Możliwość dofinansowania

LT MASTERY SZKOLENIA DLA BIZNESU PIOTR SZYMCZYK

4,9 / 5

61 ocen

NIS2 / UoKSC w praktyce – wdrożenie wymagań ustawy o krajowym systemie cyberbezpieczeństwa: SZBI, ISO 27001, zarządzanie ryzykiem, incydenty i audyt na lata 2026 – 2028 Cyfrowe Kompetencje - DigComp 2.0

Numer usługi 2026/09/14/204299/3810097

- Usługa szkoleniowa
- zdalna w czasie rzeczywistym
- Zajęcia grupowe
- 08:00 h
- 01.10.2026 do 01.10.2026

899,00 PLN brutto
899,00 PLN netto
112,38 PLN brutto/h
112,38 PLN netto/h
261,33 PLN cena rynkowa

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Identyfikatory projektów	Kierunek - Rozwój, Akademia HR, FELB.06.03-IZ.00-0003/24 ZIPH, FELB.06.08-IZ.00-0017/25, FELB.06.08-IZ.00-0083/24
Grupa docelowa usługi	Szkolenie skierowane jest do osób odpowiedzialnych za bezpieczeństwo informacji, zgodność z regulacjami oraz zarządzanie ryzykiem cybernetycznym w organizacji. Obejmuje zarówno aspekty prawno-organizacyjne, jak i techniczne, ze szczególnym uwzględnieniem ról decyzyjnych kadry kierowniczej i specjalistów IT/OT oraz cyfrowych kompetencji. Usługa adresowana jest do: • specjalistów ds. bezpieczeństwa informacji i IT (CISO, IT Manager, Security Officer) • kadry kierowniczej odpowiedzialnej za zgodność z przepisami (Compliance, Risk Manager, Prezes/Dyrektor) • inżynierów i architektów systemów odpowiedzialnych za produkty z elementami cyfrowymi (IoT, OT, systemy wbudowane, OZE) • pracowników działów prawnych i compliance obsługujących wdrożenie NIS2 / UoKSC / CRA • menedżerów projektów IT/OT realizujących projekty wymagające certyfikacji CE lub audytu bezpieczeństwa • uczestników projektów dofinansowanych: Kierunek-Rozwój, Bony Rozwojowe, MP Pociąg do Kariery, NSE i innych projektów EFS/FERS
Minimalna liczba uczestników	2
Maksymalna liczba uczestników	15

Data zakończenia rekrutacji	30-09-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Podstawa uzyskania wpisu do BUR	Certyfikat ICVC - SURE (Standard Usług Rozwojowych w Edukacji): Norma zarządzania jakością w zakresie świadczenia usług rozwojowych

Cel

Cel edukacyjny

Wyposażenie uczestników w wiedzę i praktyczne narzędzia niezbędne do wdrożenia i utrzymania zgodności z regulacjami NIS2 / UoKSC - cyfrowych kompetencji. Szkolenie umożliwia samodzielne przeprowadzenie analizy ryzyka, opracowanie wymaganej dokumentacji (Technical File / SZBI - ISO 27001), ustalenie statusu podmiotu i zaplanowanie działań audytowych, zarządzania łańcuchem dostaw, oraz reakcji na incydenty cyberbezpieczeństwa /podatności w organizacji lub dla produktu z elementami cyfrowymi.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik ustala samodzielnie, czy i w jakiej kategorii (podmiot kluczowy, ważny lub uznany) jego organizacja podlega ustawie o KSC.	Poprawnie stosuje kryterium sektorowe z Załączników nr 1 i nr 2 oraz regułę size-cap wg rozporządzenia 651/2014, uwzględniając podmioty powiązane.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik przeprowadza analizę ryzyka cyberbezpieczeństwa zgodną z ISO/IEC 27005 i prowadzi rejestr ryzyk.	Prawidłowo identyfikuje aktywa, zagrożenia, podatności i środki zabezpieczające w przykładowym scenariuszu oraz wylicza poziom ryzyka.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik przeprowadza analizę luk wobec wymagań UoKSC i priorytetyzuje luki krytyczne.	Poprawnie ocenia stan spełnienia wymagań na podstawie dowodu, wskazuje wymagany dowód audytowy i uzasadnia priorytet zamknięcia luki.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik wskazuje wymagane elementy dokumentacji SZBI zgodnej z art. 8 i art. 10 ust. 1 UoKSC oraz ISO/IEC 27001:2022.	Poprawnie wymienia i opisuje obowiązkowe składniki dokumentacji wymagane przez przepisy oraz zasady nadzoru nad dokumentami.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik klasyfikuje incydent i sporządza zgłoszenie do właściwego CSIRT w terminach 24 h / 72 h / 1 miesiąc.	Poprawnie identyfikuje moment uzyskania wiedzy o incydencie, kryterium istotności z rozporządzenia 2024/2690, właściwy CSIRT oraz terminy raportowania wg art. 11–12a UoKSC.	Test teoretyczny z wynikiem generowanym automatycznie

