Załącznik nr 1 – Opis przedmiotu zamówienia
na realizację zamówienia:
„Szkolenia z zakresu bezpieczeństwa systemów informatycznych ochrony zdrowia, wdrażanych w ramach projektu Zachodniopomorskie e-Zdrowie”

Rozdział I. Wprowadzenie

1. Zamówienie realizowane jest w ramach projektu „Zachodniopomorskie e-Zdrowie” współfinansowanego środkami Unii Europejskiej w ramach Regionalnego Programu Operacyjnego Województwa Zachodniopomorskiego na lata 2014-2020 Oś Priorytetowa 9 Infrastruktura publiczna, Działanie 9.10 Wsparcie rozwoju e-usług publicznych (e-Zdrowie).
2. Projekt realizowany jest przez:
    1) Województwo Zachodniopomorskie – Lider projektu,
    oraz podmioty lecznicze, dla których podmiotem tworzącym jest Samorząd Województwa Zachodniopomorskiego – partnerzy projektu:
    2) Zachodniopomorskie Centrum Onkologii w Szczecinie,
    3) Samodzielny Publiczny Wojewódzki Szpital Zespolony w Szczecinie,
    4) Samodzielny Publiczny Specjalistyczny Zakład Opieki Zdrowotnej „ZDROJE” w Szczecinie”,
    5) Wojewódzka Stacja Pogotowia Ratunkowego,
    6) Wojewódzki Ośrodek Medycyny Pracy - Zachodniopomorskie Centrum Leczenia i Profilaktyki,
    7) Samodzielny Publiczny Zespół Zakładów Opieki Zdrowotnej w Gryficach,
    8) Szpital Wojewódzki w Koszalinie im. Mikołaja Kopernika,
    9) Specjalistyczny Zespół Gruźlicy i Chorób Płuc w Koszalinie,
    10) Regionalny Szpital w Kołobrzegu,
    11) SP ZOZ Wojewódzki Ośrodek Terapii Uzależnienia od Alkoholu i Współuzależnienia w Stanominie,
    12) Szpital Uzdrowiskowy "Willa Fortuna"- Samodzielny Publiczny Zakład Opieki Zdrowotnej w Kołobrzegu,
    13) Zakład Opiekuńczo-Leczniczy SP ZOZ "Leśna Ustroń" w Tucznie,
    14) Wojewódzki Ośrodek Medycyny Pracy w Koszalinie.
3. Przedmiotowe postępowanie dotyczy realizacji szkolenia z zakresu bezpieczeństwa systemów informatycznych, i służy poniesieniu bezpieczeństwa użytkowania systemów wdrażanych w ramach projektu Zachodniopomorskie e-Zdrowie.

Rozdział II. Ogólny Opis przedmiotu zamówienia

1. Przedmiotem zamówienia jest świadczenie usługi polegającej na zorganizowaniu i przeprowadzeniu cyklu 2 szkoleń dla 16 uczestników zgodnie z poniższym zestawieniem.

Lp.	Temat szkolenia	Liczba uczestników	Uczestnicy
I.	Bezpieczeństwo Sieci Komputerowych	16	Administratorzy IT
II.	Atakowanie i Ochrona Webaplikacji	16	Administratorzy IT

2. Uczestnikami szkoleń będą administratorzy systemów teleinformatycznych ochrony zdrowia oraz osoby nadzorujące ich wdrożenie, biegłe w branży IT.
3. Zakres zagadnień poruszanych w ramach zorganizowanych tematów szkoleń, powinien być powiązany z występującymi zagrożeniami dotyczącymi systemów teleinformatycznych ochrony zdrowia.
4. Szkolenia zostaną przeprowadzone w języku polskim, w formie warsztatów z elementami wykładu i ćwiczeń (laboratoriów), w celu praktycznego przygotowywania uczestników szkolenia. Szkolenia odbywać się będą w formie jednoczesnego wykładu w którym wykładowca tłumaczy poszczególne zagadnienia, a także w formie pracy na platformie dostarczonej przez Wykonawcę na której uczestnik wykonuje ćwiczenia i do której dostęp posiada trener.
5. Wraz z usługą szkoleniową wykonawca zobowiązuje się do zapewnienia zakwaterowania dla uczestników szkolenia.

