z wymaganiami właściwymi dla danego rodzaju treści;
- dostępność funkcjonalności wykorzystywanych podczas webinarów i zajęć live online, w tym interfejsu uczestnictwa, komunikacji z prowadzącym i obsługi czatu, w zakresie funkcjonalności dostarczanych przez Wykonawcę;
- możliwość konfiguracji indywidualnych dostosowań egzaminów i testów, w szczególności wydłużenia czasu ich rozwiązywania oraz alternatywnych form udzielania odpowiedzi, zgodnie z wymaganiami SEC-05.

d) Wymagania dostępności cyfrowej dotyczą również aplikacji mobilnych Android i iOS, które muszą umożliwiać korzystanie z podstawowych funkcjonalności edukacyjnych z wykorzystaniem mechanizmów dostępności systemów operacyjnych, w tym technologii wspomagających, zgodnie z wymaganiami TECH-06 i FUN-24.

e) Wykonawca zobowiązany jest do uwzględnienia wymagań dostępności cyfrowej na wszystkich etapach realizacji zamówienia, w szczególności podczas analizy i projektowania rozwiązania, opracowywania interfejsów użytkownika/czki, wdrażania komponentów, konfiguracji procesów edukacyjnych, integracji systemowych oraz przeprowadzania testów.

f) Wymagania dostępności cyfrowej obejmują funkcjonalności i elementy platformy dostarczane, konfigurowane lub modyfikowane przez Wykonawcę, w tym rozwiązania zewnętrzne stanowiące integralną część dostarczonego systemu. W przypadku wykorzystania zewnętrznych usług lub komponentów, w szczególności do realizacji webinarów i transmisji live online, Wykonawca odpowiada za zapewnienie zgodności funkcjonalności udostępnianych użytkownikom/czkom NIL z wymaganiami dostępności określonymi w OPZ.

g) Wykonawca zobowiązany jest do zapewnienia możliwości publikowania i udostępniania materiałów edukacyjnych w formatach umożliwiających spełnienie wymagań dostępności cyfrowej. W odniesieniu do materiałów edukacyjnych przekazanych przez Zamawiającego Wykonawca odpowiada za ich prawidłowe udostępnienie za pośrednictwem platformy. Obowiązek ten nie obejmuje merytorycznej ani graficznej przebudowy istniejących materiałów, chyba że obowiązek taki został wyraźnie określony w OPZ.

h) Wykonawca zobowiązany jest do zapewnienia dostępności cyfrowej materiałów, dokumentów, szablonów i elementów multimedialnych opracowywanych przez niego w ramach realizacji zamówienia, w zakresie wynikającym z ich charakteru i obowiązujących wymagań. W szczególności wymaganie dotyczy szablonów certyfikatów, zaświadczeń, formularzy oraz dokumentów generowanych przez platformę.

i) Przed przekazaniem platformy do odbioru Wykonawca zobowiązany jest do przeprowadzenia weryfikacji zgodności z wymaganiami dostępności cyfrowej, obejmującej testy automatyczne oraz manualne, w tym sprawdzenie obsługi klawiaturą, współpracy z technologiami wspomagającymi, kontrastu, nawigacji oraz dostępności formularzy i elementów interaktywnych.

j) Weryfikacja dostępności cyfrowej musi obejmować reprezentatywne procesy użytkownika/czki, w szczególności rejestrację i logowanie, zapis na szkolenie, uczestnictwo w kursie asynchronicznym,

udział w zajęciach live online, rozwiązywanie testów, przesyłanie zadań, wypełnianie ankiet oraz pobieranie certyfikatów. Testy obejmą również aplikacje mobilne Android i iOS, zgodnie z wymaganiami OPZ.

k) Wyniki przeprowadzonej weryfikacji, wraz z informacją o stwierdzonych niezgodnościach i sposobie ich usunięcia, zostaną przekazane Zamawiającemu przed odbiorem platformy. W przypadku stwierdzenia niezgodności dotyczących elementów objętych odpowiedzialnością Wykonawcy jest on zobowiązany do ich usunięcia w ramach wynagrodzenia za realizację zamówienia. Odbiór dostępności odbywa się zgodnie z wymaganiami SEC-05 i rozdziału 10 OPZ.

l) W okresie utrzymania platformy Wykonawca zobowiązany jest do zachowania zgodności z wymaganiami dostępności cyfrowej, w szczególności podczas aktualizacji oprogramowania, modyfikacji istniejących funkcjonalności, wdrażania nowych komponentów oraz aktualizacji aplikacji mobilnych. Usuwanie niezgodności dotyczących elementów objętych odpowiedzialnością Wykonawcy odbywa się w ramach wynagrodzenia za utrzymanie platformy.

m) Platforma edukacyjna musi spełniać wymagania wynikające z **Wytycznych dotyczących realizacji zasad równościowych w ramach funduszy unijnych na lata 2021–2027**, w szczególności z załącznika nr 2 „Standardy dostępności dla polityki spójności 2021–2027”, w zakresie dotyczącym dostępności cyfrowej, a także wymagania określone w umowie o dofinansowanie Projektu oraz dokumentach i zaleceniach przekazanych przez Zamawiającego.

n) Wykonawca zobowiązany jest do zapewnienia możliwości opublikowania i aktualizacji deklaracji dostępności cyfrowej platformy, jeżeli obowiązek jej sporządzenia ma zastosowanie do platformy. Wykonawca przygotuje informacje techniczne dotyczące rzeczywistego stanu dostępności platformy oraz wyników przeprowadzonych testów, niezbędne do opracowania deklaracji. Treść deklaracji wymaga akceptacji Zamawiającego przed jej opublikowaniem.

