Możliwość dofinansowania

Obowiązki podmiotów publicznych w świetle aktualnej i projektowanej regulacji ustawy o Krajowy System Cyberbezpieczeństwa

Numer usługi 2026/07/20/7909/3699146

1 351,77 PLN brutto
1 099,00 PLN netto
112,65 PLN brutto/h
91,58 PLN netto/h
261,33 PLN cena rynkowa

APEXNET SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ SPÓŁKA KOMANDYTOWA

4,6 / 5

79 ocen

Usługa szkoleniowa
zdalna w czasie rzeczywistym
Zajęcia grupowe
12:00 h
24.08.2026 do 25.08.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Szkolenie jest skierowane do kierownictwa jednostek samorządu terytorialnego i urzędów oraz specjalistów ds. IT i cyberbezpieczeństwa, inspektorów ochrony danych, pracowników działów zamówień publicznych oraz osób odpowiedzialnych za ciągłość działania i zarządzanie dokumentacją. Adresowane jest do osób, które planują, nadzorują lub realizują działania w zakresie bezpieczeństwa cyfrowego, w tym przygotowują procedury, zarządzają ryzykiem i reagują na incydenty zgodnie z wymaganiami KSC i NIS2, uwzględniając współpracę z CSIRT, BCP/DR, audyty i klauzule bezpieczeństwa w umowach z dostawcami IT. **Usługa również adresowana jest dla uczestników projektu Małopolski Pociąg do Kariery-sezon 1 realizowany przez WUP w Krakowie**
Minimalna liczba uczestników	8
Maksymalna liczba uczestników	30
Data zakończenia rekrutacji	23-08-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Podstawa uzyskania wpisu do BUR	Znak Jakości TGLS Quality Alliance

Cel

Cel edukacyjny

Kurs przygotowuje do praktycznego organizowania cyberbezpieczeństwa w urzędach i jednostkach samorządu terytorialnego zgodnie z wymaganiami Ustawy o krajowym systemie cyberbezpieczeństwa oraz nadchodzącymi zmianami wynikającymi z NIS2. Uczestnicy uczą się określać odpowiedzialność w urzędzie i dzielić role między IT, kierownictwo i inne komórki, reagować na incydenty cyberbezpieczeństwa, identyfikować i zarządzać ryzykiem w systemach oraz przygotować jednostkę do nowych wymagań NIS2, korzystając

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Rozróżnia role i odpowiedzialności kierownictwa oraz komórek urzędu w zakresie cyberbezpieczeństwa i stosuje mapę odpowiedzialności RACI w praktyce.	Uczestnik wskazuje role i odpowiedzialności kierownictwa oraz komórek organizacyjnych urzędu w zakresie cyberbezpieczeństwa.	Test teoretyczny z wynikiem generowanym automatycznie
	Uczestnik rozróżnia poziomy odpowiedzialności w modelu RACI.	Test teoretyczny z wynikiem generowanym automatycznie
Identyfikuje incydenty cyberbezpieczeństwa, reaktywnie reaguje na zdarzenia (phishing, ransomware, wyciek danych) i zgłasza je zgodnie z procedurami KSC/NIS2.	Uczestnik rozpoznaje rodzaje incydentów cyberbezpieczeństwa.	Test teoretyczny z wynikiem generowanym automatycznie
	Uczestnik określa zasady reagowania i zgłaszania incydentów zgodnie z wymaganiami KSC i NIS2.	Test teoretyczny z wynikiem generowanym automatycznie
Analizuje ryzyka cyber w jednostce, tworzy rejestr ryzyk oraz priorytetyzuje działania minimalizujące zagrożenia.	Uczestnik identyfikuje źródła ryzyka cyberbezpieczeństwa w jednostce.	Test teoretyczny z wynikiem generowanym automatycznie
	Uczestnik rozróżnia poziomy ryzyka i działania służące jego ograniczaniu.	Test teoretyczny z wynikiem generowanym automatycznie
Stosuje wymogi NIS2 i KSC w zakresie środków zarządzania ryzykiem, zabezpieczeń technicznych (MFA, segmentacja, backup, patching, EDR) oraz procedur ciągłości działania usług cyfrowych.	Uczestnik rozpoznaje podstawowe wymagania NIS2 oraz KSC dotyczące cyberbezpieczeństwa	Test teoretyczny z wynikiem generowanym automatycznie
	Uczestnik wskazuje zastosowanie zabezpieczeń technicznych i procedur ciągłości działania usług cyfrowych.	Test teoretyczny z wynikiem generowanym automatycznie
Opracowuje procedury obsługi incydentów, w tym detekcję, triage, eskalację i komunikację, oraz przygotowuje dokumentację i checklisty działań w wersji urzędowej.	Uczestnik rozpoznaje etapy obsługi incydentu cyberbezpieczeństwa.	Test teoretyczny z wynikiem generowanym automatycznie
	Uczestnik identyfikuje elementy dokumentacji i zasad komunikacji stosowanych podczas obsługi incydentów.	Test teoretyczny z wynikiem generowanym automatycznie