Rozdział III. Szczegółowy opis przedmiotu zamówienia

III.1 TEMATY REALIZOWANE W RAMACH SZKOLEŃ

III.1.1 Bezpieczeństwo Sieci Komputerowych

1. Celem szkolenia jest nabycie przez uczestnika wiedzy o technikach ataków i programach wykorzystywanych przez współczesnych włamywaczy oraz umiejętności w zakresie zabezpieczenia infrastruktury sieciowej, serwerów i usług na nich pracujących przed atakami w tym wykorzystania narzędzi do testowania bezpieczeństwa sieci.
2. Minimalny zakres szkolenia:
   a. Testowanie bezpieczeństwa sieci oraz testy penetracyjne i ich metodyki.
      i. metodyki i rodzaje pentestów,
      ii. OSSTMM / OWASP,
      iii. dokumenty opisujące dobre praktyki (NIST/CIS),
      iv. różnice pomiędzy pentestami a audytami,
   b. Organizacja testów penetracyjnych:
      i. prawne aspekty,

ii. plany testów penetracyjnych,
iii. problemy spotykane podczas testów penetracyjnych.

c. Poszczególne fazy testu penetracyjnego:
   i. Rekonesans
      - pasywne metody zbierania informacji o celu
      - aktywne metody zbierania informacji o celu
      - mapowanie sieci ofiary
      - omijanie firewalli
   ii. enumeracja podatności
      - rodzaje podatności (buffer, overflow, format string, itp.)
      - dopasowywanie kodu exploita do znalezionych podatności
      - drogi wejścia do systemu
   iii. atak,
      - przegląd technik ataków na systemy (Windows/Linux) i sieci komputerowe (ataki w sieci LAN/WAN/Wi-Fi, ataki na urządzenia sieciowe, ataki denial of service, fuzzing, łamanie haseł,
      - atak przy pomocy exploita zdalnego,
      - podniesienie uprawnień do poziomu administratora
   iv. zacieranie śladów,
      - backdoorowanie przejętego systemu
      - zacieranie śladów włamania, oszukiwanie narzędzi do analizy powłamaniowej
   v. sporządzenie raportu z testu penetracyjnego.
      - budowa szczegółowego raportu technicznego
      - raport dla zarządu

d. Metody ochrony przed atakami.
   i. idea honeypotów
   ii. systemy IDS/IPS
   iii. metody hardeningu systemów Windows i Linux

e. Do każdego z powyższych punktów muszą zostać przygotowane warsztaty/laboratoria, podczas których należy przedstawić praktyczne metody ochrony przed konkretnym atakiem.

3. Szkolenie "Bezpieczeństwo Sieci Komputerowych" musi trwać **co najmniej 3 dni** szkoleniowe.
4. Wykonawca udostępni uczestnikom środowisko na którym będą odbywały się ćwiczenia. W razie konieczności Wykonawca jest zobowiązany do zapewnienia uczestnikom szkolenia oprogramowania umożliwiającego sprawne połączenie z takim środowiskiem.
5. Za dzień szkoleniowy przyjmuje się min. 8 godzin lekcyjnych (45 min).

