Sfinansowano w ramach reakcji Unii na pandemię Covid-19

Załącznik nr 1
do Zapytania ofertowego
nr 04/12/2022/KIF/7.1

Szczegółowy Opis Przedmiotu Zamówienia

dotyczy zamówienia przez Krajową Izbę Fizjoterapeutów usługi polegającej na **przeprowadzeniu audytów zewnętrznych platformy e-learningowej** w ramach realizacji projektu pn. **„FIZJO-LEARNING – większe kompetencje fizjoterapeutów w pracy z pacjentem chorującym na choroby zakaźne, w tym COVID-19”**, realizowanego w ramach Osi Priorytetowej VII. Wsparcie REACT-EU dla obszaru zdrowia, Działania 7.1 Wzmocnienie zasobów kadrowych systemu ochrony zdrowia, współfinansowanego z budżetu Unii Europejskiej ze środków Europejskiego Funduszu Społecznego Programu Operacyjnego Wiedza Edukacja Rozwój na lata 2014-2020.

I. INFORMACJE OGÓLNE

1. Przedmiotem zamówienia jest świadczenie usług audytów bezpieczeństwa, testów penetracyjnych, opracowania dokumentacji bezpieczeństwa informacji z elementami cyberbezpieczeństwa i konsultacji w dziedzinie bezpieczeństwa informacji. Usługa obejmuje 13 lokalizacji (9 UTM, 5 serwerów fizycznych, 35 VM (windows/linux) i 5 aplikacji własnych z ogólnym dostępem do Internetu, 150 stacji roboczych Windows/MacOS).

Usługa audytu obejmuje następujące zagadnienia:

a. Bezpieczeństwo infrastruktury i stron www oraz aplikacji, ocenę bezpieczeństwa przechowywania danych, analizę wykonywania i przechowywania kopii bezpieczeństwa, analizę legalności oprogramowania, ocenę ryzyka wykrytych podatności
b. przeprowadzenie audytu IT z ustaleniem infrastruktury oraz identyfikacją podatności (LAN, WAN),
c. przeprowadzenie testów penetracyjnych według wybranej metodyki i strategii, w formie automatycznej i/lub manualnej z uwzględnieniem obszarów zidentyfikowanych w fazie audytu infrastruktury IT:
   - ✓ Zabezpieczeń sieci LAN i WAN
   - ✓ Bazodanowych aplikacji desktopowych
   - ✓ Aplikacji webowych
   - ✓ Aplikacji mobilnych
d. doradztwo w zakresie metod usunięcia zidentyfikowanych podatności,
e. wsparcie przy opracowaniu procedur IT,
f. ocenę ryzyka wykrytych podatności.

2. W zakres planowanej usługi świadczenia audytów bezpieczeństwa wchodzi realizacja następujących zadań:

Krajowa Izba Fizjoterapeutów
The Polish Chamber of Physiotherapists
www.kif.info.pl

Al. Jerozolimskie 93, 02-001 Warszawa
NIP: 701-065-15-76 REGON: 366272350
biuro@kif.info.pl

Sfinansowano w ramach reakcji Unii na pandemię Covid-19

Załącznik nr 1
do Zapytania ofertowego
nr 04/12/2022/KIF/7.1

L.P.	NAZWA ZADANIA
1.	Przeprowadzenie testów penetracyjnych systemów informatycznych wskazanych przez Zamawiającego wraz z testami socjotechnicznymi: testy penetracyjne aplikacji webowych, testy penetracyjne środowiska, testy socjotechniczne w jednostce
2.	Audyt procesów zachodzących w jednostce Zamawiającego związanych z tematyką bezpieczeństwa informacji i zaprojektowanie modelu bezpieczeństwa informacji na bazie dokonanego audytu procesów
3.	Doradztwo w opracowaniu szczegółowych instrukcji wykonawczych w obszarze bezpieczeństwa teleinformatycznego dla Działu IT, uwzględniających wynik testów penetracyjnych
4.	Opracowanie szczegółowych wytycznych i rekomendacji w czasie trwania umowy w zakresie obszaru obejmującego bezpieczeństwo informacji, w tym przeprowadzenie analizy ryzyka dla funkcjonujących procesów oraz zagrożeń
5.	Sporządzenie trzech raportów w trakcie realizacji zamówienia z trzech badanych okresów

