

OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiot zamówienia.

- 1.1. Przedmiotem zamówienia jest **dostawa oraz wdrożenie platformy informatycznej do przeprowadzenia szkoleń typu e-learning, tj. systemu klasy Learning Management System („LMS”), zwanego dalej „Platformą”**. Ponadto zamówienie obejmuje opracowanie oraz wdrożenie na Platformie kursu e-learningowego Security awareness, zwanego dalej „Kursem”. Odbiorcami kursu, zwanymi dalej „Uczestnikami” będą m.in. pracownicy podmiotów medycznych.
- 1.2. Celem Kursu jest podniesienie świadomości kadry zarządzającej i pracowników podmiotów medycznych w zakresie wyzwań, metod ochrony oraz obowiązków związanych z prowadzeniem działalności w środowisku cyfrowym, w tym wdrażaniem nowych rozwiązań z zakresu poprawiających poziom bezpieczeństwa.
- 1.3. W szczególności przedmiot zamówienia obejmuje:
 - 1.3.1. Dostarczenie licencji wieczystej oraz wdrożenie Platformy na infrastrukturze Zamawiającego.
 - 1.3.2. Opracowanie, przygotowanie technicznie i graficznie Kursu w formacie i standardzie SCORM (ang. Sharable Content Object Reference Model), zgodnym z wymogami Platformy.
 - 1.3.3. Zaimportowanie przez Wykonawcę Kursu do Platformy Zamawiającego.
 - 1.3.4. Dostarczenie licencji wieczystej na Kurs bez limitu ilości przeprowadzonych Kursów.
 - 1.3.5. Przeprowadzenie instruktażu z obsługi Platformy.
 - 1.3.6. Przeprowadzenie instruktażu z obsługi Kursu.
 - 1.3.7. Zaimplementowanie layoutu Platformy zgodnie z kolorystyką CeZ ustaloną z Zamawiającym.
 - 1.3.8. Przygotowanie Kursu zgodnie z kolorystyką ustaloną z Zamawiającym.
 - 1.3.9. Zaprojektowanie oraz uruchomienie na Platformie Kursu na podstawie otrzymanych od Zamawiającego wytycznych.
 - 1.3.10. Wykonanie testów bezpieczeństwa Platformy oraz dostarczenie raportu z testów.
 - 1.3.11. Wykonanie testów z funkcjonowania Kursu na Platformie oraz dostarczenie raportu z testów.
 - 1.3.12. Dostarczenie dokumentacji powdrożeniowej Platformy.
 - 1.3.13. Przygotowanie i dostarczenie Zamawiającemu Kursu w formatach PDF oraz PPTX.
 - 1.3.14. Zapewnienie wsparcia oraz godzin rozwojowych.

2. Harmonogram realizacji przedmiotu zamówienia:

Przedmiot zamówienia zostanie dostarczony w terminie nie dłuższym niż 90 dni, liczonym od dnia zawarcia Umowy, z zastrzeżeniem, punktu 11.4 OPZ Czas świadczenia usługi rozwoju Platformy/Kursu – 24 miesiące od dnia odbioru przedmiotu Umowy. Poszczególne prace będą wykonywane w terminach wskazanych w przyjętym harmonogramie.

Etap I – Opracowanie harmonogramu oraz planu wdrożenia.

W ramach realizacji etapu Wykonawca:

- 2.1. W terminie do 5 dni od dnia zawarcia umowy, przygotuje i przedstawi Zamawiającemu harmonogram wdrożenia Platformy.
- 2.2. Przygotuje opis niezbędnych prac w celu wdrożenia Platformy wraz ze wskazaniem podziału obowiązków pomiędzy Zamawiającego i Wykonawcę w modelu RACI.
- 2.3. Przedstawi listę pracowników Wykonawcy odpowiedzialnych za wykonanie poszczególnych etapów zgodnie z przedstawionym wykazem podziału obowiązków w w/w formacie RACI wraz z danymi teleadresowymi minimalnie numer telefonu komórkowego, adres email.
- 2.4. Opracuje scenariusze testowe Platformy:
 - 2.4.1. Scenariusze testowe muszą zawierać propozycje testów wydajnościowych, funkcjonalnych i bezpieczeństwa.
 - 2.4.2. Scenariusze testowe będą przygotowane przez Wykonawcę i wymagają zatwierdzenia przez Zamawiającego.
- 2.5. Wskaże terminy wykonania następujących czynności:
 - 2.5.1. Opracowanie i akceptacja projektów scenariuszy dla każdego modułu Kursu.
 - 2.5.2. Opracowanie i akceptacja zawartości merytorycznej wszystkich modułów Kursu.

Etap II - Analiza przedwdrożeniowa.

W ramach realizacji etapu Wykonawca:

- 2.6. W terminie do 8 dni od dnia zawarcia umowy, przygotuje i przedstawi Zamawiającemu Projekt techniczny Platformy (architektura systemu) określający:
 - 2.6.1. Wykaz oprogramowania i licencji niezbędnych do poprawnej pracy Platformy;
 - 2.6.2. Wymogi takie jak ilość urządzeń fizycznych/maszyn wraz z dokładnymi parametrami jak vCPU, vRAM, vHDD wirtualnych wymaganych dla wszystkich składowych Platformy.
- 2.7. Uzgodni z Zamawiającym zakres niezbędnych prac oraz materiałów do przygotowania projektu kursu szkoleniowego na Platformie.
- 2.8. Przedstawi do akceptacji Zamawiającemu projekt interfejsu graficznego, w tym GUI frontendu oraz backendu.
- 2.9. Dostarczy oprogramowanie i licencje niezbędne do poprawnej pracy Platformy.

W zakresie Kursu Wykonawca przygotuje:

- 2.10. Projekt scenariuszy modułów Kursu, zawierający przynajmniej następujące elementy:
 - 2.10.1. Projekt każdego modułu wraz z wytycznymi zawartymi w pkt. 7 niniejszego OPZ.
 - 2.10.2. Pełną treść merytoryczną każdego modułu z uwzględnieniem podziału na ekrany.
 - 2.10.3. Projekt zawierający „Podstawowe informacje o Kursie”. Informacje w nim zawarte muszą być wyświetlane przed rozpoczęciem przez użytkownika Kursu i zawierać takie elementy jak:
 - 2.10.3.1 Szczegółowy opis zawartości kursu wraz z podziałem na poszczególne moduły.
 - 2.10.3.2 Opis minimalnych wymagań sprzętowych oraz programowych.
 - 2.10.3.3 Informację dotyczącą obsługi i nawigacji wewnątrz kursu.
 - 2.10.3.4 Informację na temat aktualności kursu zgodnie z obowiązującym stanem prawnym na dany dzień.
 - 2.10.3.5 Projekt testu podsumowującego odbyty kurs.



2.10.4. Graficzny projekt Kursu z uwzględnieniem kolorystyki CeZ, w którym zostaną zawarte takie elementy jak:

- 2.10.4.1. Graficzna koncepcja całego Kursu.
- 2.10.4.2. Graficzna koncepcja poszczególnych modułów Kursu.
- 2.10.4.3. Spójna koncepcja budowy szablonów graficznych na poszczególnych ekranach.
- 2.10.4.4. Spójny układ powtarzających się sekcji, takich jak: przypomnienia, podsumowania.

