FERS.01.05-IP.08-0473/23-00 Fundusze Europejskie dla Rozwoju Społecznego
Zakres interwencji: Wsparcie na rzecz szkolnictwa wyższego (z wyłączeniem infrastruktury)
Rozwój kompetencji przyszłości dopasowanych do oczekiwań rynku pracy
i pracodawców.

PROGRAM SZKOLENIA „CYBERBEZPIECZŃSTWO Z CERTYFIKACJĄ INSPEKTORA DANYCH OSOBOWYCH”

Z OBSZARU „W DRODZE DO CYFROWEJ GOSPODARKI”

Spis treści

FISZKA SZKOLENIA 2
Forma i miejsce szkolenia 2
Okres realizacji 2
Cel główny 2
Jednostki organizujące/prowadzące szkolenie 3
Efekty szkolenia 3
Metody dydaktyczne 4
Środki dydaktyczne 4
WSTĘP 4
METODOLOGIA 4
Metody dydaktyczne 4
Środki dydaktyczne 4
ZAKRES MERYTORYCZNY 5
Program szkolenia 5
EFEKTY KSZTAŁCENIA 7
WERYFIKACJA NABYTYCH KOMPETECJI I CERTYFIKAT 8
KADRA 9
REKRUTACJA 9
ORGANIZACJA 10
PROMOCJA 10
EWALUACJA 10

FISZKA SZKOLENIA

TYTUŁ SZKOLENIA/ OBSZAR TEMATYCZNY KURSU:

PODSTAWY CHMURY OBLICZENIOWEJ NA PRZYKŁADZIE AMAZON WEB SERVICES

GRUPA DOCELOWA	LICZBA PRZESZKOLONYCH OSÓB W 1 TURZE	LICZBA EDYCJI SZKOLENIA W BIEŻĄCYM ROKU KALENDARZOWYM	WIELKOŚĆ GRUP	LICZBA GODZIN /GRUPĘ	FORMA SZKOLENIA
Osoby w wieku 18-64 lat zamieszkałe na terenie Polski	8	Średnio 2	Ok. 8 osób	36 h	Hybrydowa

Adresaci szkolenia: Osoby w wieku 18-64 lata, zamieszkałych na terenie Polski. Szkolenie kierowane jest głównie do osób, dla których pogłębienie wiedzy, uzupełnienie luk kompetencyjnych, przekwalifikowanie będzie przepustką do wejścia/ powrotu/ utrzymania się na rynku pracy.

Oferta ma charakter otwarty, nie jest zawężona do konkretnej grupy osób, jednakże wskazano priorytety naboru, o których szerzej w części dot. rekrutacji.

Forma i miejsce szkolenia: Szkolenie prowadzone hybrydowo.

Okres realizacji: 10 edycji w terminie 01.01.2025-31.12.2029

Język: polski

Cel główny: celem projektu są działania wspierające ideę uczenia się przez całe życie oraz nabycie kwalifikacji i kompetencji przyszłości przez osoby dorosłe. Służyć temu ma przygotowanie programów i przeprowadzenie szkoleń będących odpowiedzią na zdiagnozowane potrzeby rynku pracy, pracodawców oraz uczestników w tym w obszarze cyfrowej gospodarki.

Celem szkolenia „Cyberbezpieczeństwo z certyfikacją Inspektora Danych Osobowych" jest przygotowanie uczestników do skutecznego zarządzania bezpieczeństwem informacji oraz pełnienia funkcji Inspektora Ochrony Danych (IOD) zgodnie z wymogami prawa krajowego i unijnego, w szczególności RODO. Szkolenie ma na celu: rozwój wiedzy z zakresu ochrony danych osobowych, cyberbezpieczeństwa oraz zarządzania ryzykiem, zgodnie z obowiązującymi regulacjami i najlepszymi praktykami, przygotowanie do pełnienia funkcji Inspektora Danych

Osobowych, w tym zrozumienie obowiązków, odpowiedzialności i narzędzi wspierających pracę IOD, wzmocnienie kompetencji w zakresie reagowania na incydenty bezpieczeństwa informacji oraz wdrażania odpowiednich polityk i procedur, nabycie praktycznych umiejętności w zakresie audytowania, dokumentowania i raportowania działań związanych z ochroną danych osobowych i cyberbezpieczeństwem, zdobycie certyfikatu potwierdzającego kwalifikacje zawodowe, cenionego na rynku pracy i zwiększającego wiarygodność w obszarze compliance i bezpieczeństwa. Szkolenie stanowi odpowiedź na rosnące zapotrzebowanie na specjalistów w obszarze ochrony danych i bezpieczeństwa cyfrowego oraz wspiera rozwój kompetencji kluczowych dla transformacji cyfrowej organizacji z uwzględnieniem aspektów prawnych i technicznych.

