Załącznik nr 2 do Zapytania ofertowego nr RKK 612-1/2024

**Opis przedmiotu zamówienia**

**Część 1**

**Przeprowadzenie zewnętrznego egzaminu certyfikacyjnego potwierdzającego nabycie kwalifikacji z tematu: „Zarządzanie zrównoważonym rozwojem organizacji”.**

Wykonawca przeprowadzi egzamin dla 40 Uczestników Projektu (UP).

Miejsce realizacji egzaminów:

Akademia Nauk Stosowanych Mazovia ul. Sokołowska 161, 08-110 Siedlce

Egzaminy będą realizowane w okresie od podpisania umowy do 31.12.2026 r., od poniedziałku do piątku i w weekendy w godzinach od 8:00 do 20:00, w oparciu o szczegółowy harmonogram zajęć, potwierdzony przez Zamawiającego i przekazany wybranemu oferentowi po podpisaniu umowy.

Sale do realizacji egzaminów zapewnia Zamawiający.

Wykonawca zobowiązany jest do zapewnienia niezbędnego sprzętu oraz materiałów do realizacji egzaminów.

Wykonawca opracuje/przygotuje, zorganizuje i przeprowadzi zewnętrzny egzamin certyfikacyjny, na podstawie przedstawionego poniżej programu szkolenia:

Diagnozowanie organizacji pod kątem działań z zakresu zrównoważonego rozwoju

* Przepisy prawne dotyczące zrównoważonego rozwoju na poziomie światowym, europejskim, krajowym i regionalnym.
* Regulacje istotne dla organizacji wynikające z aktów prawnych dotyczących zrównoważonego rozwoju.
* Definicja i koncepcje zrównoważonego rozwoju (CSR, ESG)
* Cele zrównoważonego rozwoju dla organizacji.
* Identyfikacja dobrych praktyk z zakresu zrównoważonego rozwoju w odniesieniu do branży i organizacji.
* Charakterystyka działań organizacji w zakresie ochrony środowiska, odnawialnych źródeł energii i zmniejszenia zużycia zasobów naturalnych.

Planowanie i wdrażanie strategii zrównoważonego rozwoju organizacji

* Opracowanie strategii zrównoważonego rozwoju.
* Definiowanie obszarów zaangażowania organizacji w działania na rzecz zrównoważonego rozwoju.
* Działania możliwe do podjęcia w obszarze środowiska, społeczeństwa, ładu korporacyjnego i praw człowieka.
* Opracowanie harmonogramu i budżetu realizacji strategii zrównoważonego rozwoju.
* Określenie zasobów niezbędnych do wdrożenia strategii.
* Zaangażowanie interesariuszy w realizację strategii zrównoważonego rozwoju.
* Opracowanie planu komunikacji strategii zrównoważonego rozwoju.

Monitorowanie wdrażania i realizacji strategii zrównoważonego rozwoju organizacji

* Dobór i stosowanie narzędzi oraz wskaźników monitorowania wdrażania strategii.
* Proponowanie kluczowych wskaźników efektywności (KPI) w odniesieniu do zrównoważonego rozwoju.
* Zbieranie i analiza danych jakościowych oraz ilościowych dotyczących zrównoważonego rozwoju.
* Definiowanie narzędzi raportowania działań z zakresu zrównoważonego rozwoju (ramy, standardy, indeksy).
* Opracowanie raportu zgodnie z obowiązującymi standardami i normami.
* Rekomendacje dotyczące przyszłych działań z zakresu zrównoważonego rozwoju dla organizacji.

Wykonawca zobowiązany będzie do zdefiniowania efektów uczenia się co najmniej w zakresie: wiedzy, umiejętności i kompetencji społecznych. Egzamin powinien weryfikować efekty uczenia się co najmniej w zakresie: wiedzy, umiejętności i kompetencji społecznych wynikające z przedstawionego programu szkolenia.

Certyfikat wydany osobom, które pomyślnie zdały egzamin certyfikacyjny winien zawierać w swej treści co najmniej:

* nazwę instytucji certyfikującej (IC),
* imię i nazwisko osoby egzaminowanej,
* nazwę/temat szkolenia i/lub kwalifikacji,
* datę i miejsce wydania,
* pieczęcie i podpisy osób upoważnionych do reprezentowania IC (instytucji certyfikującej).

Do każdego certyfikatu dołączony zostanie suplement, który winien zawierać w swej treści co najmniej:

* nazwę instytucji certyfikującej (IC),
* imię i nazwisko osoby egzaminowanej,
* nazwę/temat szkolenia i/lub kwalifikacji,
* program szkolenia i/lub nabyte efekty uczenia się w zakresie wiedzy, umiejętności   
  i kompetencji społecznych,
* uzyskane wyniki,
* datę i miejsce wydania,
* pieczęcie i podpisy osób upoważnionych do reprezentowania IC (instytucji certyfikującej).

Wykonawca zobowiązany jest do wydania certyfikatu każdemu uczestnikowi, który pomyślnie ukończy zewnętrzny egzamin certyfikacyjny. Certyfikat musi spełniać wymagania określone przez Ministerstwo Rozwoju / Ministerstwo  Funduszy i Polityki Regionalnej w odniesieniu do sposobów uzyskiwania i potwierdzania kwalifikacji w ramach projektów współfinansowanych z EFS+ w tzw. „liście sprawdzającej” do weryfikacji czy dokument można uznać za potwierdzający kwalifikację (niewłączoną do Zintegrowanego Systemu Kwalifikacji)/kompetencję na potrzeby mierzenia wskaźników monitorowania EFS+ dot. uzyskiwania kwalifikacji, zgodnie z informacjami przedstawionymi w dokumencie p.n. „Załącznik 2 Podstawowe informacje dotyczące uzyskiwania kwalifikacji w ramach projektów współfinansowanych z EFS+”: https://www.funduszeeuropejskie.gov.pl/strony/o-funduszach/dokumenty/wytyczne-dotyczace-monitorowania-postepu-rzeczowego-realizacji-programow-na-lata-2021-2027/

Wykonawca zobowiązany jest zapewnić każdemu uczestnikowi dostęp do platformy dydaktycznej wraz z materiałami dydaktycznymi w formie cyfrowej.

Wymagania platformy dydaktycznej:

1. Platforma będzie wykorzystywana jako narzędzie wspierające uczestnika w przygotowaniu się do walidacji i certyfikacji kwalifikacji.
2. Platforma ma dawać możliwość udostępniania użytkownikom treści nauczania w formie cyfrowej, udostępniania narzędzi do przystępnej i atrakcyjnej formy utrwalania wiedzy poprzez ćwiczenia interaktywne, narzędzia pracy grupowej oraz możliwości oceny różnych form aktywności przez trenerów.
3. Platforma musi też umożliwiać przyznawanie mikropoświadczeń, w postaci cyfrowych odznak, realizowanych w standardzie Open Badge 3.0 lub równoważnym, za potwierdzenie efektów uczenia się - za pomocą mechanizmów w niej zaimplementowanych, lub poprzez łączenie z innymi systemami poprzez interfejs API. Przez standard równoważny do Open Badge 3.0 Zamawiający uważa standard spełniający warunki opisane w zapytaniu ofertowym.
4. Użytkownikami platformy będą uczestnicy projektu.

Wymagania funkcjonalne platformy dydaktycznej:

1. Start i logowanie się do konta użytkownika – platforma powinna oferować formularz logowania wymagający podania nazwy użytkownika (lub adresu e-mail) i hasła oraz sprawdzać poprawność wprowadzonych danych logowania.
2. Zarządzanie kontem użytkownika powinno uwzględniać możliwość tworzenia profili dla trenerów i uczniów, w tym zarządzanie ich uprawnieniami. Platforma powinna umożliwiać tworzenie grup użytkowników (odpowiadających grupom szkoleniowym), w celu selektywnego udostępniania zawartości merytorycznej (cyfrowy podręcznik, ćwiczenia etc.). Sposób zabezpieczenia systemu opisano w sekcji opisu poświęconej wymaganiom pozafunkcjonalnym.
3. Komunikacja – platforma powinna udostępniać narzędzia do komunikacji między uczestnikami szkoleń oraz między uczestnikami i trenerem, w postaci forum dyskusyjnego, umożliwiającego wymianę myśli i dyskusje na tematy związane z tematyką szkolenia, a także czat, na potrzeby komunikacji w czasie rzeczywistym.
4. Możliwość tworzenia kursów – platforma powinna dawać możliwość łatwego tworzenia i zarządzania kursami, w tym dodawanie treści edukacyjnych, takich jak dokumenty, prezentacje, dźwięk, wideo, itp. Oraz wsparcie dla różnych formatów treści, w tym HTML, PDF, tekst, multimedia.
5. Możliwość tworzenia quizów, ćwiczeń, zadań domowych – platforma powinna dawać osobie prowadzącej szkolenie możliwość dodawania ćwiczeń oraz quizów interaktywnych w popularnych formatach e-learnigowych (HTML5, SCORM), a także innych zadań (w tym opisowych), a także możliwość punktowania i oceny tychże przez trenera.
6. Możliwość tworzenia notatek z zajęć – Użytkownicy powinni mieć możliwość tworzenia notatek z realizowanych zajęć.
7. Wsparcie dla standardów e-learningowych – platforma powinna zapewniać kompatybilność z popularnymi standardami e-learningowymi, takimi jak SCORM czy xAPI (Tin Can),   
   co umożliwia wykorzystanie zewnętrznych materiałów edukacyjnych i śledzenie interakcji z nimi.
8. Repozytorium treści – platforma zapewniać powinna repozytorium treści z możliwością zarządzania tymiż treściami, w kontekście udostępniania materiałów poszczególnym użytkownikom oraz tworzenia z nich ścieżek dydaktycznych. Wykonawca zobowiązany będzie do wypełnienia repozytorium treścią dla szkolenia stanowiącego przedmiot zamówienia.

Dostarczana zawartość powinna uwzględniać przynajmniej:

* podręcznik w formie cyfrowej, który w sposób wyczerpujący omawia wskazany wyżej program szkolenia,
* interaktywną ścieżkę dydaktyczną (umożliwiającą nawigowanie po zagadnieniach merytorycznych danego tematu),
* zestawy ćwiczeń,
* testy kompetencyjne/egzaminy próbne.

Repozytorium powinno również zawierać materiały merytoryczne, pozwalające na zapoznanie się z dostępnymi narzędziami AI (sztucznej inteligencji) pozwalającymi na wykorzystywanie generatywnej AI na potrzeby kwalifikacji stanowiącej przedmiot szkolenia.

1. Możliwość generowania mikropoświadczeń – platforma/system powinien dawać użytkownikom możliwość zdobywania mikropoświadczeń w postaci odznak cyfrowych, realizowanych zgodnie ze standardem Open Badge 3.0, za potwierdzanie efektów kształcenia nabywanych podczas realizacji szkoleń.

Zgodnie z treścią Zalecenia Rady z dnia 22 czerwca 2022 r. w sprawie europejskiego podejścia do mikropoświadczeń na potrzeby uczenia się przez całe życie i zatrudnialności, zaleca się państwom członkowskim przyjęcie i promowanie stosowania definicji mikropoświadczenia, jako: *„opis(u) efektów uczenia się, które osoba ucząca się uzyskała przy niewielkim nakładzie uczenia się. Efekty te zostały ocenione na podstawie przejrzystych i jasno określonych kryteriów. Aktywności edukacyjne prowadzące do uzyskania mikropoświadczeń są opracowywane tak, aby osoba ucząca się zdobyła konkretną wiedzę, umiejętności i kompetencje, które odpowiadają na potrzeby społeczne, osobiste i kulturowe lub na potrzeby rynku pracy. „Mikropoświadczenia są własnością osoby uczącej się i mogą być udostępniane i przenoszone. Mogą być samodzielne lub łączone w większe poświadczenia.”* (pkt 5, lit. a) Zalecenia).

Standard Open Badge 3.0 stanowi adekwatne rozwiązanie dla dopełnienia Europejskich zasad opracowywania i wydawania mikropoświadczeń (stanowiących załącznik II do Zalecenia), w zakresie wymagań przenośności (w kontekście cyfrowej formy mikropoświadczenia i stosowania otwartych standardów i modeli danych: *„Mikropoświadczenia są własnością posiadacza poświadczenia (osoby uczącej się) i mogą być przez niego łatwo przechowywane i udostępniane, w tym za pomocą bezpiecznych portfeli cyfrowych (np. Europass), zgodnie z ogólnym rozporządzeniem o ochronie danych. Infrastruktura do przechowywania danych opiera się na standardach otwartych i modelach danych. Zapewnia to interoperacyjność i bezproblemową wymianę danych oraz pozwala na sprawne sprawdzanie ich autentyczności.”*.

Tym samym system musi dawać indywidualnemu użytkownikowi możliwość swobodnego kumulowania, przenoszenia i udostępniania zdobytych odznak (również poza system), jako że zgodnie z definicją, mikropoświadczenia są własnością osoby uczącej się. Zgodnie z wymaganiami Uznawania i Autentyczności (opisanymi w załączniku II Zalecenia), rozwiązanie musi dostarczać możliwość walidacji mikropoświadczenia w celu zidentyfikowania elementów potwierdzających jego autentyczność.

Załącznik I do Zalecenia określa elementy wchodzące w skład meta danych mikropoświadczenia, które mogą posłużyć do jego autentykacji, takie jak:

- Identyfikacja osoby uczącej się,

- Tytuł mikropoświadczenia,

- Państwo(-wa)/region(y) organu wydającego,

- Organ(y) przyznający(-ce),

- Data wydania,

- Efekty uczenia się.

Powyższy zakres danych jest niezbędnym zakresem informacji zawieranych w ramach poświadczenia.

Standard Open Badge 3.0 opisuje metodę kryptograficznego kodowania tych informacji w formie pliku graficznego (odznaki), która jest przenoszalna i daje możliwość dekodowania informacji za pomocą odpowiedniej infrastruktury do walidacji.

Standard Open Badge 3.0 to otwarty, rozpoznawalny i uznawalny standard cyfrowych odznak, którego kompletną dokumentację techniczną znaleźć można pod adresem: https://www.imsglobal.org/spec/ob/v3p0/#abstract-0.

Platforma powinna realizować funkcjonalności związane z uzyskiwaniem mikropoświadczeń w zakresie:

* zapisywania mikropoświadczeń na indywidualnym koncie użytkownika - na platformie, lub systemach z nią powiązanych i dostępnych dla tego użytkownika w postaci cyfrowego „plecaka / portfela” z odznakami, z dowolnego miejsca na świecie (po zalogowaniu się na konto użytkownika),
* akumulacji mikropoświadczeń na indywidualnym koncie użytkownika - na platformie, lub systemach z nią powiązanych (dotyczy zarówno tych, zdobywanych w ramach realizowanych szkoleń, wspieranych użytkowaniem platformy, jak i osiągnięć zdobytych poza systemem), z możliwością generowania cyfrowego CV użytkownika,
* publikowania mikropoświadczeń - dzielenie się osiągnięciami z poziomu indywidualnego konta użytkownika - na platformie, lub systemów z nią powiązanych, poprzez umieszczanie odnośników do nich na platformach społecznościowych typu LinkedIn, czy Facebook, z dostępem anonimowym (bez konieczności logowania) i z uwzględnieniem ochrony danych osobowych (zgodnie z dyrektywą RODO),
* walidacji mikropoświadczeń – weryfikację autentyczności mikropoświadczenia, na potrzeby jego uznawalności, za pomocą zaimplementowanego w systemie walidatora, dostępnego również dla niezalogowanych użytkowników (np. pracodawcy, chcącego zweryfikować autentyczność osiągnięć potencjalnego pracownika),
* segmentacji mikropoświadczeń – aplikacja umożliwiać będzie uzyskanie dostępu do ścieżek rozwoju zawodowego, generowanych przez algorytm, w oparciu o tematy szkoleń, w których brać będzie udział uczestnik, a w które (pod względem merytorycznym) wpisują się zdobyte mikropoświadczenia,
* funkcjonalności związanych z grywalizacją – realizowanych przynajmniej w postaci zdobywania osiągnięć i porównywania zdobytych mikropoświadczeń i kwalifikacji w ramach rankingu użytkowników systemu.