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Wdraża środki organizacyjne i techniczne pod kątem zgodności z prawem, w tym przygotowuje „Teczki zgodności” i harmonogramy wdrożenia cyberbezpieczeństwa w jednostce.	Uczestnik rozróżnia środki organizacyjne i techniczne stosowane w cyberbezpieczeństwie.	Test teoretyczny z wynikiem generowanym automatycznie
	Uczestnik wskazuje elementy dokumentacji zgodności oraz harmonogramu wdrożenia cyberbezpieczeństwa.	Test teoretyczny z wynikiem generowanym automatycznie
Formułuje wymagania bezpieczeństwa do SIWZ/OPZ oraz uwzględnia klauzule bezpieczeństwa w umowach z dostawcami IT.	Uczestnik wskazuje wymagania bezpieczeństwa stosowane w SIWZ/OPZ.	Test teoretyczny z wynikiem generowanym automatycznie
	Uczestnik rozpoznaje klauzule bezpieczeństwa stosowane w umowach z dostawcami IT.	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

Cel edukacyjny:

Kurs przygotowuje do praktycznego organizowania cyberbezpieczeństwa w urzędach i jednostkach samorządu terytorialnego zgodnie z wymaganiami Ustawy o krajowym systemie cyberbezpieczeństwa oraz nadchodzącymi zmianami wynikającymi z NIS2. Uczestnicy uczą się określać odpowiedzialność w urzędzie i dzielić role między IT, kierownictwo i inne komórki, reagować na incydenty cyberbezpieczeństwa, identyfikować i zarządzać ryzykiem w systemach oraz przygotować jednostkę do nowych wymagań NIS2, korzystając

Szkolenie jest skierowane do:

kierownictwa jednostek samorządu terytorialnego i urzędów oraz specjalistów ds. IT i cyberbezpieczeństwa, inspektorów ochrony danych, pracowników działów zamówień publicznych oraz osób odpowiedzialnych za ciągłość działania i zarządzanie dokumentacją. Adresowane jest do osób, które planują, nadzorują lub realizują działania w zakresie bezpieczeństwa cyfrowego, w tym przygotowują procedury, zarządzają ryzykiem i reagują na incydenty zgodnie z wymaganiami KSC i NIS2, uwzględniając współpracę z CSIRT, BCP/DR, audyty i klauzule bezpieczeństwa w umowach z dostawcami IT.

Usługa również adresowana jest dla uczestników projektu Małopolski Pociąg do Kariery-sezon 1 realizowany przez WUP w Krakowie

Walidacja

Test teoretyczny z wynikiem generowanym automatycznie przeprowadzany jest za pośrednictwem formularza google doc.. Uczestnik otrzymuje link z dostępem do testu. Do jego wypełnienia wymagane jest posiadanie własnego urządzenia mobilnego z dostępem do Internetu. Warunkiem zaliczenia testu jest uzyskanie co najmniej 70%

PROGRAM:

1.Cyberbezpieczeństwo w JST/urzędzie – kontekst i odpowiedzialność kierownictwa.