6. Grupa szkoleniowa może liczyć maksymalnie 16 osób. Wykonawca będzie mieć możliwość podziału uczestników na mniejsze grupy szkoleniowe, które w okresie trwania szkolenia zrealizują ten sam program i zakres.
7. Szkolenia powinny być przeprowadzone w terminach uzgodnionych z Zamawiającym, zgodnie z harmonogramem szkolenia.
8. Uczestnicy muszą otrzymać materiały szkoleniowe w języku polskim, oznaczone zgodnie z aktualnymi Wytycznymi w zakresie informacji i promocji projektów dofinansowanych w ramach Regionalnego Programu Operacyjnego Województwa Zachodniopomorskiego na lata 2014-2020.
9. Wykonawca każdorazowo przekaże Zamawiającemu listę obecności (w terminie 5 dni roboczych od zakończenia szkolenia). Lista może być wypełniana odręcznie przez uczestników lub tworzona np. poprzez monitorowanie zalogowania do platformy i wygenerowanie raportu obecności/aktywności uczestników.
10. Dokumentacja szkoleniowa musi być oznaczona znakiem Funduszy Europejskich, barwami Rzeczpospolitej Polskiej (RP), znakiem Unii Europejskiej oraz znakiem Urzędu Marszałkowskiego Województwa Zachodniopomorskiego (wzorce znaków oraz zasady ich używania dostępne są na stronie: https://rpo.wzp.pl/realizuje-projekt/poznaj-zasady-promowania-projektu/zasady-oznakowania-dla-umow-podpisanych-od-1-stycznia-2018-r

III.1.2 Atakowanie i Ochrona Webaplikacji

1. Szkolenie realizowane w formule warsztatowej tj. oparte o realizację ćwiczeń praktycznych, które umożliwiają omawianie konkretnego ataku oraz rozwój umiejętności obrony przed nim.
2. Minimalny zakres szkolenia:
    a. Współczesne problemy bezpieczeństwa aplikacji webowych.
        i. zagrożenia wynikające z architektury webaplikacji (np. CGI, SSI, etc.)
        ii. zagrożenia wynikające z języków programowania (PHP, JS, etc.) i technologii, np. ASP, JSP
        iii. problem styku webaplikacji z bazą danych
        iv. interfejsy zewnętrzne webaplikacji
        v. zagrożenia po stronie serwera, środowiska, sieci, a zagrożenia po stronie klienta
        vi. zagrożenia stron tworzonych pod urządzenia mobilne (telefony, tablety)
    b. Ataki na aplikacje webowe – przykłady ataków oraz praktyczne metody ochrony.
        i. wyszukiwanie adresów serwerów deweloperskich
        ii. bezpieczeństwo hostingu i webserwera
        iii. brak obsługi błędów
        iv. manipulacje parametrami (metody GET, POST)
        v. techniki podsłuchu i manipulowania transmisją
        vi. atak Forcefull browsing

vii. atak Path Traversal
viii. technika Google Hacking
ix. wstrzyknięcie kodu (PHP shell) i komend systemowych do webaplikacji
x. problem filtrowania danych wejściowych
xi. ataki XSS (persistent, reflected)
xii. omijanie filtrowania danych wejściowych i encodingu wyjściowych
xiii. ataki na sesję aplikacji webowej
xiv. podsłuchiwanie sesji i kradzież ciasteczek HTTP
xv. jak poprawnie zarządzać sesją w webapikacji?
xvi. ataki CSRF/XSRF
xvii. bezpieczny upload plików
xviii. metody ułatwiające przetrwanie ataków DoS/DDoS
xix. ataki Clickjacking
xx. ataki na bazy danych
xxi. ataki SQL injection i Blind SQL injection
xxii. ochrona przed atakami SQL injection
xxiii. szyfrowanie połączenia i ataki na SSL
xxiv. szyfrowanie danych w webaplikacji
xxv. ochrona przed spamem i enumeracją zasobów oraz haseł
xxvi. podsumowanie zagrożeń i przegląd OWASP TOP10
xxvii. pozaprogramistyczne środki ochrony (systemy IDS/IPS, WAF)
xxviii. omijanie detekcji przez systemy WAF/IDS/IPS

c. Problemy przeglądarek internetowych.
   i. Same Orgin Policy
   ii. Rich Internet Applications
   iii. dziury w przeglądarkach
   iv. ataki DNS-Rebinding
   v. narzędzia podnoszące bezpieczeństwo i pomagające w testowaniu aplikacji webowych
d. Przegląd narzędzi automatyzujących wykrywanie podatności oraz ich praktyczne wykorzystanie
e. **Do każdego z powyższych punktów muszą zostać przygotowane warsztaty/laboratoria, podczas których należy przedstawić praktyczne metody ochrony przed konkretnym atakiem.**

