**Załącznik nr 1B**

**do zapytania ofertowego nr FSTZN/042/3/1/2024**

**SZCZEGÓŁOWE INFORMACJE O PRZEDMIOCIE ZAMÓWIENIA**

|  |
| --- |
| Opis przedmiotu zamówienia -  **Kursy dla uczniów dające dodatkowe kwalifikacje i umiejętności**  **Część B: Kluczowe zagadnienia cyberbezpieczeństwa– 30 osób.**  Zadanie realizowane w ramach projektu: **„Wsparcie kształcenia informatyków w Technicznych Zakładach Naukowych”** współfinansowanego ze środków Funduszy Europejskich dla Śląskiego 2021-2027 (Fundusz na rzecz Sprawiedliwej Transformacji) dla Priorytetu: FESL.10.00-Fundusze Europejskie na transformację; dla Działania: FESL.10.23-Edukacja zawodowa w procesie sprawiedliwej transformacji regionu. |

W ramach realizacji zadania do zadań i obowiązków Wykonawcy należeć będzie:

1. Organizacja i kompleksowe przeprowadzenie kursu „Kluczowe zagadnienia cyberbezpieczeństwa” dla 30 (trzydziestu) uczniów/uczennic będących uczestnikami projektu**,** a w tym:
   1. Moduł 1: Wprowadzenie do cyberbezpieczeństwa, a w tym: podstawowe zagadnienia związane z cyberbezpieczeństwem; zagrożenia i sposoby ich unikania; podstawy kryptografii; bezpieczeństwo systemów operacyjnych i aplikacji; bezpieczeństwo sieci komputerowych; bezpieczeństwo w chmurze; zarządzanie bezpieczeństwem informacji; przepisy prawne związane z cyberbezpieczeństwem; zapobieganie utracie danych; cyberbezpieczeństwo w świecie mobilnym.
   2. Moduł 2: Bezpieczeństwo informacji/ Sposoby zabezpieczenie informacji w trakcie jej transmisji oraz w trakcie przechowywania, a w tym: Szyfrowanie danych, co to jest i po co stosować: do czego jest nam potrzebne szyfrowanie, zagrożenia na jakie są narażone nasze dane, gdy nie są w żaden sposób chronione; zarys historyczny; współczesność. Rodzaje szyfrowania: Szyfrowanie kluczem symetrycznym: zasada działania; popularne rodzaje takich szyfrów; wady; zalety. Szyfrowanie asymetryczne: zasada działania RSA; wady; zalety; mechanizm DH; certyfikat; podpis cyfrowy. Szyfrowanie danych w trakcie ich przesyłania: TLS/SSL w WEB Aplikacjach; bezpieczne sieci VPN - po co w ogóle stosuje się VPN - rodzaje VPN. Szyfrowanie danych na dyskach w systemie Windows oparte na wbudowanych mechanizmach: Bitlocker - opis działania mechanizmu; Encrypted File System - opis działania mechanizmu. Szyfrowanie danych na dyskach w systemie Linux: LUKS - opis działania. Inne narzędzia: Vera-Crypt; PGP.
   3. Moduł 3: Informatyka śledcza, a w tym: omówienie umiejscowienia informatyki śledczej w dziedzinie nauk sądowych; omówienie obszarów badawczych informatyki śledczej; zabezpieczanie dowodów cyfrowych po wystąpieniu incydentu; problematyka integralności dowodu cyfrowego; metodyka prowadzenia badań z obszaru informatyki śledczej w zależności od typu dowodu; narzędzia informatyki śledczej; wyszukiwanie danych na nośnikach – typy wyszukiwania; odzysk danych skasowanych z nośników cyfrowych; ocena przydatności dowodowej wybranych dowodów cyfrowych; zabezpieczanie dowodu cyfrowego – wykonywanie kopii binarnych; obliczanie sum kontrolnych zabezpieczonego dowodu cyfrowego; montowanie nośników oraz obrazów nośników tylko do odczytu dla zachowania integralności; odzysk danych skasowanych; przeszukiwanie nośników lub obrazów nośników wg słów kluczowych; przeszukiwanie nośników lub obrazów nośników parametrów technicznych i właściwości wynikających z systemu pliku; wykonywanie zestawień i raportowanie wyników.
   4. Moduł 4: Testy penetracyjne, a w tym: wprowadzenie do tematyki testów penetracyjnych Włamanie Audyt/Auydt/Test penetracyjny Aspekty prawne Metodologie i fazy testu penetracyjnego; planowanie (Planning) Rekonesans (Reconnaissance); skanowanie (Scanning); wtargnięcie (Gaining Access); utrzymanie dostępu (MaintainingAccess); zatarcie śladów (CoveringTracks); raportowanie (Reporting) Footprinting i rekonesans; pasywne i aktywne zbieranie informacji; inżynieria społeczna; skanowanie sieci; skanery automatyczne Enumeracjapodatności; rodzaje podatności; wyszukiwanie podatności; wtargnięcie, rodzaje ataków, łamanie haseł,ataki na sieci LAN; utrzymanie dostępuBackdoory i rootkity; zatarcie śladów; raportowanie; dobre praktyki; omijanie systemów IDS oraz Firewall; honeypoty; buffer Overflow i Fuzzing; metody ochrony systemów; warsztaty Rekonesans podmiotów, skanowaniesieci, serwerów, usług Google Hacking; enumeracja zasobów; penetracja sieci; ataki phishingowe.
   5. Ilość grup szkoleniowych: 3 (trzy), Ilość osób w grupie szkoleniowej: 10 (dziesięć);