Zamawiający dostarczy uwagi do każdego z powyższych projektów w ciągu maksymalnie 5 dni roboczych od ich otrzymania. Wykonawca zobowiązany jest nanieść poprawki do projektów z uwzględnieniem uwag, w terminie maksymalnie 5 dni roboczych od ich otrzymania.

Etap III – Wdrożenie, konfiguracja i testy Systemu.

W ramach realizacji etapu Wykonawca:

- 2.11. Wdroży Platformę na infrastrukturze Zamawiającego zgodnie z zaakceptowanym harmonogramem, planem wdrożenia oraz Projektem technicznym z uwzględnieniem analizy przedwdrożeniowej oraz warunkami opisanymi w pkt. 2.6 OPZ.
- 2.12. Wykona pełną konfigurację Platformy zgodnie z Projektem technicznym będącym wynikiem analizy przedwdrożeniowej.
- 2.13. Dokona instalacji i konfiguracji pełnej wersji przygotowanego Kursu na Platformie.
- 2.14. W ramach oceny Zamawiający ma przejść instruktaż stanowiskowy w zakresie obsługi Kursu na Platformie, na nie ograniczonej liczbie osób jednak nie dłużej niż w ciągu 5 dni dla każdego modułu Kursu.
- 2.15. Przeprowadzi testy bezpieczeństwa Platformy.
- 2.16. Przeprowadzi testy funkcjonowania Kursu na Platformie oraz dostarczy raport z testów.
- 2.17. Dostarczy Dokumentację powykonawczą Platformy dla Zamawiającego.
- 2.18. Dostarczy Kurs w formatach PDF oraz PPTX dla Zamawiającego.
- 2.19. Harmonogram musi zawierać dodatkowe terminy na zgłaszanie uwag przez Zamawiającego oraz ich wprowadzanie przez Wykonawcę. Należy uwzględnić maksymalną liczbę poprawek, która została określona w zapytaniu.
- 2.20. Zamawiający dopuszcza możliwość wprowadzania zmian w harmonogramie. Każda zmiana musi być odpowiednio uzasadniona przez Wykonawcę. Zmiany wymagają akceptacji Zamawiającego, która musi zostać wyrażona drogą elektroniczną. Propozycje zmian mogą być wprowadzone dopiero po zaakceptowaniu koncepcji metodologicznej Kursu oraz ostatecznej wersji harmonogramu.

3. Wdrożenie Platformy

W ramach realizacji Etapu III, Wykonawca dokona wdrożenia Platformy, rozumianego jako:

- 3.1. Instalacja Platformy zgodna z planem wdrożenia na udostępnionym przez Zamawiającego środowisku opisanym w pkt 2.6 OPZ. Szczegóły systemowe zostaną przekazane Wykonawcy po zawarciu umowy.

- 3.2. Przygotowanie konfiguracji Platformy zgodnie z projektem technicznym opisanym w pkt 2.6 OPZ.
- 3.3. Skonfigurowanie logowania zdarzeń na Systemie i umożliwienia zapisywania ich na zewnętrznym serwerze logowania udostępnionym przez Zamawiającego (możliwość zapisywania/eksportu logów w formacie Syslog/CEF/EventLog).
- 3.4. Przeprowadzenie testów wydajnościowych, funkcjonalnych i bezpieczeństwa zainstalowanego Systemu, zgodnie z opracowanymi scenariuszami, o których mowa w punkcie 2.4.1 OPZ, z udziałem Zamawiającego. Wynikiem testów będzie raport potwierdzający spełnienie zawartych w pkt 4.3 Obligatoryjnych funkcjonalności Systemu. Raport potwierdzony zostanie przez obie strony.
- 3.5. Przygotowanie i dostarczenie Dokumentacji powykonawczej oraz dokumentacji użytkownika (administratora/operatora) systemu. Dokumentacja powinna zawierać architekturę rozwiązania, spis wszystkich wykorzystanych technologii, wdrożonych szablonów oraz kursów, opis testów akceptacyjnych i funkcjonalnych rozwiązania, opis konfiguracji systemu (w tym nietypowe ustawienia) oraz instrukcję dla użytkownika/administratora Platformy.
- 3.6. Za pełne wdrożenie Platformy uznaje się instalację systemu, przeprowadzenie z wynikiem pozytywnym testów akceptacyjnych, funkcjonalnych i bezpieczeństwa, dostarczenie kompletu dokumentacji, uruchomienie kursu szkoleniowego.

4. Wymagania dla Platformy

4.1. Wymagania ogólne

- 4.1.1. Platforma musi wspierać środowiska Hyper-V oraz Vmware.
- 4.1.2. Platforma musi wspierać jeden z systemów operacyjnych: Windows Server lub RHEL w wersjach najnowszych, stabilnych na dzień składania ofert.
- 4.1.3. Platforma musi obsługiwać popularne przeglądarki internetowe (Chrome, MS Edge, Firefox, Opera, Safari) w aktualnych wersji na dzień składania oferty.
- 4.1.4. Platforma musi być zgodna z wymaganiami RWD (Responsive Web Design).
- 4.1.5. Platforma musi prawidłowo działać na różnych typach urządzeń jak np.: komórka, tablet, komputer typu desktop.
- 4.1.6. Platforma nie może wymagać instalacji dodatkowego oprogramowania.
- 4.1.7. Platforma musi obsługiwać czcionki wielojęzyczne w systemie kodowania UTF-8.
- 4.1.8. Platforma musi spełniać wymagania WCAG 2.1 na poziomie AA zgodnie z wytycznymi zawartymi w załączniku nr 4 do Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2017 poz. 2247).
- 4.1.9. Platforma musi posiadać nowoczesny interfejs graficzny, którego projekt zostanie zaakceptowany przez Zamawiającego podczas etapu II.
- 4.1.10. Projekt layoutu/kolorystyki Platformy zostanie ustalony z Zamawiającym. Musi nawiązywać do wizerunku portali Zamawiającego, a logo Zamawiającego ma zostać dodane zgodnie z księgą znaku. Logo i księga znaku zostanie udostępniona przez Zamawiającego.
- 4.1.11. Platforma musi spełniać wymagania rekomendacji ATAG 2.0.
- 4.1.12. Wykonawca musi dostarczyć dokumentację zawierającą informację tj.:

- 4.1.12.1. Użyty silnik CMS oraz jego wersja.
- 4.1.12.2. Wykorzystane framework'i.
- 4.1.12.3. Wykorzystane biblioteki.
- 4.1.12.4. Wykorzystane wtyczki i dodatki do CMSa.
- 4.1.12.5. Wdrożone szablony.