3. Szkolenie "Atakowanie i Ochrona Webaplikacji" musi trwać **co najmniej 2 dni** szkoleniowe.
4. Wykonawca udostępni uczestnikom środowisko na którym będą odbywały się ćwiczenia. W razie konieczności Wykonawca jest zobowiązany do zapewnienia uczestnikom szkolenia oprogramowania umożliwiającego sprawne połączenie z takim środowiskiem.
5. Za dzień szkoleniowy przyjmuje się min. 8 godzin lekcyjnych (45 min).

6. Grupa szkoleniowa może liczyć maksymalnie 16 osób. Wykonawca będzie mieć możliwość podziału uczestników na mniejsze grupy szkoleniowe, które w okresie trwania szkolenia zrealizują ten sam program i zakres.
7. Szkolenia powinny być przeprowadzone w terminach uzgodnionych z Zamawiającym, zgodnie z harmonogramem szkolenia.
8. Uczestnicy muszą otrzymać materiały szkoleniowe w języku polskim.
9. Wykonawca każdorazowo przekaże Zamawiającemu listę obecności (w terminie 5 dni roboczych od zakończenia szkolenia). Lista może być wypełniana odręcznie przez uczestników lub tworzona np. poprzez monitorowanie zalogowania do platformy i wygenerowanie raportu obecności/aktywności uczestników.
10. Dokumentacja szkoleniowa musi być oznaczona znakiem Funduszy Europejskich, barwami Rzeczpospolitej Polskiej (RP), znakiem Unii Europejskiej oraz znakiem Urzędu Marszałkowskiego Województwa Zachodniopomorskiego (wzorce znaków oraz zasady ich używania dostępne są na stronie: https://rpo.wzp.pl/realizuje-projekt/poznaj-zasady-promowania-projektu/zasady-oznakowania-dla-umow-podpisanych-od-1-stycznia-2018-r

III.2 DOKUMENTACJA SZKOLENIOWA

1. Wykonawca przygotuje dokumentację szkoleniową związaną z realizacją tematu szkoleniowego obejmującą:
   a. Harmonogram szkoleń zawierający: temat szkolenia, terminy i godziny zajęć szkoleniowych, nazwiska trenerów.
   b. Program szkoleń uwzględniający zakresy tematyczne szkoleń.
   c. Materiały szkoleniowe uwzględniające zakresy tematyczne poszczególnych szkoleń, obejmujące teoretyczne oraz praktyczne aspekty zagadnień poruszanych w trakcie każdego z tematów szkoleń (materiały szkoleniowe zawierać będą instrukcje, prezentacje, opracowania graficzne i treści z zakresu omawianego tematu szkolenia, wykorzystywane w trakcie jego trwania).
   d. Listę obecności uczestników z każdego szkolenia.
   e. Imienne zaświadczenia o ukończeniu szkolenia.
   f. Wypełnione protokoły odbioru szkoleń.
2. Wykonawca, najpóźniej **3 dni** po podpisaniu umowy przekaże Zamawiającemu do zaopiniowania **harmonogram szkoleń**. Zamawiający przekaże Wykonawcy opinię/uwagi/zalecenia do przedstawionego harmonogramu szkoleń w terminie **4 dni** od jego dostarczenia.
3. Wszystkie uwagi do **harmonogramu szkoleń** zgłoszone przez Zamawiającego zostaną wprowadzone przez Wykonawcę, w terminie nie dłuższym niż 2 dni robocze od dnia ich otrzymania.