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik formułuje wymagania bezpieczeństwa wobec dostawców ICT oraz ocenia kompletność planu ciągłości działania.	Prawidłowo definiuje metryki RTO i RPO, wskazuje kluczowe elementy planu odtworzenia oraz klauzule umowne wymagane w łańcuchu dostaw.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik przygotowuje organizację do audytu z art. 15 UoKSC i opracowuje własny plan wdrożenia na 90 dni.	Poprawnie wskazuje zakres audytu i wymagane dowody oraz buduje harmonogram działań z produktem końcowym i właścicielem dla każdej pozycji.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik wymienia 10 obszarów obowiązkowych środków bezpieczeństwa z art. 8 UoKSC i przypisuje je do ról w organizacji.	Poprawnie przyporządkowuje obowiązki regulacyjne do właściwych przepisów i ról organizacyjnych; w każdym obszarze wskazuje jednego właściciela rozliczeniowego.	Test teoretyczny z wynikiem generowanym automatycznie

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem zawierają opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji i zgodnie z zaplanowanymi metodami walidacji?

TAK

Pytanie 3. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Moduł I: Zakres, rejestracja i system S46 (08:00 – 09:15, 75 min; 1,5 godz. dyd.)

- Dlaczego powstała NIS2 — studium przypadku: udokumentowany przez CERT Polska atak destrukcyjny na polską energetykę z 29 grudnia 2025 r., krok po kroku
- Od dyrektywy NIS1 do NIS2 i ustawy o krajowym systemie cyberbezpieczeństwa (Dz.U. 2026 poz. 252) — co zmienia się w praktyce

- Ujednolicona oś czasu 2026–2028: wejście w życie 3.04.2026, otwarcie rejestracji 7.05.2026, wniosek o wpis do 3.10.2026, pełne wdrożenie do 3.04.2027, koniec okresu ochronnego 3.04.2028
- Zakres podmiotowy: podmiot kluczowy, ważny i uznany; 18 sektorów z Załączników nr 1 (11) i nr 2 (7); reguła size-cap (kryterium wielkości przedsiębiorstwa) wg rozporządzenia 651/2014 z uwzględnieniem podmiotów powiązanych i partnerskich
- Drzewo decyzyjne — czy moja organizacja podlega pod UoKSC (Ćwiczenie 1: samoidentyfikacja podmiotu)
- System S46 / wykaz-ksc.gov.pl — rejestracja krok po kroku, 18 kategorii danych, dane pobierane automatycznie z KRS i REGON, wyznaczenie osób do kontaktu (art. 8e)

Efekt modułu: uczestnik potrafi samodzielnie ustalić i udokumentować status swojej organizacji oraz zna procedurę i termin wpisu do wykazu.

Moduł II: Obowiązki, odpowiedzialność i nadzór (09:30 – 10:45, 75 min; 1,5 godz. dyd.)