Wymagania pozafunkcjonalne platformy dydaktycznej:

* 1. Kompatybilność - platforma musi działać na komputerach wyposażonych w systemy operacyjne Windows, Linux oraz macOS oraz na urządzeniach mobilnych z systemami Android i iOS, z założeniem responsywności wyświetlanej zawartości.
  2. Zabezpieczenia - Bezpieczeństwo systemu powinno uwzględniać następujące elementy:
* Uwierzytelnianie i autoryzacja: Wdrożenie silnych mechanizmów uwierzytelniania i autoryzacji, w tym weryfikację i zarządzanie hasłami, aby zapewnić bezpieczeństwo danych użytkowników.
* Segmentacja dostępu: Precyzyjne określenie uprawnień dla każdej roli, aby ograniczyć dostęp do funkcjonalności systemu zgodnie z potrzebami i uprawnieniami.
* Rejestry aktywności: Monitorowanie i rejestrowanie działań użytkowników w systemie dla celów audytowych i bezpieczeństwa.
* Zapomniałem hasła: Funkcja umożliwiająca użytkownikom resetowanie zapomnianego hasła przez e-mail.
* Przesyłanie danych: Wszystkie klucze przesyłane pomiędzy systemami muszą być zaszyfrowane i gwarantować bezpieczeństwo i integralność danych w systemie.
* Limit prób logowania: W celu zapobiegania atakom bruteforce, system powinien ograniczać liczbę nieudanych prób logowania i w razie potrzeby blokować dostęp do konta na określony czas.
* Sesje i wylogowywanie: System powinien zarządzać sesjami użytkowników, umożliwiając im wylogowanie oraz automatycznie kończyć sesję po określonym czasie bezczynności.
  1. Dostępność - Interfejs aplikacji powinien być zgodny z WCAG 2.2 na poziomie A i AA oraz być dostosowany do wyświetlania na urządzeniach o różnej rozdzielczości, w tym mobilnych i odzwierciedlać dobre praktyki RWD projektowania systemów min. w zakresie:

Elastyczne siatki i układy: responsywne siatki, które dostosowują się do różnych rozmiarów ekranu zamiast ustalonych pikseli,

* Elastyczne obrazy i media: obrazy, wideo i inne elementy multimedialne prezentowane w taki sposób, aby były skalowalne,
* Czytelność tekstu: rozmiar tekstu jest czytelny na różnych urządzeniach, w tym urządzeniach mobilnych,
* Optymalizacja funkcji dotykowych: zapewnienie odpowiednio dużych obszarów dotykowych dla elementów interaktywnych, takich jak przyciski i linki, aby ułatwić obsługę na ekranach dotykowych,
* Optymalizacja wydajności: optymalizacja obrazów, minimalizacja kodu CSS i JavaScript, aby elementy ładowały się szybko.
  1. Interoperacyjność - Aplikacja musi spełniać wymóg interoperacyjności, tzn. być otwarta na integrację i być w stanie wymieniać dane z innymi systemami, poprzez odpowiednio skonstruowany interfejs API.
  2. Język - Sfera tekstowa platformy, w tym elementy UI, powinna być zrealizowana w języku polskim.

**Część 2**

**Przeprowadzenie zewnętrznego egzaminu certyfikacyjnego potwierdzającego nabycie kwalifikacji z tematu: „****Zarządzanie relacjami z klientem z wykorzystaniem systemu CRM”.**

Wykonawca przeprowadzi egzamin dla 40 Uczestników Projektu (UP).

Miejsce realizacji egzaminów:

Akademia Nauk Stosowanych Mazovia ul. Sokołowska 161, 08-110 Siedlce

Egzaminy będą realizowane w okresie od podpisania umowy do 31.12.2026 r., od poniedziałku do piątku i w weekendy w godzinach od 8:00 do 20:00, w oparciu o szczegółowy harmonogram zajęć, potwierdzony przez Zamawiającego i przekazany wybranemu oferentowi po podpisaniu umowy.

Sale do realizacji egzaminów zapewnia Zamawiający.

Wykonawca zobowiązany jest do zapewnienia niezbędnego sprzętu oraz materiałów do realizacji egzaminów.

Wykonawca zobowiązany jest do przeprowadzenia walidacji i certyfikacji zgodnej z:

* ustawą z dnia 22 grudnia 2015 r. o Zintegrowanym Systemie Kwalifikacji (t.j. Dz. U. z 2020 r., poz. 226) oraz Obwieszczenia Ministra Rozwoju, Pracy i Technologii z dnia 2021-04-15 r. w sprawie włączenia kwalifikacji rynkowej „Zarządzanie relacjami z klientem z wykorzystaniem systemu CRM” do Zintegrowanego Systemu Kwalifikacji (Monitor Polski z dnia 2021-05-05 r., poz. 421)

Zamawiający zastrzega, że w przypadku tzw. kwalifikacji funkcjonujących (w rozumieniu przepisów ustawy o Zintegrowanym Systemie Kwalifikacji) Zamawiający dopuszcza przeprowadzenie zewnętrznego egzaminu certyfikacyjnego jedynie przez instytucje  i na zasadach wskazanych w Zintegrowanym Rejestrze Kwalifikacji.

Wykonawca zobowiązany jest do wydania certyfikatu każdemu uczestnikowi, który pomyślnie ukończy zewnętrzny egzamin certyfikacyjny. Certyfikat musi spełniać wymagania określone przez Ministerstwo Rozwoju / Ministerstwo  Funduszy i Polityki Regionalnej w odniesieniu do sposobów uzyskiwania i potwierdzania kwalifikacji w ramach projektów współfinansowanych z EFS+ w tzw. „liście sprawdzającej” do weryfikacji czy dokument można uznać za potwierdzający kwalifikację (niewłączoną do Zintegrowanego Systemu Kwalifikacji)/kompetencję na potrzeby mierzenia wskaźników monitorowania EFS+ dot. uzyskiwania kwalifikacji, zgodnie z informacjami przedstawionymi w dokumencie p.n. „Załącznik 2 Podstawowe informacje dotyczące uzyskiwania kwalifikacji w ramach projektów współfinansowanych z EFS+”: https://www.funduszeeuropejskie.gov.pl/strony/o-funduszach/dokumenty/wytyczne-dotyczace-monitorowania-postepu-rzeczowego-realizacji-programow-na-lata-2021-2027/

Wykonawca zobowiązany jest zapewnić każdemu uczestnikowi dostęp do platformy dydaktycznej wraz z materiałami dydaktycznymi w formie cyfrowej.

Wymagania platformy dydaktycznej:

1. Platforma będzie wykorzystywana jako narzędzie wspierające uczestnika w przygotowaniu się do walidacji i certyfikacji kwalifikacji.
2. Platforma ma dawać możliwość udostępniania użytkownikom treści nauczania w formie cyfrowej, udostępniania narzędzi do przystępnej i atrakcyjnej formy utrwalania wiedzy poprzez ćwiczenia interaktywne, narzędzia pracy grupowej oraz możliwości oceny różnych form aktywności przez trenerów.
3. Platforma musi też umożliwiać przyznawanie mikropoświadczeń, w postaci cyfrowych odznak, realizowanych w standardzie Open Badge 3.0 lub równoważnym, za potwierdzenie efektów uczenia się - za pomocą mechanizmów w niej zaimplementowanych, lub poprzez łączenie z innymi systemami poprzez interfejs API. Przez standard równoważny do Open Badge 3.0 Zamawiający uważa standard spełniający warunki opisane w zapytaniu ofertowym.
4. Użytkownikami platformy będą uczestnicy projektu.

Wymagania funkcjonalne platformy dydaktycznej:

1. Start i logowanie się do konta użytkownika – platforma powinna oferować formularz logowania wymagający podania nazwy użytkownika (lub adresu e-mail) i hasła oraz sprawdzać poprawność wprowadzonych danych logowania.
2. Zarządzanie kontem użytkownika powinno uwzględniać możliwość tworzenia profili dla trenerów i uczniów, w tym zarządzanie ich uprawnieniami. Platforma powinna umożliwiać tworzenie grup użytkowników (odpowiadających grupom szkoleniowym), w celu selektywnego udostępniania zawartości merytorycznej (cyfrowy podręcznik, ćwiczenia etc.). Sposób zabezpieczenia systemu opisano w sekcji opisu poświęconej wymaganiom pozafunkcjonalnym.
3. Komunikacja – platforma powinna udostępniać narzędzia do komunikacji między uczestnikami szkoleń oraz między uczestnikami i trenerem, w postaci forum dyskusyjnego, umożliwiającego wymianę myśli i dyskusje na tematy związane z tematyką szkolenia, a także czat, na potrzeby komunikacji w czasie rzeczywistym.
4. Możliwość tworzenia kursów – platforma powinna dawać możliwość łatwego tworzenia i zarządzania kursami, w tym dodawanie treści edukacyjnych, takich jak dokumenty, prezentacje, dźwięk, wideo, itp. Oraz wsparcie dla różnych formatów treści, w tym HTML, PDF, tekst, multimedia.
5. Możliwość tworzenia quizów, ćwiczeń, zadań domowych – platforma powinna dawać osobie prowadzącej szkolenie możliwość dodawania ćwiczeń oraz quizów interaktywnych w popularnych formatach e-learnigowych (HTML5, SCORM), a także innych zadań (w tym opisowych), a także możliwość punktowania i oceny tychże przez trenera.
6. Możliwość tworzenia notatek z zajęć – Użytkownicy powinni mieć możliwość tworzenia notatek z realizowanych zajęć.
7. Wsparcie dla standardów e-learningowych – platforma powinna zapewniać kompatybilność z popularnymi standardami e-learningowymi, takimi jak SCORM czy xAPI (Tin Can), co umożliwia wykorzystanie zewnętrznych materiałów edukacyjnych i śledzenie interakcji z nimi.
8. Repozytorium treści – platforma zapewniać powinna repozytorium treści z możliwością zarządzania tymiż treściami, w kontekście udostępniania materiałów poszczególnym użytkownikom oraz tworzenia z nich ścieżek dydaktycznych. Wykonawca zobowiązany będzie do wypełnienia repozytorium treścią dla szkolenia stanowiącego przedmiot zamówienia.

Dostarczana zawartość powinna uwzględniać przynajmniej:

* podręcznik w formie cyfrowej, który w sposób wyczerpujący omawia wskazany wyżej program szkolenia,
* interaktywną ścieżkę dydaktyczną (umożliwiającą nawigowanie po zagadnieniach merytorycznych danego tematu),
* zestawy ćwiczeń,
* testy kompetencyjne/egzaminy próbne,

Repozytorium powinno również zawierać materiały merytoryczne, pozwalające na zapoznanie się z dostępnymi narzędziami AI (sztucznej inteligencji) pozwalającymi na wykorzystywanie generatywnej AI na potrzeby kwalifikacji stanowiącej przedmiot szkolenia.

1. Możliwość generowania mikropoświadczeń – platforma/system powinien dawać użytkownikom możliwość zdobywania mikropoświadczeń w postaci odznak cyfrowych, realizowanych zgodnie ze standardem Open Badge 3.0, za potwierdzanie efektów kształcenia nabywanych podczas realizacji szkoleń.

Zgodnie z treścią Zalecenia Rady z dnia 22 czerwca 2022 r. w sprawie europejskiego podejścia do mikropoświadczeń na potrzeby uczenia się przez całe życie i zatrudnialności, zaleca się państwom członkowskim przyjęcie i promowanie stosowania definicji mikropoświadczenia, jako: *„opis(u) efektów uczenia się, które osoba ucząca się uzyskała przy niewielkim nakładzie uczenia się. Efekty te zostały ocenione na podstawie przejrzystych i jasno określonych kryteriów. Aktywności edukacyjne prowadzące do uzyskania mikropoświadczeń są opracowywane tak, aby osoba ucząca się zdobyła konkretną wiedzę, umiejętności i kompetencje, które odpowiadają na potrzeby społeczne, osobiste i kulturowe lub na potrzeby rynku pracy. „Mikropoświadczenia są własnością osoby uczącej się i mogą być udostępniane i przenoszone. Mogą być samodzielne lub łączone w większe poświadczenia.”* (pkt 5, lit. a) Zalecenia).

Standard Open Badge 3.0 stanowi adekwatne rozwiązanie dla dopełnienia Europejskich zasad opracowywania i wydawania mikropoświadczeń (stanowiących załącznik II do Zalecenia), w zakresie wymagań przenośności (w kontekście cyfrowej formy mikropoświadczenia i stosowania otwartych standardów i modeli danych: *„Mikropoświadczenia są własnością posiadacza poświadczenia (osoby uczącej się) i mogą być przez niego łatwo przechowywane i udostępniane, w tym za pomocą bezpiecznych portfeli cyfrowych (np. Europass), zgodnie z ogólnym rozporządzeniem o ochronie danych. Infrastruktura do przechowywania danych opiera się na standardach otwartych i modelach danych. Zapewnia to interoperacyjność i bezproblemową wymianę danych oraz pozwala na sprawne sprawdzanie ich autentyczności.”*.

Tym samym system musi dawać indywidualnemu użytkownikowi możliwość swobodnego kumulowania, przenoszenia i udostępniania zdobytych odznak (również poza system), jako że zgodnie z definicją, mikropoświadczenia są własnością osoby uczącej się. Zgodnie z wymaganiami Uznawania i Autentyczności (opisanymi w załączniku II Zalecenia), rozwiązanie musi dostarczać możliwość walidacji mikropoświadczenia w celu zidentyfikowania elementów potwierdzających jego autentyczność.

Załącznik I do Zalecenia określa elementy wchodzące w skład meta danych mikropoświadczenia, które mogą posłużyć do jego autentykacji, takie jak:

- Identyfikacja osoby uczącej się,

- Tytuł mikropoświadczenia,

- Państwo(-wa)/region(y) organu wydającego,

- Organ(y) przyznający(-ce),

- Data wydania,

- Efekty uczenia się.

Powyższy zakres danych jest niezbędnym zakresem informacji zawieranych w ramach poświadczenia.

Standard Open Badge 3.0 opisuje metodę kryptograficznego kodowania tych informacji w formie pliku graficznego (odznaki), która jest przenoszalna i daje możliwość dekodowania informacji za pomocą odpowiedniej infrastruktury do walidacji.

Standard Open Badge 3.0 to otwarty, rozpoznawalny i uznawalny standard cyfrowych odznak, którego kompletną dokumentację techniczną znaleźć można pod adresem: https://www.imsglobal.org/spec/ob/v3p0/#abstract-0.

Platforma powinna realizować funkcjonalności związane z uzyskiwaniem mikropoświadczeń w zakresie:

* zapisywania mikropoświadczeń na indywidualnym koncie użytkownika - na platformie, lub systemach z nią powiązanych i dostępnych dla tego użytkownika w postaci cyfrowego „plecaka / portfela” z odznakami, z dowolnego miejsca na świecie (po zalogowaniu się na konto użytkownika),
* akumulacji mikropoświadczeń na indywidualnym koncie użytkownika - na platformie, lub systemach z nią powiązanych (dotyczy zarówno tych, zdobywanych w ramach realizowanych szkoleń, wspieranych użytkowaniem platformy, jak i osiągnięć zdobytych poza systemem), z możliwością generowania cyfrowego CV użytkownika,
* publikowania mikropoświadczeń - dzielenie się osiągnięciami z poziomu indywidualnego konta użytkownika - na platformie, lub systemów z nią powiązanych, poprzez umieszczanie odnośników do nich na platformach społecznościowych typu LinkedIn, czy Facebook, z dostępem anonimowym (bez konieczności logowania) i z uwzględnieniem ochrony danych osobowych (zgodnie z dyrektywą RODO),
* walidacji mikropoświadczeń – weryfikację autentyczności mikropoświadczenia, na potrzeby jego uznawalności, za pomocą zaimplementowanego w systemie walidatora, dostępnego również dla niezalogowanych użytkowników (np. pracodawcy, chcącego zweryfikować autentyczność osiągnięć potencjalnego pracownika),
* segmentacji mikropoświadczeń – aplikacja umożliwiać będzie uzyskanie dostępu do ścieżek rozwoju zawodowego, generowanych przez algorytm, w oparciu o tematy szkoleń, w których brać będzie udział uczestnik, a w które (pod względem merytorycznym) wpisują się zdobyte mikropoświadczenia,
* funkcjonalności związanych z grywalizacją – realizowanych przynajmniej w postaci zdobywania osiągnięć i porównywania zdobytych mikropoświadczeń i kwalifikacji w ramach rankingu użytkowników systemu.

