WL-IV.272.33.2026 Załącznik nr 5 do swz

Opis Przedmiotu Zamówienia

Przedmiotem zamówienia jest przeprowadzenie szkoleń w zakresie cyberbezpieczeństwa dedykowanych dla administratorów systemów informatycznych w celu podniesienia poziomu wiedzy i umiejętności poprzez udział w szkoleniach: Systems Security Certified Practitioner (SSCP) i Certified Information Systems Security Professional (CISSP) w ramach projektu pn.: Cyberbezpieczny Urząd - Podniesienie standardów cyberbezpieczeństwa Wojewody Małopolskiego i jednostek podległych współfinansowany przez Unię Europejską w ramach programu Krajowy Plan Odbudowy i Zwiększania Odporności.

Część 1 Systems Security Certified Practitioner (SSCP)

1. **Ogólne wymagania dotyczące szkolenia:**

1. Szkolenie będzie prowadzone w języku polskim. Dopuszczalne są podręczniki i materiały ze szkolenia w języku angielskim.
2. Szkolenie nie może odbywać się w formie e-learningu.
3. Szkolenie może się odbywać w formie zdalnej pod warunkiem, że dostawca udostępni własną platformę wideokonferencyjną, która zapewni stały kontakt z trenerem oraz innymi uczestnikami szkolenia i zapewni dostęp on-line do ćwiczeń, laboratoriów itp.
4. Szkolenie będzie odbywać się w dni robocze.
5. Szkolenie prowadzone będzie na podstawie zaakceptowanego przez Zamawiającego szczegółowego zakresu merytorycznego szkolenia dostarczonego przez Wykonawcę oraz wykazu osób szkolących spełniających wymagania z SWZ w zakresie kwalifikacji.
6. Uczestnicy szkolenia otrzymują certyfikaty ukończenia danego szkolenia.
7. Daty szkolenia zostaną ustalone z wybranym Wykonawcą.
8. Szkolenie może mieć formę szkolenia otwartego, w którym uczestniczą osoby z innych instytucji.

2. **Wykaz wymaganych szkoleń:**

Nazwa szkolenia	Liczba uczestników	Termin	Opis
Systems Security Certified Practitioner (SSCP) szkolenie autoryzowane lub równoważne ISC2*	1	1 tura	Szkolenie stanowi przegląd koncepcji bezpieczeństwa informacji i najlepszych praktyk branżowych, obejmujących siedem domen SSCP CBK: Domena 1. Operacje i administracja bezpieczeństwa Domena 2. Kontrola dostępu Domena 3. Identyfikacja, monitorowanie i analiza ryzyka Domena 4. Reagowanie na incydenty i odzyskiwanie Domena 5. Kryptografia Domena 6. Bezpieczeństwo sieci i komunikacji Domena 7. Bezpieczeństwo systemów i aplikacji

* szkolenie równoważne – spełniające co najmniej wskazania dot. tematyki i zakresu merytorycznego oraz warunki i wymagania.

3. **Zestawienie szkoleń:**

Lp.	Szkolenie	Ilość tur (osób/tura)	Terminy szkoleń
1	**Systems Security Certified Practitioner (SSCP)**	1 (jedna osoba w 1 turze)	80 dni od daty zawarcia umowy

	szkolenie autoryzowane lub równoważne ISC2*		

* szkolenie równoważne – spełniające co najmniej wskazania dot. tematyki i zakresu merytorycznego oraz warunki i wymagania.

Zamawiający wymaga, aby oferowane świadczenie, w tym wszystkie produkty ICT, usługi ICT oraz procesy ICT wykorzystywane do realizacji zamówienia, zarówno jako elementy główne, jak i komponenty, elementy środowiska świadczenia usługi lub rozwiązania towarzyszące, nie obejmowało:

- produktów ICT, usług ICT lub procesów ICT wskazanych w rekomendacji, o której mowa w art. 33 ust. 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, stwierdzającej ich negatywny wpływ na podstawowy interes bezpieczeństwa państwa;
- produktu ICT, którego typ został określony w decyzji w sprawie uznania dostawcy za dostawcę wysokiego ryzyka, o której mowa w art. 67b ust. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, ani usług ICT lub procesów ICT określonych w tej decyzji.