- Cel KSC i architektura krajowa (CSIRT-y, współpraca, rola podmiotów publicznych).
- Odpowiedzialność kierownika jednostki za organizację bezpieczeństwa (nadzór, zasoby, decyzje).
- Relacja z kontrolą zarządczą, BCP/DR, zarządzaniem dokumentacją i RODO (punkty styku).

Ćwiczenie: „Mapa odpowiedzialności" – RACI dla: IT, IOD, kancelaria/EZD, PR, kadry, zamówienia.

2.Podstawowe pojęcia KSC i praktyczne granice obowiązków.

- Incydent / incydent poważny / obsługa incydentu; podatność; ryzyko.
- Usługa kluczowa / usługa cyfrowa (w obecnym KSC) – jak to „czytać" w realiach urzędu.
- Minimalny standard: polityki, uprawnienia, rejestrowanie zdarzeń, kopie, aktualizacje, zarządzanie dostępem.

Mini-case: „Wyciek danych z poczty / phishing / ransomware w sekretariacie" – co robimy w 2h, 24h, 72h.

3.Współpraca z CSIRT, zgłaszanie incydentów i komunikacja.

- Kiedy zgłaszamy incydent, komu i w jaki sposób.
- Rola CSIRT na poziomie krajowym (NASK itp.).
- Komunikacja kryzysowa: mieszkańcy, media, organ nadzorczy (RODO), podmioty współpracujące.
- Dowody i łańcuch czynności (forensic light) – jak nie „zniszczyć" śladów.

Ćwiczenie: wypełnienie „karty incydentu" oraz przygotowanie checklisty działań.

4.Zarządzanie ryzykiem cyber w jednostce – podejście praktyczne.

- Prosta metodyka ryzyka: aktywa – zagrożenia – podatności – skutki – zabezpieczenia.
- Katalog typowych ryzyk w administracji: EZD, ePUAP/eDoręczenia, BIP, domena, AD, kopie zapasowe, dostawcy, systemy dziedzinowe.
- Priorytetyzacja działań: co daje największą redukcję ryzyka przy najmniejszym koszcie.

Ćwiczenie: przygotowanie rejestru ryzyk (top 10) dla jednostki oraz plan działań 30/60/90 dni.

5.NIS2 → KSC: nowy model podmiotów i nadzoru.

- Przejście z podziału NIS1 na podmioty kluczowe i podmioty ważne.
- Rozszerzenie katalogu sektorów i objęcie większej liczby podmiotów (w tym publicznych).
- Wzmocnienie uprawnień organów właściwych i mechanizmów nadzorczych.

Ćwiczenie: „Samoocena jednostki" – czy i dlaczego możemy wpaść w kategorię podmiotu kluczowego lub ważnego (na podstawie usług i roli jednostki).

6.Obowiązki w modelu NIS2: środki zarządzania ryzykiem.

- SZBI/ISMS „w wersji urzędowej": polityki, role, przeglądy ryzyka, szkolenia.
- Zabezpieczenia: zarządzanie dostępem, MFA, zarządzanie tożsamością, segmentacja sieci, backup 3-2-1, patching, EDR oraz logowanie zdarzeń.
- Łańcuch dostaw i dostawcy IT (umowy, SLA, audyty, wymagania bezpieczeństwa) – szczególnie istotne w zamówieniach publicznych.
- Ciągłość działania usług cyfrowych (BCP/DR) oraz minimalny katalog testów ciągłości działania.

Ćwiczenie: checklista „20 wymagań” oraz analiza luk (gap analysis): jest / częściowo / brak.

7.Incydenty w NIS2/KSC: nowe kanały i tempo zgłoszeń.

- Obowiązek i technika zgłaszania incydentów z użyciem systemu teleinformatycznego ministra (projekt).
- Rola CSIRT sektorowych (projekt) oraz współpraca operacyjna.
- Wewnętrzna procedura obsługi incydentu: detekcja → triage → eskalacja → decyzje → zgłoszenia → komunikacja.