4.2. Zarządzanie Platformą

- 4.2.1. Platforma musi umożliwiać tworzenie indywidualnych kont dla każdego użytkownika/administratora Systemu.
- 4.2.2. Platforma nie może posiadać ograniczenia na liczbę użytkowników.
- 4.2.3. Platforma musi wymagać w celu uwierzytelnienia loginu i hasła użytkownika.
- 4.2.4. Platforma musi wspierać uwierzytelnianie wieloskładnikowe.
- 4.2.5. Platforma musi umożliwiać obsługę captcha.
- 4.2.6. Platforma musi umożliwiać proces odzyskania hasła.
- 4.2.7. Platforma musi pozwalać na zdefiniowanie polityki blokowania logowania po określonej liczbie błędnych logowań.
- 4.2.8. Platforma musi umożliwiać definiowanie nazw użytkowników innych niż ich adres email.
- 4.2.9. Platforma musi zapewniać silną politykę haseł lub umożliwiać jej określenie dla użytkowników Systemu.
- 4.2.10. Platforma musi umożliwiać konfigurowanie zakresu uprawnień w Systemie z wykorzystaniem predefiniowanych ról wewnętrznych (np. dostęp tylko do raportów, administrator systemu, analityk itp.).
- 4.2.11. Platforma musi umożliwiać edytowanie oraz usuwanie istniejących kont.
- 4.2.12. Platforma musi umożliwiać hurtowe tworzenie kont poprzez import danych w co najmniej jednym z formatów: csv.
- 4.2.13. Platforma musi udostępniać możliwość rejestrowania i raportowania zdarzeń związanych z funkcjonowaniem Platformy.
- 4.2.14. Platforma musi umożliwiać tworzenie oraz edytowanie treści kursów poprzez edytor WYSIWIG dostępny w panelu zarządzania.

4.3. Obligatoryjne funkcjonalności Platformy

- 4.3.1. Platforma musi posiadać możliwość obsługi takich standardów jak: SCORM, xAPI, LTI, IMS, IMS Content Packaging.
- 4.3.2. Platforma musi mieć możliwość obsługi standardów SCORM w wersji 1.2 (Sharable Content Object Reference Model).
- 4.3.3. Platforma musi umożliwiać eksportowanie kursów oraz importowanie kursów w standardach co najmniej SCORM 1.2.
- 4.3.4. Platforma musi posiadać wbudowane narzędzia do tworzenia treści (H5P).
- 4.3.5. Platforma obsługuje czcionki wielojęzyczne z uwzględnieniem systemu kodowania UTF-8.
- 4.3.6. Platforma powinna umożliwiać integrację z Microsoft 365, Google Drive, Zoom, Trello.
- 4.3.6.1. Platforma powinna umożliwiać tworzenie i zarządzanie spotkaniami w Microsoft Teams.

- 4.3.6.2. Platforma powinna umożliwiać synchronizację kursów i zespołów z Microsoft Teams.
- 4.3.6.3. Platforma powinna umożliwiać dostęp do plików Word przechowywanych w Microsoft OneDrive.
- 4.3.6.4. Platforma powinna umożliwiać import/export plików Excel znajdujących się w usłudze Microsoft OneDrive.
- 4.3.7. Platforma musi umożliwiać zarządzanie kursami, testami, ankietami oraz mailingami z poziomu przeglądarki internetowej.
- 4.3.8. Platforma powinna być dostępna również z poziomu dedykowanej aplikacji mobilnej.
- 4.3.9. Platforma musi być w pełni personalizowana.
 - 4.3.9.1. Platforma musi nawiązywać do wizerunku portali Zamawiającego, a logo Zamawiającego ma zostać dodane zgodnie z księgą znaku.
- 4.3.10. Platforma powinna zapewniać wysoką skalowalność.
 - 4.3.10.1. Platforma musi być w stanie obsłużyć jednocześnie około tysiąca osób bez odczucia spadku wydajności systemu.
- 4.3.11. Platforma powinna obsługiwać wiele języków, przynajmniej 50 najbardziej znanych oraz umożliwiać tłumaczenie całego interfejsu systemu.
- 4.3.12. Tworzenie kursów, testów, ankiet czy mailingów musi być możliwe z poziomu dedykowanych edytorów oraz kreatorów oraz nie może wymagać znajomości języków programowania.
- 4.3.13. Platforma musi umożliwiać wysyłkę mailingów do wybranych użytkowników lub ich grup bez potrzeby instalowania dodatkowych usług lub serwerów po stronie Zamawiającego.
- 4.3.14. Platforma musi umożliwiać mailowe powiadamianie wybranych użytkowników lub ich grup o publikowanych materiałach, terminach kursów oraz o ich zmianach.
- 4.3.15. Platforma musi umożliwiać przerwanie kursu w dowolnym momencie oraz kontynuowanie szkolenia od miejsca, w którym przerwano.
- 4.3.16. Platforma musi umożliwiać wyświetlanie filmów bez konieczności dodatkowych instalacji.
- 4.3.17. Platforma musi umożliwiać umieszczanie oraz otwieranie plików w formatach: pdf, docx, txt, jpg, png, bmp, pptx, xlsx, odt, ods, odp, html, avi, mov, wmv, mp3, mp4.
- 4.3.18. Platforma musi umożliwiać wyłączanie oraz włączanie dźwięku w szkoleniu.
- 4.3.19. Platforma musi umożliwiać tworzenie testów typu:
 - 4.3.19.1. Zamkniętych pojedynczego wyboru.
 - 4.3.19.2. Zamkniętych wielokrotnego wyboru.
 - 4.3.19.3. Otwartych.
- 4.3.20. Platforma musi umożliwiać generowanie losowej kolejności pytań z określonej puli wszystkich pytań.
- 4.3.21. Platforma musi umożliwiać definiowania czasu trwania testu.
- 4.3.22. Platforma musi umożliwiać definiowanie liczby podejść do testu.
- 4.3.23. Platforma musi umożliwiać definiowanie progu zaliczenia testu.
- 4.3.24. Platforma musi umożliwiać definiowanie czasu do kiedy aktywny jest kurs oraz test.

- 4.3.25. Platforma musi umożliwiać definiowanie daty od jakiej dostępny będzie kurs oraz test, a także dla jakiej grupy użytkowników.
- 4.3.26. Platforma musi umożliwiać tworzenie kursów, testów oraz quizów z pomocą gotowych szablonów.
- 4.3.27. Platforma musi umożliwiać tworzenie własnych szablonów – „od zera” lub na podstawie istniejących szablonów.
- 4.3.28. Platforma musi umożliwiać tworzenie ankiet oceny kursów oraz testów dla użytkowników.
- 4.3.29. Platforma musi udostępniać możliwość samodzielnego zapisania się przez użytkownika na kurs. Także z pomocą zdefiniowanego klucza rejestracyjnego.
- 4.3.30. Platforma musi umożliwiać użytkownikom przeglądanie dostępnych dla nich kursów zgodnie z przydzielonymi przez administratora dostępami.
- 4.3.31. Platforma musi umożliwiać automatyczne ocenianie testów.
- 4.3.32. Platforma musi umożliwiać generowanie zdefiniowanych raportów oraz tworzenie własnych raportów.
- 4.3.33. Platforma musi umożliwiać eksport danych z raportów w co najmniej jednym z formatów: pdf, xlsx, html, csv.
- 4.3.34. Raport generowane przez Platformę muszą prezentować co najmniej dane takie jak:
 - 4.3.34.1. Liczba uczestników
 - 4.3.34.2. Postępy uczestników w kursach.
 - 4.3.34.3. Wyniki testów uczestników
 - 4.3.34.4. Wyniki ankiet
- 4.3.35. Platforma musi umożliwiać automatyczne wystawianie zdefiniowanych certyfikatów ukończenia testu.
- 4.3.36. Platforma musi umożliwiać zdefiniowanie szablonu certyfikatu ukończenia testu zgodnie z wymaganiami Zamawiającego zawierającymi m.in. kwestię kolorystyki, ogólnego layout'u oraz użycia logo Zamawiającego.
- 4.3.37. Platforma musi automatycznie uzupełniać dane uczestnika przed wystawieniem certyfikatu ukończenia testu.
- 4.3.38. Platforma musi umożliwiać mechanizm udostępnienia certyfikatu ukończenia testu użytkownikowi poprzez Platformę oraz drogą mailową.