Wymagania pozafunkcjonalne platformy dydaktycznej:

1. Kompatybilność - platforma musi działać na komputerach wyposażonych w systemy operacyjne Windows, Linux oraz macOS oraz na urządzeniach mobilnych z systemami Android i iOS, z założeniem responsywności wyświetlanej zawartości.
2. Zabezpieczenia - Bezpieczeństwo systemu powinno uwzględniać następujące elementy:

* Uwierzytelnianie i autoryzacja: Wdrożenie silnych mechanizmów uwierzytelniania i autoryzacji, w tym weryfikację i zarządzanie hasłami, aby zapewnić bezpieczeństwo danych użytkowników.
* Segmentacja dostępu: Precyzyjne określenie uprawnień dla każdej roli, aby ograniczyć dostęp do funkcjonalności systemu zgodnie z potrzebami i uprawnieniami.
* Rejestry aktywności: Monitorowanie i rejestrowanie działań użytkowników w systemie dla celów audytowych i bezpieczeństwa.
* Zapomniałem hasła: Funkcja umożliwiająca użytkownikom resetowanie zapomnianego hasła przez e-mail.
* Przesyłanie danych: Wszystkie klucze przesyłane pomiędzy systemami muszą być zaszyfrowane i gwarantować bezpieczeństwo i integralność danych w systemie.
* Limit prób logowania: W celu zapobiegania atakom bruteforce, system powinien ograniczać liczbę nieudanych prób logowania i w razie potrzeby blokować dostęp do konta na określony czas.
* Sesje i wylogowywanie: System powinien zarządzać sesjami użytkowników, umożliwiając im wylogowanie oraz automatycznie kończyć sesję po określonym czasie bezczynności.

1. Dostępność - Interfejs aplikacji powinien być zgodny z WCAG 2.2 na poziomie A i AA oraz być dostosowany do wyświetlania na urządzeniach o różnej rozdzielczości, w tym mobilnych i odzwierciedlać dobre praktyki RWD projektowania systemów min. w zakresie:

Elastyczne siatki i układy: responsywne siatki, które dostosowują się do różnych rozmiarów ekranu zamiast ustalonych pikseli,

* Elastyczne obrazy i media: obrazy, wideo i inne elementy multimedialne prezentowane w taki sposób, aby były skalowalne,
* Czytelność tekstu: rozmiar tekstu jest czytelny na różnych urządzeniach, w tym urządzeniach mobilnych,
* Optymalizacja funkcji dotykowych: zapewnienie odpowiednio dużych obszarów dotykowych dla elementów interaktywnych, takich jak przyciski i linki, aby ułatwić obsługę na ekranach dotykowych,
* Optymalizacja wydajności: optymalizacja obrazów, minimalizacja kodu CSS i JavaScript, aby elementy ładowały się szybko.

1. Interoperacyjność - Aplikacja musi spełniać wymóg interoperacyjności, tzn. być otwarta na integrację i być w stanie wymieniać dane z innymi systemami, poprzez odpowiednio skonstruowany interfejs API.
2. Język - Sfera tekstowa platformy, w tym elementy UI, powinna być zrealizowana w języku polskim.

**Część 3**

**Przeprowadzenie zewnętrznego egzaminu certyfikacyjnego potwierdzającego nabycie kwalifikacji z tematu:** **„Planowanie, tworzenie i dystrybuowanie treści marketingowych (content marketing)”.**

Wykonawca przeprowadzi egzamin dla 30 Uczestników Projektu (UP).

Miejsce realizacji egzaminów:

Akademia Nauk Stosowanych Mazovia ul. Sokołowska 161, 08-110 Siedlce

Egzaminy będą realizowane w okresie od podpisania umowy do 31.12.2026 r., od poniedziałku do piątku i w weekendy w godzinach od 8:00 do 20:00, w oparciu o szczegółowy harmonogram zajęć, potwierdzony przez Zamawiającego i przekazany wybranemu oferentowi po podpisaniu umowy.

Sale do realizacji egzaminów zapewnia Zamawiający.

Wykonawca zobowiązany jest do zapewnienia niezbędnego sprzętu oraz materiałów do realizacji egzaminów.

Wykonawca zobowiązany jest do przeprowadzenia walidacji i certyfikacji zgodnej z:

* ustawą z dnia 22 grudnia 2015 r. o Zintegrowanym Systemie Kwalifikacji (t.j. Dz. U. z 2020 r., poz. 226) oraz obwieszczenia Ministra Przedsiębiorczości i Technologii z dnia 2018-10-23 r. w sprawie włączenia kwalifikacji rynkowej „Planowanie, tworzenie i dystrybuowanie treści marketingowych (content marketing)” do Zintegrowanego Systemu Kwalifikacji (Monitor Polski z dnia 2018-11-08 r., poz. 1090)

Zamawiający zastrzega, że w przypadku tzw. kwalifikacji funkcjonujących (w rozumieniu przepisów ustawy o Zintegrowanym Systemie Kwalifikacji) Zamawiający dopuszcza przeprowadzenie zewnętrznego egzaminu certyfikacyjnego jedynie przez instytucje  i na zasadach wskazanych w Zintegrowanym Rejestrze Kwalifikacji.

Wykonawca zobowiązany jest do wydania certyfikatu każdemu uczestnikowi, który pomyślnie ukończy zewnętrzny egzamin certyfikacyjny. Certyfikat musi spełniać wymagania określone przez Ministerstwo Rozwoju/Ministerstwo  Funduszy i Polityki Regionalnej w odniesieniu do sposobów uzyskiwania i potwierdzania kwalifikacji w ramach projektów współfinansowanych z EFS+ w tzw. „liście sprawdzającej” do weryfikacji czy dokument można uznać za potwierdzający kwalifikację (niewłączoną do Zintegrowanego Systemu Kwalifikacji)/kompetencję na potrzeby mierzenia wskaźników monitorowania EFS+ dot. uzyskiwania kwalifikacji, zgodnie z informacjami przedstawionymi w dokumencie p.n. „Załącznik 2 Podstawowe informacje dotyczące uzyskiwania kwalifikacji w ramach projektów współfinansowanych z EFS+”: https://www.funduszeeuropejskie.gov.pl/strony/o-funduszach/dokumenty/wytyczne-dotyczace-monitorowania-postepu-rzeczowego-realizacji-programow-na-lata-2021-2027/

Wykonawca zobowiązany jest zapewnić każdemu uczestnikowi dostęp do platformy dydaktycznej wraz z materiałami dydaktycznymi w formie cyfrowej.

Wymagania platformy dydaktycznej:

* 1. Platforma będzie wykorzystywana jako narzędzie wspierające uczestnika w przygotowaniu się do walidacji i certyfikacji kwalifikacji.
  2. Platforma ma dawać możliwość udostępniania użytkownikom treści nauczania w formie cyfrowej, udostępniania narzędzi do przystępnej i atrakcyjnej formy utrwalania wiedzy poprzez ćwiczenia interaktywne, narzędzia pracy grupowej oraz możliwości oceny różnych form aktywności przez trenerów.
  3. Platforma musi też umożliwiać przyznawanie mikropoświadczeń, w postaci cyfrowych odznak, realizowanych w standardzie Open Badge 3.0 lub równoważnym, za potwierdzenie efektów uczenia się - za pomocą mechanizmów w niej zaimplementowanych, lub poprzez łączenie z innymi systemami poprzez interfejs API. Przez standard równoważny do Open Badge 3.0 Zamawiający uważa standard spełniający warunki opisane w zapytaniu ofertowym.
  4. Użytkownikami platformy będą uczestnicy projektu.

Wymagania funkcjonalne platformy dydaktycznej:

1. Start i logowanie się do konta użytkownika – platforma powinna oferować formularz logowania wymagający podania nazwy użytkownika (lub adresu e-mail) i hasła oraz sprawdzać poprawność wprowadzonych danych logowania.
2. Zarządzanie kontem użytkownika powinno uwzględniać możliwość tworzenia profili dla trenerów i uczniów, w tym zarządzanie ich uprawnieniami. Platforma powinna umożliwiać tworzenie grup użytkowników (odpowiadających grupom egzam.), w celu selektywnego udostępniania zawartości merytorycznej (cyfrowy podręcznik, ćwiczenia etc.). Sposób zabezpieczenia systemu opisano w sekcji opisu poświęconej wymaganiom pozafunkcjonalnym.
3. Komunikacja – platforma powinna udostępniać narzędzia do komunikacji między uczestnikami szkoleń oraz między uczestnikami i trenerem, w postaci forum dyskusyjnego, umożliwiającego wymianę myśli i dyskusje na tematy związane z tematyką szkolenia, a także czat, na potrzeby komunikacji w czasie rzeczywistym.
4. Możliwość tworzenia kursów – platforma powinna dawać możliwość łatwego tworzenia i zarządzania kursami, w tym dodawanie treści edukacyjnych, takich jak dokumenty, prezentacje, dźwięk, wideo, itp. Oraz wsparcie dla różnych formatów treści, w tym HTML, PDF, tekst, multimedia.
5. Możliwość tworzenia quizów, ćwiczeń, zadań domowych – platforma powinna dawać osobie prowadzącej szkolenie możliwość dodawania ćwiczeń oraz quizów interaktywnych w popularnych formatach e-learnigowych (HTML5, SCORM), a także innych zadań (w tym opisowych), a także możliwość punktowania i oceny tychże przez trenera.
6. Możliwość tworzenia notatek z zajęć – Użytkownicy powinni mieć możliwość tworzenia notatek z realizowanych zajęć.
7. Wsparcie dla standardów e-learningowych – platforma powinna zapewniać kompatybilność z popularnymi standardami e-learningowymi, takimi jak SCORM czy xAPI (Tin Can), co umożliwia wykorzystanie zewnętrznych materiałów edukacyjnych i śledzenie interakcji z nimi.
8. Repozytorium treści – platforma zapewniać powinna repozytorium treści z możliwością zarządzania tymiż treściami, w kontekście udostępniania materiałów poszczególnym użytkownikom oraz tworzenia z nich ścieżek dydaktycznych. Wykonawca zobowiązany będzie do wypełnienia repozytorium treścią dla szkolenia stanowiącego przedmiot zamówienia.

Dostarczana zawartość powinna uwzględniać przynajmniej:

* podręcznik w formie cyfrowej, który w sposób wyczerpujący omawia wskazany wyżej program szkolenia,
* interaktywną ścieżkę dydaktyczną (umożliwiającą nawigowanie po zagadnieniach merytorycznych danego tematu),
* zestawy ćwiczeń,
* testy kompetencyjne/egzaminy próbne,

Repozytorium powinno również zawierać materiały merytoryczne, pozwalające na zapoznanie się z dostępnymi narzędziami AI (sztucznej inteligencji) pozwalającymi na wykorzystywanie generatywnej AI na potrzeby kwalifikacji stanowiącej przedmiot szkolenia.

1. Możliwość generowania mikropoświadczeń – platforma/system powinien dawać użytkownikom możliwość zdobywania mikropoświadczeń w postaci odznak cyfrowych, realizowanych zgodnie ze standardem Open Badge 3.0, za potwierdzanie efektów kształcenia nabywanych podczas realizacji szkoleń.

Zgodnie z treścią Zalecenia Rady z dnia 22 czerwca 2022 r. w sprawie europejskiego podejścia do mikropoświadczeń na potrzeby uczenia się przez całe życie i zatrudnialności, zaleca się państwom członkowskim przyjęcie i promowanie stosowania definicji mikropoświadczenia, jako: *„opis(u) efektów uczenia się, które osoba ucząca się uzyskała przy niewielkim nakładzie uczenia się. Efekty te zostały ocenione na podstawie przejrzystych i jasno określonych kryteriów. Aktywności edukacyjne prowadzące do uzyskania mikropoświadczeń są opracowywane tak, aby osoba ucząca się zdobyła konkretną wiedzę, umiejętności i kompetencje, które odpowiadają na potrzeby społeczne, osobiste i kulturowe lub na potrzeby rynku pracy. „Mikropoświadczenia są własnością osoby uczącej się i mogą być udostępniane i przenoszone. Mogą być samodzielne lub łączone w większe poświadczenia.”* (pkt 5, lit. a) Zalecenia).

Standard Open Badge 3.0 stanowi adekwatne rozwiązanie dla dopełnienia Europejskich zasad opracowywania i wydawania mikropoświadczeń (stanowiących załącznik II do Zalecenia), w zakresie wymagań przenośności (w kontekście cyfrowej formy mikropoświadczenia i stosowania otwartych standardów i modeli danych: *„Mikropoświadczenia są własnością posiadacza poświadczenia (osoby uczącej się) i mogą być przez niego łatwo przechowywane i udostępniane, w tym za pomocą bezpiecznych portfeli cyfrowych (np. Europass), zgodnie z ogólnym rozporządzeniem o ochronie danych. Infrastruktura do przechowywania danych opiera się na standardach otwartych i modelach danych. Zapewnia to interoperacyjność i bezproblemową wymianę danych oraz pozwala na sprawne sprawdzanie ich autentyczności.”*.

Tym samym system musi dawać indywidualnemu użytkownikowi możliwość swobodnego kumulowania, przenoszenia i udostępniania zdobytych odznak (również poza system), jako że zgodnie z definicją, mikropoświadczenia są własnością osoby uczącej się. Zgodnie z wymaganiami Uznawania i Autentyczności (opisanymi w załączniku II Zalecenia), rozwiązanie musi dostarczać możliwość walidacji mikropoświadczenia w celu zidentyfikowania elementów potwierdzających jego autentyczność.

Załącznik I do Zalecenia określa elementy wchodzące w skład meta danych mikropoświadczenia, które mogą posłużyć do jego autentykacji, takie jak:

* Identyfikacja osoby uczącej się,
* Tytuł mikropoświadczenia,
* Państwo(-wa)/region(y) organu wydającego,
* Organ(y) przyznający(-ce),
* Data wydania,
* Efekty uczenia się.

Powyższy zakres danych jest niezbędnym zakresem informacji zawieranych w ramach poświadczenia.

Standard Open Badge 3.0 opisuje metodę kryptograficznego kodowania tych informacji w formie pliku graficznego (odznaki), która jest przenoszalna i daje możliwość dekodowania informacji za pomocą odpowiedniej infrastruktury do walidacji.

Standard Open Badge 3.0 to otwarty, rozpoznawalny i uznawalny standard cyfrowych odznak, którego kompletną dokumentację techniczną znaleźć można pod adresem: https://www.imsglobal.org/spec/ob/v3p0/#abstract-0.