Jednostki organizujące/prowadzące szkolenie:

- Akademia WSB, Dąbrowa Górnicza, ul. Cieplaka 1c
- MARR S.A., Kraków, ul. Kordylewskiego 11
- Śląski Związek Pracodawców Lewiatan, Katowice, ul. Mickiewicza 29

Efekty szkolenia:

Uczestnik szkolenia:

- Nabędzie zaawansowaną wiedzę z zakresu ochrony danych osobowych i cyberbezpieczeństwa, zgodnie z wymogami prawa krajowego i unijnego (w szczególności RODO).
- Będzie potrafił samodzielnie wdrażać i nadzorować polityki ochrony danych osobowych oraz systemy zarządzania bezpieczeństwem informacji w organizacji.
- Rozwinie umiejętności praktyczne w zakresie audytowania, dokumentowania i raportowania działań związanych z ochroną danych osobowych oraz reagowania na incydenty bezpieczeństwa.
- Będzie przygotowany do pełnienia funkcji Inspektora Ochrony Danych, w tym do analizy ryzyka, wdrażania środków technicznych i organizacyjnych oraz współpracy z działami IT i compliance.
- Zdobędzie certyfikat potwierdzający kwalifikacje zawodowe, zwiększający jego wiarygodność na rynku pracy i umożliwiający podjęcie pracy na stanowiskach związanych z ochroną danych i cyberbezpieczeństwem.
- Ponadto rozwinie kompetencje w zakresie praktycznego rozwiązywania problemów, analizowania przypadków incydentów, prowadzenia szkoleń wewnętrznych, a także korzystania z narzędzi wspierających pracę IOD.

Certyfikat szkolenia: tak (szczegóły zamieszczone w części dot. weryfikacji umiejętności)

Metody dydaktyczne: wykład, ćwiczenia, dyskusja moderowana (zogniskowana), ‘burza mózgów’, praca indywidualna/zespołowa, case study - studium przypadku, praca warsztatowo-laboratoryjna
Środki dydaktyczne**:** prezentacja, Laboratoria, praca na systemie Kadrowo – płacowym, narzędzia do zbierania odpowiedzi uczestników (ankiety, Mentimeter), tablica whiteboard (Mural lub Jamboard), flipchart, projektor, opisy przypadków, karty pracy, testy, materiały dydaktyczne.

WSTĘP

METODOLOGIA

Edukacja jest obszarem, w którym szczególnego znaczenia nabiera konieczność stosowania metod i technik dydaktycznych ukierunkowanych na kształcenie umiejętności praktycznych oraz skutecznego i samodzielnego rozwiązywania postawionych problemów. W trakcie planowanych zajęć szkoleniowych wykorzystane zostaną nowoczesne techniki informacyjno-komunikacyjne w zakresie kształcenia. Położony zostanie nacisk na kreatywność, twórczość i nieszablonowy sposób myślenia. Zastosowanie nowoczesnych metod dydaktycznych (np. metoda tekstu przewodniego, metoda projektu edukacyjnego, metoda webquest, metoda peer learning).

Metodologia prowadzenia zajęć będzie opierała się przede wszystkim na aktywnym uczestnictwie w zajęciach z zastosowaniem metod pracy indywidulanej i zespołowej. Weryfikacja nabytych kompetencji/wiedzy będzie zawierała formułę testu/ankiety.

Metody dydaktyczne: wykład, ćwiczenia, metody interaktywne, dyskusja moderowana (zogniskowana), ‘burza mózgów’, praca indywidualna/zespołowa, case study - studium przypadku, quiz, metoda tekstu przewodniego, metoda projektu edukacyjnego, metoda webquest, metoda flipped classroom – ‘odwrócone nauczanie’, metoda peer learning.

Środki dydaktyczne**:** prezentacja, narzędzia do zbierania odpowiedzi uczestników (ankiety, Mentimeter), tablica whiteboard (Mural lub Jamboard), flipchart, projektor, opisy przypadków, karty pracy, testy, materiał dydaktyczny.
.

ZAKRES MERYTORYCZNY

Program szkolenia

Program szkolenia CYBERBEZPIECZEŃSTWO Z CERTYFIKACJĄ INSPEKTORA DANYCH OSOBOWYCH" został skomponowany w sposób zapewniający uczestnikom zdobycie kompetencji niezbędnych do pełnienia funkcji Inspektora Ochrony Danych oraz specjalisty ds. cyberbezpieczeństwa, z naciskiem na praktyczne umiejętności zarządzania bezpieczeństwem informacji i ochrony danych osobowych.