4. Zamawiający w terminie **2 dni** roboczych od dnia dostarczenia przez Wykonawcę poprawionego **harmonogramu szkoleń**, poinformuje Wykonawcę o jego akceptacji lub konieczności wprowadzenia zmian.
5. Zamawiający nie później niż **5 dni** roboczych przed datą rozpoczęcia szkolenia, przekaże Wykonawcy w formie elektronicznej **wykaz uczestników** danej edycji szkolenia.
6. Wykonawca, najpóźniej **3 dni** przed rozpoczęciem szkolenia, przekaże **materiały szkoleniowe** wszystkim uczestnikom danej edycji szkolenia w formie elektronicznej (e-mail), na adresy poczty elektronicznej wskazane przez Zamawiającego.
7. Dokumentacja szkoleniowa wymieniona w rozdz. III.2 pkt 1. musi być oznaczona znakiem Funduszy Europejskich, barwami Rzeczpospolitej Polskiej (RP), znakiem Unii Europejskiej oraz znakiem Urzędu Marszałkowskiego Województwa Zachodniopomorskiego (wzorce znaków oraz zasady ich używania dostępne są na stronie: https://rpo.wzp.pl/realizuje-projekt/poznaj-zasady-promowaniaprojektu/zasady-oznakowania-dla-umow-podpisanych-od-1-stycznia-2018-r

III.3 ORGANIZACJA SZKOLEŃ

1. Szkolenie będzie prowadzone w języku polskim, w formie stacjonarnej.
2. Każde ze szkoleń odbędzie się w kolejno następujących po sobie dniach szkoleniowych od poniedziałku do piątku.
3. Pierwszego dnia, szkolenie musi rozpocząć się nie wcześniej niż o godzinie 9.30. W pozostałych dniach, szkolenia mogą rozpocząć się nie wcześniej niż o godz. 8.00 i zakończyć się nie później niż o godz. 16:00. Podczas każdego dnia szkolenia będzie minimum jedna przerwa 45 minutowa oraz dwie 15 minutowe.
4. Na początku każdej edycji szkolenia Wykonawca poinformuje uczestników, że po zakończeniu szkolenia mogą zostać poproszeni o wypełnienie ankiety AOS (Ankieta Oceniająca Szkolenie), co ma na celu zebranie informacji na temat jakości szkolenia. Niedopuszczalne jest sugerowanie uczestnikom odpowiedzi na pytania zawarte w ankiecie. Wyniki przeprowadzonej ankiety Wykonawca przekaże Zamawiającemu. Wykonawca po zakończeniu każdego szkolenia przygotuje dla każdego uczestnika imienne zaświadczenie o ukończeniu szkolenia, które będzie zawierało następujące informacje: imię i nazwisko uczestnika szkolenia, tytuł szkolenia, datę przeprowadzenia szkolenia, pieczątkę Wykonawcy, identyfikowalny podpis trenera prowadzącego szkolenie, liczbę godzin.
5. Warunkiem wydania zaświadczenia jest obecność uczestnika w każdym dniu zajęć w ramach danego szkolenia, potwierdzona na liście obecności, przygotowanej przez Wykonawcę.
6. Imienne zaświadczenia w wersji elektronicznej Wykonawca przekaże w ciągu 5 dni od zakończenia każdej edycji szkolenia, na adresy mailowe uczestników każdej edycji szkolenia, a także elektronicznie do Zamawiającego z dołączeniem wykazu wydanych zaświadczeń potwierdzających ukończenie szkolenia.

7. Imienne zaświadczenia w wersji papierowej Wykonawca dostarczy w ciągu 7 dni od zakończenia każdej edycji szkolenia, na adresy jednostek, w których pracują uczestnicy każdej edycji szkolenia. Adresy pocztowe jednostek zostaną przekazane Wykonawcy przez Zamawiającego.
8. Wypełniony protokół odbioru szkolenia Wykonawca dostarczy Zamawiającemu w formie papierowej lub elektronicznej w ciągu 3 dni roboczych od zakończenia danej edycji szkolenia.