ZADANIE NR 1	
Przeprowadzenie testów penetracyjnych systemów informatycznych wraz z testami socjotechnicznymi	
1.	Wymaga się aby przedmiot zamówienia został zrealizowany przez odpowiednie testy aplikacji i oprogramowania systemowego, wywiady z pracownikami, weryfikacje konfiguracji systemów informatycznych, wizje lokalne: a. Testy penetracyjne aplikacji webowych b. Testy penetracyjne środowiska c. Testy socjotechniczne w jednostce Prace będą nadzorowane przez pracowników Zamawiającego w dni robocze w godzinach 08:00-15:00. Prace będą odbywać się w siedzibie Zamawiającego oraz w zewnętrznych lokalizacjach hostingodawców.
2.	Warstwy poddane testowaniu: a. Aplikacje webowe oraz mobilne b. Bezpieczne logowanie <https://logowanie.kif.info.pl/> SSO c. Systemy CMS, strony www d. Sieciowe urządzenia brzegowe e. Routery ekranujące i bramy f. Systemy firewall g. Serwery Proxy h. Usługi VPN i. Systemy antywirusowe j. Systemy tworzenia i odtwarzania kopii zapasowych k. Serwery aplikacji l. Systemy monitorowania dostępności m. Serwery DNS n. Serwery i usługi poczty elektronicznej o. Systemy operacyjne p. Systemy baz danych q. System usług katalogowych (Active Directory) r. Warstwy dostępowe do usługi bankowości elektronicznej

Krajowa Izba Fizjoterapeutów
The Polish Chamber of Physiotherapists
www.kif.info.pl

Al. Jerozolimskie 93, 02-001 Warszawa
NIP: 701-065-15-76 REGON: 366272350
biuro@kif.info.pl

Załącznik nr 1
do Zapytania ofertowego
nr 04/12/2022/KIF/7.1

	s. System obiegu dokumentów t. Usługi dostępu do danych dedykowane dla urządzeń mobilnych oraz konfiguracje urządzeń mobilnych u. Usługi udostępniane dla użytkowników systemów wspierających realizowanie statutowych zadań Zamawiającego
3.	Systemy Zamawiającego poddane testowaniu i audytowi: a) Serwis Bezpieczne Logowanie (SSO) do Fizja e-learning : https://logowanie.kif.info.pl/ oraz jego działanie w wykorzystujących ten system usługach i serwisach dla fizjoterapeutów: - Platforma e-learningowa - Znajdź fizjoterapeutę - Finezjo - Portal fizjoterapeuty - CRM b) Strona internetowa platforma e-learningowa Fizja c) rejestr d) rejestracja
4.	Rodzaje, metody oraz częstotliwość przeprowadzonych testów Testowanie będzie polegało na przeprowadzeniu: a. Testu penetracyjnego , automatycznego oraz następnie manualnego – w I etapie realizacji przedmiotu umowy, przy użyciu co najmniej następujących narzędzi lub równoważnych: • Burp Suite • Fuff • Nmap • Nikto2 • Scapy • Nessus • W3af • SQLmap • Metasploit b. Testu socjotechnicznego w siedzibie Zamawiającego oraz 2 retestów penetracyjnych c. Testy będą prowadzone zgodnie z ustalonym z Zamawiającym harmonogramem d. Systemy poddane testowaniu będą prowadzone metodą black box, gray box i white box. Pierwsze testy będą prowadzone metodą black box, a kolejne metodami gray box i white box. e. Sprawdzenie zgodności z wytycznymi • OWASP (Open Web Application Security Project); • OWASP ASVS (Application Security Verification Standard Project) • PN-ISO/IEC serii 27000.
5.	Dostęp Wykonawcy do dokumentacji systemowej /dotyczy metod gray box i white box/ Dostęp do dokumentacji systemów Zamawiającego, w tym informacji zostanie udzielony: do 14 dni od daty podpisania umowy w formie elektronicznej / podczas wizji lokalnej przeprowadzone

Krajowa Izba Fizjoterapeutów
The Polish Chamber of Physiotherapists
www.kif.info.pl