Platforma powinna realizować funkcjonalności związane z uzyskiwaniem mikropoświadczeń w zakresie:

* zapisywania mikropoświadczeń na indywidualnym koncie użytkownika - na platformie, lub systemach z nią powiązanych i dostępnych dla tego użytkownika w postaci cyfrowego „plecaka /portfela” z odznakami, z dowolnego miejsca na świecie (po zalogowaniu się na konto użytkownika),
* akumulacji mikropoświadczeń na indywidualnym koncie użytkownika - na platformie, lub systemach z nią powiązanych (dotyczy zarówno tych, zdobywanych w ramach realizowanych szkoleń, wspieranych użytkowaniem platformy, jak i osiągnięć zdobytych poza systemem), z możliwością generowania cyfrowego CV użytkownika,
* publikowania mikropoświadczeń - dzielenie się osiągnięciami z poziomu indywidualnego konta użytkownika - na platformie, lub systemów z nią powiązanych, poprzez umieszczanie odnośników do nich na platformach społecznościowych typu LinkedIn, czy Facebook, z dostępem anonimowym (bez konieczności logowania) i z uwzględnieniem ochrony danych osobowych (zgodnie z dyrektywą RODO),
* walidacji mikropoświadczeń – weryfikację autentyczności mikropoświadczenia, na potrzeby jego uznawalności, za pomocą zaimplementowanego w systemie walidatora, dostępnego również dla niezalogowanych użytkowników (np. pracodawcy, chcącego zweryfikować autentyczność osiągnięć potencjalnego pracownika),
* segmentacji mikropoświadczeń – aplikacja umożliwiać będzie uzyskanie dostępu do ścieżek rozwoju zawodowego, generowanych przez algorytm, w oparciu o tematy szkoleń, w których brać będzie udział uczestnik, a w które (pod względem merytorycznym) wpisują się zdobyte mikropoświadczenia,
* funkcjonalności związanych z grywalizacją – realizowanych przynajmniej w postaci zdobywania osiągnięć i porównywania zdobytych mikropoświadczeń i kwalifikacji w ramach rankingu użytkowników systemu.

Wymagania pozafunkcjonalne platformy dydaktycznej:

1. Kompatybilność - platforma musi działać na komputerach wyposażonych w systemy operacyjne Windows, Linux oraz macOS oraz na urządzeniach mobilnych z systemami Android i iOS, z założeniem responsywności wyświetlanej zawartości.
2. Zabezpieczenia - Bezpieczeństwo systemu powinno uwzględniać następujące elementy:

* Uwierzytelnianie i autoryzacja: Wdrożenie silnych mechanizmów uwierzytelniania i autoryzacji, w tym weryfikację i zarządzanie hasłami, aby zapewnić bezpieczeństwo danych użytkowników.
* Segmentacja dostępu: Precyzyjne określenie uprawnień dla każdej roli, aby ograniczyć dostęp do funkcjonalności systemu zgodnie z potrzebami i uprawnieniami.
* Rejestry aktywności: Monitorowanie i rejestrowanie działań użytkowników w systemie dla celów audytowych i bezpieczeństwa.
* Zapomniałem hasła: Funkcja umożliwiająca użytkownikom resetowanie zapomnianego hasła przez e-mail.
* Przesyłanie danych: Wszystkie klucze przesyłane pomiędzy systemami muszą być zaszyfrowane i gwarantować bezpieczeństwo i integralność danych w systemie.
* Limit prób logowania: W celu zapobiegania atakom bruteforce, system powinien ograniczać liczbę nieudanych prób logowania i w razie potrzeby blokować dostęp do konta na określony czas.
* Sesje i wylogowywanie: System powinien zarządzać sesjami użytkowników, umożliwiając im wylogowanie oraz automatycznie kończyć sesję po określonym czasie bezczynności.

1. Dostępność - Interfejs aplikacji powinien być zgodny z WCAG 2.2 na poziomie A i AA oraz być dostosowany do wyświetlania na urządzeniach o różnej rozdzielczości, w tym mobilnych i odzwierciedlać dobre praktyki RWD projektowania systemów min. w zakresie:

* Elastyczne siatki i układy: responsywne siatki, które dostosowują się do różnych rozmiarów ekranu zamiast ustalonych pikseli,
* Elastyczne obrazy i media: obrazy, wideo i inne elementy multimedialne prezentowane w taki sposób, aby były skalowalne,
* Czytelność tekstu: rozmiar tekstu jest czytelny na różnych urządzeniach, w tym urządzeniach mobilnych,
* Optymalizacja funkcji dotykowych: zapewnienie odpowiednio dużych obszarów dotykowych dla elementów interaktywnych, takich jak przyciski i linki, aby ułatwić obsługę na ekranach dotykowych,
* Optymalizacja wydajności: optymalizacja obrazów, minimalizacja kodu CSS i JavaScript, aby elementy ładowały się szybko.

1. Interoperacyjność - Aplikacja musi spełniać wymóg interoperacyjności, tzn. być otwarta na integrację i być w stanie wymieniać dane z innymi systemami, poprzez odpowiednio skonstruowany interfejs API.
2. Język - Sfera tekstowa platformy, w tym elementy UI, powinna być zrealizowana w języku polskim.

**Część 4**

**Przeprowadzenie zewnętrznego egzaminu certyfikacyjnego potwierdzającego nabycie kwalifikacji z tematu: „Ochrona danych osobowych”.**

Wykonawca przeprowadzi egzamin dla 40 Uczestników Projektu (UP).

Miejsce realizacji egzaminów:

Akademia Nauk Stosowanych Mazovia ul. Sokołowska 161, 08-110 Siedlce

Egzaminy będą realizowane w okresie od podpisania umowy do 31.12.2026 r., od poniedziałku do piątku i w weekendy w godzinach od 8:00 do 20:00, w oparciu o szczegółowy harmonogram zajęć, potwierdzony przez Zamawiającego i przekazany wybranemu oferentowi po podpisaniu umowy.

Sale do realizacji egzaminów zapewnia Zamawiający.

Wykonawca zobowiązany jest do zapewnienia niezbędnego sprzętu oraz materiałów do realizacji egzaminów.

Wykonawca opracuje/przygotuje, zorganizuje i przeprowadzi zewnętrzny egzamin certyfikacyjny, na podstawie przedstawionego poniżej programu szkolenia:

Wprowadzenie do ochrony danych osobowych:

* Definicje i podstawowe pojęcia związane z ochroną danych osobowych.
* Znaczenie ochrony danych w kontekście nowoczesnych organizacji.
* Przegląd najważniejszych aktów prawnych: RODO, krajowe ustawy.

Zakres zastosowania RODO:

* Kogo dotyczy RODO – zakres podmiotowy i przedmiotowy.
* Rodzaje danych osobowych – dane zwykłe a dane szczególnej kategorii.
* Rola administratora danych i podmiotu przetwarzającego.

Zasady przetwarzania danych osobowych:

* Legalność, rzetelność i przejrzystość przetwarzania.
* Ograniczenie celu, minimalizacja danych, dokładność, ograniczenie przechowywania.
* Poufność i integralność danych.

Prawa osób, których dane dotyczą:

* Prawo do dostępu, sprostowania i usunięcia danych (prawo do bycia zapomnianym).
* Prawo do przenoszenia danych.
* Prawo do sprzeciwu i ograniczenia przetwarzania.
* Prawo do bycia poinformowanym.

Obowiązki administratorów danych:

* Wdrożenie odpowiednich środków technicznych i organizacyjnych.
* Rejestry czynności przetwarzania danych.
* Zgłaszanie naruszeń ochrony danych osobowych.

Ocena skutków dla ochrony danych (DPIA):

* Kiedy konieczna jest ocena skutków dla ochrony danych.
* Jak przeprowadzić DPIA – procedura i praktyczne przykłady.

Współpraca z organem nadzorczym:

* Rola i zadania Prezesa Urzędu Ochrony Danych Osobowych.
* Procedury w przypadku kontroli.

Podstawy prawne przetwarzania danych osobowych:

* Zgoda jako podstawa przetwarzania danych.
* Przetwarzanie na podstawie umowy, obowiązku prawnego, interesu publicznego, prawnie uzasadnionego interesu.

Bezpieczeństwo danych osobowych:

* Środki techniczne i organizacyjne w zakresie ochrony danych.
* Praktyczne przykłady zabezpieczeń danych w firmach i instytucjach.
* Postępowanie w przypadku naruszeń bezpieczeństwa danych.

Praktyczne wdrożenie procedur związanych z ochroną danych osobowych:

* Jak opracować i wdrożyć politykę ochrony danych osobowych.
* Przykłady dokumentów: polityka prywatności, regulaminy, klauzule informacyjne.
* Praktyczne ćwiczenia – jak przygotować organizację na audyt RODO.

Odpowiedzialność za naruszenia ochrony danych osobowych:

* Sankcje administracyjne i finansowe w przypadku naruszenia RODO.
* Odpowiedzialność cywilna i karna.

Wykonawca zobowiązany będzie do zdefiniowania efektów uczenia się co najmniej w zakresie: wiedzy, umiejętności i kompetencji społecznych. Egzamin powinien weryfikować efekty uczenia się co najmniej w zakresie: wiedzy, umiejętności i kompetencji społecznych wynikające z przedstawionego programu szkolenia.

Certyfikat wydany osobom, które pomyślnie zdały egzamin certyfikacyjny winien zawierać w swej treści co najmniej:

* nazwę instytucji certyfikującej (IC),
* imię i nazwisko osoby egzaminowanej,
* nazwę/temat szkolenia i/lub kwalifikacji,
* datę i miejsce wydania,
* pieczęcie i podpisy osób upoważnionych do reprezentowania IC (instytucji certyfikującej).

Do każdego certyfikatu dołączony zostanie suplement, który winien zawierać w swej treści co najmniej:

* nazwę instytucji certyfikującej (IC),
* imię i nazwisko osoby egzaminowanej,
* nazwę/temat szkolenia i/lub kwalifikacji,
* program szkolenia i/lub nabyte efekty uczenia się w zakresie wiedzy, umiejętności i kompetencji społecznych,
* uzyskane wyniki,
* datę i miejsce wydania,
* pieczęcie i podpisy osób upoważnionych do reprezentowania IC (instytucji certyfikującej).

Wykonawca zobowiązany jest do wydania certyfikatu każdemu uczestnikowi, który pomyślnie ukończy zewnętrzny egzamin certyfikacyjny. Certyfikat musi spełniać wymagania określone przez Ministerstwo Rozwoju / Ministerstwo  Funduszy i Polityki Regionalnej w odniesieniu do sposobów uzyskiwania i potwierdzania kwalifikacji w ramach projektów współfinansowanych z EFS+ w tzw. „liście sprawdzającej” do weryfikacji czy dokument można uznać za potwierdzający kwalifikację (niewłączoną do Zintegrowanego Systemu Kwalifikacji)/kompetencję na potrzeby mierzenia wskaźników monitorowania EFS+ dot. uzyskiwania kwalifikacji, zgodnie z informacjami przedstawionymi w dokumencie p.n. „Załącznik 2 Podstawowe informacje dotyczące uzyskiwania kwalifikacji w ramach projektów współfinansowanych z EFS+”: https://www.funduszeeuropejskie.gov.pl/strony/o-funduszach/dokumenty/wytyczne-dotyczace-monitorowania-postepu-rzeczowego-realizacji-programow-na-lata-2021-2027/

Wykonawca zobowiązany jest zapewnić każdemu uczestnikowi dostęp do platformy dydaktycznej wraz z materiałami dydaktycznymi w formie cyfrowej.

Wymagania platformy dydaktycznej:

1. Platforma będzie wykorzystywana jako narzędzie wspierające uczestnika w przygotowaniu się do walidacji i certyfikacji kwalifikacji.
2. Platforma ma dawać możliwość udostępniania użytkownikom treści nauczania w formie cyfrowej, udostępniania narzędzi do przystępnej i atrakcyjnej formy utrwalania wiedzy poprzez ćwiczenia interaktywne, narzędzia pracy grupowej oraz możliwości oceny różnych form aktywności przez trenerów.
3. Platforma musi też umożliwiać przyznawanie mikropoświadczeń, w postaci cyfrowych odznak, realizowanych w standardzie Open Badge 3.0 lub równoważnym, za potwierdzenie efektów uczenia się - za pomocą mechanizmów w niej zaimplementowanych, lub poprzez łączenie z innymi systemami poprzez interfejs API. Przez standard równoważny do Open Badge 3.0 Zamawiający uważa standard spełniający warunki opisane w zapytaniu ofertowym.
4. Użytkownikami platformy będą uczestnicy projektu.

Wymagania funkcjonalne platformy dydaktycznej:

1. Start i logowanie się do konta użytkownika – platforma powinna oferować formularz logowania wymagający podania nazwy użytkownika (lub adresu e-mail) i hasła oraz sprawdzać poprawność wprowadzonych danych logowania.
2. Zarządzanie kontem użytkownika powinno uwzględniać możliwość tworzenia profili dla trenerów i uczniów, w tym zarządzanie ich uprawnieniami. Platforma powinna umożliwiać tworzenie grup użytkowników (odpowiadających grupom szkoleniowym), w celu selektywnego udostępniania zawartości merytorycznej (cyfrowy podręcznik, ćwiczenia etc.). Sposób zabezpieczenia systemu opisano w sekcji opisu poświęconej wymaganiom pozafunkcjonalnym.
3. Komunikacja – platforma powinna udostępniać narzędzia do komunikacji między uczestnikami szkoleń oraz między uczestnikami i trenerem, w postaci forum dyskusyjnego, umożliwiającego wymianę myśli i dyskusje na tematy związane z tematyką szkolenia, a także czat, na potrzeby komunikacji w czasie rzeczywistym.
4. Możliwość tworzenia kursów – platforma powinna dawać możliwość łatwego tworzenia i zarządzania kursami, w tym dodawanie treści edukacyjnych, takich jak dokumenty, prezentacje, dźwięk, wideo, itp. Oraz wsparcie dla różnych formatów treści, w tym HTML, PDF, tekst, multimedia.
5. Możliwość tworzenia quizów, ćwiczeń, zadań domowych – platforma powinna dawać osobie prowadzącej szkolenie możliwość dodawania ćwiczeń oraz quizów interaktywnych w popularnych formatach e-learnigowych (HTML5, SCORM), a także innych zadań (w tym opisowych), a także możliwość punktowania i oceny tychże przez trenera.
6. Możliwość tworzenia notatek z zajęć – Użytkownicy powinni mieć możliwość tworzenia notatek z realizowanych zajęć.
7. Wsparcie dla standardów e-learningowych – platforma powinna zapewniać kompatybilność z popularnymi standardami e-learningowymi, takimi jak SCORM czy xAPI (Tin Can), co umożliwia wykorzystanie zewnętrznych materiałów edukacyjnych i śledzenie interakcji z nimi.
8. Repozytorium treści – platforma zapewniać powinna repozytorium treści z możliwością zarządzania tymiż treściami, w kontekście udostępniania materiałów poszczególnym użytkownikom oraz tworzenia z nich ścieżek dydaktycznych. Wykonawca zobowiązany będzie do wypełnienia repozytorium treścią dla szkolenia stanowiącego przedmiot zamówienia.

Dostarczana zawartość powinna uwzględniać przynajmniej:

* podręcznik w formie cyfrowej, który w sposób wyczerpujący omawia wskazany wyżej program szkolenia,
* interaktywną ścieżkę dydaktyczną (umożliwiającą nawigowanie po zagadnieniach merytorycznych danego tematu),
* zestawy ćwiczeń,
* testy kompetencyjne/egzaminy próbne,

Repozytorium powinno również zawierać materiały merytoryczne, pozwalające na zapoznanie się z dostępnymi narzędziami AI (sztucznej inteligencji) pozwalającymi na wykorzystywanie generatywnej AI na potrzeby kwalifikacji stanowiącej przedmiot szkolenia.

1. Możliwość generowania mikropoświadczeń – platforma/system powinien dawać użytkownikom możliwość zdobywania mikropoświadczeń w postaci odznak cyfrowych, realizowanych zgodnie ze standardem Open Badge 3.0, za potwierdzanie efektów kształcenia nabywanych podczas realizacji szkoleń.

