Możliwość dofinansowania

Cyberbezpieczeństwo: NIS2, KRI i uoKSC w praktyce – szkolenie stacjonarne

Numer usługi 2025/12/23/32642/3228562

1 900,00 PLN brutto
1 900,00 PLN netto
271,43 PLN brutto/h
271,43 PLN netto/h

Fundacja CODE:ME

4,7 / 5

104 oceny

Gdańsk / stacjonarna
Usługa szkoleniowa
7 h
23.01.2026 do 23.01.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Szkolenie skierowane jest do osób zatrudnionych w administracji publicznej oraz podmiotach realizujących zadania publiczne, które w ramach swoich obowiązków uczestniczą w zarządzaniu, nadzorze lub realizacji działań związanych z bezpieczeństwem informacji i cyberbezpieczeństwem. Adresatami szkolenia są w szczególności: kadra zarządzająca jednostek samorządu terytorialnego i jednostek organizacyjnych (m.in. burmistrzowie, prezydenci miast, sekretarze, skarbnicy, dyrektorzy wydziałów), Inspektorzy Ochrony Danych, Administratorzy Bezpieczeństwa Informacji, główni informatycy oraz pracownicy administracji odpowiedzialni za wdrażanie lub stosowanie wymogów wynikających z NIS2, KRI, ustawy o Krajowym Systemie Cyberbezpieczeństwa oraz RODO. Szkolenie nie wymaga specjalistycznej wiedzy technicznej ani doświadczenia informatycznego. Wskazane jest podstawowe doświadczenie zawodowe w administracji publicznej oraz znajomość procesów organizacyjnych i obiegu informacji w jednostce.
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	20-01-2026
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	7
Podstawa uzyskania wpisu do BUR	Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

Cel

Cel edukacyjny

Celem szkolenia jest przygotowanie uczestnika do charakteryzowania aktualnych zagrożeń cyberbezpieczeństwa w administracji publicznej, definiowania obowiązków wynikających z NIS2, KRI, ustawy o Krajowym Systemie Cyberbezpieczeństwa oraz RODO, a także do oceny stanu cyberbezpieczeństwa organizacji. Uczestnik będzie przygotowany do organizowania działań w przypadku incydentu cyberbezpieczeństwa oraz do odpowiedzialnego podejmowania decyzji w sytuacjach zagrożenia bezpieczeństwa informacji.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Charakteryzuje aktualne zagrożenia cyberbezpieczeństwa występujące w administracji publicznej.	Uczestnik poprawnie identyfikuje rodzaje zagrożeń oraz ich skutki w pytaniach testowych.	Test teoretyczny z wynikiem generowanym automatycznie
Definiuje obowiązki organizacyjne wynikające z NIS2, KRI, ustawy o Krajowym Systemie Cyberbezpieczeństwa oraz RODO.	Uczestnik poprawnie przyporządkowuje obowiązki do właściwych regulacji w teście.	Test teoretyczny z wynikiem generowanym automatycznie
Ocenia stan cyberbezpieczeństwa organizacji w odniesieniu do wymogów regulacyjnych.	Uczestnik poprawnie wskazuje obszary ryzyka i niezgodności w opisanym scenariuszu.	Test teoretyczny z wynikiem generowanym automatycznie
Organizuje działania w przypadku wystąpienia incydentu cyberbezpieczeństwa.	Uczestnik poprawnie określa kolejność działań oraz obowiązki zgłoszeniowe w teście.	Test teoretyczny z wynikiem generowanym automatycznie
Odpowiedzialnie podejmuje decyzje w sytuacjach zagrożenia bezpieczeństwa informacji.	Uczestnik wybiera właściwe działania w scenariuszach decyzyjnych zawartych w teście.	Test teoretyczny z wynikiem generowanym automatycznie

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

Blok I: Stan faktyczny – analiza rzeczywistości

- Polskie urzędy pod ostrzałem ransomware: przypadki z województwa pomorskiego i innych regionów Polski – analiza przyczyn i skutków incydentów.
- BEC (Business Email Compromise) – wyrafinowane oszustwa wymierzone w administrację publiczną, skutkujące stratami finansowymi w skali milionów złotych.
- InfoStealers i wycieki danych osobowych – ryzyko ekspozycji danych wrażliwych obywateli (PESEL, wizerunek, dane kontaktowe).
- Dane statystyczne: 54% Polaków otrzymało podejrzane komunikaty elektroniczne, 38% zostało poszkodowanych w wyniku oszustw internetowych.