Al. Jerozolimskie 93, 02-001 Warszawa
NIP: 701-065-15-76 REGON: 366272350
biuro@kif.info.pl

Załącznik nr 1
do Zapytania ofertowego
nr 04/12/2022/KIF/7.1

	w siedzibie Zamawiającego. Celem umówienia terminu wizji prosimy o wysłanie zgłoszenie na adres osoby wskazanej do kontaktów w ramach realizacji Zapytania ofertowego.
6.	Cel i oczekiwane przez Zamawiającego efekty związane z realizacją zamówienia Identyfikacja podatności, błędów aplikacji i portali webowych KIF – w celu ich usunięcia, minimalizacji ich negatywnego wpływu na systemy KIF, bezpieczeństwo przetwarzanych danych. Dla każdego z testowanych systemów, Zamawiający oczekuje przeprowadzenia testów zmierzających do: a. Podniesienia poziomu uprawnień uwierzytelnionego lub anonimowego użytkownika b. Przejęcia danych uwierzytelnienia lub sesji kont innych użytkowników c. Uzyskania nieautoryzowanego dostępu do danych lub nieuprawnionej zmiany danych d. Przejęcia kontroli nad sposobem działania usług e. Zablokowania działania usług f. Wykazania braku możliwości redundantnego działania zdublowanych podsystemów g. Uruchomienia własnych usług nie ujętych w dokumentacji systemów h. Wykrycia wszelkich podatności mających wpływ na dostępność, poufność oraz integralności danych i. Wykazania poziomu świadomości pracowników i podatności na działania socjotechniczne W przypadku stwierdzenia podatności krytycznych Wykonawca powiadomi o nich niezwłocznie Zamawiającego. Zakłada się, że w wyniku analizy ryzyka przeprowadzonej w ramach audytu warstwy fizycznej zostaną wydzielone co najmniej dwa poziomy/strefy bezpieczeństwa, do których będą miały zastosowanie odmienne rekomendowane poziomy środków bezpieczeństwa. Wymaga się by wymienione powyżej testy zostały wykonane zgodnie z kluczowymi testami przewidzianymi w podręczniku OWASP Testing Guide v4. Testy te muszą przewidywać próby dokonania ataków za pośrednictwem sieci WAN (Internet), sieci LAN/WLAN Zamawiającego, usługi Active Directory Zamawiającego. Testy powinny obejmować swoim zakresem wszelkie podatności ujawnione w publicznie dostępnych bazach (m.in. www.exploit-db.com, www.rapid7.com, www.wuldb.com). Wymaga się przeprowadzenia audytu warstwy zabezpieczeń systemów i danych w siedzibie Zamawiającego. W szczególności audytowi poddane zostaną: • Warstwa procedur organizacyjnych mający na celu utrzymanie określonych poziomów bezpieczeństwa i dostępności systemów teleinformatycznych • Warstwa fizycznych zabezpieczeń dostępu do danych • Warstwa wymiany danych z systemami zewnętrznymi • Warstwa uprawnień określonych użytkowników oraz grup użytkowników do określonych zbiorów danych Audyt warstw, o których mowa powyżej, powinien być przeprowadzony przy założeniu, że pożądanym stanem rzeczy jest: zachowanie zasady minimalnego koniecznego dostępu do danych oraz zasad zabezpieczeń danych przed wyciekiem oraz próbami uzyskania nieautoryzowanego dostępu. Oczekuje się, że Wykonawca przeprowadzi co najmniej trzy próby uzyskania nieuprawnionego, fizycznego dostępu od infrastruktury teleinformatycznej Zamawiającego w obszarze stacji roboczych posiadających dostęp do kluczowych systemów Zamawiającego, infrastruktury sieciowej oraz serwerowej.

