Możliwość dofinansowania

Cyberbezpieczeństwo i zarządzanie kryzysowe w organizacji

Numer usługi 2026/05/21/160205/3575611

5 600,00 PLN brutto
5 600,00 PLN netto
140,00 PLN brutto/h
140,00 PLN netto/h
261,33 PLN cena rynkowa

INSTYTUT ROZWOJU I NAUKI SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

4,9 / 5

823 oceny

Usługa szkoleniowa
zdalna w czasie rzeczywistym
Zajęcia grupowe
40:00 h
07.09.2026 do 11.09.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Szkolenie kierowane jest do wszystkich pracowników organizacji — niezależnie od zajmowanego stanowiska i wykształcenia technicznego — którzy w swojej codziennej pracy korzystają z systemów informatycznych, poczty elektronicznej, narzędzi do pracy zdalnej lub obsługują dane klientów i partnerów biznesowych. Adresaci szkolenia: • Pracownicy działów sprzedaży, obsługi klienta, marketingu i administracji — jako pierwsza linia obrony przed atakami socjotechnicznymi i phishingiem. • Pracownicy działów finansowych i księgowości — narażeni na ataki BEC (Business Email Compromise) i wyłudzenia faktur. • Kadra kierownicza i właściciele firm — odpowiedzialni za decyzje dotyczące bezpieczeństwa i zarządzania kryzysowego. • Pracownicy działów HR i zaopatrzenia — przetwarzający wrażliwe dane osobowe pracowników i kontrahentów. • Osoby odpowiedzialne za IT i bezpieczeństwo informacji (w roli koordynatorów / pierwszego wsparcia) — bez specjalistycznego wykształcenia IT. • Osoby prowadzące jednoosobową działalność
Minimalna liczba uczestników	3
Maksymalna liczba uczestników	30
Data zakończenia rekrutacji	06-09-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym

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

Rozwinięcie praktycznych kompetencji uczestników w zakresie cyberbezpieczeństwa i zarządzania kryzysowego, umożliwiających skuteczną ochronę zasobów informacyjnych organizacji, reagowanie na incydenty bezpieczeństwa oraz budowanie odporności operacyjnej w obliczu rosnących zagrożeń cyfrowych i geopolitycznych.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Wiedza — uczestnik po szkoleniu wie i rozumie: Rodzaje i mechanizmy współczesnych zagrożeń cybernetycznych: phishing, spear phishing, ransomware, BEC, social engineering, ataki na łańcuch dostaw. Aktualne statystyki i przykłady incydentów cybernetycznych w firmach z sektora usługowego i handlowego w Polsce i na świecie. Zasady bezpiecznego zarządzania hasłami, uwierzytelniania wieloskładnikowego (MFA) i kontroli dostępu do systemów IT. Obowiązki pracownika i organizacji wynikające z RODO w zakresie ochrony danych osobowych klientów, pracowników i partnerów. Podstawowe wymogi dyrektywy NIS2 dotyczące podmiotów ważnych i kluczowych oraz obowiązki w zakresie zarządzania ryzykiem IT. Procedurę reagowania na incydent bezpieczeństwa: identyfikacja, zgłoszenie, izolacja, dokumentacja, komunikacja. Zasady planowania ciągłości działania (BCP) i tworzenia planów awaryjnych na wypadek ataku ransomware lub wycieku danych. Rodzaje i zakres odpowiedzialności prawnej pracownika i pracodawcy za naruszenia bezpieczeństwa informacji.	ocena umiejętności praktycznego wykorzystania zdobytej wiedzy	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Umiejętności — uczestnik po szkoleniu potrafi: Rozpoznać w praktyce próbę ataku phishingowego, spear phishingowego lub socjotechnicznego i podjąć właściwe działania (nie kliknąć, zgłosić, ostrzec). Zastosować bezpieczne praktyki pracy z pocztą elektroniczną, aplikacjami chmurowymi i narzędziami do pracy zdalnej. Poprawnie skonfigurować i stosować uwierzytelnianie wieloskładnikowe (MFA) na używanych kontach i platformach. Wypełnić wewnętrzny formularz zgłoszenia incydentu bezpieczeństwa i podjąć pierwsze kroki ograniczające jego skutki. Uczestniczyć aktywnie w symulowanym ćwiczeniu zarządzania kryzysem cybernetycznym (tabletop exercise) i wypracowywać procedury reagowania w grupie. Ocenić, czy dane zdarzenie stanowi incydent bezpieczeństwa wymagający zgłoszenia do UODO lub innych organów. Zastosować zasadę ograniczonego zaufania i weryfikacji tożsamości w komunikacji elektronicznej z klientami i dostawcami. Sporządzić prosty plan działania na wypadek ataku ransomware dla swojego działu lub stanowiska pracy.	ocena umiejętności praktycznego wykorzystania zdobytej wiedzy	Test teoretyczny
Kompetencje społeczne — uczestnik po szkoleniu: Rozumie swoją rolę jako aktywnego ogniwa w systemie bezpieczeństwa organizacji i podejmuje odpowiedzialne działania na co dzień. Potrafi komunikować kwestie bezpieczeństwa współpracownikom i przełożonym w sposób jasny i konstruktywny. Wykazuje gotowość do zgłaszania podejrzanych zdarzeń i incydentów bez obawy przed konsekwencjami (kultura bezpieczeństwa). Współdziała w grupie podczas sytuacji kryzysowej — potrafi koordynować działania, komunikować się i zachować spokój pod presją. Rozumie znaczenie aktualnej wiedzy z zakresu cyberbezpieczeństwa i wykazuje motywację do samodzielnego śledzenia zagrożeń.	ocena umiejętności praktycznego wykorzystania zdobytej wiedzy	Test teoretyczny

