F-PRO.093.20.2018
13.2022.EW

OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)

Kierując się zasadą uczciwej konkurencji i równego traktowania Wykonawców, a także zasadą efektywnego zarządzania finansami planuje się udzielenie zamówienia publicznego jakim jest **zakup licencji wieczystej na szkolenie w wersji elektronicznej (e-learning) z zakresu bezpieczeństwa informacji i bezpieczeństwa teleinformatycznego dedykowanego dla pracowników Uniwersytetu Szczecińskiego w celu podniesienia kompetencji kadr uczelni** w ramach projektu ***UNIWERSYTET 2.0 – STREFA KARIERY,*** nr umowy: **POWR.03.05.00-00-Z064/17-00.**

W tym celu Uniwersytet Szczeciński jako Beneficjent projektu kieruje zapytanie o przedstawienie oferty cenowej w celu oszacowania wartości zamówienia.

I. INFORMACJE DLA WYKONAWCY

1. Grupę docelową stanowią pracownicy Uniwersytetu Szczecińskiego (US).
    - Celowość realizowanych kursów/szkoleń: kadra zarządcza i administracyjna uczelni: zdobycie dodatkowej wiedzy i umiejętności prowadzących do **uzyskania kompetencji zarządczych, w tym informatycznych w zakresie bezpiecznego korzystania z komputerów, Internetu i urządzeń mobilnych.**

II. ZAKRES PRZEDMIOTU ZAMÓWIENIA

1. **Przedmiot zamówienia:** Wieczysta licencja na szkolenie w wersji elektronicznej (e-learning) z zakresu bezpieczeństwa informacji i bezpieczeństwa teleinformatycznego. Szkolenia dedykowane dla pracowników biurowych (nietechnicznych) pracujących z komputerami i przetwarzających różnego rodzaju informacje o różnym poziomie poufności. Szkolenia muszą być w formie gotowego produktu dostarczanego Zamawiającemu bezzwłocznie po złożeniu zamówienia / podpisaniu umowy. Zamawiający musi mieć możliwość swobodnego wykorzystania szkoleń bez ograniczeń czasowych oraz liczby odbiorców. Szkolenia nie mogą być w formie usługi.
2. **Forma e-learning:** Szkolenie musi być w postaci oddzielnych lekcji dla każdej z kategorii z niżej opisanego zakresu. Jedna lekcja szkolenia powinna zawierać minimum 20 slajdów. Czas jednej lekcji (tematu) powinien oscylować w granicach 15-30 min. Czas trwania całego szkolenia powinno wynieść min. 7 godzin zegarowych. Lekcje powinny być multimedialne z wykorzystaniem scenek rodzajowych z możliwością odtworzenia w postaci dźwiękowej z użyciem lektora. Nie mogą to być same zdjęcia, definicje lub zagadnienia opisane w formie tekstowej i odtwarzane w postaci dźwiękowej. Podczas lekcji powinna być na bieżąco weryfikowana wiedza (uwaga) użytkownika poprzez np. ćwiczenia sprawdzające.
3. **Zakres tematyczny szkolenia** (szkolenie musi posiadać oddzielne lekcje dla co najmniej następujących zagadnień):
    a. Czym jest bezpieczeństwo informacji;
    b. Aspekty prawne związane z bezpieczeństwem informacji;
    c. Czym jest phishing?
    d. Zasady korzystania z Internetu;
    e. Zasady korzystania z portali społecznościowych;

f. Zasady korzystania z poczty elektronicznej i zagrożenia z tym związane;
g. Zasady korzystania z bezpiecznych haseł;
h. Zagrożenia i sposoby zabezpieczania sprzętu mobilnego;
i. Metody pozyskiwania informacji (socjotechnika);
j. Bezpieczeństwo w zakresie płatności elektronicznych;
k. Bezpieczeństwo fizyczne w zakresie zabezpieczania pomieszczeń, dokumentacji, sprzętu IT;
l. Czym jest ransomware i jak wygląda w praktyce;
m. Jak bezpiecznie korzystać z menedżera haseł w praktyce;
n. Techniki stosowane przez cyberprzestępców;
o. Uważaj by nie zostać „mułem finansowym"
p. Bezprzewodowe życie.
q. Praca zdalna - jak zrealizować ją bezpiecznie?
r. Vishing… co to jest?
s. Phishing – stare problemy, nowe sposoby. Przykłady aktualnych cyberataków i sposoby ochrony przed nimi.
t. Jak cyberprzestępcy kradną dane przez telefon.
u. Fake news i dezinformacja.

