Możliwość dofinansowania

Europejska Agencja Rozwoju Mirosław Kopik

5,0 / 5

3 857 ocen

CYBERBEZPIECZEŃSTWO W JEDNOSTKACH SAMORZĄDOWYCH. STRATEGIE ZAPOBIEGANIA I REAKCJI NA INCYDENTY - szkolenie

Numer usługi 2026/08/04/27209/3729583

- Kielce
- Usługa szkoleniowa
- stacjonarna
- Zajęcia grupowe
- 08:00 h
- 22.10.2026 do 22.10.2026

2 120,00 PLN brutto
2 120,00 PLN netto
265,00 PLN brutto/h
265,00 PLN netto/h
154,44 PLN cena rynkowa

Informacje podstawowe

Kategoria	Biznes / Organizacja
Grupa docelowa usługi	Pracownicy oraz kadra zarządzająca jednostek samorządu terytorialnego (JST) wszystkich szczebli (gminnych, powiatowych, wojewódzkich) oraz podległych im jednostek organizacyjnych (np. jednostki oświatowe, kulturalne). Kadra kierownicza i zarządzająca: wójtowie, burmistrzowie, prezydenci miast, starostowie, sekretarze, skarbnicy, dyrektorzy i naczelnicy wydziałów oraz jednostek podległych (osoby odpowiedzialne za zarządzanie ryzykiem i realizację wymogów prawnych). Pracownicy administracyjni i urzędnicy, osoby przetwarzające dane osobowe, obsługujące dokumentację elektroniczną, podpis elektroniczny, pocztę e-mail oraz korzystające ze służbowych urządzeń i pracy w trybie zdalnym/hybrydowym. Pracownicy wyznaczeni do spraw bezpieczeństwa i IT oraz osoby, które chcą przekwalifikować się; osoby, które chcą doskonalić umiejętności zawodowe, aby zapobiec utracie zatrudnienia; osoby poszukujące nowych możliwości zawodowych.
Minimalna liczba uczestników	4
Maksymalna liczba uczestników	24
Data zakończenia rekrutacji	21-10-2026
Forma prowadzenia usługi	stacjonarna
Podstawa uzyskania wpisu do BUR	Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

Cel

Cel edukacyjny

Usługa przygotowuje do: pełnienia obowiązków służbowych w jednostkach samorządowych zgodnie z wymogami ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC), Dyrektywy NIS2 oraz RODO w JST; skutecznej identyfikacji cyberzagrożeń (phishing, ransomware, AI/deepfake), bezpiecznej obsługi dokumentów cyfrowych, pracy zdalnej, ochrony tożsamości; natychmiastowego reagowania na incydenty, współpracy z IT i IOD, realizacji procedur ciągłości działania (BCP); współtworzenia kultury cyberbezpieczeństwa.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Wyjaśnia obowiązki prawne JST wynikające z KSC i NIS2 oraz podstawowe pojęcia z zakresu cyberbezpieczeństwa.	Definiuje pojęcia: incydent, podatność, ryzyko, socjotechnika, BEC.	Test teoretyczny
	Wskazuje obowiązki kierownictwa i pracowników w kontekście NIS2 i KSC.	Test teoretyczny
Charakteryzuje aktualne typy cyberataków oraz zagrożenia związane z wykorzystaniem AI.	Opisuje mechanizmy ataków typu phishing, ransomware, BEC i deepfake.	Test teoretyczny
	Wyjaśnia zasady bezpiecznego korzystania z haseł, MFA i urządzeń służbowych.	Test teoretyczny
Identyfikuje próby ataków socjotechnicznych oraz wyłudzenia informacji w codziennej komunikacji.	Wskazuje cechy charakterystyczne próby phishingu/BEC w symulowanej wiadomości.	Test teoretyczny
	Przeprowadza dwukanałową weryfikację tożsamości nadawcy (weryfikacja poza pasmem).	Test teoretyczny
Realizuje pierwsze działania po wykryciu incydentu i stosuje procedury bezpiecznego przesyłania danych.	Odłącza zakażone urządzenie od sieci i poprawnie wypełnia formularz zgłoszenia incydentu.	Obserwacja w warunkach symulowanych
	Szyfruje plik z danymi osobowymi przed wysyłką e-mailem i przekazuje hasło odrębnym kanałem.	Obserwacja w warunkach symulowanych
Promuje odpowiedzialne nawyki cyfrowe w urzędzie.	Przekazuje zgłoszenie o incydencie do zespołu IT/IOD bez obawy przed konsekwencjami.	Obserwacja w warunkach symulowanych
	Wykazuje dbałość o ochronę zasobów informacyjnych JST podczas analizy studium przypadku.	Obserwacja w warunkach symulowanych

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

Szkolenie adresowane jest do osób chcących zdobyć wiedzę, umiejętności oraz kompetencje społeczne z zakresu rozpoznawania cyberzagrożeń, stosowania zasad higieny cyfrowej oraz realizacji procedur ochrony danych i reagowania na incydenty zgodnie z wymogami prawnymi (KSC, NIS2, RODO) obowiązującymi w jednostkach samorządu terytorialnego (JST).