- 10 obszarów obowiązkowych środków bezpieczeństwa — art. 8 UoKSC / art. 21 NIS2, omówione jeden po drugim z przykładami wdrożeniowymi
- Osobista odpowiedzialność kierownictwa — art. 73a: zatwierdzanie polityk, nadzór nad SZBI i realne konsekwencje majątkowe (do 300 % miesięcznego wynagrodzenia)
- Obowiązkowe roczne szkolenie kierownictwa (art. 8e) oraz wymóg niekaralności (art. 8f)
- Kary administracyjne dla podmiotów — progi do 10 mln EUR albo 2 % przychodu, minima ustawowe, okres ochronny do 3.04.2028
- Wymóg dokumentacji identyfikowalnej, aktualnej i dostępnej dla organu (art. 10 ust. 1)
- Organy nadzoru: kto kontroluje, czego żąda i czym różni się nadzór ex-ante nad podmiotem kluczowym od nadzoru ex-post nad podmiotem ważnym
- Podział ról w organizacji i macierz odpowiedzialności (Ćwiczenie 2: macierz RACI dla 10 obszarów art. 8)

Efekt modułu: uczestnik wie, kto w jego organizacji odpowiada za każdy z obowiązków ustawowych i jakie konsekwencje wiążą się z ich niedopełnieniem.

Moduł III: SZBI, ISO 27001, analiza ryzyka i analiza luk (11:00 – 12:45, 105 min; + 2 godz. dyd.)

- System Zarządzania Bezpieczeństwem Informacji jako system procesowy — czym jest, czym nie jest i ile realnie trwa jego wdrożenie (7–8 miesięcy od zera)
- Cykl PDCA jako mechanizm zapewniający wymaganą przez ustawę systematyczność
- ISO/IEC 27001:2022 jako rama wdrożeniowa — klauzule 4–10 i 93 kontrole Załącznika A
- Tabela mapowania: 10 obszarów art. 8 UoKSC → konkretne kontrole ISO/IEC 27001:2022, oraz wskazanie, gdzie ustawa wykracza poza normę
- Dokumentacja SZBI — trzy poziomy, katalog dokumentów, właściciel, wersja i data przeglądu, zasady nadzoru nad dokumentami
- Analiza ryzyka w 6 krokach wg ISO/IEC 27005 — sześć kroków, sześć artefaktów (Ćwiczenie 3: rejestr ryzyk)
- Metodyka analizy luk wobec wymagań UoKSC — ocena na podstawie dowodu, nie deklaracji (Ćwiczenie 4: checklista audytowa)

Moduł rozszerzony do 2 godzin dydaktycznych ze względu na kluczowy charakter SZBI i analizy ryzyka dla całego procesu wdrożenia.

Efekt modułu: uczestnik potrafi przeprowadzić i udokumentować analizę ryzyka oraz analizę luk wymagane przez ustawę i zbudować na nich plan wdrożenia.

Moduł IV: Środki techniczne, incydenty i CSIRT (13:15 – 14:30, 75 min; 1,5 godz. dyd.)

- Konkretne środki techniczne wymagane przez art. 8: MFA (uwierzytelnianie wieloskładnikowe), szyfrowanie, zarządzanie tożsamością i dostępem (IAM), dostęp uprzywilejowany (PAM), centralne logowanie i retencja
- Segmentacja sieci, model Purdue i specyfika środowisk OT / ICS
- Obowiązek objęcia systemu informacyjnego monitorowaniem w trybie ciągłym oraz modele wdrożenia SOC dla podmiotów kluczowych i ważnych
- Zarządzanie podatnościami, SLA patchowania i obowiązek udostępnienia kanału przyjmowania zgłoszeń podatności (CVD)
- Klasyfikacja incydentu poważnego według rozporządzenia wykonawczego Komisji (UE) 2024/2690 — kryteria horyzontalne i sektorowe
- Terminy zgłoszeń wg art. 11–12a UoKSC: 24 h wczesne ostrzeżenie, 72 h zgłoszenie incydentu, 1 miesiąc sprawozdanie końcowe; właściwość CSIRT NASK / GOV / MON
- Obowiązki równoległe: Prezes UODO, organ sektorowy, odbiorcy usługi (Ćwiczenie 5: symulacja „pierwsze 24 godziny”)

Efekt modułu: uczestnik wie, jak wykrywać, klasyfikować, reagować i raportować incydenty zgodnie z wymogami ustawowymi oraz jakie środki techniczne stanowią minimalny standard.

