Możliwość dofinansowania

Cyberbezpieczeństwo i przeciwdziałanie cyberprzestępczości w praktyce – cyfrowe i zielone kompetencje dla MŚP

Numer usługi 2025/10/19/7675/3089051

7 687,50 PLN brutto
6 250,00 PLN netto
192,19 PLN brutto/h
156,25 PLN netto/h

Zakłady Badań i Atestacji "ZETOM" im. prof. F. Stauba w Katowicach Spółka z ograniczoną odpowiedzialnością

4,9 / 5

6 247 ocen

Katowice
Usługa szkoleniowa
stacjonarna
40:00 h
06.10.2026 do 20.10.2026

Informacje podstawowe

Kategoria	Biznes / Zarządzanie przedsiębiorstwem
Grupa docelowa usługi	Szkolenie skierowane jest do wszystkich osób zainteresowanych tematyką cyberbezpieczeństwa i ochrony danych w środowisku pracy, w szczególności do pracowników mikro, małych i średnich przedsiębiorstw z województwa śląskiego biorących udział w projekcie 5.15. Uczestnikami mogą być pracownicy administracyjni, biurowi, kadra zarządzająca oraz właściciele firm, którzy chcą zwiększyć poziom bezpieczeństwa cyfrowego organizacji oraz odpowiedzialnie zarządzać danymi i zasobami.
Minimalna liczba uczestników	4
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	05-10-2026
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	40
Podstawa uzyskania wpisu do BUR	Certyfikat systemu zarządzania jakością wg. ISO 9001:2015 (PN-EN ISO 9001:2015) - w zakresie usług szkoleniowych

Cel

Cel edukacyjny

Szkolenie przygotowuje do rozpoznawania i przeciwdziałania zagrożeniom cybernetycznym w środowisku pracy. Uczestnicy rozwijają wiedzę o rodzajach cyberataków i regulacjach prawnych, umiejętności zabezpieczania danych, urządzeń i komunikacji oraz kompetencje społeczne w zakresie odpowiedzialności i współpracy. Szkolenie wspiera rozwój cyfrowych i zielonych kompetencji w przedsiębiorstwach, wzmacniając świadomość bezpieczeństwa i odpowiedzialne zarządzanie informacją.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Charakteryzuje podstawowe rodzaje cyberzagrożeń i ich wpływ na organizacje	Uczestnik wskazuje i opisuje najczęstsze zagrożenia (phishing, malware, socjotechnika)	Test teoretyczny
Wyjaśnia podstawowe przepisy dotyczące cyberbezpieczeństwa (RODO, NIS2, KSC)	Uczestnik poprawnie wskazuje obowiązki organizacji wynikające z przepisów	Test teoretyczny
Opisuje zasady bezpiecznego korzystania z Internetu, poczty i urządzeń mobilnych	Uczestnik wskazuje konkretne działania zabezpieczające	Test teoretyczny
Rozróżnia podstawowe narzędzia ochrony danych i systemów	Uczestnik przypisuje zastosowanie narzędzi do rodzaju zagrożenia	Test teoretyczny
Uzasadnia znaczenie cyberbezpieczeństwa dla zrównoważonego rozwoju i ESG	Uczestnik wskazuje, jak bezpieczeństwo wpływa na efektywność i ochronę zasobów	Test teoretyczny
Rozpoznaje próby cyberataków (phishing, oszustwa) i reaguje zgodnie z procedurami	Uczestnik analizuje przykładowe wiadomości i stosuje odpowiednie działania	Analiza dowodów i deklaracji
Stosuje zasady cyberhigieny i podstawowe środki ochrony w miejscu pracy	Uczestnik poprawnie wykonuje ćwiczenia praktyczne i przestrzega zasad bezpieczeństwa	Analiza dowodów i deklaracji
Tworzy proste procedury bezpieczeństwa informacji dostosowane do środowiska MŚP	bezpieczeństwa informacji dostosowane do środowiska MŚP Uczestnik opracowuje szkic polityki lub procedury bezpieczeństwa	Analiza dowodów i deklaracji
Wykazuje odpowiedzialność za bezpieczeństwo danych i współpracuje z zespołem w budowaniu bezpiecznego środowiska pracy	Uczestnik aktywnie uczestniczy w ćwiczeniach grupowych i stosuje zasady bezpieczeństwa	Analiza dowodów i deklaracji

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?