Ćwiczenie: symulacja „incydent krytyczny w systemie dziedzinowym” – decyzje kierownictwa, działania IT oraz ścieżka formalna.

8.Odpowiedzialność, sankcje, kary administracyjne – jak się zabezpieczyć organizacyjnie.

- Kary administracyjne w projektowanej nowelizacji oraz obszary ryzyka niezgodności.
- Jak „dowodzić” należytej staranności: dokumenty, protokoły przeglądów, testy, szkolenia oraz audyty.

Ćwiczenie: przygotowanie „Teczki zgodności KSC/NIS2” – spisu dokumentów i dowodów.

9.Plan wdrożenia w jednostce: 90 dni / 6 miesięcy / 12 miesięcy.

- Szybkie działania podnoszące poziom bezpieczeństwa (quick wins): MFA, kopie zapasowe, segmentacja sieci, zarządzanie uprawnieniami, aktualizacje systemów, rejestr zasobów.
- Organizacja zarządzania cyberbezpieczeństwem: zespół ds. cyberbezpieczeństwa, cykl przeglądów, planowanie budżetu, raportowanie do kierownictwa jednostki.
- Integracja z EZD i zarządzaniem dokumentacją (incydent jako dokumentacja; retencja dokumentów; prowadzenie rejestrów).

Przygotowanie harmonogramu wdrożenia wraz z właścicielami działań i wskaźnikami realizacji.

„Wdrożenie na dokumentach” – warsztat.

- Projekt procedury obsługi incydentu cyberbezpieczeństwa (wersja urzędowa).
- Rejestr usług i systemów teleinformatycznych wraz z klasyfikacją krytyczności.
- Rejestr ryzyk cyberbezpieczeństwa (skala 1–4) oraz plan postępowania z ryzykiem.
- Wymagania bezpieczeństwa do SIWZ/OPZ oraz klauzule bezpieczeństwa do umów z dostawcami IT.
- Szkolenie ma charakter zdalny w czasie rzeczywistym 13h dydaktycznych,
- **1 godzina usługi = 45 minut dydaktycznych,**
- Przerwy nie są wliczone w całkowity czas trwania usługi.

Harmonogram

Liczba pozycji harmonogramu: 28

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 28 Dzień I_1.Cyberbezpieczeństwo w JST/urzędzie – kontekst i odpowiedzialność kierownictwa.	Zajęcia	Małgorzata Czartoryska	24-08-2026	09:30	10:30	01:00

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
2 z 28 Ćwiczenie: „Mapa odpowiedzialności” – RACI dla: IT, IOD, kancelaria/EZD, PR, kadry, zamówienia.	Zajęcia	Małgorzata Czartoryska	24-08-2026	10:30	10:50	00:20
3 z 28 -	Przerwa	-	24-08-2026	10:50	11:00	00:10
4 z 28 2.Podstawowe pojęcia KSC i praktyczne granice obowiązków.	Zajęcia	Małgorzata Czartoryska	24-08-2026	11:00	11:40	00:40
5 z 28 Mini-case: „Wyciek danych z poczty / phishing / ransomware w sekretariacie” – co robimy w 2h, 24h, 72h.	Zajęcia	Małgorzata Czartoryska	24-08-2026	11:40	12:00	00:20
6 z 28 -	Przerwa	-	24-08-2026	12:00	12:30	00:30
7 z 28 3.Współpraca z CSIRT, zgłaszanie incydentów i komunikacja.	Zajęcia	Małgorzata Czartoryska	24-08-2026	12:30	13:10	00:40
8 z 28 Ćwiczenie: wypełnienie „karty incydentu” oraz przygotowanie checklisty działań.	Zajęcia	Małgorzata Czartoryska	24-08-2026	13:10	13:30	00:20
9 z 28 -	Przerwa	-	24-08-2026	13:30	13:40	00:10