Moduł V: Dostawcy, ciągłość działania, audyt i plan wdrożenia (14:40 – 15:30, 50 min; 1 godz. dyd.)

- Bezpieczeństwo łańcucha dostaw ICT — inwentaryzacja i klasyfikacja krytyczności dostawców, ocena bezpieczeństwa, klauzule umowne, roczny przegląd
- Usługi chmurowe: model współdzielonej odpowiedzialności, lokalizacja danych, termin powiadomienia o incydencie po stronie dostawcy i plan wyjścia
- Ciągłość działania: analiza wpływu na działalność (BIA), metryki RTO i RPO zaakceptowane przez biznes, kopie zapasowe wg zasady 3-2-1 z kopią offline, coroczne testy odtworzenia
- Audyt bezpieczeństwa z art. 15 UoKSC — sześć obszarów, terminy (pierwszy audyt w ciągu 24 miesięcy od wpisu, kolejne co najmniej co 3 lata), szablon sprawozdania
- Pięć najczęstszych ustaleń audytowych i komplet dowodów do przygotowania
- Mapa drogowa wdrożenia i indywidualny plan na 90 dni (Ćwiczenie 6)

Efekt modułu: uczestnik rozumie wymagania audytowe i wychodzi ze szkolenia z własnym, wypełnionym planem wdrożenia na najbliższe 90 dni.

Sesja końcowa (15:30 – 16:00, 30 min; 0,5 godz. dyd.)

- Podsumowanie, odpowiedzi na pytania zaparkowane w trakcie dnia, indywidualne rekomendacje wdrożeniowe (15:30 – 15:45)
- Walidacja: post-test wiedzy online, 20 pytań, zaliczenie od 60 % (15:45 – 16:00)

Całkowity czas trwania szkolenia : 8 godzin zegarowych (5 godzin zegarowych przekazywania wiedzy + 1,5 godziny warsztatów + 30 min walidacji wiedzy + 60 min przerw)

Czas nauki oraz warsztatów: 6 godzin 45 minut

Czas walidacji wiedzy: 15 min

Czas przerw: 2 x 15 minut + 1 x 30 minut + 1 x 10 minut (razem 70 min)

· Egzamin wewnętrzny / walidacja jest wliczona w czas trwania szkolenia.