5. Wymagania techniczne Kursu

Wykonawca dokona wdrożenia Kursu na Platformie. Kurs musi być zbudowany z uwzględnieniem wymagań i funkcjonalności świadczonych przez Platformę w pkt 4, ze szczególnym uwzględnieniem pkt: 4.1.4, 4.1.5, 4.1.7, 4.1.8, 4.1.11, 4.3.1, 4.3.2, 4.3.3, 4.3.4, 4.3.6, 4.3.17, 4.3.19.

6. Tematyka Kursu

6.1. Uczestnicy szkoleń zostaną zapoznani oraz przeszkoleni z tematyki dot. cyberbezpieczeństwa, w tym z zakresu poznania i stosowania odpowiednich technologii, procedur czy procesów dot. np. kontroli, minimalizacji ryzyk skutecznych cyberataków, i podniesienia poziomu ochrony przed nieuprawnionym wykorzystaniem systemów, sieci czy przechwycenia bądź utraty danych. Dzięki

szkoleniom zmniejszone zostanie ryzyko popełniania przez pracowników Podmiotów medycznych błędów czy naruszeń w obszarze cyberbezpieczeństwa. Dodatkowo w przypadku kadry zarządzającej niezmiernie istotne jest podniesienie świadomości osób zarządzających Podmiotami w zakresie konieczności ciągłego podnoszenia stopnia zabezpieczenia placówek przed niepożądanymi zdarzeniami jakimi są cyberprzestępstwa, szczególnie z uwagi na zakres danych wrażliwych jakie zbierane i przetwarzane są przez Podmioty medyczne.

6.2. Zamawiający dzieli zamówienie w pkt. dot. przygotowania szczegółowej agendy - dla trzech szkoleń (modułów) dedykowanych konkretnej (jednej z trzech) grup odbiorców:

6.2.1. Szkolenia z podstaw cyberbezpieczeństwa dla wszystkich pracowników Podmiotów medycznych, którzy na co dzień w bieżącej pracy korzystają z systemów teleinformatycznych, Internetu oraz urządzeń elektronicznych które przetwarzają dane w podmiotach (np.: laptopy, tablety, drukarki).

6.2.2. Szkolenia z podstaw cyberbezpieczeństwa dla kadry zarządzającej w Podmiocie medycznym.

6.2.3. Szkolenia z podstaw cyberbezpieczeństwa dla pracowników działów IT Podmiotów medycznych, ze szczególnym uwzględnieniem zagadnień związanych z zasadami eksploatacji i sprawowania nadzoru nad infrastrukturą Podmiotu zapewniających bezpieczeństwo informacji.

6.3. Wykonawca odpowiada za opracowanie szczegółowej agendy dla ww. modułów szkoleń oraz materiałów szkoleniowych w tym prezentacji i skryptu trenera.

6.4. Zamawiający jest otwarty na sugestie Wykonawcy w zakresie poszerzenia tematyki danego modułu Kursu.

6.5. Zamawiający nie dopuszcza łączenia modułów szkoleniowych w jedną całość.

7. Minimalny zakres tematyczny poszczególnych modułów

7.1. Moduł 1 „Podstawy cyberbezpieczeństwa dla każdego”

7.1.1. Podstawowe pojęcia związane z cyberbezpieczeństwem: Omówienie podstawowych zagrożeń, takich jak phishing, malware, ransomware i hakerstwo, a także zasad bezpiecznego korzystania z urządzeń elektronicznych.

7.1.2. Bezpieczeństwo haseł i kont użytkowników: Zapoznanie z zasadami tworzenia silnych haseł, unikalnych dla różnych kont użytkowników oraz sposobami przechowywania ich w bezpieczny sposób. Przedstawienie podstawowych narzędzi do zarządzania hasłami.

7.1.3. Bezpieczeństwo sieci i urządzeń: Omówienie zasad bezpieczeństwa w sieciach i na urządzeniach, takich jak stosowanie firewalli, szyfrowanie danych, aktualizacja systemów i oprogramowania antywirusowego.

7.1.4. Bezpieczeństwo e-maili: Zapoznanie z technikami rozpoznawania i unikania phishingowych wiadomości e-mail, w tym podejrzanych linków i załączników oraz sposobami reagowania na takie zagrożenia.

7.1.5. Bezpieczeństwo podczas przeglądania stron internetowych: Omówienie zasad bezpiecznego korzystania z przeglądarki internetowej i unikania szkodliwych witryn internetowych.

- 7.1.6. Bezpieczeństwo podczas korzystania z mediów społecznościowych: Omówienie zasad bezpiecznego korzystania z mediów społecznościowych, takich jak Facebook, Instagram, X (dawniej Twitter) i LinkedIn, w tym unikania nadużyć i ochrony prywatności.
- 7.1.7. Zasady korzystania z urządzeń firmowych: Omówienie zasad korzystania z urządzeń firmowych, takich jak komputery, laptopy, tablety i smartfony, w tym zasad odpowiedzialności za ich bezpieczeństwo i konsekwencje naruszeń.
- 7.1.8. Zgłaszanie incydentów: Przedstawienie sposobów zgłaszania podejrzanych działań oraz incydentów związanych z bezpieczeństwem informacji, w tym sposobów raportowania problemów i konsekwencji braku zgłaszania incydentów.
- 7.2. Moduł 2 „Podstawy cyberbezpieczeństwa dla kadry kierowniczej”
- 7.2.1. Wprowadzenie do cyberbezpieczeństwa: Omówienie podstawowych pojęć i definicji związanych z cyberbezpieczeństwem, takich jak zagrożenia, ataki, ochrona i przepisy.
- 7.2.2. Bezpieczeństwo haseł i kont użytkowników: Zapoznanie z zasadami tworzenia silnych haseł oraz unikalnych haseł dla różnych kont. Omówienie wymogów wynikających z przepisów dotyczących ochrony danych osobowych, w tym zasad RODO.
- 7.2.3. Bezpieczeństwo sieci i urządzeń: Omówienie zasad ochrony sieci i urządzeń przed atakami, w tym stosowanie firewalli, szyfrowanie danych i wirtualnych sieci prywatnych (VPN). Zapoznanie z wymogami przepisów dotyczących ochrony danych w sieciach teleinformatycznych.
- 7.2.4. Bezpieczeństwo korespondencji elektronicznej: Zapoznanie z technikami rozpoznawania i unikania phishingowych wiadomości e-mail, w tym podejrzanych linków i załączników. Omówienie zasad związanych z przetwarzaniem danych w poczcie elektronicznej.
- 7.2.5. Polityka bezpieczeństwa: Omówienie zasad korzystania z systemów i zasobów informatycznych, odpowiedzialności za naruszenia bezpieczeństwa oraz procedur reagowania na incydenty. Zapoznanie z wymogami wynikającymi z przepisów dotyczących ochrony danych osobowych oraz polityki informacyjnej przedsiębiorstwa.
- 7.2.6. Szkolenie pracowników: Szkolenie pracowników w zakresie bezpieczeństwa IT, w tym zasad korzystania z systemów informatycznych, rozpoznawania zagrożeń i raportowania podejrzanych działań. Omówienie wymogów wynikających z przepisów dotyczących szkoleń w zakresie ochrony danych osobowych.
- 7.2.7. Monitorowanie i raportowanie incydentów: Metody monitorowania systemów informatycznych w celu wykrycia i zgłoszenia incydentów, w tym wykorzystanie systemów detekcji zagrożeń (IDS) i systemów zapobiegania zagrożeniom (IPS). Zapoznanie z wymogami przepisów dotyczących raportowania incydentów bezpieczeństwa informacji.
- 7.2.8. Ochrona danych i zgodność z przepisami: Zapewnienie ochrony prywatności i zgodność z przepisami dotyczącymi ochrony danych osobowych oraz monitorowanie i zarządzanie dostępem do poufnych informacji. Omówienie wymogów wynikających z przepisów dotyczących ochrony danych w systemach informatycznych.