TAK

Pytanie 3. Czy dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

1. **Wprowadzenie do cyberbezpieczeństwa i cyberprzestępczości**

Przedstawienie pojęć cyberprzestrzeni, zagrożeń oraz wpływu cyberprzestępczości na firmy i środowisko. Omówienie roli bezpieczeństwa cyfrowego w strategiach ESG i transformacji zielonej.

2 Podstawowe rodzaje cyberzagrożeń

Omówienie popularnych form ataków: phishing, ransomware, malware, ataki socjotechniczne. Przykłady incydentów z życia firm sektora MŚP.

3 Aspekty prawne i regulacyjne cyberbezpieczeństwa w Polsce i UE

Przegląd najważniejszych przepisów: RODO, NIS2, ustawy o KSC. Znaczenie zgodności z przepisami dla odpowiedzialnego prowadzenia biznesu.

4 Identyfikacja zagrożeń w środowisku pracy

Rozpoznawanie potencjalnych słabych punktów w organizacji: nieaktualne oprogramowanie, słabe hasła, niebezpieczne zachowania pracowników.

5 Bezpieczne korzystanie z Internetu i poczty elektronicznej

Praktyczne zasady bezpiecznej komunikacji: rozpoznawanie podejrzanych wiadomości, załączników i linków. Wskazanie elementów, które powinny wzbudzać czujność.

6 Cyberhigiena w miejscu pracy

Wprowadzenie do codziennych praktyk bezpieczeństwa: zarządzanie hasłami, aktualizacje, polityka czystego biurka i ekranu. Powiązanie cyberhigieny z efektywnym wykorzystaniem zasobów i ochroną środowiska.

7 Bezpieczeństwo urządzeń mobilnych i pracy zdalnej

Zasady ochrony urządzeń przenośnych i komputerów używanych poza biurem. Wskazanie najczęstszych błędów popełnianych przez użytkowników.

8 Zarządzanie danymi i kopie zapasowe

Znaczenie prawidłowego przechowywania i zabezpieczania danych. Omówienie zasad tworzenia i weryfikowania kopii zapasowych. Wpływ właściwego zarządzania danymi na ograniczenie strat finansowych i środowiskowych.

9 Podstawy bezpiecznego uwierzytelniania

Omówienie zasad silnych haseł, uwierzytelniania dwuskładnikowego i bezpiecznego logowania. Praktyczne wskazówki dostosowane do środowiska MŚP.

10 Cyberbezpieczeństwo jako element zrównoważonego rozwoju

Pokazanie, w jaki sposób ochrona danych i systemów wpływa na efektywne zarządzanie zasobami, zmniejszenie kosztów, ograniczenie ryzyka oraz realizację celów ESG.

11 Rozpoznawanie prób phishingu i ataków socjotechnicznych

Praktyczne przykłady wiadomości e-mail, SMS i stron internetowych wykorzystywanych do oszustw. Uczestnicy uczą się rozpoznawać i reagować na typowe schematy ataków.

12 Zachowania pracowników a bezpieczeństwo organizacji

Omówienie wpływu ludzkich błędów na bezpieczeństwo firmy. Przykłady incydentów wynikających z nieostrożności oraz sposoby budowania odpowiedzialnych nawyków.

13 Podstawowe narzędzia ochrony przed zagrożeniami

Przegląd najczęściej stosowanych rozwiązań: zapory sieciowe, oprogramowanie antywirusowe, filtry antyspamowe. Wyjaśnienie, jak działają i jakie mają ograniczenia.

14 Bezpieczne korzystanie z chmury obliczeniowej

Wprowadzenie do zasad ochrony danych w usługach chmurowych. Rozróżnienie ról użytkownika i dostawcy. Najczęstsze błędy popełniane przez firmy przy korzystaniu z chmury.

15 Zabezpieczanie nośników danych i informacji wrażliwych

Zasady ochrony pamięci przenośnych, dokumentów elektronicznych i papierowych. Wskazanie procedur minimalizujących ryzyko wycieku informacji.

16 Postępowanie w sytuacjach podejrzenia incydentu

Wskazówki dotyczące rozpoznawania oznak włamania lub naruszenia danych. Omówienie podstawowych procedur reagowania w małych i średnich firmach.