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
10 z 28 4.Zarządzanie ryzykiem cyber w jednostce – podejście praktyczne.	Zajęcia	Małgorzata Czartoryska	24-08-2026	13:40	14:20	00:40
11 z 28 Ćwiczenie: przygotowanie rejestru ryzyk (top 10) dla jednostki oraz plan działań 30/60/90 dni.	Zajęcia	Małgorzata Czartoryska	24-08-2026	14:20	14:40	00:20
12 z 28 -	Przerwa	-	24-08-2026	14:40	14:50	00:10
13 z 28 5.NIS2 → KSC: nowy model podmiotów i nadzoru.	Zajęcia	Małgorzata Czartoryska	24-08-2026	14:50	15:15	00:25
14 z 28 Ćwiczenie: „Samoocena jednostki” – czy i dlaczego możemy wpaść w kategorię podmiotu kluczowego lub ważnego (na podstawie usług i roli jednostki).	Zajęcia	Małgorzata Czartoryska	24-08-2026	15:15	15:30	00:15
15 z 28 Dzień II_6.Obowiązki w modelu NIS2: środki zarządzania ryzykiem.	Zajęcia	Małgorzata Czartoryska	25-08-2026	09:30	10:30	01:00

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
16 z 28 Ćwiczenie: checklista „20 wymagań” oraz analiza luk (gap analysis): jest / częściowo / brak.	Zajęcia	Małgorzata Czartoryska	25-08-2026	10:30	10:50	00:20
17 z 28 -	Przerwa	-	25-08-2026	10:50	11:00	00:10
18 z 28 7.Incydenty w NIS2/KSC: nowe kanały i tempo zgłoszeń.	Zajęcia	Małgorzata Czartoryska	25-08-2026	11:00	11:40	00:40
19 z 28 Ćwiczenie: symulacja „incydent krytyczny w systemie dziedzinowym ” – decyzje kierownictwa, działania IT oraz ścieżka formalna.	Zajęcia	Małgorzata Czartoryska	25-08-2026	11:40	12:00	00:20
20 z 28 -	Przerwa	-	25-08-2026	12:00	12:30	00:30
21 z 28 8.Odpowiedzialność, sankcje, kary administracyjne – jak się zabezpieczyć organizacyjnie.	Zajęcia	Małgorzata Czartoryska	25-08-2026	12:30	13:10	00:40
22 z 28 Ćwiczenie: przygotowanie „Teczki zgodności KSC/NIS2” – spisu dokumentów i dowodów.	Zajęcia	Małgorzata Czartoryska	25-08-2026	13:10	13:30	00:20

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
23 z 28 -	Przerwa	-	25-08-2026	13:30	13:40	00:10
24 z 28 9.Plan wdrożenia w jednostce: 90 dni / 6 miesięcy / 12 miesięcy.	Zajęcia	Małgorzata Czartoryska	25-08-2026	13:40	14:20	00:40
25 z 28 Przygotowanie harmonogramu wdrożenia wraz z właścicielami działań i wskaźnikami realizacji.	Zajęcia	Małgorzata Czartoryska	25-08-2026	14:20	14:40	00:20
26 z 28 -	Przerwa	-	25-08-2026	14:40	14:50	00:10
27 z 28 „Wdrożenie na dokumentach” – warsztat.	Zajęcia	Małgorzata Czartoryska	25-08-2026	14:50	15:20	00:30
28 z 28 -	Walidacja	-	25-08-2026	15:20	15:30	00:10

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	12:00
w tym suma godzin zajęć	09:50
w tym suma godzin walidacji	00:10
w tym suma przerw	02:00
Suma godzin dydaktycznych bez przerw	13:15

Cennik

Jeżeli korzystasz z dofinansowania i usługa stanowi usługę kształcenia zawodowego lub przekwalifikowania zawodowego wraz z usługą lub dostawą towarów ściśle związaną z usługami kształcenia zawodowego lub przekwalifikowania zawodowego to możesz mieć możliwość skorzystania za zwolnienia z podatku VAT na

podstawie art. 43 ust. 1 pkt 29 lit. c ustawy z dnia 11 marca 2024 r. o podatku od towarów i usług, jeśli usługa w całości jest finansowana ze środków publicznych lub § 3 ust. 1 pkt 14 rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień w przypadku, gdy usługa jest finansowana w co najmniej 70% ze środków publicznych.