7.3. Moduł 3 „Podstawy cyberbezpieczeństwa dla pracowników IT”

- 7.3.1. Podstawowe pojęcia związane z cyberbezpieczeństwem: Omówienie podstawowych zagrożeń, takich jak phishing, malware, ransomware i hakerstwo, a także zasad bezpiecznego korzystania z urządzeń elektronicznych.
- 7.3.2. Bezpieczeństwo haseł i kont użytkowników: Zapoznanie z zasadami tworzenia silnych haseł, unikalnych dla różnych kont użytkowników oraz sposobami przechowywania ich w bezpieczny sposób. Przedstawienie podstawowych narzędzi do zarządzania hasłami.
- 7.3.3. Bezpieczeństwo sieci i urządzeń: Omówienie zasad bezpieczeństwa w sieciach i na urządzeniach, takich jak stosowanie firewalli, szyfrowanie danych, aktualizacja systemów i oprogramowania antywirusowego.
- 7.3.4. Bezpieczeństwo e-maili: Zapoznanie z technikami rozpoznawania i unikania phishingowych wiadomości e-mail, w tym podejrzanych linków i załączników oraz sposobami reagowania na takie zagrożenia.
- 7.3.5. Bezpieczeństwo podczas przeglądania stron internetowych: Omówienie zasad bezpiecznego korzystania z przeglądarki internetowej i unikania szkodliwych witryn internetowych.
- 7.3.6. Bezpieczeństwo podczas korzystania z mediów społecznościowych: Omówienie zasad bezpiecznego korzystania z mediów społecznościowych, takich jak Facebook, Instagram, Twitter i LinkedIn, w tym unikania nadużyć i ochrony prywatności.
- 7.3.7. Zabezpieczanie systemów i aplikacji: Omówienie zasad zabezpieczania systemów i aplikacji przed atakami z zewnątrz oraz wewnętrznych zagrożeń, w tym uwierzytelnianie, kontrola dostępu i monitorowanie zdarzeń.
- 7.3.8. Zgłaszanie incydentów i reagowanie na nie: Przedstawienie sposobów zgłaszania podejrzanych działań oraz incydentów związanych z bezpieczeństwem informacji, w tym sposobów raportowania problemów, reagowania na incydenty i konsekwencji braku zgłaszania incydentów.

8. Wymagania ogólne

- 8.1. Kurs ma być przygotowany w języku polskim i przed uruchomieniem wymaga akceptacji Zamawiającego. Powinien być wolny od błędów stylistycznych, ortograficznych, typograficznych oraz interpunkcyjnych.
- 8.2. Zamawiający wymaga, aby Kurs był zgodny z polskim prawem obowiązującym w dniu podpisania protokołu zdawczo-odbiorczego. W przypadku zmiany przepisów w obszarze tematycznym Kursu przed tym terminem, Wykonawca jest zobowiązany do wprowadzenia odpowiednich korekt w treściach merytorycznych, niezależnie od aktualnie realizowanego etapu zamówienia.
- 8.3. Projekt layoutu/kolorystyki Kursu zostanie ustalony z Zamawiającym. Musi nawiązywać do wizerunku portali Zamawiającego, a logo Zamawiającego ma zostać dodane zgodnie z księgą znaku. Księga znaku zostanie udostępniona przez Zamawiającego.
- 8.4. Łączny czas trwania Kursu nie powinien przekraczać 5 godzin zegarowych (300 minut). Czas ten obejmuje okres potrzebny uczestnikowi na pełne przejście przez Kurs, w tym przyswojenie treści

w formie tekstów, materiałów wideo lub audio, a także wykonanie wszystkich ćwiczeń oraz pytań testowych stanowiących nieodłączny element Kursu.

- 8.5. Kurs będzie podzielony na 3 moduły, których minimalny zakres tematyczny został określony w pkt. 7 niniejszego OPZ.
- 8.6. Każdy moduł będzie zawierał część informacyjną oraz praktyczne przykłady przedstawiające omawiane zagadnienie, wraz z opisem rodzaju środka zaradczego, który można zastosować w danym przypadku (minimum 5 na moduł).
- 8.7. Każdy moduł ma zawierać minimalnie 40 ekranów merytorycznych, opracowanych zgodnie z metodologią. Liczba ekranów będzie uzależniona od skomplikowania tematu i powinna go w pełni wyczerpywać.
 - 8.7.1. Powinno znajdować się minimalnie 30 ekranów informacyjnych z tekstem lub tekstem i grafiką.
 - 8.7.2. Powinno znajdować się minimalnie 10 ekranów przedstawiających praktyczne przykłady omawianego zagadnienia.
- 8.8. Zamawiający może wyrazić zgodę na zmianę liczby ekranów, na przykład w sytuacji, gdy temat Kursu został całkowicie omówiony i nie wymaga dalszego rozszerzania.
- 8.9. Po zakończeniu modułu Kursu, uczestnik przystępuje do testu podsumowującego. Test końcowy powinien zawierać co najmniej 20 pytań, losowo wybranych z bazy minimum 30 pytań, które obejmują treści merytoryczne danego modułu.
 - 8.9.1. Zmniejszenie liczby pytań w teście wymaga zgody Zamawiającego. Uczestnik będzie mógł przystępować do testu dowolną liczbę razy, jednak każde podejście będzie miało określony limit czasowy. Wykonawca proponuje czas, który będzie odpowiedni do treści testu.
 - 8.9.2. Test będzie składał się z pytań jednokrotnego i wielokrotnego wyboru, z czterema możliwymi odpowiedziami. Ekran z oceną poprawności odpowiedzi będzie zawierał pełne pytania oraz odpowiedzi, z zaznaczeniem udzielonej i prawidłowej odpowiedzi. Uczestnik uzyska dostęp do testu końcowego po ukończeniu całego modułu Kursu.
- 8.10. Zamawiający ma prawo do dokonania przeglądu oraz wprowadzenia zmian w scenariuszach modułów Kursu, grafice, informacjach wstępnych o Kursie oraz koncepcji metodologicznej.
- 8.11. Wykonawca przedstawi projekty koncepcji metodologicznej Kursu i harmonogramu Zamawiającemu w ciągu 10 dni kalendarzowych od dnia podpisania umowy. Zamawiający ma 5 dni roboczych na zgłoszenie uwag. Wykonawca wprowadzi wymagane zmiany w ciągu 5 dni roboczych od ich otrzymania.
- 8.12. Kurs ma być przygotowany z uwzględnieniem metod i technik przekazywania wiedzy, które zapewnią efektywną naukę i przyswajanie treści przez uczestników, np. w formie quizów, ćwiczeń oraz symulacji. Forma prezentacji powinna obejmować teksty uzupełnione grafikami, infografikami oraz materiałami wideo.