17 Wprowadzenie do planowania reakcji na incydenty (Incident Response)

Przedstawienie prostych schematów postępowania krok po kroku. Rola komunikacji wewnętrznej i współpracy działów w ograniczaniu skutków ataków.

18 Rola bezpieczeństwa informacji w odpowiedzialnym zarządzaniu firmą

Pokazanie, jak działania z obszaru cyberbezpieczeństwa przekładają się na ciągłość biznesową, ochronę środowiska i zrównoważony rozwój przedsiębiorstwa.

19 Aktualizacje i polityka zarządzania oprogramowaniem

Wyjaśnienie znaczenia regularnych aktualizacji, stosowania legalnego oprogramowania oraz tworzenia polityk bezpieczeństwa IT w firmie.

20 Tworzenie prostych procedur bezpieczeństwa w MŚP

Omówienie, jak krok po kroku opracować wewnętrzne instrukcje bezpieczeństwa dostosowane do małych firm. Praktyczne przykłady i wskazówki.

21 Zarządzanie hasłami w organizacji

Praktyczne zasady tworzenia i przechowywania silnych haseł. Omówienie menedżerów haseł i ich roli w zwiększaniu bezpieczeństwa bez dodatkowych kosztów środowiskowych (np. redukcja wydruków, uporządkowanie procesów).

22 Uwierzytelnianie wieloskładnikowe (MFA) w praktyce

Wprowadzenie do metod MFA, ich zastosowania w środowisku MŚP oraz sposobów konfiguracji. Dyskusja o wpływie MFA na zmniejszenie ryzyka ataków.

23 Bezpieczna komunikacja wewnętrzna i zewnętrzna

Zasady ochrony danych podczas komunikacji mailowej, telefonicznej i za pomocą komunikatorów. Dobre praktyki szyfrowania i kontroli dostępu do informacji.

24 Tworzenie i stosowanie polityki bezpieczeństwa informacji

Omówienie podstawowych elementów polityki bezpieczeństwa. Przykłady dokumentów i sposoby ich wdrażania w małych organizacjach.

25 Budowanie świadomości bezpieczeństwa wśród pracowników

Metody skutecznego angażowania zespołów w działania proaktywnie chroniące dane i systemy. Znaczenie edukacji i regularnych szkoleń w minimalizowaniu ryzyka.

26 Rola liderów i kadry zarządzającej w ochronie danych

Wskazanie obowiązków i odpowiedzialności kadry kierowniczej w kontekście bezpieczeństwa informacji. Podkreślenie znaczenia podejścia strategicznego w zarządzaniu ryzykiem.

27 Podstawy analizy ryzyka w cyberbezpieczeństwie

Prosty model identyfikacji zagrożeń i oceny ryzyka dostosowany do małych i średnich firm. Uczestnicy poznają metody porządkowania priorytetów bezpieczeństwa.

28 Wprowadzenie do audytu bezpieczeństwa

Praktyczne omówienie, jak w małej firmie przeprowadzić wewnętrzną kontrolę procedur bezpieczeństwa, bez konieczności zaawansowanych narzędzi.

29 Cyberbezpieczeństwo a ciągłość działania organizacji

Pokazanie, jak odpowiednie zabezpieczenia wpływają na stabilność procesów biznesowych, minimalizowanie przestojów i strat zasobów — również środowiskowych.

30 Zielony wymiar cyberbezpieczeństwa w strategii firmy

Podsumowanie roli cyberbezpieczeństwa w strategiach ESG i transformacji cyfrowej. Wskazanie, jak odpowiedzialne zarządzanie danymi przyczynia się do ochrony środowiska i efektywności energetycznej.

31 Warsztaty: rozpoznawanie prób phishingu i oszustw

Ćwiczenia praktyczne z analizą realnych przykładów wiadomości i stron. Uczestnicy uczą się identyfikować podejrzane elementy i stosować odpowiednie procedury reagowania.

32 Warsztaty: tworzenie i testowanie polityki bezpieczeństwa

Uczestnicy w grupach opracowują szkic wewnętrznej polityki bezpieczeństwa informacji dopasowanej do specyfiki MŚP. Prezentacja i omówienie efektów.