III.4 ZAPLECZE TECHNICZNE

1. Wykonawca musi zapewnić odpowiednio wyposażoną salę do przeprowadzenie szkolenia.
    a) wielkość sali dostosowana do liczby uczestników, spełniająca wymogi przepisów dotyczących bezpieczeństwa i higieny pracy oraz ochrony przeciw pożarowej.
    b) sala musi posiadać wydajny system wentylacyjny bądź klimatyzację;
    c) rolety zaciemniające (lub inną możliwość zasłaniania okien);
    d) miejsca siedzące dla wszystkich uczestników;
    e) odpowiednie do potrzeb nagłośnienie;
    f) tablica typu flipchart oraz wszelkie inne niezbędne sprzęty i przybory;
    g) zaplecze sanitarne, szatnia;
2. Wykonawca, na czas trwania szkolenia, zapewni odpowiednie rozwiązania teleinformatyczne tj. dla każdego uczestnika kompletny zestaw komputerowy (lub laptop) oraz połączenie internetowe które zapewnią stabilny i komfortowy dostęp do platformy, na której uczestnicy będą wykonywali ćwiczenia i do której dostęp będzie posiadał trener.
3. Wykonawca przygotuje dla każdego z uczestników instrukcję dotyczącą sposobu korzystania z użytego przez Wykonawcę rozwiązania teleinformatycznego wykorzystanego do przeprowadzenia każdej edycji szkoleń.
4. Wykonawca zapewni każdemu uczestnikowi szkolenia komplet materiałów szkoleniowych.
5. Wykonawca zapewni obsługę uczestników przez cały czas trwania szkolenia (m.in. koordynacja zakwaterowania w hotelu, przekazanie materiałów szkoleniowych, udzielanie informacji uczestnikom w sprawach organizacyjnych - np. dotyczących harmonogramu szkolenia, godzin posiłków, obiektu, zakwaterowania, itp.).

III.5 MIEJSCA SZKOLENIA

1. Miejsce szkolenia powinno być zlokalizowane w Szczecinie lub w miejscowości oddalonej maksymalnie 50 km od Szczecina, do której bezpośrednie dotarcie możliwe jest za pomocą komunikacji publicznej.
2. Zamawiający dopuszcza organizacje szkolenia w innej miejscowości, jeżeli będzie to uzasadnione koniecznością zapewnienia odpowiedniego zaplecza technicznego.
3. Miejsce szkolenia będzie punktowane przy ocenie ofert – maksymalnie 40 pkt.

a. W przypadku Szkolenia w Szczecinie lub miejscowości oddalonej maksymalnie 50 km od Szczecina – 40 pkt.;
b. W przypadku miejscowości oddalonej od Szczecina od 51 do 300 km (np. Poznań) – 30 pkt.;
c. W przypadku miejscowości oddalonej od Szczecina od 301 do 450 km (np. Wrocław) – 20 pkt.;
d. W przypadku miejscowości oddalonej od Szczecina od 451 do 600 km (np. Warszawa) – 10 pkt.;
e. W przypadku miejscowości oddalonej od Szczecina o ponad 601 km (np. Kraków) – 0 pkt.;
f. Odległość będzie sprawdzona za pomocą aplikacji Google Maps, poprzez wybranie najszybszej dostępnej trasy samochodowej z pkt. A („Szczecin") do pkt. B. („Miejscowość organizacji szkolenia")