- 8.13. Zamawiający nabywa prawo do licencji wieczystej na Kurs bez limitu powieleń szkolenia. Szkolenia powielone będą wykorzystywane zgodnie z pkt. 1 niniejszego OPZ.
- 8.14. Zamawiający zastrzega sobie prawo do późniejszej edycji Kursu, np. w zakresie podmioty przestarzałych grafik, kontentu na aktualne.

9. Bezpieczeństwo aplikacji

- 9.1. Dostarczenie wyników testów penetracyjnych wykonanych na zgodność ze standardem OWASP ASVS w najnowszym wydaniu na poziomie przynajmniej L1. Testy muszą wykazać brak podatności na poziomie średnim, wysokim i krytycznych.
- 9.2. Dostarczenie deklaracji zgodności Platformy z wymaganiami standardu ASVS L2 fundacji OWASP.
- 9.3. Dostarczenie wyników skanów podatności wykonanego aktualnym systemem klasy skaner podatności. Testy muszą wykazać brak podatności na poziomie średnim, wysokim i krytycznych.
- 9.4. W szczególnych przypadkach, gdy nie możliwe będzie usunięcie podatności konieczne będzie wypracowanie wspólnie z Zamawiającym metody mitygacji.

10. Warunki udziału w postępowaniu

- 10.1. Zamawiający wymaga, aby Wykonawca ciągu ostatnich 5 lat, a jeśli okres działalności jest krótszy – w tym czasie, zrealizował przynajmniej 2 usługi związane z tworzeniem dedykowanych kursów e-learningowych. Usługi te muszą obejmować przygotowanie kursu pod względem merytorycznym, graficznym i metodologicznym, a także jego wdrożenie. Oferenci powinni załączyć dowody potwierdzające należyte wykonanie tych usług.
- 10.2. Wykonawca powinien dysponować co najmniej:
- 10.2.1. Jednym metodykiem e-learningu/dydaktykiem multimedialnym (Instructional System Designer), który w ciągu ostatnich 5 lat stworzył co najmniej 2 scenariusze oraz 2 koncepcje metodologiczne kursów e-learningowych.
- 10.2.2. Jednym informatykiem, który w ciągu ostatnich 5 lat wdrożył co najmniej 2 kursy e-learningowe na platformie zgodnej ze standardem SCORM.
- 10.2.3. Jednym grafikiem komputerowym, który w ciągu ostatnich 5 lat zaprojektował graficznie co najmniej 2 kursy e-learningowe, obejmujące layout kursu, wizualizację treści, szatę graficzną oraz oprawę wizualną treści.
- 10.2.4. Jednym ekspertem z wykształceniem wyższym informatycznym, który w ciągu ostatnich 5 lat przeprowadzili co najmniej 3 szkolenia/warsztaty z zakresu Cyberbezpieczeństwa IT. Do ofert należy dołączyć materiały szkoleniowe, na podstawie których przeprowadzono co najmniej 2 z tych szkoleń.
- 10.2.4.1. Posiada wiedzę z zakresu i technologii związanych z zapewnianiem poziomu bezpieczeństwa infrastruktury, systemów, aplikacji, sieci i protokołów, IDS, IPS, zapór ogniowych, VPN, systemów operacyjnych: Linux, Windows i dedykowanych aplikacji oraz standardy podatności typu: DREAD, CVSS, CVE, CWE.
- 10.2.4.2. Spełnia łącznie co najmniej 2 z podanych niżej zakresów:
- 10.2.4.2.1. Nadzór i prowadzenie audytów bezpieczeństwa na zgodność z KRI lub KSC.

- 10.2.4.2.2. Udział w wykonywaniu testów penetracyjnych (aplikacje webowe, infrastruktura, aplikacje mobilne).
 - 10.2.4.2.3. Audyty kodu źródłowego.
 - 10.2.4.2.4. Działania inżynierii społecznej w tym prowadzenie szkoleń z security awareness.
 - 10.2.4.2.5. Analizy śledczej.
 - 10.2.4.2.6. Badania złośliwego oprogramowania.
 - 10.2.4.2.7. Nadzór i konfiguracja systemów bezpieczeństwa typu UTM, AV, EDR, SMG.
 - 10.2.4.2.8. Monitorowanie zagrożeń w systemach klasy SIEM.
- 10.3. W przypadku usług świadczonych przez każdą z wyżej wymienionych osób, Wykonawca przedstawi dowody potwierdzające ich doświadczenie. Dowodami mogą być kopie referencji, protokołów odbioru lub inne dokumenty, które potwierdzają należyte wykonanie usługi.
- 10.4. Poszczególne role wymienione w pkt. 10.2.1 – 10.2.4 mogą być łączone, aczkolwiek niezbędne minimum to 3 osoby.

11. Usługa rozwoju Platformy i Kursu – Zamawiający będzie mógł zlecać w okresie 24 miesięcy od dnia odbioru zamówienia.

- 11.1. Wykonawca będzie świadczył usługi programistyczne związane ze zmianą lub dodaniem nowych funkcjonalności do Platformy.
- 11.2. Wykonawca będzie świadczył usługi związane ze zmianą lub dodaniem nowych treści do Kursu.
- 11.3. Zapotrzebowanie na prace rozwojowe może być zgłaszane przez cały okres trwania umowy.
- 11.4. Maksymalna liczba godzin rozwojowych nie może przekroczyć 240 godzin roboczych. Czas świadczenia usługi rozwoju Platformy/Kursu – 24 miesiące od dnia odbioru przedmiotu Umowy.
- 11.5. Rozliczenie liczby wykorzystanych godzin oraz rozliczenie kosztów z nimi związanych będzie się odbywać w cyklach miesięcznych.



12. Gwarancja

- 12.1. W ramach realizacji przedmiotu zamówienia, wykonawca będzie świadczył usługi gwarancyjne na:
- 12.1.1. Wdrożony System
 - 12.1.2. Oprogramowanie
 - 12.1.3. Dostarczony Kurs
- 12.2. Wykonawca oświadcza, że Oprogramowanie przez niego dostarczone objęte jest gwarancją producenta.
- 12.3. Wykonawca udziela gwarancji na Platformę oraz Kurs, która obowiązuje przez 24 miesiące od dnia podpisania odpowiedniego Protokołu Odbioru, wskazanego w Umowie.
- 12.4. Wykonawca zobowiązany jest w okresie realizacji Umowy do usuwania Błędów Platformy/Kursu na zasadach opisanych w niniejszym załączniku.
- 12.5. Zakres świadczeń w ramach Gwarancji obejmuje:
- 12.5.1. usuwanie Błędów Platformy i Kursu, zgodnie z Czasami Reakcji, Czasami Naprawy, Czas Propozycji Rozwiązania i dla poszczególnych kategorii Błędów,
 - 12.5.2. dostarczanie nowych wersji Oprogramowania,
 - 12.5.3. aktualizację Dokumentacji w przypadku wprowadzania zmian w Platformie lub Kursie w wyniku naprawy Błędu, w terminie 5 Dni roboczych od dnia naprawy

Priorytet	Czas podjęcia	Czas na rozwiązanie
Błąd Krytyczny Platformy	Do 2 godzin roboczych	Do 1 dni roboczych
Błąd Istotny Kursu	Do 4 godzin roboczych	Do 1 dzień roboczy
Błąd Merytoryczny Kursu	Do 8 godzin roboczych	Do 3 dni roboczych
Błąd Istotny Platformy	Do 8 godzin roboczych	Do 5 dni roboczych
Inne Błędy oraz pytania do wsparcia	Do 8 godzin roboczych	Do 5 dni roboczych

Definicje:

Błąd Krytyczny Platformy	Błąd Platformy, który uniemożliwia wykorzystywanie podstawowych funkcji, w szczególności uniemożliwiających logowanie do Platformy przez administratorów oraz użytkowników, a także powodujący nie zgodne z projektem wyświetlanie Platformy.
Błąd Istotny Kursu	Błąd w Kursie, który jest spowodowany nieprawidłowym działaniem lub brakiem oczekiwanej funkcji.
Błąd Merytoryczny Kursu	Błąd w Kursie, który zawiera nieścisłość lub nieprawidłową informację zawartą w materiałach edukacyjnych, która jest sprzeczna z faktami, wiedzą lub obowiązującymi standardami.