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

DZIEŃ 1 — Krajobraz zagrożeń cybernetycznych

- Wprowadzenie do cyberbezpieczeństwa — dlaczego to dotyczy każdego. Statystyki incydentów w Polsce i na świecie. Gospodarcze skutki cyberataków dla sektora usługowego i handlowego.
- Rodzaje zagrożeń cybernetycznych: phishing, spear phishing, smishing, vishing — mechanizmy działania i przykłady. Ransomware i ataki szyfrujące dane. Ataki BEC (Business Email Compromise) — wyłudzenia faktur i przelewów.
- Social engineering — manipulacja psychologiczna jako narzędzie ataku. Jak rozpoznać próbę ataku w codziennej komunikacji. Ćwiczenie praktyczne: analiza podejrzanych wiadomości e-mail.
- Kontekst geopolityczny: zagrożenia hybrydowe i ich wpływ na firmy prywatne. Ataki na łańcuch dostaw. Podsumowanie dnia i quiz weryfikujący wiedzę.

DZIEŃ 2 — Bezpieczna praca z danymi i systemami IT

- Polityka haseł — tworzenie silnych haseł, menedżery haseł, błędy najczęściej popełniane przez pracowników. Ćwiczenie: audyt własnych praktyk zarządzania hasłami.
- Uwierzytelnianie wieloskładnikowe (MFA) — rodzaje, konfiguracja i praktyczne stosowanie w systemach używanych w organizacji. Ćwiczenie: uruchomienie MFA na wybranych platformach.
- Bezpieczna praca zdalna i chmurowa — VPN, bezpieczne połączenia Wi-Fi, Microsoft 365 / Google Workspace. Ochrona urządzeń mobilnych (BYOD). Zasada minimalnych uprawnień.
- Bezpieczne korzystanie z systemów branżowych (CRM, ERP, sklepy internetowe) — zarządzanie dostępami, logowanie, sesje. Podsumowanie i quiz.

DZIEŃ 3 — RODO, NIS2 i wymogi prawne w praktyce

- RODO w praktyce organizacji usługowej i handlowej — jakie dane przetwarzamy, podstawy prawne przetwarzania, prawa osób fizycznych. Dane klientów, pracowników i kontrahentów.
- Naruszenie ochrony danych — jak rozpoznać, kiedy zgłaszać do UODO, terminy i obowiązki. Ćwiczenie: analiza przypadku naruszenia i decyzja o zgłoszeniu.
- Dyrektywa NIS2 — zakres stosowania, podmioty ważne i kluczowe, obowiązki w zakresie zarządzania ryzykiem IT, rejestracja, kary. Co zmienia się dla sektora usługowego i handlowego.
- Odpowiedzialność prawna pracownika i pracodawcy za naruszenia bezpieczeństwa informacji. Polityki wewnętrzne — jak je tworzyć i egzekwować. Podsumowanie i quiz.