Zgodnie z treścią Zalecenia Rady z dnia 22 czerwca 2022 r. w sprawie europejskiego podejścia do mikropoświadczeń na potrzeby uczenia się przez całe życie i zatrudnialności, zaleca się państwom członkowskim przyjęcie i promowanie stosowania definicji mikropoświadczenia, jako: *„opis(u) efektów uczenia się, które osoba ucząca się uzyskała przy niewielkim nakładzie uczenia się. Efekty te zostały ocenione na podstawie przejrzystych i jasno określonych kryteriów. Aktywności edukacyjne prowadzące do uzyskania mikropoświadczeń są opracowywane tak, aby osoba ucząca się zdobyła konkretną wiedzę, umiejętności i kompetencje, które odpowiadają na potrzeby społeczne, osobiste i kulturowe lub na potrzeby rynku pracy. „Mikropoświadczenia są własnością osoby uczącej się i mogą być udostępniane i przenoszone. Mogą być samodzielne lub łączone w większe poświadczenia.”* (pkt 5, lit. a) Zalecenia).

Standard Open Badge 3.0 stanowi adekwatne rozwiązanie dla dopełnienia Europejskich zasad opracowywania i wydawania mikropoświadczeń (stanowiących załącznik II do Zalecenia), w zakresie wymagań przenośności (w kontekście cyfrowej formy mikropoświadczenia i stosowania otwartych standardów i modeli danych: *„Mikropoświadczenia są własnością posiadacza poświadczenia (osoby uczącej się) i mogą być przez niego łatwo przechowywane i udostępniane, w tym za pomocą bezpiecznych portfeli cyfrowych (np. Europass), zgodnie z ogólnym rozporządzeniem o ochronie danych. Infrastruktura do przechowywania danych opiera się na standardach otwartych i modelach danych. Zapewnia to interoperacyjność i bezproblemową wymianę danych oraz pozwala na sprawne sprawdzanie ich autentyczności.”*.

Tym samym system musi dawać indywidualnemu użytkownikowi możliwość swobodnego kumulowania, przenoszenia i udostępniania zdobytych odznak (również poza system), jako że zgodnie z definicją, mikropoświadczenia są własnością osoby uczącej się. Zgodnie z wymaganiami Uznawania i Autentyczności (opisanymi w załączniku II Zalecenia), rozwiązanie musi dostarczać możliwość walidacji mikropoświadczenia w celu zidentyfikowania elementów potwierdzających jego autentyczność.

Załącznik I do Zalecenia określa elementy wchodzące w skład meta danych mikropoświadczenia, które mogą posłużyć do jego autentykacji, takie jak:

- Identyfikacja osoby uczącej się,

- Tytuł mikropoświadczenia,

- Państwo(-wa)/region(y) organu wydającego,

- Organ(y) przyznający(-ce),

- Data wydania,

- Efekty uczenia się.

Powyższy zakres danych jest niezbędnym zakresem informacji zawieranych w ramach poświadczenia.

Standard Open Badge 3.0 opisuje metodę kryptograficznego kodowania tych informacji w formie pliku graficznego (odznaki), która jest przenoszalna i daje możliwość dekodowania informacji za pomocą odpowiedniej infrastruktury do walidacji.

Standard Open Badge 3.0 to otwarty, rozpoznawalny i uznawalny standard cyfrowych odznak, którego kompletną dokumentację techniczną znaleźć można pod adresem: https://www.imsglobal.org/spec/ob/v3p0/#abstract-0.

Platforma powinna realizować funkcjonalności związane z uzyskiwaniem mikropoświadczeń w zakresie:

* zapisywania mikropoświadczeń na indywidualnym koncie użytkownika - na platformie, lub systemach z nią powiązanych i dostępnych dla tego użytkownika w postaci cyfrowego „plecaka / portfela” z odznakami, z dowolnego miejsca na świecie (po zalogowaniu się na konto użytkownika),
* akumulacji mikropoświadczeń na indywidualnym koncie użytkownika - na platformie, lub systemach z nią powiązanych (dotyczy zarówno tych, zdobywanych w ramach realizowanych szkoleń, wspieranych użytkowaniem platformy, jak i osiągnięć zdobytych poza systemem), z możliwością generowania cyfrowego CV użytkownika,
* publikowania mikropoświadczeń - dzielenie się osiągnięciami z poziomu indywidualnego konta użytkownika - na platformie, lub systemów z nią powiązanych, poprzez umieszczanie odnośników do nich na platformach społecznościowych typu LinkedIn, czy
* Facebook, z dostępem anonimowym (bez konieczności logowania) i z uwzględnieniem ochrony danych osobowych (zgodnie z dyrektywą RODO),
* walidacji mikropoświadczeń – weryfikację autentyczności mikropoświadczenia, na potrzeby jego uznawalności, za pomocą zaimplementowanego w systemie walidatora, dostępnego również dla niezalogowanych użytkowników (np. pracodawcy, chcącego zweryfikować autentyczność osiągnięć potencjalnego pracownika),
* segmentacji mikropoświadczeń – aplikacja umożliwiać będzie uzyskanie dostępu do ścieżek rozwoju zawodowego, generowanych przez algorytm, w oparciu o tematy szkoleń, w których brać będzie udział uczestnik, a w które (pod względem merytorycznym)
* wpisują się zdobyte mikropoświadczenia,
* funkcjonalności związanych z grywalizacją – realizowanych przynajmniej w postaci zdobywania osiągnięć i porównywania zdobytych mikropoświadczeń i kwalifikacji w ramach rankingu użytkowników systemu.

Wymagania pozafunkcjonalne platformy dydaktycznej:

1. Kompatybilność - platforma musi działać na komputerach wyposażonych w systemy operacyjne Windows, Linux oraz macOS oraz na urządzeniach mobilnych z systemami Android i iOS, z założeniem responsywności wyświetlanej zawartości.
2. Zabezpieczenia - Bezpieczeństwo systemu powinno uwzględniać następujące elementy:

* Uwierzytelnianie i autoryzacja: Wdrożenie silnych mechanizmów uwierzytelniania i autoryzacji, w tym weryfikację i zarządzanie hasłami, aby zapewnić bezpieczeństwo danych użytkowników.
* Segmentacja dostępu: Precyzyjne określenie uprawnień dla każdej roli, aby ograniczyć dostęp do funkcjonalności systemu zgodnie z potrzebami i uprawnieniami.
* Rejestry aktywności: Monitorowanie i rejestrowanie działań użytkowników w systemie dla celów audytowych i bezpieczeństwa.
* Zapomniałem hasła: Funkcja umożliwiająca użytkownikom resetowanie zapomnianego hasła przez e-mail.
* Przesyłanie danych: Wszystkie klucze przesyłane pomiędzy systemami muszą być zaszyfrowane i gwarantować bezpieczeństwo i integralność danych w systemie.
* Limit prób logowania: W celu zapobiegania atakom bruteforce, system powinien ograniczać liczbę nieudanych prób logowania i w razie potrzeby blokować dostęp do konta na określony czas.
* Sesje i wylogowywanie: System powinien zarządzać sesjami użytkowników, umożliwiając im wylogowanie oraz automatycznie kończyć sesję po określonym czasie bezczynności.

1. Dostępność - Interfejs aplikacji powinien być zgodny z WCAG 2.2 na poziomie A i AA oraz być dostosowany do wyświetlania na urządzeniach o różnej rozdzielczości, w tym mobilnych i odzwierciedlać dobre praktyki RWD projektowania systemów min. w zakresie:

* Elastyczne siatki i układy: responsywne siatki, które dostosowują się do różnych rozmiarów ekranu zamiast ustalonych pikseli,
* Elastyczne obrazy i media: obrazy, wideo i inne elementy multimedialne prezentowane w taki sposób, aby były skalowalne,
* Czytelność tekstu: rozmiar tekstu jest czytelny na różnych urządzeniach, w tym urządzeniach mobilnych,
* Optymalizacja funkcji dotykowych: zapewnienie odpowiednio dużych obszarów dotykowych dla elementów interaktywnych, takich jak przyciski i linki, aby ułatwić obsługę na ekranach dotykowych,
* Optymalizacja wydajności: optymalizacja obrazów, minimalizacja kodu CSS i JavaScript, aby elementy ładowały się szybko.

1. Interoperacyjność - Aplikacja musi spełniać wymóg interoperacyjności, tzn. być otwarta na integrację i być w stanie wymieniać dane z innymi systemami, poprzez odpowiednio skonstruowany interfejs API.
2. Język - Sfera tekstowa platformy, w tym elementy UI, powinna być zrealizowana w języku polskim.

**Część 5**

**Przeprowadzenie zewnętrznego egzaminu certyfikacyjnego potwierdzającego nabycie kwalifikacji z tematu:** **„Zarządzanie zrównoważonym rozwojem miasta w kontekście Smart City”.**

Wykonawca przeprowadzi egzamin dla 30 Uczestników Projektu (UP).

Miejsce realizacji egzaminów:

Akademia Nauk Stosowanych Mazovia ul. Sokołowska 161, 08-110 Siedlce

Egzaminy będą realizowane w okresie od podpisania umowy do 31.12.2026 r., od poniedziałku do piątku i w weekendy w godzinach od 8:00 do 20:00, w oparciu o szczegółowy harmonogram zajęć, potwierdzony przez Zamawiającego i przekazany wybranemu oferentowi po podpisaniu umowy.

Sale do realizacji egzaminów zapewnia Zamawiający.

Wykonawca zobowiązany jest do zapewnienia niezbędnego sprzętu oraz materiałów do realizacji egzaminów.

Wykonawca opracuje/przygotuje, zorganizuje i przeprowadzi zewnętrzny egzamin certyfikacyjny, na podstawie przedstawionego poniżej programu szkolenia:

1. Geneza koncepcji zrównoważonego rozwoju;
2. Kryzys ekologiczny lat 60. XX wieku
3. Raporty dla Klubu Rzymskiego;
4. Raport Brundtland;
5. Szczyt Ziemi  w Rio (1992) – założenia Agendy 21;
6. Implementacyjny plan działań  z Johannesburga (2002) Przyszłość jakiej chcemy;
7. Nowa Agenda na rzecz Zrównoważonego Rozwoju do 2030 roku
8. Podstawy zrównoważonego rozwoju miasta;
9. Aksjologia zrównoważonego rozwoju;
10. Ład zintegrowany
11. Idea Smart City;
12. Definicje i obszary smart;
13. Wdrażanie koncepcji Smart City;
14. Pokonywanie barier w procesie wdrażania Smary City przykłady
15. Zarządzanie smart wspólnotą – wybrane aspekty;
16. Zarządzanie przez rezultaty;
17. Budżet zadaniowy, kontrola zarządcza Partycypacja społeczna;
18. E-administracja;
19. Systemy informatyczne w JST
20. Mieszkańcy gminy –  jako czynnik zrównoważonego rozwoju Smart City;
21. Kapitał ludzki;
22. Kapitał społeczny;
23. Kapitał kreatywny;
24. Innowacje społeczne;
25. Koncepcja łańcucha wartości dodanej w sektorze edukacji
26. Budowanie partnerstw z wykorzystaniem teorii interesariuszy.
27. Edukacja dla zrównoważonego rozwoju;
28. Edukacja dla bezpieczeństwa i kształtowanie kultury bezpieczeństwa;
29. Edukacja dla demokracji;
30. Edukacja ekologiczna i kształtowanie świadomości i kultury ekologicznej;
31. Dziedzictwo kulturowe i jego ochrona dla zrównoważonego rozwoju;
32. Kształtowanie kompetencji społeczeństwa przyszłości w perspektywie rozwoju przemysłu 4.0 i społeczeństwa 4.0
33. Monitorowanie, planowanie i prognozowanie zrównoważonego rozwoju miasta;
34. Metody i narzędzia;
35. Wskaźniki;
36. Zarządzanie ryzykiem

Wykonawca zobowiązany będzie do zdefiniowania efektów uczenia się co najmniej w zakresie: wiedzy, umiejętności i kompetencji społecznych. Egzamin powinien weryfikować efekty uczenia się co najmniej w zakresie: wiedzy, umiejętności i kompetencji społecznych wynikające z przedstawionego programu szkolenia.

Certyfikat wydany osobom, które pomyślnie zdały egzamin certyfikacyjny winien zawierać w swej treści co najmniej:

* nazwę instytucji certyfikującej (IC),
* imię i nazwisko osoby egzaminowanej,
* nazwę/temat szkolenia i/lub kwalifikacji,
* datę i miejsce wydania,
* pieczęcie i podpisy osób upoważnionych do reprezentowania IC (instytucji certyfikującej).

Do każdego certyfikatu dołączony zostanie suplement, który winien zawierać w swej treści co najmniej:

* nazwę instytucji certyfikującej (IC),
* imię i nazwisko osoby egzaminowanej,
* nazwę/temat szkolenia i/lub kwalifikacji,
* program szkolenia i/lub nabyte efekty uczenia się w zakresie wiedzy, umiejętności i kompetencji społecznych,
* uzyskane wyniki,
* datę i miejsce wydania,
* pieczęcie i podpisy osób upoważnionych do reprezentowania IC (instytucji certyfikującej).

Wykonawca zobowiązany jest do wydania certyfikatu każdemu uczestnikowi, który pomyślnie ukończy zewnętrzny egzamin certyfikacyjny. Certyfikat musi spełniać wymagania określone przez Ministerstwo Rozwoju / Ministerstwo  Funduszy i Polityki Regionalnej w odniesieniu do sposobów uzyskiwania i potwierdzania kwalifikacji w ramach projektów współfinansowanych z EFS+ w tzw. „liście sprawdzającej” do weryfikacji czy dokument można uznać za potwierdzający kwalifikację (niewłączoną do Zintegrowanego Systemu Kwalifikacji)/kompetencję na potrzeby mierzenia wskaźników monitorowania EFS+ dot. uzyskiwania kwalifikacji, zgodnie z informacjami przedstawionymi w dokumencie p.n. „Załącznik 2 Podstawowe informacje dotyczące uzyskiwania kwalifikacji w ramach projektów współfinansowanych z EFS+”: https://www.funduszeeuropejskie.gov.pl/strony/o-funduszach/dokumenty/wytyczne-dotyczace-monitorowania- postepu-rzeczowego-realizacji-programow-na-lata-2021-2027/

Wykonawca zobowiązany jest zapewnić każdemu uczestnikowi dostęp do platformy dydaktycznej wraz z materiałami dydaktycznymi w formie cyfrowej.

Wymagania platformy dydaktycznej:

* 1. Platforma będzie wykorzystywana jako narzędzie wspierające uczestnika w przygotowaniu się do walidacji i certyfikacji kwalifikacji.
  2. Platforma ma dawać możliwość udostępniania użytkownikom treści nauczania w formie cyfrowej, udostępniania narzędzi do przystępnej i atrakcyjnej formy utrwalania wiedzy poprzez ćwiczenia interaktywne, narzędzia pracy grupowej oraz możliwości oceny różnych form aktywności przez trenerów.
  3. Platforma musi też umożliwiać przyznawanie mikropoświadczeń, w postaci cyfrowych odznak, realizowanych w standardzie Open Badge 3.0 lub równoważnym, za potwierdzenie efektów uczenia się - za pomocą mechanizmów w niej zaimplementowanych, lub poprzez łączenie z innymi systemami poprzez interfejs API. Przez standard równoważny do Open Badge 3.0 Zamawiający uważa standard spełniający warunki opisane w zapytaniu ofertowym.
  4. Użytkownikami platformy będą uczestnicy projektu.