Błąd Istotny Platformy	Błąd inny niż opisany w Błędzie krytycznym, w szczególności taki błąd w Platformie, który ma niewielki bezpośredni wpływ na działanie Platformy, a wszystkie podstawowe funkcjonalności są zachowane lub dostępne za zasadzie obejścia.
Inne Błędy oraz pytania wsparcia	Błąd działania lub błędne działanie Platformy/Kursu niezgodne z założeniami, specyfikacją techniczną, za które odpowiada Wykonawca.

- 12.6. Wykonawca zobowiązuje się do świadczenia usług w ramach Gwarancji w sposób zapobiegający utracie jakichkolwiek danych.
- 12.7. W ramach świadczenia przez Wykonawcę usług w ramach Gwarancji, Wykonawca zobowiązany jest do umożliwienia osobom wskazanym przez Zamawiającego obserwacji prac Wykonawcy.
- 12.8. W przypadku wykrycia przez Zamawiającego Błędu, Zamawiający dokona kwalifikacji zgłoszenia (Błąd Krytyczny Platformy / Błąd Istotny Kursu / Błąd Merytoryczny Kursu / Błąd Istotny Platformy / Inne Błędy oraz pytania wsparcia) według własnego uznania na podstawie zdefiniowanych kryteriów. Zgłoszenie zawierać będzie posiadane przez Zamawiającego informacje na temat nieprawidłowego działania Platformy/Kursu istotne w ocenie Zamawiającego dla zdiagnozowania i usunięcia nieprawidłowości.
- 12.9. Formalne potwierdzenie Zgłoszenia stanowi przesłanie przez Zamawiającego do Wykonawcy informacji o wystąpieniu Błędu i opisie jego symptomów.
- 12.10. Wykonawca zobowiązuje się rejestrować zgłaszane Błędy wykorzystując rozwiązania umożliwiające raportowanie Zgłoszeń - w tym Czas Reakcji, Czas Propozycji Rozwiązania oraz Czas Naprawy.
- 12.11. Wykonawca będzie przyjmował Zgłoszenia przez cały czas, tj. w systemie 8:00-16:00 Dni robocze.
- 12.12. Wykonawca będzie przyjmował Zgłoszenia przekazywane w jeden z następujących sposobów:
- 12.12.1. za pomocą aplikacji serwisowej (interfejsu serwisowego);
- 12.12.2. przez przesłanie Zgłoszenia pocztą elektroniczną
- 12.13. W razie otrzymania przez Wykonawcę Zgłoszenia lub w razie uzyskania przez Wykonawcę wiedzy o wystąpieniu Błędu z innego źródła niż Zgłoszenie, Wykonawca zobowiązany będzie do podjęcia działań zmierzających do usunięcia Błędu.

- 12.14. Jeżeli Zamawiający nie wie o istnieniu Błędu, Wykonawca poinformuje w ciągu 24 godzin, Zamawiającego o jej wystąpieniu.
- 12.15. Jeżeli Wada została wykryta przez Wykonawcę, Wykonawca nada jej odpowiednią wstępną kategorię (Błąd Krytyczny Platformy / Błąd Istotny Kursu / Błąd Merytoryczny Kursu / Błąd Istotny Platformy / Inne Błędy oraz pytania wsparcia). W ciągu 24 godzin od powiadomienia przez Wykonawcę Zamawiający ma prawo zmienić kategorię Błędu.
- 12.16. Ostatecznie o klasyfikacji kategorii Błędu (Błąd Krytyczny Platformy / Błąd Istotny Kursu / Błąd Merytoryczny Kursu / Błąd Istotny Platformy / Inne Błędy oraz pytania wsparcia) decyduje Zamawiający.
- 12.17. Wykonawca zobowiązany jest do potwierdzenia przyjęcia Zgłoszenia odpowiednim wpisem we własnej aplikacji serwisowej (dotyczy to również Zgłoszeń składanych pocztą elektroniczną) oraz o nadaniu indywidualnego identyfikatora zgłoszenia. Chwila potwierdzenia przyjęcia Zgłoszenia nie ma wpływu na Czas Reakcji, Czas Propozycji Rozwiązania, Czas Naprawy. Wykonawca jest zobowiązany do udostępnienia Zamawiającemu własnej aplikacji serwisowej w zakresie przeglądania Zgłoszeń związanych z realizacją Umowy.
- 12.18. Jeżeli Wykonawca stwierdzi, iż nieprawidłowe działanie Platformy/Kursu, którego dotyczy Zgłoszenie nie jest spowodowane Błędem, za który odpowiedzialny jest Wykonawca, wówczas Wykonawca zobowiązany jest:
- 12.18.1. Wskazać przyczynę nieprawidłowego działania poprzez wskazanie elementu, który ją powoduje,
- 12.18.2. Udzielić wsparcia Zamawiającemu lub innej osobie trzeciej wskazanej przez Zamawiającego usuwającej przyczyny Zgłoszenia, w tym udzielić takiej osobie wszelkich informacji o Platformie potrzebnych do przywrócenia pełnej funkcjonalności.
- 12.19. Po przeprowadzeniu Naprawy, Wykonawca zgłosi ją do odbioru poprzez przekazanie informacji:
- 12.19.1. Za pomocą aplikacji serwisowej (interfejsu serwisowego);
- 12.19.2. Przez przesłanie pocztą elektroniczną
- 12.20. Po weryfikacji dokonania Naprawy, przedstawiciel Zamawiającego niezwłocznie potwierdzi w systemie lub drogą elektroniczną skuteczność lub nieskuteczność Naprawy. Data i godzina rejestracji w systemie lub wysłania maila przez przedstawiciela Zamawiającego jest datą i godziną wykonania usługi Naprawy.
- 12.21. W przypadku stwierdzenia dokonania skutecznej Naprawy Wykonawca zamyka Zgłoszenie i potwierdza jego wykonanie poprzez „zamknięcie” zgłoszenia w aplikacji serwisowej.



12.22. Naprawa, co do której Wykonawca poinformował o jej wykonaniu, a która została odrzucona przez przedstawiciela Zamawiającego ze względu na fakt, iż testy przeprowadzone przez Zamawiającego wykazują, że Błąd nadal występuje, trwa do czasu jej skutecznego wykonania.