DZIEŃ 4 — Reagowanie na incydenty i ochrona danych

- Procedura reagowania na incydent (IRP) — etapy: wykrycie, zgłoszenie, izolacja, analiza, dokumentacja, komunikacja, odtworzenie. Ćwiczenie: wypełnienie formularza zgłoszenia incydentu.
- Case studies — analiza rzeczywistych incydentów w firmach sektora usługowego i handlowego: atak ransomware na sklep internetowy, wyciek bazy klientów, wyłudzenie przelewu przez BEC. Wypracowanie wniosków.
- Strategie backupu i odtwarzania danych (DRP) — zasada 3-2-1, backup w chmurze, testowanie kopii zapasowych. Bezpieczne usuwanie danych i urządzeń.
- Bezpieczeństwo płatności elektronicznych i transakcji online — PCI DSS w skrócie, weryfikacja kontrahentów, ochrona przed wyłudzeniami. Podsumowanie i quiz.

DZIEŃ 5 — Zarządzanie kryzysowe, ciągłość działania i zaliczenie

- Planowanie ciągłości działania (BCP) — co to jest, jak budować plan, kluczowe elementy: RTO, RPO, scenariusze awarii. Przykładowy plan BCP dla firmy usługowej/handlowej.
- Komunikacja kryzysowa — jak informować pracowników, klientów, partnerów i media w sytuacji incydentu. Zasady transparentności vs. ochrony informacji.
- Tabletop exercise — symulacja zarządzania kryzysem cybernetycznym. Scenariusz: atak ransomware paraliżujący systemy sprzedaży. Praca w grupach: identyfikacja, decyzje, komunikacja, dokumentacja, odtworzenie. Prezentacja wyników i omówienie.
- Budowanie kultury bezpieczeństwa w organizacji — jak wdrożyć polityki IT security, angażować pracowników, prowadzić regularne szkolenia i testy. Action plan dla uczestnika.
- Test wiedzy końcowy (30 pytań, 70% zaliczenia). Podsumowanie szkolenia, wręczenie zaświadczeń, ankieta ewaluacyjna.