Wymagania funkcjonalne platformy dydaktycznej:

1. Start i logowanie się do konta użytkownika – platforma powinna oferować formularz logowania wymagający podania nazwy użytkownika (lub adresu e-mail) i hasła oraz sprawdzać poprawność wprowadzonych danych logowania.
2. Zarządzanie kontem użytkownika powinno uwzględniać możliwość tworzenia profili dla trenerów i uczniów, w tym zarządzanie ich uprawnieniami. Platforma powinna umożliwiać tworzenie grup użytkowników (odpowiadających grupom szkoleniowym), w celu selektywnego udostępniania zawartości merytorycznej (cyfrowy podręcznik, ćwiczenia etc.). Sposób zabezpieczenia systemu opisano w sekcji opisu poświęconej wymaganiom pozafunkcjonalnym.
3. Komunikacja – platforma powinna udostępniać narzędzia do komunikacji między uczestnikami szkoleń oraz między uczestnikami i trenerem, w postaci forum dyskusyjnego, umożliwiającego wymianę myśli i dyskusje na tematy związane z tematyką szkolenia, a także czat, na potrzeby komunikacji w czasie rzeczywistym.
4. Możliwość tworzenia kursów – platforma powinna dawać możliwość łatwego tworzenia i zarządzania kursami, w tym dodawanie treści edukacyjnych, takich jak dokumenty, prezentacje, dźwięk, wideo, itp. Oraz wsparcie dla różnych formatów treści, w tym HTML, PDF, tekst, multimedia.
5. Możliwość tworzenia quizów, ćwiczeń, zadań domowych – platforma powinna dawać osobie prowadzącej szkolenie możliwość dodawania ćwiczeń oraz quizów interaktywnych w popularnych formatach e-learnigowych (HTML5, SCORM), a także innych zadań (w tym opisowych), a także możliwość punktowania i oceny tychże przez trenera.
6. Możliwość tworzenia notatek z zajęć – Użytkownicy powinni mieć możliwość tworzenia notatek z realizowanych zajęć.
7. Wsparcie dla standardów e-learningowych – platforma powinna zapewniać kompatybilność z popularnymi standardami e-learningowymi, takimi jak SCORM czy xAPI (Tin Can), co umożliwia wykorzystanie zewnętrznych materiałów edukacyjnych i śledzenie interakcji z nimi.
8. Repozytorium treści – platforma zapewniać powinna repozytorium treści z możliwością zarządzania tymiż treściami, w kontekście udostępniania materiałów poszczególnym użytkownikom oraz tworzenia z nich ścieżek dydaktycznych. Wykonawca zobowiązany będzie do wypełnienia repozytorium treścią dla szkolenia stanowiącego przedmiot zamówienia.

Dostarczana zawartość powinna uwzględniać przynajmniej:

* podręcznik w formie cyfrowej, który w sposób wyczerpujący omawia wskazany wyżej program szkolenia,
* interaktywną ścieżkę dydaktyczną (umożliwiającą nawigowanie po zagadnieniach merytorycznych danego tematu),
* zestawy ćwiczeń,
* testy kompetencyjne/egzaminy próbne,

Repozytorium powinno również zawierać materiały merytoryczne, pozwalające na zapoznanie się z dostępnymi narzędziami AI (sztucznej inteligencji) pozwalającymi na wykorzystywanie generatywnej AI na potrzeby kwalifikacji stanowiącej przedmiot szkolenia.

1. Możliwość generowania mikropoświadczeń – platforma/system powinien dawać użytkownikom możliwość zdobywania mikropoświadczeń w postaci odznak cyfrowych, realizowanych zgodnie ze standardem Open Badge 3.0, za potwierdzanie efektów kształcenia nabywanych podczas realizacji szkoleń.

Zgodnie z treścią Zalecenia Rady z dnia 22 czerwca 2022 r. w sprawie europejskiego podejścia do mikropoświadczeń na potrzeby uczenia się przez całe życie i zatrudnialności, zaleca się państwom członkowskim przyjęcie i promowanie stosowania definicji mikropoświadczenia, jako: *„opis(u) efektów uczenia się, które osoba ucząca się uzyskała przy niewielkim nakładzie uczenia się. Efekty te zostały ocenione na podstawie przejrzystych i jasno określonych kryteriów. Aktywności edukacyjne prowadzące do uzyskania mikropoświadczeń są opracowywane tak, aby osoba ucząca się zdobyła konkretną wiedzę, umiejętności i kompetencje, które odpowiadają na potrzeby społeczne, osobiste i kulturowe lub na potrzeby rynku pracy. „Mikropoświadczenia są własnością osoby uczącej się i mogą być udostępniane i przenoszone. Mogą być samodzielne lub łączone w większe poświadczenia.”* (pkt 5, lit. a) Zalecenia).

Standard Open Badge 3.0 stanowi adekwatne rozwiązanie dla dopełnienia Europejskich zasad opracowywania i wydawania mikropoświadczeń (stanowiących załącznik II do Zalecenia), w zakresie wymagań przenośności (w kontekście cyfrowej formy mikropoświadczenia i stosowania otwartych standardów i modeli danych: *„Mikropoświadczenia są własnością posiadacza poświadczenia (osoby uczącej się) i mogą być przez niego łatwo przechowywane i udostępniane, w tym za pomocą bezpiecznych portfeli cyfrowych (np. Europass), zgodnie z ogólnym rozporządzeniem o ochronie danych. Infrastruktura do przechowywania danych opiera się na standardach otwartych i modelach danych. Zapewnia to interoperacyjność i bezproblemową wymianę danych oraz pozwala na sprawne sprawdzanie ich autentyczności.”*.

Tym samym system musi dawać indywidualnemu użytkownikowi możliwość swobodnego kumulowania, przenoszenia i udostępniania zdobytych odznak (również poza system), jako że zgodnie z definicją, mikropoświadczenia są własnością osoby uczącej się. Zgodnie z wymaganiami Uznawania i Autentyczności (opisanymi w załączniku II Zalecenia), rozwiązanie musi dostarczać możliwość walidacji mikropoświadczenia w celu zidentyfikowania elementów potwierdzających jego autentyczność.

Załącznik I do Zalecenia określa elementy wchodzące w skład meta danych mikropoświadczenia, które mogą posłużyć do jego autentykacji, takie jak:

* Identyfikacja osoby uczącej się,
* Tytuł mikropoświadczenia,
* Państwo(-wa)/region(y) organu wydającego,
* Organ(y) przyznający(-ce),
* Data wydania,
* Efekty uczenia się.

Powyższy zakres danych jest niezbędnym zakresem informacji zawieranych w ramach poświadczenia.

Standard Open Badge 3.0 opisuje metodę kryptograficznego kodowania tych informacji w formie pliku graficznego (odznaki), która jest przenoszalna i daje możliwość dekodowania informacji za pomocą odpowiedniej infrastruktury do walidacji.

Standard Open Badge 3.0 to otwarty, rozpoznawalny i uznawalny standard cyfrowych odznak, którego kompletną dokumentację techniczną znaleźć można pod adresem: https://www.imsglobal.org/spec/ob/v3p0/#abstract-0.

Platforma powinna realizować funkcjonalności związane z uzyskiwaniem mikropoświadczeń w zakresie:

* zapisywania mikropoświadczeń na indywidualnym koncie użytkownika - na platformie, lub systemach z nią powiązanych i dostępnych dla tego użytkownika w postaci cyfrowego „plecaka / portfela”  z odznakami, z dowolnego miejsca na świecie (po zalogowaniu się na konto użytkownika),
* akumulacji mikropoświadczeń na indywidualnym koncie użytkownika - na platformie, lub systemach z nią powiązanych (dotyczy zarówno tych, zdobywanych w ramach realizowanych szkoleń, wspieranych użytkowaniem platformy, jak i osiągnięć zdobytych poza systemem), z możliwością generowania cyfrowego CV użytkownika,
* publikowania mikropoświadczeń - dzielenie się osiągnięciami z poziomu indywidualnego konta użytkownika - na platformie, lub systemów z nią powiązanych, poprzez umieszczanie odnośników do nich na platformach społecznościowych typu LinkedIn, czy
* Facebook, z dostępem anonimowym (bez konieczności logowania) i z uwzględnieniem ochrony danych osobowych (zgodnie z dyrektywą RODO),
* walidacji mikropoświadczeń – weryfikację autentyczności mikropoświadczenia, na potrzeby jego uznawalności, za pomocą zaimplementowanego w systemie walidatora, dostępnego również dla niezalogowanych użytkowników (np. pracodawcy, chcącego zweryfikować autentyczność osiągnięć potencjalnego pracownika),
* segmentacji mikropoświadczeń – aplikacja umożliwiać będzie uzyskanie dostępu do ścieżek rozwoju zawodowego, generowanych przez algorytm, w oparciu o tematy szkoleń, w których brać będzie udział uczestnik, a w które (pod względem merytorycznym) wpisują się zdobyte mikropoświadczenia,
* funkcjonalności związanych z grywalizacją – realizowanych przynajmniej w postaci zdobywania osiągnięć i porównywania zdobytych mikropoświadczeń i kwalifikacji w ramach rankingu użytkowników systemu.

Wymagania pozafunkcjonalne platformy dydaktycznej:

1. Kompatybilność - platforma musi działać na komputerach wyposażonych w systemy operacyjne Windows, Linux oraz macOS oraz na urządzeniach mobilnych z systemami Android i iOS, z założeniem responsywności wyświetlanej zawartości.
2. Zabezpieczenia - Bezpieczeństwo systemu powinno uwzględniać następujące elementy:

* Uwierzytelnianie i autoryzacja: Wdrożenie silnych mechanizmów uwierzytelniania i autoryzacji, w tym weryfikację i zarządzanie hasłami, aby zapewnić bezpieczeństwo danych użytkowników.
* Segmentacja dostępu: Precyzyjne określenie uprawnień dla każdej roli, aby ograniczyć dostęp do funkcjonalności systemu zgodnie z potrzebami i uprawnieniami.
* Rejestry aktywności: Monitorowanie i rejestrowanie działań użytkowników w systemie dla celów audytowych i bezpieczeństwa.
* Zapomniałem hasła: Funkcja umożliwiająca użytkownikom resetowanie zapomnianego hasła przez e-mail.
* Przesyłanie danych: Wszystkie klucze przesyłane pomiędzy systemami muszą być zaszyfrowane i gwarantować bezpieczeństwo i integralność danych w systemie.
* Limit prób logowania: W celu zapobiegania atakom bruteforce, system powinien ograniczać liczbę nieudanych prób logowania i w razie potrzeby blokować dostęp do konta na określony czas.
* Sesje i wylogowywanie: System powinien zarządzać sesjami użytkowników, umożliwiając im wylogowanie oraz automatycznie kończyć sesję po określonym czasie bezczynności.

1. Dostępność - Interfejs aplikacji powinien być zgodny z WCAG 2.2 na poziomie A i AA oraz być dostosowany do wyświetlania na urządzeniach o różnej rozdzielczości, w tym mobilnych i odzwierciedlać dobre praktyki RWD projektowania systemów min. w zakresie:

* Elastyczne siatki i układy: responsywne siatki, które dostosowują się do różnych rozmiarów ekranu zamiast ustalonych pikseli,
* Elastyczne obrazy i media: obrazy, wideo i inne elementy multimedialne prezentowane w taki sposób, aby były skalowalne,
* Czytelność tekstu: rozmiar tekstu jest czytelny na różnych urządzeniach, w tym urządzeniach mobilnych,
* Optymalizacja funkcji dotykowych: zapewnienie odpowiednio dużych obszarów dotykowych dla elementów interaktywnych, takich jak przyciski i linki, aby ułatwić obsługę na ekranach dotykowych,
* Optymalizacja wydajności: optymalizacja obrazów, minimalizacja kodu CSS i JavaScript, aby elementy ładowały się szybko.

1. Interoperacyjność - Aplikacja musi spełniać wymóg interoperacyjności, tzn. być otwarta na integrację i być w stanie wymieniać dane z innymi systemami, poprzez odpowiednio skonstruowany interfejs API.
2. Język - Sfera tekstowa platformy, w tym elementy UI, powinna być zrealizowana w języku polskim.

**Część 6**

**Przeprowadzenie zewnętrznego egzaminu certyfikacyjnego potwierdzającego nabycie kwalifikacji z tematu: „Emisja głosu”.**

Wykonawca przeprowadzi egzamin dla 20 Uczestników Projektu (UP).

Miejsce realizacji egzaminów:

Akademia Nauk Stosowanych Mazovia ul. Sokołowska 161, 08-110 Siedlce

Egzaminy będą realizowane w okresie od podpisania umowy do 31.12.2026 r., od poniedziałku do piątku i w weekendy w godzinach od 8:00 do 20:00, w oparciu o szczegółowy harmonogram zajęć, potwierdzony przez Zamawiającego i przekazany wybranemu oferentowi po podpisaniu umowy.

Sale do realizacji egzaminów zapewnia Zamawiający.

Wykonawca zobowiązany jest do zapewnienia niezbędnego sprzętu oraz materiałów do realizacji egzaminów.

Wykonawca opracuje/przygotuje, zorganizuje i przeprowadzi zewnętrzny egzamin certyfikacyjny, na podstawie przedstawionego poniżej programu szkolenia:

1. Głos – podstawowe narzędzie pracy
2. Warunki prawidłowej emisji
3. Proces wydobywania głosu od strony technicznej
4. Higiena głosu i praca na głosem
5. Wpływ postawy ciała i oddechu na głos
6. Techniki oddychania
7. Ekspresja mowy
8. Budowanie kontaktu z innymi za pomocą głosu
9. Podstawowe ćwiczenia oddechowe – świadome używanie oddechu przeponowego, wykorzystanie technik relaksacji w celu rozwijania możliwości głosowych
10. Higiena aparatu głosowego w pracy

Wykonawca zobowiązany będzie do zdefiniowania efektów uczenia się co najmniej w zakresie: wiedzy, umiejętności i kompetencji społecznych. Egzamin powinien weryfikować efekty uczenia się co najmniej w zakresie: wiedzy, umiejętności i kompetencji społecznych wynikające z przedstawionego programu szkolenia.

Certyfikat wydany osobom, które pomyślnie zdały egzamin certyfikacyjny winien zawierać w swej treści co najmniej:

* nazwę instytucji certyfikującej (IC),
* imię i nazwisko osoby egzaminowanej,
* nazwę/temat szkolenia i/lub kwalifikacji,
* datę i miejsce wydania,
* pieczęcie i podpisy osób upoważnionych do reprezentowania IC (instytucji certyfikującej).

Do każdego certyfikatu dołączony zostanie suplement, który winien zawierać w swej treści co najmniej:

* nazwę instytucji certyfikującej (IC),
* imię i nazwisko osoby egzaminowanej,
* nazwę/temat szkolenia i/lub kwalifikacji,
* program szkolenia i/lub nabyte efekty uczenia się w zakresie wiedzy, umiejętności i kompetencji społecznych,

− uzyskane wyniki,

− datę i miejsce wydania,

− pieczęcie i podpisy osób upoważnionych do reprezentowania IC (instytucji certyfikującej).

Wykonawca zobowiązany jest do wydania certyfikatu każdemu uczestnikowi, który pomyślnie ukończy zewnętrzny egzamin certyfikacyjny. Certyfikat musi spełniać wymagania określone przez Ministerstwo Rozwoju / Ministerstwo  Funduszy i Polityki Regionalnej w odniesieniu do sposobów uzyskiwania i potwierdzania kwalifikacji w ramach projektów współfinansowanych z EFS+ w tzw. „liście sprawdzającej” do weryfikacji czy dokument można uznać za potwierdzający kwalifikację (niewłączoną do Zintegrowanego Systemu Kwalifikacji)/kompetencję na potrzeby mierzenia wskaźników monitorowania EFS+ dot. uzyskiwania kwalifikacji, zgodnie z informacjami przedstawionymi w dokumencie p.n. „Załącznik 2 Podstawowe informacje dotyczące uzyskiwania kwalifikacji w ramach projektów współfinansowanych z EFS+”: https://www.funduszeeuropejskie.gov.pl/strony/o-funduszach/dokumenty/wytyczne-dotyczace-monitorowania-postepu-rzeczowego-realizacji-programow-na-lata-2021-2027/

Wykonawca zobowiązany jest zapewnić każdemu uczestnikowi dostęp do platformy dydaktycznej wraz z materiałami dydaktycznymi w formie cyfrowej.