Krajowa Izba Fizjoterapeutów
The Polish Chamber of Physiotherapists
www.kif.info.pl

Al. Jerozolimskie 93, 02-001 Warszawa
NIP: 701-065-15-76 REGON: 366272350
biuro@kif.info.pl

Sfinansowano w ramach reakcji Unii na pandemię Covid-19

Załącznik nr 1
do Zapytania ofertowego
nr 04/12/2022/KIF/7.1

ZADANIE NR 2	
Audyt procesów związanych z tematyką bezpieczeństwa informacji wraz z zaprojektowaniem modelu bezpieczeństwa na bazie dokonanego audytu procesów	
1.	Zadanie polega na przeprowadzeniu wstępnego przeglądu (ustalenia procesów w jednostce, wstępnej oceny spełnienia wymagań w zakresie bezpieczeństwa informacji, w tym wymagań prawnych i wymagań w oparciu o normy międzynarodowe)
2.	Identyfikacja struktury organizacyjnej oraz procesów jednostki Uzgodnienia organizacyjne oraz konsultacje w zakresie kwalifikacji dokumentu jako wymaganego do dostarczenia, odbiór i zapoznanie się z dokumentacją obrazującą funkcjonowanie KIF w zakresie docelowego obszaru bezpieczeństwa informacji tj.: a. Infrastruktura IT: w ujęciu technicznym i organizacyjnym b. Relacje z klientami usług świadczonych przez KIF c. Relacje z dostawcami usług w tym z podwykonawcami d. Realizacja statutowych zadań (usługi) e. Bezpieczeństwo informacji f. Marketing
3.	Wstępne przygotowanie przez Wykonawcę mapy procesów oraz identyfikacja Interesariuszy, a następnie przekazanie ww. ustaleń do KIF
4.	Wstępne wprowadzenie Interesariuszy w sposób realizacji zadania a następnie: a. Identyfikacja procesów oraz zasobów uczestniczących (zbiory wraz z przepływami danych, systemy informatyczne, infrastruktura IT oraz techniczna, lokacje fizyczne, środki zabezpieczenia) przy współudziale zidentyfikowanych (w trakcie wstępnej analizy, a także podczas wywiadu) Interesariuszy (wywiad z Interesariuszami), b. Sporządzenie finalnej mapy procesów i przypisanych im zasobów wraz z listą Interesariuszy.
5.	Ocena zgodności zidentyfikowanych procesów z wymaganiami w zakresie bezpieczeństwa informacji, t.j. wymaganiami prawnymi, wymaganiami norm, dobrymi praktykami i kodeksami postępowania oraz w wymaganym zakresie ustalenie działań korygujących: a. Ocena zgodności (dokumentacja/procesy) z wymaganiami prawnymi i normy ISO 27001; b. Wstępna, szacunkowa identyfikacja ryzyk (metoda SWIFT lub BTA, przy niesprzeczności z metodykami ISO 27005 lub ISO 31000) dla procesów oraz sporządzenie dokumentacji z przeprowadzonego szacowania; c. Konsultacje z Zamawiającym w zakresie doboru zabezpieczeń w ramach środków zabezpieczeń niepodlegających wyłączeniu.
6.	Opracowanie raportu z audytu procesów wraz z zaproponowanym modelem bezpieczeństwa informacji i ich przedstawienie Zamawiającemu.

Krajowa Izba Fizjoterapeutów
The Polish Chamber of Physiotherapists
www.kif.info.pl

Al. Jerozolimskie 93, 02-001 Warszawa
NIP: 701-065-15-76 REGON: 366272350
biuro@kif.info.pl

Załącznik nr 1
do Zapytania ofertowego
nr 04/12/2022/KIF/7.1

ZADANIE NR 3	
Doradztwo w opracowaniu szczegółowych instrukcji wykonawczych w obszarze bezpieczeństwa teleinformatycznego uwzględniających wynik testów penetracyjnych	
1.	Wykonawca na podstawie wyników testów penetracyjnych, weryfikacji infrastruktury IT oraz konsultacji przeprowadzonych z Kierownikiem Działu Cyfryzacji Zamawiającego, opracuje wzorce instrukcji wykonawczych dla obszaru IT.
2.	Szczegółowy zakres instrukcji zostanie ustalony na etapie konsultacji z Kierownikiem Działu IT adekwatnie do potrzeb Zamawiającego.