12.23. Wykonawca zobowiązany jest do prowadzenia ewidencji otwartych i zamkniętych Zgłoszeń, obejmującej w szczególności opis stanu realizacji danej Naprawy. Powyższe dane dostępne są cały czas dla Zamawiającego za pośrednictwem aplikacji serwisowej.

12.24. Wraz z dokonaniem Naprawy Wykonawca zobowiązany jest opracować i przekazać Zamawiającemu odpowiednie Dokumenty, o ile zachodzi taka potrzeba.

12.25. Jeżeli Wykonawca nie dokona Naprawy Błędu w terminie określonym w niniejszym załączniku to Zamawiający może:

12.25.1. Zawiadamiając uprzednio Wykonawcę usunąć Błąd we własnym zakresie lub powierzyć jej usunięcie innym podmiotom trzecim na ryzyko i koszt Wykonawcy, co nie spowoduje utraty przysługujących Zamawiającemu uprawnień z tytułu Gwarancji– przy czym koszty poniesione przez Zamawiającego przy usunięciu Błędu mogą być potrącone z wynagrodzenia przysługującego Wykonawcy lub z zabezpieczenia należytego wykonania przedmiotu Umowy, na co Wykonawca wyraża zgodę;

12.25.2. Obciążyć Wykonawcę karą umowną.

12.26. Jeżeli w trakcie realizacji zobowiązań z tytułu Gwarancji dojdzie do wprowadzenia zmian w Dokumentach, wówczas do przejścia autorskich praw majątkowych do zmienionych Dokumentów stosuje się odpowiednio postanowienia Umowy, w zakresie Dokumentów będących wynikiem zmian. W zakresie Oprogramowania lub jego dokumentacji, ich producent z chwilą wykonania zobowiązań z tytułu gwarancji udziela licencji na zasadach określonych w Umowie.

12.27. W uzasadnionych przypadkach Strony mogą podjąć decyzję o wydłużeniu Czasu Naprawy.

13. Warunki Gwarancji dla Oprogramowania

13.1. Gwarancją objęta jest całość dostarczonego Oprogramowania.

13.2. Wykonawca zapewni elektroniczny dostęp do informacji na temat dostarczonego Oprogramowania oraz biuletynów technicznych, poprawek, aktualizacji, nowych wersji Oprogramowania.

13.3. W przypadku Oprogramowania:

13.3.1. Wykonawca zapewnia Zamawiającemu dostarczanie aktualizacji, nowych wersji oraz zmian w Oprogramowania/ opracowanych przez producentów w okresie gwarancji. Wykonawca zapewnia, że dostarczane aktualizacje, nowe wersje lub zmiany są produktami wykonanymi przez producenta, a tym samym nie naruszają praw własności intelektualnej oraz że Wykonawca posiada prawo do ich dostarczania osobom trzecim na zasadach określonych w niniejszym załączniku oraz Umowie.

13.3.2. Aktualizację Oprogramowania, w szczególności dostarczania i instalacji nowych wersji Oprogramowania systemowego i Oprogramowania, dostarczania i instalacji wersji podwyższonych, wydań uzupełniających oraz poprawek programistycznych, bez dodatkowych opłat licencyjnych;

13.3.3. Informuje o najlepszych praktykach i zasadach postępowania.

14. Instruktaż z obsługi Platformy i Kursu dla pracowników Zamawiającego

W terminie ustalonym z Zamawiającym, ale nie dłuższym niż 45 dni, liczonym od dnia zawarcia Umowy Wykonawca przeprowadzi na grupie maksymalnie 15 pracowników Zamawiającego instruktaż z **obsługi Platformy i Kursu**. Przygotuje on wskazanych pracowników do samodzielnego konfigurowania Platformy, prowadzenia Kursów, operowania platformą z poziomu administratora oraz użytkownika, a także z zarządzania Platformą skonfigurowaną w specyficznej infrastrukturze Zamawiającego, w szczególności do samodzielnej konfiguracji w celu szybkiego wykrywania błędów i zapewnienia ciągłości działania.

- 14.1. Lista uczestników instruktażu zostanie ustalona drogą mailową z Wykonawcą po zawarciu umowy.
- 14.2. Instruktaż zostanie zorganizowany w czasie trwania wdrożenia zamówienia.
- 14.3. Termin przeprowadzenia instruktażu zostanie ustalony pomiędzy Zamawiającym a Wykonawcą.
- 14.4. Instruktaż będzie realizowany w dni robocze w godzinach 8:00-16:00 w siedzibie Zamawiającego lub zdalnie za zgodą Zamawiającego. Instruktaż może się odbyć w postaci zdalnego spotkania o ile zostaną spełnione wszystkie wymagania instruktażu.
- 14.5. Instruktaż Platformy będzie trwał minimum 4 Dni Robocze (łącznie minimum 32 godzin zegarowych).
- 14.6. Instruktaż Kursu będzie trwał nie dłużej niż 5 Dni Roboczych (łącznie 40 godzin zegarowych).
- 14.7. Harmonogramy zajęć zostaną ustalone drogą mailową z Zamawiającym.
- 14.8. Wykonawca musi posiadać doświadczenie w obsłudze dostarczonej Platformy i Kursu w zakresie wymagany w instruktażu z wdrożonej u Zamawiającego Platformy i Kursu.
- 14.9. Dla uczestników instruktażu Wykonawca przygotowuje środowisko testowe z zainstalowaną wersją Platformy i Kursem tożsamą dla wdrożonego u Zamawiającego Systemu pozwalające na zapoznanie się, z elementami interfejsu graficznego oraz wykonanie ćwiczeń w warunkach

możliwie zbliżonych do realnych. Dopuszczalne jest, za zgodą Zamawiającego, wykorzystanie dostarczonej i zainstalowanej u Zamawiającego Platformy.

14.10. Wykonawca zapewni dla każdego uczestnika wersję elektroniczną materiałów dydaktycznych zawierających streszczenie/omówienie wszystkich zagadnień zawartych w programie instruktażu oraz prezentacje wykorzystane podczas instruktażu;

14.11. Jeśli na potrzeby realizacji instruktażu powstaną materiały edukacyjne będące utworami w rozumieniu ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2022 r. poz. 2509) będą udostępnione na wolnej licencji zapewniającej licencjobiorcy prawo do dowolnego wykorzystywania utworów do celów komercyjnych i niekomercyjnych, tworzenia i rozpowszechniania kopii utworów w całości lub we fragmentach oraz wprowadzania zmian i rozpowszechniania utworów zależnych.

14.12. Zakres tematyczny instruktażu będzie zawierał się w niniejszych obszarach:

- 14.12.1. Przygotowanie i publikacja kursu.
- 14.12.2. Nadawanie i zarządzanie dostęпами do kursów.
- 14.12.3. Przegląd statystyk, wyników oraz przygotowanie raportów z kursów.
- 14.12.4. Skonfigurowanie certyfikatów na zakończenie kursu.
- 14.12.5. Import oraz eksport kursów w obsługiwanych formatach – co najmniej SCORM.
- 14.12.6. Zarządzanie Platformą – prace administratora na poziomie OS oraz bazy danych:
 - 14.12.6.1. Kopia zapasowa konfiguracji
 - 14.12.6.2. Kopia zapasowa kursów
 - 14.12.6.3. Kopia zapasowa bazy danych
 - 14.12.6.4. Wykonanie kopii zapasowej aplikacji oraz jej odtworzenie.