33 Warsztaty: reagowanie na incydenty

Symulacja prostych scenariuszy incydentów (np. utrata hasła, podejrzana wiadomość, awaria systemu). Uczestnicy ćwiczą reakcję zgodnie z procedurami.

34 Warsztaty: tworzenie bezpiecznych haseł i konfiguracja MFA

Praktyczne ćwiczenia z generowania silnych haseł i włączania uwierzytelniania wieloskładnikowego na przykładowych kontach i usługach.

35 Warsztaty: analiza podstawowego ryzyka

Uczestnicy wykonują prostą analizę ryzyka w odniesieniu do własnego środowiska pracy. Identyfikacja zagrożeń, oszacowanie skutków i zaproponowanie działań zabezpieczających.

36 Case study: incydent w firmie usługowej

Analiza przykładowego przypadku naruszenia danych w małej firmie. Uczestnicy omawiają błędy i wypracowują plan działań naprawczych i zapobiegawczych.

37 Case study: atak phishingowy na dział administracji

Przykład rzeczywistego ataku – omówienie mechanizmu, skutków i działań naprawczych. Wskazanie roli edukacji i procedur w zapobieganiu podobnym sytuacjom.

38 Przyszłość cyberbezpieczeństwa w MŚP

Przegląd trendów i nowych zagrożeń (np. deepfake, AI w cyberatakach). Dyskusja o konieczności ciągłego podnoszenia kompetencji i dostosowywania strategii firm.

39 Podsumowanie wiedzy – quiz i dyskusja

Blok podsumowujący w formie testu i otwartej dyskusji. Uczestnicy utrwalają kluczowe informacje z całego szkolenia.

40 WALIDACJA - test teoretyczny, analiza dowodów i deklaracji

Program został opracowany zgodnie z potrzebami uczestników i celami usługi, koncentrując się na podstawowych zagadnieniach cyberbezpieczeństwa w środowisku MŚP. Obejmuje 40 godzin dydaktycznych, w tym **25 godzin zajęć teoretycznych** oraz **15 godzin zajęć praktycznych**. Szkolenie prowadzone jest stacjonarnie. Zapewnione są odpowiednie warunki organizacyjne dla aktywnego udziału każdego uczestnika.Przerwy nie wliczają się do czasu trwania usługi.

Walidacja efektów uczenia się odbywa się poprzez test teoretyczny (pytania zamknięte) oraz analizę dowodów i deklaracji. W trakcie szkolenia stosowane są quizy, ćwiczenia praktyczne, case studies oraz podsumowania grupowe i indywidualne. Przerwy są wliczone w czas szkolenia. Szkolenie obejmuje jedną dziedzinę kompetencyjną.

Harmonogram

Liczba pozycji harmonogramu: 45

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 45 Wprowadzenie do cyberbezpieczeństwa i cyberprzestępczości	Łukasz Buryan	06-10-2026	08:00	08:45	00:45
2 z 45 Podstawowe rodzaje cyberzagrożeń	Łukasz Buryan	06-10-2026	08:45	09:30	00:45
3 z 45 Aspekty prawne i regulacyjne cyberbezpieczeństwa w Polsce i UE	Łukasz Buryan	06-10-2026	09:30	10:15	00:45
4 z 45 Identyfikacja zagrożeń w środowisku pracy	Łukasz Buryan	06-10-2026	10:15	11:00	00:45

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
5 z 45 Przerwa	Łukasz Buryan	06-10-2026	11:00	11:15	00:15
6 z 45 Bezpieczne korzystanie z Internetu i poczty elektronicznej	Łukasz Buryan	06-10-2026	11:15	12:00	00:45
7 z 45 Cyberhigiena w miejscu pracy	Łukasz Buryan	06-10-2026	12:00	12:45	00:45
8 z 45 Bezpieczeństwo urządzeń mobilnych i pracy zdalnej	Łukasz Buryan	06-10-2026	12:45	13:30	00:45
9 z 45 Zarządzanie danymi i kopie zapasowe	Łukasz Buryan	06-10-2026	13:30	14:15	00:45
10 z 45 Podstawy bezpiecznego uwierzytelniania	Łukasz Buryan	07-10-2026	08:00	08:45	00:45
11 z 45 Cyberbezpieczeństwo jako element zrównoważonego rozwoju	Łukasz Buryan	07-10-2026	08:45	09:30	00:45
12 z 45 Rozpoznawanie prób phishingu i ataków socjotechnicznych	Łukasz Buryan	07-10-2026	09:30	10:15	00:45
13 z 45 Zachowania pracowników a bezpieczeństwo organizacji	Łukasz Buryan	07-10-2026	10:15	11:00	00:45
14 z 45 Przerwa	Łukasz Buryan	07-10-2026	11:00	11:15	00:15