· Przerwy nie są wliczone w czas trwania szkolenia

Harmonogram

Liczba pozycji harmonogramu: 15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 15 Wprowadzenie, pre-test i studium przypadku: atak na polską energetykę z 29.12.2025. Ramy prawne NIS2 i UoKSC, oś czasu 2026–2028	Zajęcia	Piotr Szymczyk	01-10-2026	08:00	08:45	00:45
2 z 15 Zakres podmiotowy: 18 sektorów, podmiot kluczowy / ważny / uznany, reguła size-cap. Rejestracja w wykazie i system S46. Ćwiczenie 1	Zajęcia	Piotr Szymczyk	01-10-2026	08:45	09:15	00:30
3 z 15 -	Przerwa	-	01-10-2026	09:15	09:30	00:15
4 z 15 10 obszarów obowiązkowych środków bezpieczeństwa – art. 8 UoKSC / art. 21 NIS2	Zajęcia	Piotr Szymczyk	01-10-2026	09:30	10:15	00:45
5 z 15 Odpowiedzialność kierownictwa (art. 73a, 8e, 8f), kary i organy nadzoru. Podział ról w organizacji – Ćwiczenie 2 (macierz RACI)	Zajęcia	Piotr Szymczyk	01-10-2026	10:15	10:45	00:30
6 z 15 -	Przerwa	-	01-10-2026	10:45	11:00	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
7 z 15 SZBI wg art. 8 ust. 1 UoKSC i ISO/IEC 27001:2022 – mapowanie wymagań, cykl PDCA, dokumentacja SZBI i jej nadzór	Zajęcia	Piotr Szymczyk	01-10-2026	11:00	11:45	00:45
8 z 15 Analiza ryzyka w 6 krokach wg ISO 27005 i metodyka analizy luk – Ćwiczenia 3 i 4 (rejestr ryzyk, checklista gap analysis)	Zajęcia	Piotr Szymczyk	01-10-2026	11:45	12:45	01:00
9 z 15 -	Przerwa	-	01-10-2026	12:45	13:15	00:30
10 z 15 Środki techniczne z art. 8: MFA, szyfrowanie, IAM i PAM, logowanie, segmentacja IT/OT, monitorowanie ciągłe, zarządzanie podatnościami	Zajęcia	Piotr Szymczyk	01-10-2026	13:15	14:00	00:45
11 z 15 Klasyfikacja incydentu poważnego wg rozporządzenia 2024/2690, terminy 24 h / 72 h / 1 miesiąc i właściwość CSIRT – Ćwiczenie 5	Zajęcia	Piotr Szymczyk	01-10-2026	14:00	14:30	00:30
12 z 15 -	Przerwa	-	01-10-2026	14:30	14:40	00:10

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
13 z 15 Bezpieczeństwo dostawców ICT i chmura, ciągłość działania (BIA, RTO/RPO, testy), audyt z art. 15 – Ćwiczenie 6 (plan na 90 dni)	Zajęcia	Piotr Szymczyk	01-10-2026	14:40	15:30	00:50
14 z 15 Podsumowanie, Q&A i indywidualne rekomendacje wdrożeniowe	Zajęcia	Piotr Szymczyk	01-10-2026	15:30	15:45	00:15
15 z 15 -	Walidacja	Piotr Szymczyk	01-10-2026	15:45	16:00	00:15

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	08:00
w tym suma godzin zajęć	06:35
w tym suma godzin walidacji	00:15
w tym suma przerw	01:10
Suma godzin dydaktycznych bez przerw	09:05

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	899,00 PLN

Podmiot uprawniony do zwolnienia z VAT na podstawie art. 113 ust. 1 ustawy o VAT ze względu na wartość sprzedaży

Koszt przypadający na 1 uczestnika netto	899,00 PLN
Koszt osobogodziny brutto	112,38 PLN
Koszt osobogodziny netto	112,38 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	08:00

Prowadzący

Liczba prowadzących: 1

1 z 1

Piotr Szymczyk

Dynamiczny menedżer i trener z wieloletnim doświadczeniem w sektorze IT oraz usługach bezpieczeństwa dla globalnych korporacji (blue-chip). Specjalizuje się w budowaniu odporności cyfrowej organizacji, optymalizacji procesów serwisowych oraz wdrażaniu standardów zgodnych z najnowszymi dyrektywami unijnymi (w tym NIS2). Jako praktyk biznesu, Piotr nie tylko przekazuje wiedzę teoretyczną, ale uczy, jak zarządzać zmianą w środowisku wysokiej zmienności i niepewności (VUCA). Jego szkolenia charakteryzują się wysokim poziomem merytorycznym, ścisłą orientacją na cele biznesowe oraz praktycznym podejściem do technologii, co pozwala uczestnikom na natychmiastowe wdrożenie zdobytych umiejętności.
OBSZARY EKSPERTYZY SZKOLENIOWEJ
• Cyberbezpieczeństwo i Zgodność: Kompleksowe wdrażanie dyrektywy NIS2, nowelizacja UoKSC, implementacja SZBI, audyt systemów informatycznych zgodnie z normami ISO 27001
• Zarządzanie Usługami IT (ITIL): Optymalizacja procesów dostarczania usług, zarządzanie incydentami oraz planowanie ciągłości działania (BCP/DRP)
• Change Management: Prowadzenie organizacji przez procesy transformacji cyfrowej i przełamywanie oporu wobec zmian technologicznych
• Przywództwo w IT: Budowanie i szkolenie wielokulturowych zespołów technicznych, coaching menedżerski oraz strategiczne zarządzanie talentami
Certyfikaty: AgilePM® Foundation & Practitioner, Change Management® Foundation, ISO 27001 Audytor Wewnętrzny, Akademia Bezpieczeństwa Informacji (EITCA/IS), ITIL® 4 Foundation