Harmonogram

Liczba pozycji harmonogramu: 37

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 37 Wprowadzenie do cyberbezpieczeństwa — dlaczego to dotyczy każdego. Statystyki incydentów w Polsce i na świecie. Gospodarcze skutki cyberataków dla sektora usługowego i handlowego.	Zajęcia	Marcin Wrzoskiewicz	07-09-2026	08:00	09:30	01:30
2 z 37 -	Przerwa	-	07-09-2026	09:30	09:45	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
3 z 37 Zagrożenia cybernetyczne: phishing (spear, smishing, vishing), ransomware oraz ataki BEC – wyłudzenia faktur i przelewów; mechanizmy działania i przykłady.	Zajęcia	Marcin Wrzoskiewicz	07-09-2026	09:45	11:45	02:00
4 z 37 -	Przerwa	-	07-09-2026	11:45	12:15	00:30
5 z 37 Social engineering — manipulacja psychologiczna jako narzędzie ataku. Jak rozpoznać próbę ataku w codziennej komunikacji. Ćwiczenie praktyczne: analiza podejrzanych wiadomości e-mail.	Zajęcia	Marcin Wrzoskiewicz	07-09-2026	12:15	14:15	02:00
6 z 37 -	Przerwa	-	07-09-2026	14:15	14:30	00:15
7 z 37 Kontekst geopolityczny: zagrożenia hybrydowe i ich wpływ na firmy prywatne. Ataki na łańcuch dostaw. Podsumowanie dnia i quiz weryfikujący wiedzę.	Zajęcia	Marcin Wrzoskiewicz	07-09-2026	14:30	16:00	01:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
8 z 37 Polityka haseł — tworzenie silnych haseł, menedżery haseł, błędy najczęściej popełniane przez pracowników. Ćwiczenie: audyt własnych praktyk zarządzania hasłami.	Zajęcia	Marcin Wrzoskiewicz	08-09-2026	08:00	10:00	02:00
9 z 37 -	Przerwa	-	08-09-2026	10:00	10:15	00:15
10 z 37 Uwierzytelnianie wieloskładnikowe (MFA) — rodzaje, konfiguracja i praktyczne stosowanie w systemach używanych w organizacji. Ćwiczenie: uruchomienie MFA na wybranych platformach.	Zajęcia	Marcin Wrzoskiewicz	08-09-2026	10:15	11:45	01:30
11 z 37 -	Przerwa	-	08-09-2026	11:45	12:15	00:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
12 z 37 Bezpieczna praca zdalna i chmurowa — VPN, bezpieczne połączenia Wi-Fi, Microsoft 365 / Google Workspace. Ochrona urządzeń mobilnych (BYOD). Zasada minimalnych uprawnień.	Zajęcia	Marcin Wrzoskiewicz	08-09-2026	12:15	14:15	02:00
13 z 37 -	Przerwa	-	08-09-2026	14:15	14:30	00:15
14 z 37 Bezpieczne korzystanie z systemów branżowych (CRM, ERP, sklepy internetowe) — zarządzanie dostępami, logowanie, sesje. Podsumowanie i quiz.	Zajęcia	Marcin Wrzoskiewicz	08-09-2026	14:30	16:00	01:30
15 z 37 RODO w praktyce organizacji usługowej i handlowej — jakie dane przetwarzamy, podstawy prawne przetwarzania, prawa osób fizycznych. Dane klientów, pracowników i kontrahentów.	Zajęcia	Marcin Wrzoskiewicz	09-09-2026	08:00	10:00	02:00
16 z 37 -	Przerwa	-	09-09-2026	10:00	10:15	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
17 z 37 Naruszenie ochrony danych — jak rozpoznać, kiedy zgłaszać do UODO, terminy i obowiązki. Ćwiczenie: analiza przypadku naruszenia i decyzja o zgłoszeniu.	Zajęcia	Marcin Wrzoskiewicz	09-09-2026	10:15	11:45	01:30
18 z 37 -	Przerwa	-	09-09-2026	11:45	12:15	00:30