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	1 351,77 PLN
Koszt przypadający na 1 uczestnika netto	1 099,00 PLN
Koszt osobogodziny brutto	112,65 PLN
Koszt osobogodziny netto	91,58 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	12:00

Prowadzący

Liczba prowadzących: 1

1 z 1

Małgorzata Czartoryska

Prawnik, wykładowca przedmiotów prawniczych Wyższej Szkoły Bankowej we Wrocławiu oraz Uniwersytetu Ekonomicznego we Wrocławiu. Certyfikowany trener z wieloletnim doświadczeniem. Specjalista z dziedzin: postępowanie egzekucyjne w administracji i sądowe, prawo administracyjne materialne, postępowanie administracyjne, samorząd terytorialny, finanse publiczne, prawo cywilne materialne i procedura cywilna. Osoba prowadząca usługę posiada minimum 5-letnie doświadczenie zawodowe i trenerskie w obszarze tematycznym szkolenia w ciągu ostatnich 5 lat.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

- Szkolenie on-line na żywo
- EduBox, czyli paczkę materiałów wysłaną pocztą
- 60 dni dostępu do nagrania szkolenia
- Aplikację mobilną z ustawą Pzp na Android i iOS
- Materiały z ustawą Pzp w formie książki

- Roczny dostęp do EduStrefy
- Certyfikat ukończenia szkolenia
- Nagrania z webinarów ApexNet
- Wzór regulaminu zamówień do 170 tys. zł

Warunki uczestnictwa

Rezerwacji miejsca szkoleniowego można dokonać za pośrednictwem BUR.

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

Informacje dodatkowe

zaakceptowano Regulamin dla instytucji szkoleniowych.

Koszt wydania certyfikatu/zaświadczenia – wliczony w cenę szkolenia.

Po zakończeniu usługi uczestnik otrzyma certyfikat.

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 prawna stawki zwolnionej: Rozporządzenie Ministra finansów z 20 grudnia 2013 w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień (Dz. U. z 2020r.poz.1983 z 10.11.2020) § 3 pkt 1 ust. 14

Warunki techniczne

Szkolenie odbywa się na żywo w formie online na platformie ClickMeeting. Wymagania techniczne dla tej platformy:

1. Do platformy ClickMeeting potrzebna jest najaktualniejsza wersja jednej z przeglądarek: Google Chrome,
2. Mozilla Firefox, Safari, Edge (Chromium) lub Opera.
3. Możliwy jest również dostęp mobilny za pomocą przeglądarki Chrome lub Safari na telefonie lub
4. dedykowanej aplikacji mobilnej Clickmeeting (do pobrania ze sklepu Google Play lub App Store).
5. Minimalne wymagania techniczne to urządzenie z dostępem do internetu o przepustowości łącza 1,5 Mbps
6. dla transmisji dźwięku i obrazu, posiadające:

• procesor dwurdzeniowy 2GHz lub lepszy (zalecany czterordzeniowy);

• 2 GB pamięci RAM (zlecane 4GB lub więcej);

• system operacyjny taki jak Windows 8 (zalecany Windows 10), Mac OS wersja 10.13 (zalecana najnowsza wersja), Linux, Chrome OS;

• standardowe oprogramowanie obsługujące pliki pdf, doc, xls.

Otrzymują Państwo od nas link do pokoju szkoleniowego.

Podczas szkolenia mają Państwo możliwość kontaktu z Moderatorem i Trenerem szkolenia za pomocą czatu.

Kontakt

Aleksandra Wlazło

E-mail aleksandra.wlazlo@apexnet.pl
Telefon (+48) 222 058 902