Blok II: Co mówią przepisy – i dlaczego to ma znaczenie

- NIS2 – nowe wymagania, które zmieniają reguły gry dla operatorów usług kluczowych.
- KRI (Krajowe Ramy Interoperacyjności) – minimalne standardy, których NIE MOŻNA zignorować.
- uoKSC (Ustawa o Krajowym Systemie Cyberbezpieczeństwa) – kto, co i kiedy musi zgłaszać (24h, 72h, 30 dni).
- RODO – bo naruszenie ochrony danych to nie tylko kara finansowa, to utrata zaufania obywateli.

Blok III: Jak to wdrożyć – praktyka, nie PowerPoint

- System Zarządzania Bezpieczeństwem Informacji (SZBI) – nie teoria, ale konkretne działania.
- 2FA – dlaczego hasło to za mało (nawet "Malbork^1410!DawnoTemu").
- Procedury reagowania na incydenty – co robić w pierwszych minutach ataku.
- BEC Defense – jak nie dać się oszukać fałszywemu CEO.
- Ransomware Response – odizolować, nie płacić, przywrócić.

Blok IV: Symulacje – teoria spotyka praktykę

- Vishing w praktyce – jak rozpoznać oszusta po drugiej stronie słuchawki.
- QR Code Phishing – jeden skan i wszystko stracone.
- Zarządzanie incydentem pod presją – 30 minut na raport dla Burmistrza, CSIRT NASK czeka na zgłoszenie.
- Audyt SZBI na żywo – czy Twój urząd przetrwałby kontrolę?

Harmonogram

Liczba przedmiotów/zajęć: 6

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 6 Blok I: Stan faktyczny, Blok II: Co mówią przepisy – analiza rzeczywistości - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, rozmowa	Andrzej Piotrowski	23-01-2026	09:00	12:00	03:00
2 z 6 Przerwa	Andrzej Piotrowski	23-01-2026	12:00	12:20	00:20
3 z 6 Blok III: Jak to wdrożyć – praktyka, nie PowerPoint - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, rozmowa	Andrzej Piotrowski	23-01-2026	12:20	14:20	02:00
4 z 6 Przerwa	Andrzej Piotrowski	23-01-2026	14:20	15:00	00:40
5 z 6 Blok IV: Symulacje – teoria spotyka praktykę – praktyka, nie PowerPoint - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, rozmowa	Andrzej Piotrowski	23-01-2026	15:00	15:50	00:50
6 z 6 Walidacja w formie testu teoretycznego z wynikiem generowanym automatycznie	-	23-01-2026	15:50	16:00	00:10

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	1 900,00 PLN
Koszt przypadający na 1 uczestnika netto	1 900,00 PLN
Koszt osobogodziny brutto	271,43 PLN
Koszt osobogodziny netto	271,43 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Andrzej Piotrowski

Doświadczony tester i developer, który robi co może, aby wszystko działało. Głównie w roli support Validatora/Test Automation/Performance testing. Członek Ministerstwa Cyfryzacji w grupie roboczej ds. IoT oraz Współautor publikacji IoT- Polska Gospodarka IoT. Często łamie zasady dla pokazania błędów systemów i procesów. Organizator LocalTrojmiasto IssaPolska.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Każdy uczestnik przed rozpoczęciem szkolenia otrzyma informacje organizacyjne jak przygotować się do szkolenia.

W trakcie kursu uczestnik otrzyma materiały szkoleniowe w postaci prezentacji (pliki pdf).

Informacje dodatkowe

Uczestnicy po zakończeniu kursu otrzymają Certyfikat ukończenia kursu.

Usługa rozwojowa nie jest świadczona przez podmiot pełniący funkcję Operatora lub Partnera Operatora w danym projekcie PSF lub w którymkolwiek Regionalnym Programie lub FERS albo przez podmiot powiązany z Operatorem lub Partnerem kapitałowo lub osobowo.

Cena usługi nie obejmuje kosztów niezwiązanych bezpośrednio z usługa rozwojową, w szczególności kosztów środków trwałych przekazywanych Uczestnikom projektu, kosztów dojazdu i zakwaterowania.

Zawarto umowę z WUP w Toruniu w ramach Projektu Kierunek – Rozwój;

Dodatkowo, w przypadku projektu Kierunek - Rozwój między Uczestnikiem Usługi a Usługodawcą zostanie zawarta Umowa na kurs.

Zawarto umowę z Wojewódzkim Urzędem Pracy w Szczecinie na świadczenie usług rozwojowych z wykorzystaniem elektronicznych bonów szkoleniowych w ramach projektu Zachodniopomorskie Bony Szkoleniowe.

Adres

Gdańsk
Gdańsk
woj. pomorskie

Udogodnienia w miejscu realizacji usługi

- Wi-fi

Kontakt

Monika Sciubilecka

E-mail kontakt@codeme.pl
Telefon (+48) 537 492 774