4. Forma szkolenia:

a. Szkolenie musi posiadać atrakcyjną formę przekazu materiału, zachęcającą osoby uczące się do aktywnego odbywania szkolenia. Zamawiający wymaga atrakcyjnej formy przekazu materiału szkolenia. Atrakcyjna forma to m.in. grafika oparta na scenkach, postaciach, dialogach, przykładach, ćwiczeniach, testach sprawdzających wiedzę oraz dźwięk – głos lektorów indywidualny dla każdej z postaci występujących w szkoleniu.
b. Szkolenie musi posiadać interaktywną formę, zwiększającą zaangażowanie osób uczących się. Szkolenie musi zostać wyposażone w elementy interakcji (np. kliknięcia, ćwiczenia), tak aby uczestnik był aktywny podczas szkolenia i nie miał możliwości zaliczenia szkolenia w sposób bierny tj. poprzez samoczynne odtworzenia filmu/ szkolenia.
c. E-szkolenie powinno mieć dodatkową funkcjonalność dla użytkownika, który ukończy w całości dany moduł/zakres tematyczny umożliwiającą wygenerowanie, pobranie i wydrukowanie zaświadczenia/certyfikatu potwierdzającego nabycie kompetencji zarządczych w zakresie bezpieczeństwa w cyberprzestrzeni.
d. Lekcje szkolenia muszą kłaść duży nacisk na umiejętności praktyczne, nie tylko teorię bezpieczeństwa IT. W celu zwiększenia praktycznej przydatności szkolenia musi ono zostać opracowane tak, aby zajęcia kładły większy nacisk na umiejętności praktyczne użytkowników komputerów (np. wykrywanie sytuacji zagrożenia w trakcie korzystania z serwisów społecznościowych, właściwe postępowanie w razie incydentu) niż samą teorię bezpieczeństwa IT.
e. Cały materiał szkolenia musi być dostępny w języku polskim i przedstawiony w sposób zrozumiały przez osoby nietechniczne. Szkolenie musi posiadać techniczną możliwość dokupienia wersji w innych językach.
f. Szkolenie musi posiadać wysoką jakość merytoryczną przygotowanego scenariusza. Scenariusz szkolenia musi zostać opracowany we współpracy z ekspertem bezpieczeństwa IT posiadającym certyfikat Lead Auditor 27001.

5. **Wymagania techniczne:** Szkolenie w wersji elektronicznej musi być zgodne ze standardem umożliwiającym prezentację na platformie MOODLE w wersji 3 lub wyższej. Szkolenie powinno być dostarczone w technologii HTML5. Szkolenia powinny być podzielone tematycznie w taki sposób, aby można było operować (zarządzać dostępnością, harmonogramem, itp.) poszczególnymi tematami z osobna.
6. **Warunki licencji:** Wykonawca udzieli Zamawiającemu wieczystej, nieograniczonej czasowo licencji na szkolenie.
7. **Termin dostawy:** 14 dni od daty zawarcia umowy.

III. WYMAGANIA WOBEC WYKONAWCÓW

O udzielenie zamówienia będą mogli ubiegać się Wykonawcy, którzy:

1. posiadają zdolność techniczną i zawodową do wykonania niniejszego zamówienia,
2. posiadają uprawnienia do wykonywania określonej działalności lub czynności, jeżeli przepisy prawa nakładają obowiązek ich posiadania,
3. posiadają wiedzę i doświadczenie w realizacji usług z zakresu podobnego do przedmiotu zamówienia i w okresie ostatnich 3 lat przed terminem składania ofert zrealizowali należycie co najmniej 3 usługi z zakresu podobnego adekwatnego do przedmiotu zamówienia,
4. dysponują na czas realizacji przedmiotowego zamówienia osobami zdolnymi do wykonania zamówienia, minimalne wymagania: kwalifikacje: wykształcenie wyższe lub certyfikaty/ zaświadczenia/inne umożliwiające opracowanie scenariusza danego szkolenia/kursu - **Scenariusz szkolenia musi zostać opracowany we współpracy z ekspertem bezpieczeństwa IT posiadającym certyfikat Lead Auditor 27001**; doświadczenie: minimalne doświadczenie zawodowe w danej dziedzinie nie może być krótsze niż 2 lata.