19 z 37 Dyrektywa NIS2 — zakres stosowania, podmioty ważne i kluczowe, obowiązki w zakresie zarządzania ryzykiem IT, rejestracja, kary. Co zmienia się dla sektora usługowego i handlowego.	Zajęcia	Marcin Wrzoskiewicz	09-09-2026	12:15	14:15	02:00
20 z 37 -	Przerwa	-	09-09-2026	14:15	14:30	00:15
21 z 37 Odpowiedzialność prawna pracownika i pracodawcy za naruszenia bezpieczeństwa informacji. Polityki wewnętrzne — jak je tworzyć i egzekwować. Podsumowanie i quiz.	Zajęcia	Marcin Wrzoskiewicz	09-09-2026	14:30	16:00	01:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
22 z 37 Procedura reagowania na incydent (IRP) — etapy: wykrycie, zgłoszenie, izolacja, analiza, dokumentacja, komunikacja, odtworzenie. Ćwiczenie: wypełnienie formularza zgłoszenia incydentu.	Zajęcia	Marcin Wrzoskiewicz	10-09-2026	08:00	10:00	02:00
23 z 37 -	Przerwa	-	10-09-2026	10:00	10:15	00:15
24 z 37 Case studies: analiza incydentów w usługach i handlu – ransomware w e-sklepie, wyciek bazy klientów, wyłudzenie przelewu BEC oraz wypracowanie wniosków.	Zajęcia	Marcin Wrzoskiewicz	10-09-2026	10:15	12:15	02:00
25 z 37 -	Przerwa	-	10-09-2026	12:15	12:45	00:30
26 z 37 Strategie backupu i odtwarzania danych (DRP) — zasada 3-2-1, backup w chmurze, testowanie kopii zapasowych. Bezpieczne usuwanie danych i urządzeń.	Zajęcia	Marcin Wrzoskiewicz	10-09-2026	12:45	14:15	01:30
27 z 37 -	Przerwa	-	10-09-2026	14:15	14:30	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
28 z 37 Bezpieczeństwo płatności elektronicznych i transakcji online — PCI DSS w skrócie, weryfikacja kontrahentów, ochrona przed wyłudzeniami. Podsumowanie i quiz.	Zajęcia	Marcin Wrzoskiewicz	10-09-2026	14:30	16:00	01:30
29 z 37 Planowanie ciągłości działania (BCP) — co to jest, jak budować plan, kluczowe elementy: RTO, RPO, scenariusze awarii. Przykładowy plan BCP dla firmy usługowej/handlowej.	Zajęcia	Marcin Wrzoskiewicz	11-09-2026	08:00	09:30	01:30
30 z 37 -	Przerwa	-	11-09-2026	09:30	09:45	00:15
31 z 37 Komunikacja kryzysowa — jak informować pracowników, klientów, partnerów i media w sytuacji incydentu. Zasady transparentności vs. ochrony informacji.	Zajęcia	Marcin Wrzoskiewicz	11-09-2026	09:45	10:45	01:00
32 z 37 -	Przerwa	-	11-09-2026	10:45	11:15	00:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
33 z 37 Tabletop exercise: symulacja kryzysu cybernetycznego po ataku ransomware na systemy sprzedaży. Identyfikacja zagrożeń, decyzje, komunikacja, dokumentacja, odtworzenie i omówienie wyników.	Zajęcia	Marcin Wrzoskiewicz	11-09-2026	11:15	13:45	02:30
34 z 37 -	Przerwa	-	11-09-2026	13:45	14:00	00:15
35 z 37 Budowanie kultury bezpieczeństwa w organizacji — jak wdrożyć polityki IT security, angażować pracowników, prowadzić regularne szkolenia i testy. Action plan dla uczestnika.	Zajęcia	Marcin Wrzoskiewicz	11-09-2026	14:00	15:00	01:00
36 z 37 Podsumowanie oraz omówienie szkolenia szkolenia.	Zajęcia	Marcin Wrzoskiewicz	11-09-2026	15:00	15:50	00:50
37 z 37 -	Walidacja	-	11-09-2026	15:50	16:00	00:10