Na szkoleniu część teoretyczna zajmuje około 20-25% czasu szkolenia, część praktyczna to 75-80% czasu szkolenia.

Szkolenie prowadzone jest w grupie od 4 do 24 osób, a warunki organizacyjne są zawsze dostosowywane do liczby osób na szkoleniu. Podczas szkolenia odbywa się zarówno praca zbiorowa (np. mini-wykład), praca indywidualna (np. ćwiczenia indywidualne), jak i praca w grupach (od 2 do 6 osób) zależności od potrzeb.

Ostatnie 30 minut usługi przeznaczone jest na przeprowadzenie walidacji efektów uczenia się. Narzędzia walidacyjne (test wiedzy oraz lista kontrolna) przygotowuje wyznaczony Walidator, wskazany w Karcie Usługi.

Procedura przeprowadzenia walidacji:

1. Po zakończeniu części dydaktycznej prowadzonej przez Trenera, Walidator dołącza do grupy w sali szkoleniowej.
2. Walidator udostępnia uczestnikom wydrukowane arkusze testu teoretycznego, nadzoruje ich samodzielne wypełnianie, a następnie je zbiera, sprawdza i ocenia, weryfikując poziom uzyskanej wiedzy. Uczestnicy są niezwłocznie informowani o osiągniętym wyniku.
3. Walidator przeprowadza również obserwację w warunkach symulowanych, oceniając stopień osiągnięcia efektów z zakresu umiejętności oraz kompetencji społecznych na podstawie przygotowanej Listy Kontrolnej (Checklisty).
4. Na podstawie zgromadzonych wyników Walidator sporządza i podpisuje Protokół z przebiegu walidacji.

Opisana procedura gwarantuje pełną rozdzielność funkcji Trenera i Walidatora. Osoba przeprowadzająca walidację nie prowadzi zajęć dydaktycznych ani nie jest obecna na sali szkoleniowej podczas części szkoleniowej usługi.

Przywitanie, prezentacja trenera oraz programu szkolenia, kontrakt z uczestnikami.

Moduł 1. Podstawy cyberbezpieczeństwa i obowiązki jednostek samorządowych. Cyberbezpieczeństwo jako element bezpieczeństwa funkcjonowania jednostek samorządu terytorialnego.Aktualne zagrożenia – charakterystyka najczęściej występujących cyberataków.Podstawowe pojęcia: cyberbezpieczeństwo, incydent, podatność, ryzyko, cyberatak, socjotechnika.Krajowy System Cyberbezpieczeństwa (KSC) – cele, założenia oraz obowiązki jednostek samorządowych i pracowników.Dyrektywa NIS2 – najważniejsze wymagania dotyczące zarządzania ryzykiem, odpowiedzialności kierownictwa oraz budowania odporności organizacji.Rola pracownika w systemie bezpieczeństwa informacji.Polityki bezpieczeństwa, procedury wewnętrzne oraz dobre praktyki organizacyjne.

Metody pracy:wykład interaktywny, prezentacja multimedialna, dyskusja moderowana.

Moduł 2. Bezpieczna praca z informacją i ochrona tożsamości cyfrowej. Ochrona danych osobowych i informacji przetwarzanych w jednostkach samorządowych.Tożsamość cyfrowa pracownika. Tworzenie silnych haseł, zarządzanie hasłami oraz uwierzytelnianie wieloskładnikowe (MFA).Bezpieczne korzystanie z poczty elektronicznej, Internetu oraz usług chmurowych.Bezpieczeństwo urządzeń służbowych, nośników danych oraz pracy zdalnej.Bezpieczne udostępnianie dokumentów i korzystanie z podpisu elektronicznego.Ochrona informacji przed nieuprawnionym dostępem.

Metody pracy: wykład interaktywny, prezentacja multimedialna, dyskusja moderowana.

Moduł 3. Rozpoznawanie zagrożeń i reagowanie na incydenty cyberbezpieczeństwa. Phishing, spear phishing, vishing, smishing oraz Business Email Compromise (BEC).Ransomware oraz inne rodzaje złośliwego oprogramowania.Zagrożenia wykorzystujące sztuczną inteligencję (AI), w tym wiadomości generowane przez AI i deepfake.Studium przypadków rzeczywistych incydentów w jednostkach samorządowych.Procedury zgłaszania incydentów zgodnie z obowiązującymi regulacjami.Pierwsze działania pracownika po wykryciu incydentu.Współpraca z działem IT, administratorem systemów oraz osobami odpowiedzialnymi za bezpieczeństwo informacji.

Metody pracy: wykład interaktywny, studium przypadku, ćwiczenia praktyczne, praca w grupach.