Na etapie szacowania wartości zamówienia Zamawiający nie określa więcej szczegółowych warunków ani sposobu potwierdzenia spełniania ich przez Wykonawcę.

IV. TERMIN WYKONANIA ZAMÓWIENIA

Planowany termin wykonania realizacji usługi: 14 dni od dnia podpisania umowy, jednak nie dłużej niż do 30.09.2022.

V. INNE ISTOTNE INFORMACJE

1. Planowane rozliczenie finansowe: rozliczenia częściowe, zapłata wynagrodzenia nastąpi przelewem na rachunek Wykonawcy w terminie do 14 dni, licząc od dnia otrzymania przez Zamawiającego prawidłowej pod względem formalnym i merytorycznym faktury oraz protokołu odbioru.
2. Ze względu na fakt, iż zamówienie realizowane jest w ramach projektu współfinansowanego z Funduszy Europejskich w ramach Europejskiego Funduszu Społecznego, Wykonawca zapewni w okresie od daty zawarcia umowy do dnia 31 grudnia 2027 roku prawo wglądu Zamawiającemu oraz wszelki instytucjom przeprowadzającym kontrolę realizowanego projektu, we wszystkie dokumenty, w tym finansowe, przechowywane w każdej formie a związane wykonanym zamówieniem.
3. Wykonawca przeniesie na Zamawiającego przysługujące mu autorskie prawa majątkowe do wytworzonych przez siebie utworów (jeżeli dotyczy).
4. Wykonawca zobowiąże się do przygotowania dokumentów lub innych materiałów niezbędnych do realizacji przedmiotu zamówienia opatrzonych odpowiednimi logotypami Unii Europejskiej, Programu Operacyjnego Wiedza Edukacja Rozwój oraz nazwą projektu, które Zamawiający przekaże Wykonawcy drogą mailową.

VI. KRYTERIA OCEN NA ETAPIE SZACOWANIA WARTOŚCI ZAMÓWIENIA

Na etapie szacowaniu wartości zamówienia Zamawiający kieruje się kryterium - cena.
Kryterium jest obliczone za pomocą następującego wzoru:

C = [(Cn : Cb) x 100 %] x 100

gdzie:

Cn - cena brutto najniższa
Cb - cena brutto wynikająca z oferty badanej

VII. SPOSÓB ZŁOŻENIA OFERTY CENOWEJ

1. Oferty cenowe można składać za pośrednictwem platformy zakupowej w terminie do **23.06.2022 r. do godz. 10:00** w formie podpisanego skanu formularza cenowego (załącznik).
2. Oferent może zwrócić się do Zamawiającego za pośrednictwem platformy zakupowej lub drogą elektroniczną lub telefoniczną (Konrad Mielko tel. 91/4441057; email: konrad.mielko@usz.edu.pl; Eliza Wancerz tel. 91/4441142, email: eliza.wancerz@usz.edu.pl) z zapytaniem o wyjaśnienie treści Opisu Przedmiotu Zamówienia lub z prośbą o przekazanie od Zamawiającego niezbędnych informacji w celu przestawienia oferty cenowej.
3. W toku badania oferty cenowej Zamawiający może żądać od Oferentów wyjaśnień dotyczących treści złożonych ofert cenowych lub wezwać do uzupełnienia oferty.

UWAGA: Inne kryteria oraz szczegółowe warunki udziału w postępowaniu będą wskazane w postępowaniu o udzielenie zamówienia publicznego.

ZAŁĄCZNIKI:
- formularz cenowy.