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	40:00

Rodzaj godzin	Liczba godzin
w tym suma godzin zajęć	34:50
w tym suma godzin walidacji	00:10
w tym suma przerw	05:00
Suma godzin dydaktycznych bez przerw	46:30

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto Podmiot uprawniony do zwolnienia z VAT na podstawie art. 43 ust. 1 ustawy o VAT	5 600,00 PLN
Koszt przypadający na 1 uczestnika netto	5 600,00 PLN
Koszt osobogodziny brutto	140,00 PLN
Koszt osobogodziny netto	140,00 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	40:00

Prowadzący

Liczba prowadzących: 1

1 z 1

Marcin Wrzoskiewicz

Marcin Wrzoskiewicz -sprzedaż, obsługa klienta, marketing, zarządzanie zasobami ludzkimi, umiejętności miękkie,
02.2020 - ALEF Centrum Nauki, Rozwoju i Doradztwa - trener, szkoleniowiec
2020 College Medyczny- trener, szkoleniowiec
2020 Konsorcjum Naukowo-Edukacyjne - wykładowca, trener
2018 Akademia Humanistyczno-Ekonomiczna w Łodzi - wykładowca, trener

2014-2019 Specjalista ds. sprzedaży samochodów osobowych marki Mercedes-Benz "Rita Motors"
2013-2014 Specjalista ds. sprzedaży samochodów osobowych marki Hyundai- "Folwark samochodowy"
2012-2013 Specjalista ds. ubezpieczeń- PZU
1999-2012 Prowadzenie własnej firmy- Sprzedaż pamiątek regionalnych
1996-1997 Zamek w Chęcinach Obsługa Ruchu Turystycznego
1997-2002 Akademia Pedagogiczna im. Komisji Edukacji Narodowej, Kraków, Studia Magisterskie, Historia
2003-2004 Akademia Świętokrzyska, Kielce Studia Podyplomowe - Informatyka, Logopedia, Doradztwo zawodowe i coaching.
KURSY, SZKOLENIA, STUDIA PODYPLOMOWE
• Trener umiejętności społecznych
• AAC – Wspomagające i alternatywne metody komunikacji
• Szkolenie PECS- szybkie nauczenia umiejętności porozumiewania się osoby, które nie posiadają funkcjonalnej mowy.
• Narzędzia komunikacji interpersonalnej w codziennej pracy nauczyciela
• Rozwijanie zdolności poznawczych uczniów i kreatywności
• Nie straszny lęk i stres. Jak pomóc dzieciom i młodzieży radzić sobie z emocjami, lękiem i stresem?

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały szkoleniowe w formie pdf w wersji elektronicznej na podany adres email uczestnicy szkolenia mogą otrzymać po zgłoszeniu chęci ich otrzymania usługodawcy

Warunki uczestnictwa

Warunkiem uczestnictwa jest zarejestrowanie się i założenie konta w Bazie Usług Rozwojowych oraz zapisanie się na szkolenie za pośrednictwem Bazy.

Informacje dodatkowe

Zajęcia realizowane będą w oparciu o godzinę zegarową; przerwy organizacyjne nie są wliczane do liczby godzin wskazanych w harmonogramie. Szkolenie prowadzone będzie w formie zdalnej w czasie rzeczywistym. W zależności od potrzeb dydaktycznych stosowane będą różne metody pracy, w tym ćwiczenia, testy i ankiety.

Uczestnik ma obowiązek uczestniczyć w co najmniej 80% zajęć. W przypadku formy zdalnej potwierdzeniem obecności będzie raport logowania w czasie rzeczywistym.

Usługa szkoleniowa jest zwolniona z podatku VAT na podstawie art. 43 ust. 1 pkt 29 lit. c ustawy z 11 marca 2004 r. o podatku od towarów i usług (Dz.U. z późn. zm.).

Warunki techniczne

Zajęcia odbywać będą się zdalnie w czasie rzeczywistym na platformie Zoom.

Procesor jednordzeniowy 1 GB lub szybszy Pamięć RAM 1 GB lub większa

: wymagane jest połączenie internetowe przewodowe lub bezprzewodowe (3G, 4G, LTE) o następujących parametrach: - dla transmisji wideo w jakości HD 720p minimalna przepustowość łącza internetowego wynosi: 1.5Mbps/1.5Mbps (wysyłanie/odbieranie). - dla transmisji wideo w jakości FullHD 1080p minimalna przepustowość łącza internetowego wynosi: 3Mbps/3Mbps (wysyłanie/odbieranie). Oprogramowanie: Urządzenie może ale nie musi mieć zainstalowanej aplikacji Zoom. Może działać poprzez stronę internetową: https://meet.jit.si/ System operacyjny: Urządzenie musi działać pod kontrolą jednego z systemów operacyjnych obsługiwany przez komunikator zoom: Android OS 4.0x lub nowszy macOS X 10.7 lub nowszy IOS 7.0 lub nowszy iPadOS 13 lub nowszy Windows 10 Home, Pro, lub Enterprise (Wersja “S” nie jest obsługiwana) Windows 8 or 8.1 Windows 7 Windows Vista with SP1 lub nowszy Windows XP with SP3 lub nowszy Ubuntu 12.04 lub nowszy Mint 17.1 lub nowszy Red Hat Enterprise Linux 6.4 lub nowszy Oracle Linux 6.4 lub nowszy CentOS 6.4 lub nowszy A Fedora 21 lub nowszy OpenSUSE 13.2 lub nowszy ArchLinux (tylko 64-bitowy)

Kontakt

PATRYCJA CHABA

E-mail patrycja.chaba@irin.pl

Telefon (+48) 453 049 912