Moduł 4. Zarządzanie bezpieczeństwem informacji i budowanie odporności w jednostce samorządowej. Zarządzanie ryzykiem cyberbezpieczeństwa zgodnie z wymaganiami KSC i NIS2. Zasady zapewnienia ciągłości działania po incydencie cyberbezpieczeństwa. Tworzenie, przechowywanie i odtwarzanie kopii zapasowych.Bezpieczne archiwizowanie dokumentów elektronicznych.Audyty bezpieczeństwa, monitorowanie zagrożeń oraz doskonalenie procedur.Budowanie kultury cyberbezpieczeństwa w jednostce samorządowej.Dobre praktyki zwiększające odporność organizacji na cyberzagrożenia.

Metody pracy: warsztat, wykład interaktywny, prezentacja multimedialna, dyskusja moderowana.

Podsumowanie szkolenia.

Walidacja

Harmonogram

Liczba pozycji harmonogramu: 9

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 9 Przywitanie...	Zajęcia	Dawid Koziorowski	22-10-2026	08:00	08:30	00:30
2 z 9 Moduł 1.	Zajęcia	Dawid Koziorowski	22-10-2026	08:30	10:00	01:30
3 z 9 -	Przerwa	-	22-10-2026	10:00	10:15	00:15
4 z 9 Moduł 2.	Zajęcia	Dawid Koziorowski	22-10-2026	10:15	11:45	01:30
5 z 9 -	Przerwa	-	22-10-2026	11:45	12:00	00:15
6 z 9 Moduł 3.	Zajęcia	Dawid Koziorowski	22-10-2026	12:00	13:30	01:30
7 z 9 -	Przerwa	-	22-10-2026	13:30	14:00	00:30
8 z 9 Moduł 4.	Zajęcia	Dawid Koziorowski	22-10-2026	14:00	15:30	01:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
9 z 9 -	Walidacja	-	22-10-2026	15:30	16:00	00:30

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	08:00
w tym suma godzin zajęć	06:30
w tym suma godzin walidacji	00:30
w tym suma przerw	01:00
Suma godzin dydaktycznych bez przerw	09:15

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	2 120,00 PLN
Podmiot uprawniony do zwolnienia z VAT na podstawie art. 43 ust. 1 ustawy o VAT	
Koszt przypadający na 1 uczestnika netto	2 120,00 PLN
Koszt osobogodziny brutto	265,00 PLN
Koszt osobogodziny netto	265,00 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	08:00

Prowadzący

Liczba prowadzących: 1

1 z 1

Dawid Koziorowski

Trener IT z ponad 10 letnim doświadczeniem, certyfikowany „etyczny haker” oraz instruktor EC-COUNCIL. Na co dzień zajmuje się realizacją testów penetracyjnych symulujących realne ataki hakerskie na infrastrukturę sieciowe oraz aplikacje webowe. Specjalizuje się w socjotechnice oraz działaniach typu Red Team. Jako trener realizował szkolenia z zakresu cyberbezpieczeństwa m.in. dla specjalnych (CBZC, ABW, CBA), oraz dla administracji (m.in. Krajowa Izba Skarbowa). Obszar specjalizacji: Cyberbezpieczeństwo, Osint (Biały wywiad), inżynieria społeczna, Phishing, Hacking. Założyciel i właściciel Akademii Portal – Centrum Szkoleń IT.
Wykształcenie: wyższe informatyczne, specjalizacja: Cyberbezpieczeństwo i Informatyka Śledcza.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnik szkolenia otrzyma autorskie materiały szkoleniowe (prezentacja multimedialna lub skrypt).

Nasi uczestnicy na szkoleniu otrzymują pakiet szkoleniowy (segregator, notes i długopis).

Warunki uczestnictwa

Osoba zainteresowana skorzystaniem z usługi rozwojowej z dofinansowaniem musi zarejestrować się w Bazie Usług Rozwojowych oraz dokonać zapisu na usługę przed jej rozpoczęciem, z użyciem numeru ID wsparcia.

Informacje dodatkowe

Czas trwania usługi szkoleniowej to 8 godzin zegarowych. Szkolenie jest jednodniowe, ujęte w 4 moduły. Planujemy przerwy pomiędzy modułami.

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 oraz szczegółowych warunków stosowania tych zwolnień (Dz. U. z 2018 r. poz. 701 z późn. zm.).

Adres

ul. Klonowa 55/34
25-553 Kielce
woj. świętokrzyskie

Siedziba firmy: Europejska Agencja Rozwoju Mirosław Kopik
Budynek "Relaks", wejście B, winda po lewej stronie,
III piętro, drzwi na wprost windy.

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi
- Naszym uczestnikom zapewniamy obiad i przerwy kawowe (kawa, herbata, woda, sok, ciastka).

Kontakt

Mirosław Kopik

E-mail mirek.kopik@eurodotacje.pl

Telefon (+48) 505 060 800