Wymagania platformy dydaktycznej:

* 1. Platforma będzie wykorzystywana jako narzędzie wspierające uczestnika w przygotowaniu się do walidacji i certyfikacji kwalifikacji.
  2. Platforma ma dawać możliwość udostępniania użytkownikom treści nauczania w formie cyfrowej, udostępniania narzędzi do przystępnej i atrakcyjnej formy utrwalania wiedzy poprzez ćwiczenia interaktywne, narzędzia pracy grupowej oraz możliwości oceny różnych form aktywności przez trenerów.
  3. Platforma musi też umożliwiać przyznawanie mikropoświadczeń, w postaci cyfrowych odznak, realizowanych w standardzie Open Badge 3.0 lub równoważnym, za potwierdzenie efektów uczenia się - za pomocą mechanizmów w niej zaimplementowanych, lub poprzez łączenie z innymi systemami poprzez interfejs API. Przez standard równoważny do Open Badge 3.0 Zamawiający uważa standard spełniający warunki opisane w zapytaniu ofertowym.
  4. Użytkownikami platformy będą uczestnicy projektu.

Wymagania funkcjonalne platformy dydaktycznej:

1. Start i logowanie się do konta użytkownika – platforma powinna oferować formularz logowania wymagający podania nazwy użytkownika (lub adresu e-mail) i hasła oraz sprawdzać poprawność wprowadzonych danych logowania.
2. Zarządzanie kontem użytkownika powinno uwzględniać możliwość tworzenia profili dla trenerów i uczniów, w tym zarządzanie ich uprawnieniami. Platforma powinna umożliwiać tworzenie grup użytkowników (odpowiadających grupom szkoleniowym), w celu selektywnego udostępniania zawartości merytorycznej (cyfrowy podręcznik, ćwiczenia etc.). Sposób zabezpieczenia systemu opisano w sekcji opisu poświęconej wymaganiom pozafunkcjonalnym.
3. Komunikacja – platforma powinna udostępniać narzędzia do komunikacji między uczestnikami szkoleń oraz między uczestnikami i trenerem, w postaci forum dyskusyjnego, umożliwiającego wymianę myśli i dyskusje na tematy związane z tematyką szkolenia, a także czat, na potrzeby komunikacji w czasie rzeczywistym.
4. Możliwość tworzenia kursów – platforma powinna dawać możliwość łatwego tworzenia i zarządzania kursami, w tym dodawanie treści edukacyjnych, takich jak dokumenty, prezentacje, dźwięk, wideo, itp. Oraz wsparcie dla różnych formatów treści, w tym HTML, PDF, tekst, multimedia.
5. Możliwość tworzenia quizów, ćwiczeń, zadań domowych – platforma powinna dawać osobie prowadzącej szkolenie możliwość dodawania ćwiczeń oraz quizów interaktywnych w popularnych formatach e-learnigowych (HTML5, SCORM), a także innych zadań (w tym opisowych), a także możliwość punktowania i oceny tychże przez trenera.
6. Możliwość tworzenia notatek z zajęć – Użytkownicy powinni mieć możliwość tworzenia notatek z realizowanych zajęć.
7. Wsparcie dla standardów e-learningowych – platforma powinna zapewniać kompatybilność z popularnymi standardami e-learningowymi, takimi jak SCORM czy xAPI (Tin Can), co umożliwia wykorzystanie zewnętrznych materiałów edukacyjnych i śledzenie interakcji z nimi.
8. Repozytorium treści – platforma zapewniać powinna repozytorium treści z możliwością zarządzania tymiż treściami, w kontekście udostępniania materiałów poszczególnym użytkownikom oraz tworzenia z nich ścieżek dydaktycznych. Wykonawca zobowiązany będzie do wypełnienia repozytorium treścią dla szkolenia stanowiącego przedmiot zamówienia.

Dostarczana zawartość powinna uwzględniać przynajmniej:

* podręcznik w formie cyfrowej, który w sposób wyczerpujący omawia wskazany wyżej program szkolenia,
* interaktywną ścieżkę dydaktyczną (umożliwiającą nawigowanie po zagadnieniach merytorycznych danego tematu),
* zestawy ćwiczeń,
* testy kompetencyjne/egzaminy próbne,

Repozytorium powinno również zawierać materiały merytoryczne, pozwalające na zapoznanie się z dostępnymi narzędziami AI (sztucznej inteligencji) pozwalającymi na wykorzystywanie generatywnej AI na potrzeby kwalifikacji stanowiącej przedmiot szkolenia.

1. Możliwość generowania mikropoświadczeń – platforma/system powinien dawać użytkownikom możliwość zdobywania mikropoświadczeń w postaci odznak cyfrowych, realizowanych zgodnie ze standardem Open Badge 3.0, za potwierdzanie efektów kształcenia nabywanych podczas realizacji szkoleń.

Zgodnie z treścią Zalecenia Rady z dnia 22 czerwca 2022 r. w sprawie europejskiego podejścia do mikropoświadczeń na potrzeby uczenia się przez całe życie i zatrudnialności, zaleca się państwom członkowskim przyjęcie i promowanie stosowania definicji mikropoświadczenia, jako: *„opis(u) efektów uczenia się, które osoba ucząca się uzyskała przy niewielkim nakładzie uczenia się. Efekty te zostały ocenione na podstawie przejrzystych i jasno określonych kryteriów. Aktywności edukacyjne prowadzące do uzyskania mikropoświadczeń są opracowywane tak, aby osoba ucząca się zdobyła konkretną wiedzę, umiejętności i kompetencje, które odpowiadają na potrzeby społeczne, osobiste i kulturowe lub na potrzeby rynku pracy. „Mikropoświadczenia są własnością osoby uczącej się i mogą być udostępniane i przenoszone. Mogą być samodzielne lub łączone w większe poświadczenia.”* (pkt 5, lit. a) Zalecenia).

Standard Open Badge 3.0 stanowi adekwatne rozwiązanie dla dopełnienia Europejskich zasad opracowywania i wydawania mikropoświadczeń (stanowiących załącznik II do Zalecenia), w zakresie wymagań przenośności (w kontekście cyfrowej formy mikropoświadczenia i stosowania otwartych standardów i modeli danych: *„Mikropoświadczenia są własnością posiadacza poświadczenia (osoby uczącej się) i mogą być przez niego łatwo przechowywane i udostępniane, w tym za pomocą bezpiecznych portfeli cyfrowych (np. Europass), zgodnie z ogólnym rozporządzeniem o ochronie danych. Infrastruktura do przechowywania danych opiera się na standardach otwartych i modelach danych. Zapewnia to interoperacyjność i bezproblemową wymianę danych oraz pozwala na sprawne sprawdzanie ich autentyczności.”*.

Tym samym system musi dawać indywidualnemu użytkownikowi możliwość swobodnego kumulowania, przenoszenia i udostępniania zdobytych odznak (również poza system), jako że zgodnie z definicją, mikropoświadczenia są własnością osoby uczącej się. Zgodnie z wymaganiami Uznawania i Autentyczności (opisanymi w załączniku II Zalecenia), rozwiązanie musi dostarczać możliwość walidacji mikropoświadczenia w celu zidentyfikowania elementów potwierdzających jego autentyczność.

Załącznik I do Zalecenia określa elementy wchodzące w skład meta danych mikropoświadczenia, które mogą posłużyć do jego autentykacji, takie jak:

* Identyfikacja osoby uczącej się,
* Tytuł mikropoświadczenia,
* Państwo(-wa)/region(y) organu wydającego,
* Organ(y) przyznający(-ce),
* Data wydania,
* Efekty uczenia się.

Powyższy zakres danych jest niezbędnym zakresem informacji zawieranych w ramach poświadczenia.

Standard Open Badge 3.0 opisuje metodę kryptograficznego kodowania tych informacji w formie pliku graficznego (odznaki), która jest przenoszalna i daje możliwość dekodowania informacji za pomocą odpowiedniej infrastruktury do walidacji.

Standard Open Badge 3.0 to otwarty, rozpoznawalny i uznawalny standard cyfrowych odznak, którego kompletną dokumentację techniczną znaleźć można pod adresem: https://www.imsglobal.org/spec/ob/v3p0/#abstract-0.

Platforma powinna realizować funkcjonalności związane z uzyskiwaniem mikropoświadczeń w zakresie:

* zapisywania mikropoświadczeń na indywidualnym koncie użytkownika - na platformie, lub systemach z nią powiązanych i dostępnych dla tego użytkownika w postaci cyfrowego „plecaka / portfela” z odznakami, z dowolnego miejsca na świecie (po zalogowaniu się na konto użytkownika),
* akumulacji mikropoświadczeń na indywidualnym koncie użytkownika - na platformie, lub systemach z nią powiązanych (dotyczy zarówno tych, zdobywanych w ramach realizowanych szkoleń, wspieranych użytkowaniem platformy, jak i osiągnięć zdobytych poza systemem), z możliwością generowania cyfrowego CV użytkownika,
* publikowania mikropoświadczeń - dzielenie się osiągnięciami z poziomu indywidualnego konta użytkownika - na platformie, lub systemów z nią powiązanych, poprzez umieszczanie odnośników do nich na platformach społecznościowych typu LinkedIn, czy Facebook, z dostępem anonimowym (bez konieczności logowania) i z uwzględnieniem ochrony danych osobowych (zgodnie z dyrektywą RODO),
* walidacji mikropoświadczeń – weryfikację autentyczności mikropoświadczenia, na potrzeby jego uznawalności, za pomocą zaimplementowanego w systemie walidatora, dostępnego również dla niezalogowanych użytkowników (np. pracodawcy, chcącego zweryfikować autentyczność osiągnięć potencjalnego pracownika),
* segmentacji mikropoświadczeń – aplikacja umożliwiać będzie uzyskanie dostępu do ścieżek rozwoju zawodowego, generowanych przez algorytm, w oparciu o tematy szkoleń, w których brać będzie udział uczestnik, a w które (pod względem merytorycznym) wpisują się zdobyte mikropoświadczenia,
* funkcjonalności związanych z grywalizacją – realizowanych przynajmniej w postaci zdobywania osiągnięć i porównywania zdobytych mikropoświadczeń i kwalifikacji w ramach rankingu użytkowników systemu.

Wymagania pozafunkcjonalne platformy dydaktycznej:

1. Kompatybilność - platforma musi działać na komputerach wyposażonych w systemy operacyjne Windows, Linux oraz macOS oraz na urządzeniach mobilnych z systemami Android i iOS, z założeniem responsywności wyświetlanej zawartości.
2. Zabezpieczenia - Bezpieczeństwo systemu powinno uwzględniać następujące elementy:

* Uwierzytelnianie i autoryzacja: Wdrożenie silnych mechanizmów uwierzytelniania i autoryzacji, w tym weryfikację i zarządzanie hasłami, aby zapewnić bezpieczeństwo danych użytkowników.
* Segmentacja dostępu: Precyzyjne określenie uprawnień dla każdej roli, aby ograniczyć dostęp do funkcjonalności systemu zgodnie z potrzebami i uprawnieniami.
* Rejestry aktywności: Monitorowanie i rejestrowanie działań użytkowników w systemie dla celów audytowych i bezpieczeństwa.
* Zapomniałem hasła: Funkcja umożliwiająca użytkownikom resetowanie zapomnianego hasła przez e-mail.
* Przesyłanie danych: Wszystkie klucze przesyłane pomiędzy systemami muszą być zaszyfrowane i gwarantować bezpieczeństwo i integralność danych w systemie.
* Limit prób logowania: W celu zapobiegania atakom bruteforce, system powinien ograniczać liczbę nieudanych prób logowania i w razie potrzeby blokować dostęp do konta na określony czas.
* Sesje i wylogowywanie: System powinien zarządzać sesjami użytkowników, umożliwiając im wylogowanie oraz automatycznie kończyć sesję po określonym czasie bezczynności.

1. Dostępność - Interfejs aplikacji powinien być zgodny z WCAG 2.2 na poziomie A i AA oraz być dostosowany do wyświetlania na urządzeniach o różnej rozdzielczości, w tym mobilnych i odzwierciedlać dobre praktyki RWD projektowania systemów min. w zakresie:

* Elastyczne siatki i układy: responsywne siatki, które dostosowują się do różnych rozmiarów ekranu zamiast ustalonych pikseli,
* Elastyczne obrazy i media: obrazy, wideo i inne elementy multimedialne prezentowane w taki sposób, aby były skalowalne,
* Czytelność tekstu: rozmiar tekstu jest czytelny na różnych urządzeniach, w tym urządzeniach mobilnych,
* Optymalizacja funkcji dotykowych: zapewnienie odpowiednio dużych obszarów dotykowych dla elementów interaktywnych, takich jak przyciski i linki, aby ułatwić obsługę na ekranach dotykowych,
* Optymalizacja wydajności: optymalizacja obrazów, minimalizacja kodu CSS i JavaScript, aby elementy ładowały się szybko.

1. Interoperacyjność - Aplikacja musi spełniać wymóg interoperacyjności, tzn. być otwarta na integrację i być w stanie wymieniać dane z innymi systemami, poprzez odpowiednio skonstruowany interfejs API.
2. Język - Sfera tekstowa platformy, w tym elementy UI, powinna być zrealizowana w języku polskim.

**Część 7**

**Przeprowadzenie zewnętrznego egzaminu certyfikacyjnego potwierdzającego nabycie kwalifikacji z tematu: „****Pozyskiwanie i rozliczanie dotacji na działalność Kół Gospodyń Wiejskich”.**

Wykonawca przeprowadzi egzamin dla 20 Uczestników Projektu (UP).

Miejsce realizacji egzaminów:

Akademia Nauk Stosowanych Mazovia ul. Sokołowska 161, 08-110 Siedlce

Egzaminy będą realizowane w okresie od podpisania umowy do 31.12.2026 r., od poniedziałku do piątku i w weekendy w godzinach od 8:00 do 20:00, w oparciu o szczegółowy harmonogram zajęć, potwierdzony przez Zamawiającego i przekazany wybranemu oferentowi po podpisaniu umowy.

Sale do realizacji egzaminów zapewnia Zamawiający.

Wykonawca zobowiązany jest do zapewnienia niezbędnego sprzętu oraz materiałów do realizacji egzaminów.

Wykonawca opracuje/przygotuje, zorganizuje i przeprowadzi zewnętrzny egzamin certyfikacyjny, na podstawie przedstawionego poniżej programu szkolenia:

Źródła finansowania dla Kół Gospodyń Wiejskich:

* Przegląd dostępnych programów wsparcia i źródeł dotacji:
* Pozyskiwanie wsparcia od samorządów lokalnych i partnerów prywatnych.
* Możliwości współpracy z organizacjami pozarządowymi.

Procedury pozyskiwania dotacji (4 godz.):

* Zrozumienie zasad i procedur aplikacyjnych:
* Jakie warunki musi spełniać Koło Gospodyń Wiejskich, aby uzyskać dotację.
* Wymogi formalne i dokumentacyjne w procesie aplikacyjnym.
* Analiza ogłoszeń konkursowych i harmonogramów naborów.

Przygotowanie wniosków dotacyjnych:

* Struktura wniosku dotacyjnego:
* Dokumenty załączane do wniosków – jak je przygotować i uzupełnić.
* Przykłady dobrze przygotowanych wniosków dotacyjnych.
* Ćwiczenia praktyczne: przygotowanie wniosku dotacyjnego dla KGW.
* Błędy najczęściej popełniane przy składaniu wniosków i jak ich unikać.

Monitorowanie realizacji projektów dotacyjnych:

* Jak efektywnie monitorować realizację projektu w KGW.
* Odpowiedzialność za realizację celów i terminowość działań.
* Komunikacja z instytucjami przyznającymi dotacje i partnerami projektu.
* Dokumentacja projektowa – jak prowadzić rejestry, raporty i sprawozdania z realizacji.

Rozliczanie dotacji – jak prawidłowo rozliczyć przyznane środki:

* Zasady i terminy rozliczania dotacji – na co zwrócić uwagę.
* Jak prawidłowo rozliczać wydatki zgodnie z budżetem projektu.
* Sporządzanie raportów końcowych – wymagania formalne.
* Przykłady i ćwiczenia praktyczne z zakresu rozliczania dotacji.
* Co zrobić w przypadku konieczności zwrotu niewykorzystanych środków.

Podsumowanie i najważniejsze wskazówki:

* Wskazówki praktyczne i dobre praktyki w pozyskiwaniu i rozliczaniu dotacji.
* Odpowiedzi na pytania uczestników, konsultacje indywidualne.
* Przykłady sukcesów Kół Gospodyń Wiejskich w pozyskiwaniu dotacji.