ZADANIE NR 4	
Opracowanie szczegółowych wytycznych/rekomendacji w czasie trwania umowy w zakresie bezpieczeństwa informacji	
1.	Wykonawca w okresie obowiązywania umowy na zlecenie Zamawiającego opracuje szczegółowe wytyczne związane z tematyką bezpieczeństwa informacji – adekwatnie do potrzeb Zamawiającego, np. w kontekście zmieniającego się otoczenia prawnego, zaleceń Ministerstwa Zdrowia, przetwarzania danych osobowych w aplikacjach itp.
2.	Konsultacje z Inspektorem Ochrony Danych i w razie potrzeby z innymi komórkami organizacyjnymi przetwarzającymi dane osobowe w organizacji.
3.	Sporządzenie i przedstawienie Kierownictwu jednostki przy udziale Inspektora Ochrony Danych, rekomendacji w zakresie ewentualnej możliwej poprawy stworzonego systemu ochrony danych osobowych.
4.	Zamawiający ustala maksymalny czas 80 roboczogodzin w ramach ww. zadania

ZADANIE NR 5	
Sporządzenie trzech raportów w trakcie realizacji zamówienia z trzech badanych okresów	
1.	Raport 1 po 3 miesiącach od podpisania umowy obejmujący: - Architekturę serwerową (metroklaster) - Bezpieczne logowanie KIF - Panel administracyjny - Moduł szkoleń stacjonarnych
2.	Raport 2 po 8 miesiącach od podpisania umowy obejmujący: - Podatności nowej infrastruktury (metroklaster) - Moduł kontaktu z trenerem - Integrację z KRF - System helpdesk
3.	Raport 3 do 11 miesiąca od podpisania umowy obejmujący: - Kompleksowy panel administracyjny do zarządzania całym produktem - Mechanizmy integracji z systemem bazodanowym KIF - Integrację z portalem znajdź fizjoterapeutę - Testy po refactoringu kodu - Ogólny audyt podatności - retest

Krajowa Izba Fizjoterapeutów
The Polish Chamber of Physiotherapists
www.kif.info.pl

Al. Jerozolimskie 93, 02-001 Warszawa
NIP: 701-065-15-76 REGON: 366272350
biuro@kif.info.pl

Sfinansowano w ramach reakcji Unii na pandemię Covid-19

Załącznik nr 1
do Zapytania ofertowego
nr 04/12/2022/KIF/7.1

II. WYMAGANIA ZAMAWIAJĄCEGO

1. Audyt musi zostać przeprowadzony przez osoby posiadające odpowiednie uprawnienia, zgodnie z wymaganiami Ministerstwa Cyfryzacji z dnia 12.10.2018 roku, w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U. poz. 1999) w rozumieniu art. 15 ustawy z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2020 roku poz. 1369 z późn. zm.).
2. Audyt musi być przeprowadzony zgodnie z harmonogramem zatwierdzonym przez Zamawiającego i obejmuje sporządzenie raportów po 3, 8 i maksymalnie do 11 miesięcy po podpisaniu umowy Wykonawcą.
3. Audyt oraz przekazanie wszystkich raportów musi być przeprowadzone w nieprzekraczalnym terminie do 15.12.2023 r.
4. Zamówienie zostanie zrealizowane w trzech etapach, zgodnie z harmonogramem:
   1) I raport z przeprowadzonego audytu – najpóźniej po 3 miesiącach od dnia podpisania umowy
   2) II raport z przeprowadzonego audytu – najpóźniej po 8 miesiącach od dnia podpisania umowy
   3) III raport z przeprowadzonego audytu – najpóźniej do 11 miesięcy od dnia podpisania umowy.

III. OBOWIĄZKI WYKONAWCY

1. Wykonawca posiada pełne i niezaprzeczalne prawo do wykonania usługi będącej przedmiotem niniejszego postępowania na terenie Polski.
2. Wykonawca ponosi pełną odpowiedzialność w przypadku wystąpienia roszczeń ze strony osób trzecich z tytułu naruszenia praw autorskich, wynalazczych i innych związanych z realizacją zamówienia.
3. W przypadku poniesienia przez Zamawiającego jakichkolwiek strat wynikłych z tego tytułu, straty te będą w całości rekompensowane przez Wykonawcę, z uwzględnieniem wszelkich kosztów dodatkowych, sądowych oraz prawniczych.

Krajowa Izba Fizjoterapeutów
The Polish Chamber of Physiotherapists
www.kif.info.pl

Al. Jerozolimskie 93, 02-001 Warszawa
NIP: 701-065-15-76 REGON: 366272350
biuro@kif.info.pl