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
15 z 45 Podstawowe narzędzia ochrony przed zagrożeniami	Łukasz Buryan	07-10-2026	11:15	12:00	00:45
16 z 45 Bezpieczne korzystanie z chmury obliczeniowej	Łukasz Buryan	07-10-2026	12:00	12:45	00:45
17 z 45 Zabezpieczanie nośników danych i informacji wrażliwych	Łukasz Buryan	07-10-2026	12:45	13:30	00:45
18 z 45 Postępowanie w sytuacjach podejrzenia incydentu	Łukasz Buryan	07-10-2026	13:30	14:15	00:45
19 z 45 Wprowadzenie do planowania reakcji na incydenty (Incident Response)	Łukasz Buryan	13-10-2026	08:00	08:45	00:45
20 z 45 Rola bezpieczeństwa informacji w odpowiedzialnym zarządzaniu firmą	Łukasz Buryan	13-10-2026	08:45	09:30	00:45
21 z 45 Aktualizacje i polityka zarządzania oprogramowaniem	Łukasz Buryan	13-10-2026	09:30	10:15	00:45
22 z 45 Tworzenie prostych procedur bezpieczeństwa w MŚP	Łukasz Buryan	13-10-2026	10:15	11:00	00:45
23 z 45 Przerwa	Łukasz Buryan	13-10-2026	11:00	11:15	00:15

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
24 z 45 Zarządzanie hasłami w organizacji	Łukasz Buryan	13-10-2026	11:15	12:00	00:45
25 z 45 Uwierzytelnianie wieloskładnikowe (MFA) w praktyce	Łukasz Buryan	13-10-2026	12:00	12:45	00:45
26 z 45 Bezpieczna komunikacja wewnętrzna i zewnętrzna	Łukasz Buryan	13-10-2026	12:45	13:30	00:45
27 z 45 Tworzenie i stosowanie polityki bezpieczeństwa informacji	Łukasz Buryan	13-10-2026	13:30	14:15	00:45
28 z 45 Budowanie świadomości bezpieczeństwa wśród pracowników	Łukasz Buryan	14-10-2026	08:00	08:45	00:45
29 z 45 Rola liderów i kadry zarządzającej w ochronie danych	Łukasz Buryan	14-10-2026	08:45	09:30	00:45
30 z 45 Podstawy analizy ryzyka w cyberbezpieczeństwie	Łukasz Buryan	14-10-2026	09:30	10:15	00:45
31 z 45 Wprowadzenie do audytu bezpieczeństwa	Łukasz Buryan	14-10-2026	10:15	11:00	00:45
32 z 45 Przerwa	Łukasz Buryan	14-10-2026	11:00	11:15	00:15
33 z 45 Cyberbezpieczeństwo a ciągłość działania organizacji	Łukasz Buryan	14-10-2026	11:15	12:00	00:45

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
34 z 45 Zielony wymiar cyberbezpieczeństwa w strategii firmy	Łukasz Buryan	14-10-2026	12:00	12:45	00:45
35 z 45 Warsztaty: rozpoznawanie prób phishingu i oszustw	Łukasz Buryan	14-10-2026	12:45	13:30	00:45
36 z 45 Warsztaty: tworzenie i testowanie polityki bezpieczeństwa	Łukasz Buryan	14-10-2026	13:30	14:15	00:45
37 z 45 Warsztaty: reagowanie na incydenty	Łukasz Buryan	20-10-2026	08:00	08:45	00:45
38 z 45 Warsztaty: tworzenie bezpiecznych haseł i konfiguracja MFA	Łukasz Buryan	20-10-2026	08:45	09:30	00:45
39 z 45 Warsztaty: analiza podstawowego ryzyka	Łukasz Buryan	20-10-2026	09:30	10:15	00:45
40 z 45 Case study: incydent w firmie usługowej	Łukasz Buryan	20-10-2026	10:15	11:00	00:45
41 z 45 Przerwa	Łukasz Buryan	20-10-2026	11:00	11:15	00:15
42 z 45 Case study: atak phishingowy na dział administracji	Łukasz Buryan	20-10-2026	11:15	12:00	00:45
43 z 45 Przyszłość cyberbezpieczeństwa w MŚP	Łukasz Buryan	20-10-2026	12:00	12:45	00:45