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

- prezentację ze szkolenia (w formacie PDF)
- wzory szablonów i narzędzi: checklista wymagań NIS2, wzór rejestru ryzyka, wzór procedury reagowania na incydent
- przykłady wzorów dokumentów takich jak polityki / instrukcje / raporty / rejestry zgodne z SZBI
- scenariusz studium przypadku: opis przykładowej organizacji zbudowany na faktach z raportu CERT Polska o ataku z 29.12.2025, wykorzystywany we wszystkich ćwiczeniach

- komplet 6 szablonów roboczych do ćwiczeń w formacie edytowalnym: formularz samoidentyfikacji podmiotu, macierz RACI dla 10 obszarów art. 8, rejestr ryzyk, checklista analizy luk, arkusz „pierwsze 24 godziny” z formularzem wczesnego ostrzeżenia, arkusz planu wdrożenia na 90 dni
- kompendium wiedzy NIS2 / UoKSC / SZBI / ISO 27001
- checklista audytowa NIS2 / UoKSC dla podmiotów kluczowych i ważnych
- zaświadczenie / certyfikat o ukończeniu szkolenia - **roczny obowiązkowy wymóg nakładany przez ustawę o KSC**

Warunki uczestnictwa

- Podstawowa wiedza w zakresie kompetencji cyfrowych
- Logowanie się pełnym imieniem i nazwiskiem
- Warunkiem uzyskania zaświadczenia jest uczestnictwo w co najmniej 80%–100% zajęć usługi rozwojowej (w zależności od programu dofinansowania i podpisanej umowy z Operatorem)
- W ramach realizacji usług szkoleniowych Organizator utrwala wizerunek Uczestników w formie nagrań wideo, fotografii lub innych materiałów audiowizualnych wyłącznie w celach archiwizacyjnych, kontrolnych oraz dokumentacyjnych związanych z projektem dofinansowanym
- Uczestnik zapisując się na szkolenie wyraża zgodę na utrwalenie i wykorzystanie jego wizerunku w wyżej wymienionych celach

Informacje dodatkowe

Usługa jest zwolniona z podatku VAT w przypadku, kiedy przedsiębiorstwo zwolnione jest z podatku VAT lub dofinansowanie wynosi co najmniej 70%. W innej sytuacji do ceny netto doliczany jest podatek VAT w wysokości 23%.

Podstawa: §3 ust. 1 pkt. 14 rozporządzenia Ministra Finansów z dnia 20.12.2013 r. w sprawie zwolnień od podatku od towarów i usług orazszczegółowych warunków stosowania tych zwolnień (Dz.U. z 2018 r., poz. 701).

Całe szkolenie jest rejestrowane w celach kontroli oraz audytu.

Wykorzystanie nagrania w innym celu niż kontrola czy audyt wymaga zgody trenera oraz uczestników.

Uczestnicy otrzymają zaświadczenie / certyfikat, potwierdzające ukończenie szkolenia.

Usługa zdalna w czasie rzeczywistym - prowadzona na żywo.

