

OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest wykonanie zewnętrznych usług doradczych oraz audytu informatycznego mających na celu badanie rzeczywistego poziomu bezpieczeństwa informacji oraz zastosowanych zabezpieczeń w zrealizowanym projekcie, a także zgodności tego poziomu z wymaganiami określonymi w normie PN-ISO/IEC 27001:2017-06.

1. Zakres prac obejmuje:

Etap 1: Usługa doradcza realizowana na etapie realizacji projektu zostanie zrealizowana w okresie 2 miesięcy od dnia podpisania umowy **w wymiarze minimum 100 roboczogodzin.**

Etap 2: Usługa audytu końcowego zostanie zrealizowana od kwietnia 2023 r. do maja 2023 r., lecz nie później niż do 30.06.2023 r. Wykonawca zobowiązany będzie do wykonania czynności audytowych w siedzibie Zamawiającego lub zdalnie np. z siedziby Wykonawcy. **Zakładany czas audytu końcowego to minimum 20 dni roboczych.**

Zamawiający zakłada, że prace stacjonarne będą stanowiły maksymalnie 20 % czasu pracy zakładanego w zakresie realizacji Etapu I i II. W pozostałym wymiarze Zamawiający pracę w formie zdalnej.

2. Opis czynności

Usługi doradcze oraz prace audytowe wykonywane będą w obszarach rozumianych jako systemy informatyczne:

- posiadanych już przez Zamawiającego, które w ramach realizowanego projektu będą rozbudowywane,
- tworzonych w ramach projektu.

Zakres prac audytowych obejmuje zarówno audyt aplikacji jak i infrastruktury technicznej. **Wykonawca zobowiązany jest do udziału w spotkaniach stacjonarnych i online, które będą zorganizowane przez Zamawiającego w celu omówienia przygotowanych dokumentów, postępu prac i wyników prac audytowych.**

3. Wykonawca Etapu 1 jest zobowiązany do realizacji następujących czynności:

- a) Doradztwo na etapie realizacji projektu,
- b) Przygotowanie szczegółowego planu przeprowadzenia audytu końcowego,
- c) **Przygotowanie szczegółowego harmonogramu przeprowadzenia audytu w uzgodnieniu z Zamawiającym w terminie 30 dni od daty podpisania umowy.**

4. Wykonawca Etapu 2 jest zobowiązany do realizacji następujących czynności:

- 1) przeprowadzenia audytu końcowego, których celem będzie dostarczenie informacji o rzeczywistym poziomie bezpieczeństwa informacji oraz zastosowanych zabezpieczeniach, a także zgodności tego poziomu z wymaganiami określonymi w normie PN-ISO/IEC 27001:2017-06,
- 2) przeprowadzenie audytu w obszarze zgodności z wymogami:
 - a. WCAG 2.1,
 - b. W3C,
 - c. RWD,



Fundusze Europejskie
Polska Cyfrowa



**Rzeczpospolita
Polska**

Strona 1 z 2

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



- 3) przeprowadzenie audytu w obszarze:
 - a. poprawności opisu architektury oprogramowania:
 - i. role użytkowników,
 - ii. komunikacja międzysystemowa,
 - iii. dostęp do aplikacji sieć wewnętrzna/zewnętrzna,
 - b. poprawności i kompletności dokumentacji baz danych,
 - c. poprawności i kompletności dokumentacji interfejsów (API),
 - d. poprawności i kompletności:
 - i. podręcznika użytkownika oprogramowania w formie instrukcji stanowiskowej,
 - ii. podręcznika administratora oprogramowania (opis funkcji administratora, procesu instalacji, konfiguracji parametrów oprogramowania itp.)
 - e. przeprowadzenia audytów bezpieczeństwa informacji dla każdego z produktów projektu. W ramach prac audytowych zrealizowane zostaną prace sprawdzające których efektem będzie wskazanie zagrożeń i podatności oraz ocena aktualnego poziomu bezpieczeństwa,
 - f. dostarczenia wniosków, zaleceń i rekomendacji w celu dokładnego rozpoznania i redukcji zidentyfikowanego ryzyka, zagrożeń i podatności oraz wskazanie adekwatnych działań mających na celu jak najszybsze ich wyeliminowanie.

Przeprowadzone badania i analizy w trakcie Etapu 2 audytu powinny wskazać ewentualne zagrożenia i ryzyka wynikające z:

- 1) zastosowanych technologii i standardów zabezpieczeń,
- 2) słabości oprogramowania oraz poprawności konfiguracji komponentów takich jak:
 - a) infrastruktura/systemy sieciowe i serwerowe,
 - b) systemy bazodanowe,
 - c) przyjętej koncepcji realizacji oprogramowania przez Wykonawcę,
- 3) faktu istnienia interfejsów wymiany danych pomiędzy różnymi systemami działającymi u Zamawiającego,
- 4) poprawności i kompletności implementacji kodów śledzenia Google Analytics, dla określonych obszarów,
- 5) opracowanie raportu z Audytu,
- 6) weryfikacja usunięcia podatności znalezionych w trakcie audytu,
- 7) opracowanie raportu z retestów po usunięciu podatności

Efektom przeprowadzonych prac w ramach Etapu 1 będą:

- 1) Plan przeprowadzenia audytu końcowego

Efektom przeprowadzonych prac w ramach Etapu 2 będą:

- 1) raporty zawierające wnioski, zalecenia i rekomendacje mające na celu dokładne rozpoznanie i redukcję zidentyfikowanego ryzyka, zagrożeń, podatności i odstępstw od dobrych praktyk wraz ze wskazaniem konkretnych działań naprawczych.
- 2) Raporty będą zawierały również:
 - a) wnioski i obserwacje audytowe,
 - b) wyniki testów i ich interpretację,
 - c) listę wykrytych podatności opatrzonej komentarzem audytora wraz z ich kwalifikacją w zależności od stopnia ich znaczenia dla bezpieczeństwa,
 - d) zalecenia i rekomendacje, zakres czynności i zadań niezbędnych do zaimplementowania rekomendacji po audytowych,
 - e) w przypadku konieczności wykonania zmian konfiguracyjnych lub zainstalowania uaktualnień („patchy”) Wykonawca przedstawi dokładny opis konfiguracji lub instalacji.