Niespełnienie powyższego wymagania skutkuje odrzuceniem oferty odpowiednio na podstawie art. 226 ust. 1 pkt 17 albo pkt 19 ustawy Pzp.

Część 2 Certified Information Systems Security Professional (CISSP)

1. <u>Ogólne wymagania dotyczące szkolenia:</u>

1. Szkolenie będzie prowadzone w języku polskim. Dopuszczalne są podręczniki i materiały ze szkolenia w języku angielskim.
2. Szkolenie nie może odbywać się w formie e-learningu.
3. Szkolenie może się odbywać w formie zdalnej pod warunkiem, że dostawca udostępni własną platformę wideokonferencyjną, która zapewni stały kontakt z trenerem oraz innymi uczestnikami szkolenia i zapewni dostęp on-line do ćwiczeń, laboratoriów itp.
4. Szkolenie będzie odbywać się w dni robocze.
5. Szkolenie prowadzone będzie na podstawie zaakceptowanego przez Zamawiającego szczegółowego zakresu merytorycznego szkolenia dostarczonego przez Wykonawcę oraz wykazu osób szkolących spełniających wymagania z SWZ w zakresie kwalifikacji.
6. Uczestnicy szkolenia otrzymują certyfikaty ukończenia danego szkolenia.
7. Daty szkolenia zostaną ustalone z wybranym Wykonawcą.
8. Szkolenie może mieć formę szkolenia otwartego, w którym uczestniczą osoby z innych instytucji.

2. <u>Wykaz wymaganych szkoleń:</u>

Nazwa szkolenia	Liczba uczestników	Termin	Opis
Certified Information Systems Security Professional (CISSP) – szkolenie autoryzowane lub równoważne ISC2*	3	2 tury szkolenia	Szkolenie ma pozwolić na pozyskanie wiedzy, kwalifikacji i kompetencji w 8 domenach CISSP CBK. Domena 1. Bezpieczeństwo i zarządzanie ryzykiem Domena 2. Bezpieczeństwo aktywów Domena 3. Architektura i inżynieria bezpieczeństwa Domena 4. Komunikacja i bezpieczeństwo sieci Domena 5. Zarządzanie tożsamością i dostępem (IAM) Domena 6. Ocena i testowanie bezpieczeństwa Domena 7. Operacje bezpieczeństwa Domena 8. Bezpieczeństwo rozwoju oprogramowania

* szkolenie równoważne – spełniające co najmniej wskazania dot. tematyki i zakresu merytorycznego oraz warunki i wymagania.

3. <u>Zestawienie szkoleń:</u>

Lp.	Szkolenie	Ilość tur (osób/tura)	Terminy szkoleń	Uwagi do terminów
1	**Certified Information Systems Security Professional (CISSP)** szkolenie autoryzowane lub równoważne ISC2*	2 tury (dwie osoby w 1 turze, jedna osoba w 2 turze)	80 dni od daty zawarcia umowy	terminy poszczególnych tur szkoleń nie mogą się pokrywać

* szkolenie równoważne – spełniające co najmniej wskazania dot. tematyki i zakresu merytorycznego oraz warunki i wymagania.

Zamawiający wymaga, aby oferowane świadczenie, w tym wszystkie produkty ICT, usługi ICT oraz procesy ICT wykorzystywane do realizacji zamówienia, zarówno jako elementy główne, jak i komponenty, elementy środowiska świadczenia usługi lub rozwiązania towarzyszące, nie obejmowało:

- produktów ICT, usług ICT lub procesów ICT wskazanych w rekomendacji, o której mowa w art. 33 ust. 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, stwierdzającej ich negatywny wpływ na podstawowy interes bezpieczeństwa państwa;
- produktu ICT, którego typ został określony w decyzji w sprawie uznania dostawcy za dostawcę wysokiego ryzyka, o której mowa w art. 67b ust. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, ani usług ICT lub procesów ICT określonych w tej decyzji.

Niespełnienie powyższego wymagania skutkuje odrzuceniem oferty odpowiednio na podstawie art. 226 ust. 1 pkt 17 albo pkt 19 ustawy Pzp.