Uczestnik ma możliwość złożenia reklamacji po zrealizowanej usłudze, sporządzając ją w formie pisemnej na formularzu reklamacji i odsyłając na adres: biuro@legacyturn.com

Warunki techniczne

Poniżej opisane są minimalne wymagania techniczne dotyczące uczestnictwa w szkoleniu przy pomocy platformy TEAMS:

1. Parametry urządzenia: komputer / laptop / tablet

- Procesor dwurdzeniowy 1–2 GHz minimalnie; zalecany dual-core 2 GHz lub lepszy (Intel i3/i5 lub równoważny)
- 2 GB pamięci RAM (zalecane 4 GB lub więcej).
- System operacyjny: Windows 10/11, macOS 10.13+ (lub nowsze), Linux (nowsze dystrybucje wspierane), iOS 13+/Android 8+
    - • • • zainstalowany TEAMS (najświeższa wersja) oraz najnowsza wersja Chrome/Edge/Firefox;

1. Kamera i mikrofon

- TEAMS współpracuje z wbudowanymi kamerami w laptopach oraz większością kamer internetowych.
    - słuchawki z mikrofonem zalecane dla lepszej jakości dźwięku.
    - zaawansowane lub profesjonalne kamery/mikrofony, mogą wymagać zainstalowanie dodatkowego oprogramowania .

1. Urządzenia mobilne

- Jeżeli łączysz się z urządzenia mobilnego, pobierz i zainstaluj aplikację TEAMS z App Store (Apple) lub Google Play
- Aby korzystać z dźwięku i obrazu, użyj zestawu słuchawkowego z mikrofonem lub głośników podłączonych do urządzenia.
- Przed rozpoczęciem szkolenia sprawdź, czy urządzenie rozpoznaje wybrane urządzenie audio oraz czy nie jest ono jednocześnie zajęte przez inną aplikację
- Upewnij się, że aplikacja ma przyznane uprawnienia do korzystania z mikrofonu i kamery.

1. Wymagania dla łącza internetowego:

- *min. 1,5 Mbps download i upload* dla podstawowego udziału
- zalecane 3 Mbps+ dla stabilnego wideo HD i udostępniania ekranu
- najnowsza wersja używanej przeglądarki internetowej

1. Link do szkolenia oraz warunki / wymagania dodatkowe:
    - Link do szkolenia zostanie dosłany drogą elektroniczną przed rozpoczęciem usługi na adres email podany przez uczestnika szkolenia.

- Link do szkolenia będzie ważny w dniach i godzinach określonych w harmonogramie usługi.

1. Podczas szkolenia online zapewniamy:
    - Wygodną formę szkolenia, gdzie wystarczy dostęp do urządzenia z internetem (komputer, tablet, telefon), słuchawki lub głośniki.

- Szkolenie zdalne w czasie rzeczywistym w wirtualnym pokoju konferencyjnym, w niewielkiej grupie uczestników.
- Możliwość pełnej interakcji z trenerem, który prowadzi zajęcia "na żywo" z włączoną kamerą w czasie trwania całego szkolenia.
- Możliwości zadawania pytań, omawiania indywidulanych zagadnień oraz aktywny udział w ćwiczeniach.

Przed szkoleniem:

- Upewnij się, że masz stabilne połączenie internetowe, które spełnia minimalne wymagane prędkości dla transmisji audio oraz wideo.
- Przetestuj dostęp i uruchomienie aplikacji TEAMS w wykorzystaniem kamery oraz mikrofonu.
- Rekomenduje się przygotowanie zapasowego zestawu awaryjnego sprzętu w celu zapewnienia ciągłości realizacji szkolenia. Powinien on obejmować kluczowe komponenty: komputer, kamerę, mikrofon/głośnik, klawiaturę, myszkę oraz alternatywne źródło dostępu do Internetu (np. modem Hot-Spot).

Podstawą do rozliczenia usługi jest wygenerowanie z systemu raportu, umożliwiającego identyfikację wszystkich uczestników oraz zastosowanego narzędzia.

Kontakt

PIOTR SZYMCZYK

E-mail szyplodz@yahoo.com
Telefon (+48) 501 435 131