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
44 z 45 Podsumowanie wiedzy – quiz i dyskusja	Łukasz Buryan	20-10-2026	12:45	13:30	00:45
45 z 45 WALIDACJA - test teoretyczny, analiza dowodów i deklaracji	-	20-10-2026	13:30	14:15	00:45

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	7 687,50 PLN
Koszt przypadający na 1 uczestnika netto	6 250,00 PLN
Koszt osobogodziny brutto	192,19 PLN
Koszt osobogodziny netto	156,25 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Łukasz Buryan

Absolwent studiów licencjackich na kierunku zarządzanie na uczelni ASBiRO w Łodzi. Certyfikowany coach z kwalifikacją Vocational Competence Certificate (VCC) nr 235920, członek stowarzyszenia „Superwizja na Uniwersytecie Śląskim". Prowadzi indywidualny coaching i doradztwo dla freelancerów, wspierając ich w budowaniu systemów sprzedażowych, optymalizacji komunikacji z klientem oraz zwiększaniu wartości oferowanych usług. Posiada 5 letnie doświadczenie w prowadzeniu szkoleń o podobnej tematyce dla osób dorosłych , koncentrując się na rozwijaniu kompetencji w zakresie prowadzenia rozmów sprzedażowych oraz prezentacji ofert. Specjalizuje się także w tworzeniu treści w mediach społecznościowych i lejków sprzedażowych, które pomagają klientom przyciągać właściwe kontakty i efektywnie zamykać sprzedaż. Doświadczenie zdobywał również jako przedstawiciel handlowy, co pozwala mu łączyć perspektywę praktyka sprzedaży z narzędziami rozwojowymi. Skupia się na działaniu i rezultatach, dbając jednocześnie o to, by komunikacja była autentyczna i „miękka" — dzięki temu klienci budują pewność siebie i trwalsze relacje z odbiorcami. Od ponad dwóch lat aktywnie wykorzystuje narzędzia sztucznej inteligencji w

codziennej pracy, ze szczególnym naciskiem na automatyzację procesów sprzedażowych. Dzięki temu potrafi zwiększać efektywność działań, skracać czas reakcji na potrzeby klienta oraz skalować procesy sprzedaży bez utraty jakości komunikacji.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Każdy uczestnik otrzyma niezbędne materiały szkoleniowe w postaci skryptu prezentacji multimedialnej wykorzystywanej podczas zajęć, notesu, długopisu .

Informacje dodatkowe

Ujęte godziny szkoleniowe są godzinami dydaktycznymi i tj. godzina = 45 min

Warunkiem uzyskania zaświadczenia jest uczestnictwo w co najmniej 80% zajęć oraz zaliczenia zajęć w formie uzyskania 80% punktów z testu wiedzy oraz analizy dowodów i deklaracji

Dokument potwierdza, że zostały zastosowane rozwiązania zapewniające rozdzielenie procesów kształcenia i szkolenia od walidacji. tzn. osoba prowadząca usługę, nie dokonuje weryfikacji efektów uczenia się uczestników usługi.

Trener przygotowuje walidację: zaprojektował efekty uczenia się, kryteria weryfikacji przez określenie metod ich oceny po przygotowanie zestawu pytań testowych. Trener rozda testy uczestnikom . Nie ingeruje w jakiejkolwiek formie w ocenę wyników testu ani w proces jego wypełniania. Osoba walidująca zostaje zaangażowana dopiero na etapie oceny i weryfikacji efektów uczenia się uczestników. Nie prowadzi bezpośrednio działań związanych z tworzeniem i kompletowaniem dokumentacji walidacyjnej.

Adres

ul. ks. bpa Herberta Bednorza 17
40-384 Katowice
woj. śląskie

Kontakt

Małgorzata Hajduk

E-mail m.hajduk@zetom.eu
Telefon (+48) 882 062 298