   6. Minimalna liczba godzin kursu: 32 (trzydzieści dwie) godziny lekcyjne, 1 (jedna) godzina=45 (czterdzieści pięć) minut;
   7. Kurs musi być przeprowadzony zgodnie z obowiązującymi przepisami i warunkami a w tym:
2. Umożliwienie uczestnikowi uzyskanie certyfikatu potwierdzającego uzyskane kompetencji. Wydawany certyfikat będzie potwierdzał posiadane kompetencje i wiedzę we wskazanym zakresie;
   1. Zapewnienie trenera/ trenów posiadających uprawnienia do przeprowadzenia przedmiotowego kursu;
   2. Przeprowadzenie zajęć szkoleniowych w oparciu o zatwierdzony przez Zamawiającego program   
      i harmonogram:
3. Program musi uwzględniać minimum: tytuł szkolenia, liczbę godzin szkolenia, imię i nazwisko wykładowcy, datę i miejsce realizacji szkolenia, cele szkolenia, tematykę zajęć wraz z liczbą godzin szkolenia z danego tematu;
4. Program szkolenia powinien odpowiadać zakresowi niezbędnemu do podniesienia umiejętności uczestników szkolenia;
5. Wykonawca musi uwzględnić możliwość realizacji zadania w soboty i w niedziele oraz w trybie zdalnym – w formie elektronicznej.
   1. Przygotowanie i wydanie uczestnikom niezbędnych dokumentów potwierdzających ukończenie kursu obejmującego „Kluczowe zagadnienia cyberbezpieczeństwa” w postaci certyfikatów ukończenia kursu.
   2. Po zakończeniu kursu Wykonawca zobowiązany jest dostarczyć następujące dokumenty:
6. Listy obecności uczestników kursu;
7. Dzienniki zajęć zawierające: listę obecności, wymiar godzin i tematy zajęć, karty zajęć teoretycznych  
    i praktycznych;
8. Oświadczenia uczestników potwierdzające odbiór materiałów szkoleniowych;
9. Kopie, potwierdzone za zgodność z oryginałem certyfikatów ukończenia kursu;
10. W ramach realizacji przedmiotowego zadania Wykonawca zorganizuje i kompleksowo przeprowadzi kurs dla 30 (trzydziestu) uczennic/uczniówbędących uczestnikami projektu**,** obejmującego „Kluczowe zagadnienia cyberbezpieczeństwa”.
    1. Uczestnikami projektu są uczennice/uczniowie w szkole technicznej - Techniczne Zakłady Naukowe w Dąbrowie Górniczej (Technikum nr 2)
11. Miejsce realizacji kursu – szkoła biorąca udział w projekcie w salach udostępnionych przez Zamawiającego.
12. Wykonawca zobowiązany jest do ochrony danych osobowych uczestników kursu i przetwarzania ich danych osobowych zgodnie z Ustawą z dnia 10 maja o ochronie danych osobowych (Dz. U. 2019.0.1781 t.j.) oraz Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).
13. Wykonawca zobowiązany jest do przekazywania informacji telefonicznie lub za pośrednictwem poczty elektronicznej, o każdym Uczestniku kursu, który nie stawił się na umówione szkolenie oraz o wszelkich problemach i trudnościach, które mogą wpłynąć na prawidłową realizację usługi.
14. Wykonawca zobowiązany jest do przekazywania, w terminie 5 dni kalendarzowych od zakończenia miesiąca, wszystkich dokumentów potwierdzających realizację usługi w zakończonym miesiącu (listy obecności, program kursu i indywidualne harmonogramy).
15. Prowadzenie dokumentacji związanej z realizacją usługi. na wzorach zaakceptowanych przez Zamawiającego m.in.: listy obecności, program kursu i indywidualne harmonogramy. Dokumenty związane   
    z realizacją umowy Wykonawca jest zobowiązany drukować na własny koszt.
16. Zapewnienie uczestnikom projektu niezbędnych materiałów dydaktycznych (np. testów, ćwiczeń)   
    i oznaczania ich zgodnie z wytycznymi znajdującymi się na stronie <https://funduszeue.slaskie.pl/> *.*
17. Wykonawca dysponuje wykwalifikowaną i doświadczoną kadrą szkoleniowo- dydaktyczną, która będzie uczestniczyć w realizacji przedmiotu umowy.
18. Zamawiający zastrzega sobie prawo do:
    1. Zmiany liczby osób objętych zadaniem, np. w przypadku zmniejszenia/zwiększenia się liczby uczestników projektu (Wykonawca otrzyma należność za faktyczną liczbę osób, dla których zrealizował usługę); przy czym zwiększenie liczby uczestników do 10% nie stanowi zmiany warunków postępowania.
    2. Przesunięcia okresów realizacji usługi, np. w przypadku problemów z rekrutacją uczestników.
19. Wykonawca zobowiązany jest do udostępnienia do wglądu dokumentów firmy związanych   
    z realizowanym zadaniem, w tym dokumentów finansowych oraz do przedłożenia ww. dokumentów na wezwanie Zarządu Województwa Śląskiego pełniącego rolę Instytucji Zarządzającej Funduszami Europejskimi dla Śląskiego 2021-2027.
20. Wykonawca zobowiązany jest do informowania Uczestników Projektu o współfinansowaniu zadania ze środków Unii Europejskiej ze środków Funduszy Europejskich dla Śląskiego 2021-2027 (Fundusz na rzecz Sprawiedliwej Transformacji).