15.2. Weryfikacja i odbiór

Weryfikacja spełnienia wymagań dostępności cyfrowej nastąpi w ramach testów i odbiorów określonych w OPZ, w szczególności w fazach F4 i F5, zgodnie z SEC-05 i rozdziałem 10. Wykonawca przedstawi wyniki testów, raporty z audytu dostępności oraz potwierdzenie usunięcia stwierdzonych niezgodności. Wymagania obejmują zarówno platformę WWW, jak i aplikacje mobilne Android i iOS. Raporty dotyczące wcześniejszych wersji produktów lub rozwiązań nie zastępują weryfikacji rozwiązania dostarczonego i skonfigurowanego dla NIL.

16. Wymagania dotyczące zasad równościowych i niedyskryminacji

16.1. Wymagania dotyczące zasad równościowych i niedyskryminacji

a) Platforma edukacyjna, w tym jej projekt graficzny, interfejs użytkownika/czki, aplikacje mobilne Android i iOS, struktura, funkcjonalności, elementy wizualne oraz treści i materiały opracowywane przez Wykonawcę w ramach realizacji zamówienia, muszą być przygotowane zgodnie z zasadą równości kobiet i mężczyzn oraz zasadą równości szans i niedyskryminacji, w szczególności ze względu na płeć, rasę lub pochodzenie etniczne, religię lub światopogląd, niepełnosprawność, wiek lub orientację seksualną.

b) Wykonawca zobowiązany jest do uwzględnienia, w zakresie adekwatnym do przedmiotu zamówienia, zasad i polityk horyzontalnych Unii Europejskiej, w szczególności zasady równości kobiet i mężczyzn, zasady równości szans i niedyskryminacji oraz zasady dostępności dla osób z niepełnosprawnościami, zgodnie z Wytycznymi dotyczącymi realizacji zasad równościowych w ramach funduszy unijnych na lata 2021–2027 oraz postanowieniami umowy o dofinansowanie Projektu.

c) Treści, komunikaty systemowe, etykiety, formularze, powiadomienia, szablony dokumentów, certyfikaty oraz inne elementy tekstowe opracowywane przez Wykonawcę powinny posługiwać się językiem równościowym, niedyskryminującym i niewykluczającym oraz, w zakresie uzasadnionym charakterem treści, uwzględniać żeńskie i męskie formy nazw zawodów, funkcji i stanowisk.

d) Projekt graficzny platformy i aplikacji mobilnych oraz treści, przykłady, ilustracje, grafiki i inne materiały opracowywane przez Wykonawcę nie mogą zawierać elementów utrwalających stereotypy lub mogących prowadzić do dyskryminacji bądź nierównego traktowania jakiejkolwiek grupy osób.

e) Funkcjonalności platformy, w tym mechanizmy rejestracji, uwierzytelniania, dostępu do szkoleń, uczestnictwa w zajęciach, realizacji testów i egzaminów oraz korzystania z materiałów edukacyjnych, muszą być zaprojektowane w sposób zapewniający równe traktowanie użytkowników/czek, z uwzględnieniem uzasadnionych zasad dostępu i uprawnień określonych przez Zamawiającego.

f) Platforma musi umożliwiać uwzględnienie indywidualnych potrzeb uczestników/czek szkoleń, w szczególności osób z niepełnosprawnościami i osób ze szczególnymi potrzebami, w zakresie funkcjonalności określonych w OPZ, w tym dostosowań testów i egzaminów zgodnie z SEC-05. Rozwiązania te powinny zapewniać możliwość udziału w procesie edukacyjnym na równych zasadach, z uwzględnieniem charakteru i wymagań poszczególnych szkoleń.

g) Wykonawca zobowiązany jest do uwzględniania powyższych zasad zarówno na etapie projektowania i wdrażania platformy, jak i podczas realizacji prac rozwojowych oraz wprowadzania zmian w okresie jej utrzymania, w zakresie dotyczącym prac wykonywanych przez Wykonawcę.

h) Wymagania określone w niniejszym rozdziale dotyczą elementów i funkcjonalności opracowywanych, dostarczanych lub modyfikowanych przez Wykonawcę. Nie obejmują merytorycznej weryfikacji ani przebudowy istniejących materiałów edukacyjnych przekazanych przez Zamawiającego, chyba że obowiązek taki został wyraźnie określony w OPZ.

16.2. Weryfikacja i odbiór

Spełnienie wymagań dotyczących zasad równościowych i niedyskryminacji podlega weryfikacji podczas odbioru platformy, w szczególności w zakresie projektów interfejsów, formularzy, komunikatów systemowych, szablonów dokumentów oraz funkcjonalności umożliwiających indywidualne dostosowanie procesu edukacyjnego. W przypadku stwierdzenia niezgodności dotyczących zakresu objętego zamówieniem Wykonawca zobowiązany jest do ich usunięcia w ramach wynagrodzenia za realizację zamówienia.