4. Koszt dojazdu do miejsca szkolenia będzie poniesiony bezpośrednio przez uczestników.

III.6 ZAKWATEROWANIE

1. Wykonawca jest zobowiązany zapewnić zakwaterowanie na rzecz uczestników szkolenia w hotelu co najmniej trzygwiazdkowym lub ośrodku rekreacyjno-szkoleniowym spełniającym standard hotelu co najmniej trzygwiazdkowego w miejscowości w której będzie realizowane szkolenie.
2. Wykonawca zapewni pokoje 1 osobowe z własnym węzłem sanitarnym, wraz z ręcznikami i środkami czystości/higieny oraz możliwością zaparkowania samochodu (koszt parkingu porywają bezpośrednio uczestnicy).
3. Godziny i dni zakwaterowania:
    a. W przypadku szkoleń w Szczecinie i w obrębie granic administracyjnych Województwa Zachodniopomorskiego:
        i. Bezpieczeństwo Sieci Komputerowych – 2 doby hotelowe, w tym przyjazd w pierwszym dniu szkolenia, wyjazd w ostatnim dniu szkolenia
        ii. Atakowanie i Ochrona Webaplikacji – 1 doba hotelowa, przyjazd w pierwszym dniu szkolenia, wyjazd w drugim dniu szkolenia
    b. W przypadku szkoleń w miejscowości poza granicami administracyjnymi Województwa Zachodniopomorskiego:
        i. Bezpieczeństwo Sieci Komputerowych – 3 doby hotelowe, w tym przyjazd w przeddzień szkolenia, wyjazd w ostatnim dniu szkolenia
        ii. Atakowanie i Ochrona Webaplikacji – 2 doby hotelowa, w tym przyjazd w przeddzień szkolenia, wyjazd w drugim dniu szkolenia
4. Jeśli Wykonawca zaproponuje organizację szkoleń opisanych w rozdz. III ust. 1.1 Bezpieczeństwo Sieci Komputerowych oraz rozdz. III ust. 1.2 Atakowanie i Ochrona Webaplikacji w terminach bezpośrednio następujących po sobie (dni szkoleniowe ciągiem), to

do okresu zakwaterowania wskazanego w rozdz. III.ust. 6.3 pkt a. oraz pkt. b. należy doliczyć dodatkowo, jedną dobę hotelową dla wszystkich uczestników.

5. W przypadku rozbicia terminu szkoleń na dwa odrębne cykle dotyczące zakresów wskazanych w III.1.1 oraz III.1.2, to terminy ich organizacji muszą być oddzielone od siebie co najmniej o 5 dni roboczych.
6. Godziny obowiązywania doby hotelowej, powinny być zgodne z harmonogramem realizacji szkoleń, w tym z godzinami ich rozpoczęcia w pierwszym dniu, i zakończenia w dniu ostatnim.
7. Wykonawca jest zobowiązany zapewnić wyżywienie dla uczestników szkolenia:
    a. Śniadania i kolacje (dla uczestników deklarujących korzystanie z noclegów): w formie stołu szwedzkiego, zawierające: potrawę gorącą, pieczywo, sery, wędliny, sałatki warzywne itp. oraz gorące i zimne napoje;
    b. W trakcie szkolenia:
        i. W przerwie kawowej: gorąca kawa i herbata, mleko do kawy, cukier, kruche ciastka, owoce, 2 rodzaje soków, woda mineralna gazowana i niegazowana;
        ii. obiad: składający się co najmniej z: zupy (co najmniej 350 ml), dania głównego ze sztuką mięsa lub np. ryby (co najmniej 150g - bez sosu, z sosem 170g) i zestawem surówek, soku owocowego i wody mineralnej oraz deseru;
    c. kompleksowy serwis gastronomiczny: przygotowanie, nakrycie stołów, sprzątanie po wszystkich posiłkach oraz zastawa z wyłączeniem naczyń jednorazowego użytku;
8. Wykonawca zapewni że posiłki będą przygotowane zgodnie z zasadami określonymi w ustawie z dnia 25 sierpnia 2006 r. o bezpieczeństwie żywności i żywienia (t.j. Dz. U. 2023 poz.1448);
9. Osobom, które zadeklarują korzystanie ze specjalnej diety (wegetariańskiej, dla diabetyków, bezglutenowej) Wykonawca zapewni posiłek dostosowany do indywidualnych potrzeb.

Rozdział IV. Termin realizacji Przedmiotu Zamówienia

1. Przedmiot zamówienia zostanie zrealizowany w terminie **nie dłuższym niż 1 miesiąc** od dnia zawarcia umowy, jednak nie później niż **do dnia 08 grudnia 2023 roku.**
2. Płatność nastąpi w terminie 14 dni liczonych od dnia otrzymania prawidłowo wystawione faktury VAT. Faktura może być wystawiona po podpisaniu protokołu odbioru.