Wykonawca zobowiązany będzie do zdefiniowania efektów uczenia się co najmniej w zakresie: wiedzy, umiejętności i kompetencji społecznych. Egzamin powinien weryfikować efekty uczenia się co najmniej w zakresie: wiedzy, umiejętności i kompetencji społecznych wynikające z przedstawionego programu szkolenia.

Certyfikat wydany osobom, które pomyślnie zdały egzamin certyfikacyjny winien zawierać w swej treści co najmniej:

* nazwę instytucji certyfikującej (IC),
* imię i nazwisko osoby egzaminowanej,
* nazwę/temat szkolenia i/lub kwalifikacji,
* datę i miejsce wydania,
* pieczęcie i podpisy osób upoważnionych do reprezentowania IC (instytucji certyfikującej).

Do każdego certyfikatu dołączony zostanie suplement, który winien zawierać w swej treści co najmniej:

* nazwę instytucji certyfikującej (IC),
* imię i nazwisko osoby egzaminowanej,
* nazwę/temat szkolenia i/lub kwalifikacji,
* program szkolenia i/lub nabyte efekty uczenia się w zakresie wiedzy, umiejętności i kompetencji społecznych,
* uzyskane wyniki,
* datę i miejsce wydania,
* pieczęcie i podpisy osób upoważnionych do reprezentowania IC (instytucji certyfikującej).

Wykonawca zobowiązany jest do wydania certyfikatu każdemu uczestnikowi, który pomyślnie ukończy zewnętrzny egzamin certyfikacyjny. Certyfikat musi spełniać wymagania określone przez Ministerstwo Rozwoju / Ministerstwo  Funduszy i Polityki Regionalnej w odniesieniu do sposobów uzyskiwania i potwierdzania kwalifikacji w ramach projektów współfinansowanych z EFS+ w tzw. „liście sprawdzającej” do weryfikacji czy dokument można uznać za potwierdzający kwalifikację (niewłączoną do Zintegrowanego Systemu Kwalifikacji)/kompetencję na potrzeby mierzenia wskaźników monitorowania EFS+ dot. uzyskiwania kwalifikacji, zgodnie z informacjami przedstawionymi w dokumencie p.n. „Załącznik 2 Podstawowe informacje dotyczące uzyskiwania kwalifikacji w ramach projektów współfinansowanych z EFS+”: https://www.funduszeeuropejskie.gov.pl/strony/o-funduszach/dokumenty/wytyczne-dotyczace-monitorowania-postepu-rzeczowego-realizacji-programow-na-lata-2021-2027/

Wykonawca zobowiązany jest zapewnić każdemu uczestnikowi dostęp do platformy dydaktycznej wraz z materiałami dydaktycznymi w formie cyfrowej.

Wymagania platformy dydaktycznej:

1. Platforma będzie wykorzystywana jako narzędzie wspierające uczestnika w przygotowaniu się do walidacji i certyfikacji kwalifikacji.
2. Platforma ma dawać możliwość udostępniania użytkownikom treści nauczania w formie cyfrowej, udostępniania narzędzi do przystępnej i atrakcyjnej formy utrwalania wiedzy poprzez ćwiczenia interaktywne, narzędzia pracy grupowej oraz możliwości oceny różnych form aktywności przez trenerów.
3. Platforma musi też umożliwiać przyznawanie mikropoświadczeń, w postaci cyfrowych odznak, realizowanych w standardzie Open Badge 3.0 lub równoważnym, za potwierdzenie efektów uczenia się - za pomocą mechanizmów w niej zaimplementowanych, lub poprzez łączenie z innymi systemami poprzez interfejs API. Przez standard równoważny do Open Badge 3.0 Zamawiający uważa standard spełniający warunki opisane w zapytaniu ofertowym.
4. Użytkownikami platformy będą uczestnicy projektu.

Wymagania funkcjonalne platformy dydaktycznej:

1. Start i logowanie się do konta użytkownika – platforma powinna oferować formularz logowania wymagający podania nazwy użytkownika (lub adresu e-mail) i hasła oraz sprawdzać poprawność wprowadzonych danych logowania.
2. Zarządzanie kontem użytkownika powinno uwzględniać możliwość tworzenia profili dla trenerów i uczniów, w tym zarządzanie ich uprawnieniami. Platforma powinna umożliwiać tworzenie grup użytkowników (odpowiadających grupom szkoleniowym), w celu selektywnego udostępniania zawartości merytorycznej (cyfrowy podręcznik, ćwiczenia etc.). Sposób zabezpieczenia systemu opisano w sekcji opisu poświęconej wymaganiom pozafunkcjonalnym.
3. Komunikacja – platforma powinna udostępniać narzędzia do komunikacji między uczestnikami szkoleń oraz między uczestnikami i trenerem, w postaci forum dyskusyjnego, umożliwiającego wymianę myśli i dyskusje na tematy związane z tematyką szkolenia, a także czat, na potrzeby komunikacji w czasie rzeczywistym.
4. Możliwość tworzenia kursów – platforma powinna dawać możliwość łatwego tworzenia i zarządzania kursami, w tym dodawanie treści edukacyjnych, takich jak dokumenty, prezentacje, dźwięk, wideo, itp. Oraz wsparcie dla różnych formatów treści, w tym HTML, PDF, tekst, multimedia.
5. Możliwość tworzenia quizów, ćwiczeń, zadań domowych – platforma powinna dawać osobie prowadzącej szkolenie możliwość dodawania ćwiczeń oraz quizów interaktywnych w popularnych formatach e-learnigowych (HTML5, SCORM), a także innych zadań (w tym opisowych), a także możliwość punktowania i oceny tychże przez trenera.
6. Możliwość tworzenia notatek z zajęć – Użytkownicy powinni mieć możliwość tworzenia notatek z realizowanych zajęć.
7. Wsparcie dla standardów e-learningowych – platforma powinna zapewniać kompatybilność z popularnymi standardami e-learningowymi, takimi jak SCORM czy xAPI (Tin Can), co umożliwia wykorzystanie zewnętrznych materiałów edukacyjnych i śledzenie interakcji z nimi.
8. Repozytorium treści – platforma zapewniać powinna repozytorium treści z możliwością zarządzania tymiż treściami, w kontekście udostępniania materiałów poszczególnym użytkownikom oraz tworzenia z nich ścieżek dydaktycznych. Wykonawca zobowiązany będzie do wypełnienia repozytorium treścią dla szkolenia stanowiącego przedmiot zamówienia.

Dostarczana zawartość powinna uwzględniać przynajmniej:

* podręcznik w formie cyfrowej, który w sposób wyczerpujący omawia wskazany wyżej program szkolenia,
* interaktywną ścieżkę dydaktyczną (umożliwiającą nawigowanie po zagadnieniach merytorycznych danego tematu),
* zestawy ćwiczeń,
* testy kompetencyjne/egzaminy próbne.

Repozytorium powinno również zawierać materiały merytoryczne, pozwalające na zapoznanie się z dostępnymi narzędziami AI (sztucznej inteligencji) pozwalającymi na wykorzystywanie generatywnej AI na potrzeby kwalifikacji stanowiącej przedmiot szkolenia.

1. Możliwość generowania mikropoświadczeń – platforma/system powinien dawać użytkownikom możliwość zdobywania mikropoświadczeń w postaci odznak cyfrowych, realizowanych zgodnie ze standardem Open Badge 3.0, za potwierdzanie efektów kształcenia nabywanych podczas realizacji szkoleń.

Zgodnie z treścią Zalecenia Rady z dnia 22 czerwca 2022 r. w sprawie europejskiego podejścia do mikropoświadczeń na potrzeby uczenia się przez całe życie i zatrudnialności, zaleca się państwom członkowskim przyjęcie i promowanie stosowania definicji mikropoświadczenia, jako: *„opis(u) efektów uczenia się, które osoba ucząca się uzyskała przy niewielkim nakładzie uczenia się. Efekty te zostały ocenione na podstawie przejrzystych i jasno określonych kryteriów. Aktywności edukacyjne prowadzące do uzyskania mikropoświadczeń są opracowywane tak, aby osoba ucząca się zdobyła konkretną wiedzę, umiejętności i kompetencje, które odpowiadają na potrzeby społeczne, osobiste i kulturowe lub na potrzeby rynku pracy. „Mikropoświadczenia są własnością osoby uczącej się i mogą być udostępniane i przenoszone. Mogą być samodzielne lub łączone w większe poświadczenia.”* (pkt 5, lit. a) Zalecenia).

Standard Open Badge 3.0 stanowi adekwatne rozwiązanie dla dopełnienia Europejskich zasad opracowywania i wydawania mikropoświadczeń (stanowiących załącznik II do Zalecenia), w zakresie wymagań przenośności (w kontekście cyfrowej formy mikropoświadczenia i stosowania otwartych standardów i modeli danych: *„Mikropoświadczenia są własnością posiadacza poświadczenia (osoby uczącej się) i mogą być przez niego łatwo przechowywane i udostępniane, w tym za pomocą bezpiecznych portfeli cyfrowych (np. Europass), zgodnie z ogólnym rozporządzeniem o ochronie danych. Infrastruktura do przechowywania danych opiera się na standardach otwartych i modelach danych. Zapewnia to interoperacyjność i bezproblemową wymianę danych oraz pozwala na sprawne sprawdzanie ich autentyczności.”*.

Tym samym system musi dawać indywidualnemu użytkownikowi możliwość swobodnego kumulowania, przenoszenia i udostępniania zdobytych odznak (również poza system), jako że zgodnie z definicją, mikropoświadczenia są własnością osoby uczącej się. Zgodnie z wymaganiami Uznawania i Autentyczności (opisanymi w załączniku II Zalecenia), rozwiązanie musi dostarczać możliwość walidacji mikropoświadczenia w celu zidentyfikowania elementów potwierdzających jego autentyczność.

Załącznik I do Zalecenia określa elementy wchodzące w skład meta danych mikropoświadczenia, które mogą posłużyć do jego autentykacji, takie jak:

* Identyfikacja osoby uczącej się,
* Tytuł mikropoświadczenia,
* Państwo(-wa)/region(y) organu wydającego,
* Organ(y) przyznający(-ce),
* Data wydania,
* Efekty uczenia się.

Powyższy zakres danych jest niezbędnym zakresem informacji zawieranych w ramach poświadczenia.

Standard Open Badge 3.0 opisuje metodę kryptograficznego kodowania tych informacji w formie pliku graficznego (odznaki), która jest przenoszalna i daje możliwość dekodowania informacji za pomocą odpowiedniej infrastruktury do walidacji.

Standard Open Badge 3.0 to otwarty, rozpoznawalny i uznawalny standard cyfrowych odznak, którego kompletną dokumentację techniczną znaleźć można pod adresem: https://www.imsglobal.org/spec/ob/v3p0/#abstract-0.

Platforma powinna realizować funkcjonalności związane z uzyskiwaniem mikropoświadczeń w zakresie:

* zapisywania mikropoświadczeń na indywidualnym koncie użytkownika - na platformie, lub systemach z nią powiązanych i dostępnych dla tego użytkownika w postaci cyfrowego „plecaka /portfela” z odznakami, z dowolnego miejsca na świecie (po zalogowaniu się na konto użytkownika),
* akumulacji mikropoświadczeń na indywidualnym koncie użytkownika - na platformie, lub systemach z nią powiązanych (dotyczy zarówno tych, zdobywanych w ramach realizowanych szkoleń, wspieranych użytkowaniem platformy, jak i osiągnięć zdobytych poza systemem), z możliwością generowania cyfrowego CV użytkownika,
* publikowania mikropoświadczeń - dzielenie się osiągnięciami z poziomu indywidualnego konta użytkownika - na platformie, lub systemów z nią powiązanych, poprzez umieszczanie odnośników do nich na platformach społecznościowych typu LinkedIn, czy Facebook, z dostępem anonimowym (bez konieczności logowania) i z uwzględnieniem ochrony danych osobowych (zgodnie z dyrektywą RODO),
* walidacji mikropoświadczeń – weryfikację autentyczności mikropoświadczenia, na potrzeby jego uznawalności, za pomocą zaimplementowanego w systemie walidatora, dostępnego również dla niezalogowanych użytkowników (np. pracodawcy, chcącego zweryfikować autentyczność osiągnięć potencjalnego pracownika),
* segmentacji mikropoświadczeń – aplikacja umożliwiać będzie uzyskanie dostępu do ścieżek rozwoju zawodowego, generowanych przez algorytm, w oparciu o tematy szkoleń, w których brać będzie udział uczestnik, a w które (pod względem merytorycznym) wpisują się zdobyte mikropoświadczenia,
* funkcjonalności związanych z grywalizacją – realizowanych przynajmniej w postaci zdobywania osiągnięć i porównywania zdobytych mikropoświadczeń i kwalifikacji w ramach rankingu użytkowników systemu.

Wymagania pozafunkcjonalne platformy dydaktycznej:

1. Kompatybilność - platforma musi działać na komputerach wyposażonych w systemy operacyjne Windows, Linux oraz macOS oraz na urządzeniach mobilnych z systemami Android i iOS, z założeniem responsywności wyświetlanej zawartości.
2. Zabezpieczenia - Bezpieczeństwo systemu powinno uwzględniać następujące elementy:

* Uwierzytelnianie i autoryzacja: Wdrożenie silnych mechanizmów uwierzytelniania i autoryzacji, w tym weryfikację i zarządzanie hasłami, aby zapewnić bezpieczeństwo danych użytkowników.
* Segmentacja dostępu: Precyzyjne określenie uprawnień dla każdej roli, aby ograniczyć dostęp do funkcjonalności systemu zgodnie z potrzebami i uprawnieniami.
* Rejestry aktywności: Monitorowanie i rejestrowanie działań użytkowników w systemie dla celów audytowych i bezpieczeństwa.
* Zapomniałem hasła: Funkcja umożliwiająca użytkownikom resetowanie zapomnianego hasła przez e-mail.
* Przesyłanie danych: Wszystkie klucze przesyłane pomiędzy systemami muszą być zaszyfrowane i gwarantować bezpieczeństwo i integralność danych w systemie.
* Limit prób logowania: W celu zapobiegania atakom bruteforce, system powinien ograniczać liczbę nieudanych prób logowania i w razie potrzeby blokować dostęp do konta na określony czas.
* Sesje i wylogowywanie: System powinien zarządzać sesjami użytkowników, umożliwiając im wylogowanie oraz automatycznie kończyć sesję po określonym czasie bezczynności.

1. Dostępność - Interfejs aplikacji powinien być zgodny z WCAG 2.2 na poziomie A i AA oraz być dostosowany do wyświetlania na urządzeniach o różnej rozdzielczości, w tym mobilnych i odzwierciedlać dobre praktyki RWD projektowania systemów min. w zakresie:

* Elastyczne siatki i układy: responsywne siatki, które dostosowują się do różnych rozmiarów ekranu zamiast ustalonych pikseli,
* Elastyczne obrazy i media: obrazy, wideo i inne elementy multimedialne prezentowane w taki sposób, aby były skalowalne,
* Czytelność tekstu: rozmiar tekstu jest czytelny na różnych urządzeniach, w tym urządzeniach mobilnych,
* Optymalizacja funkcji dotykowych: zapewnienie odpowiednio dużych obszarów dotykowych dla elementów interaktywnych, takich jak przyciski i linki, aby ułatwić obsługę na ekranach dotykowych,
* Optymalizacja wydajności: optymalizacja obrazów, minimalizacja kodu CSS i JavaScript, aby elementy ładowały się szybko.

1. Interoperacyjność - Aplikacja musi spełniać wymóg interoperacyjności, tzn. być otwarta na integrację i być w stanie wymieniać dane z innymi systemami, poprzez odpowiednio skonstruowany interfejs API.
2. Język - Sfera tekstowa platformy, w tym elementy UI, powinna być zrealizowana w języku polskim.