Niżej przedstawiony program szkoleniowy umożliwia kompleksowe zrozumienie tematów związanych z obszarami prawa ochrony danych, technicznymi i organizacyjnymi środkami bezpieczeństwa, zarządzaniem ryzykiem, a także audytem i dokumentacją związaną z ochroną danych i cyberbezpieczeństwem.

Program nauczania będzie zawierał m.in. szczegółowe omówienie regulacji prawnych (RODO i przepisów krajowych), analizę i zarządzanie ryzykiem, techniczne aspekty bezpieczeństwa informacji, audyt i dokumentację działań IOD, a także praktyczne umiejętności związane z wykrywaniem i reagowaniem na incydenty bezpieczeństwa.

Program Szkolenia: "CYBEZBEZPIECZŃSTWO Z CERTYFIKACJĄ INSPEKTORA DANYCH OSOBOWYCH" 36 (godziny / 4 dni)

TEMAT (moduły /treści szkoleniowe)	CZAS TRWANIA	METODA, ŚRODEK DYDAKTYCZNY
TEST wejściowy określenie początkowego poziomu wiedzy i umiejętności		entry test, ankieta, test wyboru (online/stacjonarnie)
DZIEŃ 1. (9 godzin) Podstawy prawne i techniczne ochrony danych oraz cyberbezpieczeństwa		
Podstawy prawne ochrony danych osobowych – RODO, przepisy krajowe, nowe regulacje	3 h	Wykład, case study, prezentacja
Kluczowe pojęcia: dane osobowe, przetwarzanie, podmiot danych, pseudoanimizacja, anonimizacja	2 h	Wykład, ćwiczenia, prezentacja
Cyberbezpieczeństwo: zagrożenia, wektory ataków, podatności systemów informatycznych	2 h	Wykład, case study prezentacja

TEMAT (moduły /treści szkoleniowe)	CZAS TRWANIA	METODA, ŚRODEK DYDAKTYCZNY
Środki techniczne ochrony danych: szyfrowanie, kontrola dostępu, bezpieczne przechowywanie i przesyłanie danych	2 h	Demonstracje, ćwiczenia
Dzień 2: (9 godzin) Zarządzanie bezpieczeństwem informacji i reagowanie na incydenty		
Systemy zarządzania bezpieczeństwem informacji (ISMS) – standardy (ISO 27001, 27701) i ich znaczenie	2 h	Wykład interaktywny, dyskusja
Identyfikacja i ocena ryzyka w zakresie ochrony danych osobowych i cyberbezpieczeństwa	2 h	Wykład, ćwiczenia
Projektowanie i wdrażanie polityk bezpieczeństwa danych osobowych	2 h	Ćwiczenia, case study, praca w grupach
Reagowanie na incydenty bezpieczeństwa – metody wykrywania, eskalacji i dokumentowania	2 h	Case study: symulacja incydentu, omówienie działań
Dokumentowanie naruszeń i raportowanie do PUODO, analiza ryzyka po incydencie	1 h	Studium przypadku, ćwiczenia
Dzień 3: (9 godzin) Praktyka techniczna i organizacyjna		
Praktyczne wdrażanie środków technicznych – konfiguracja zabezpieczeń (np. VPN, kontrola dostępu, backup)	3 h	Ćwiczenia, warsztaty praktyczne, demonstracje
Praktyczne wdrażanie środków organizacyjnych – rejestry czynności, dokumentacja ochrony danych	2 h	Ćwiczenia
Audyt wewnętrzny ochrony danych osobowych – przygotowanie, przeprowadzanie, dokumentowanie	2 h	Studium przypadku, ćwiczenia
Cyberbezpieczeństwo w praktyce – najlepsze praktyki użytkowników i administratorów IT	2 h	Ćwiczenia, test/quiz
Dzień 4: (9 godzin) Specjalistyczne aspekty IOD i cyberbezpieczeństwa		

TEMAT (moduły /treści szkoleniowe)	CZAS TRWANIA	METODA, ŚRODEK DYDAKTYCZNY
Wymagania prawne i techniczne dla administratorów i podmiotów przetwarzających (umowy powierzenia, oceny skutków, rejestry)	3 h	Wykład, case study
Cyberbezpieczeństwo a ochrona danych osobowych – jak budować mosty między IT a prawem	2 h	Burza mózgów, ćwiczenia
Praktyczne aspekty szacowania ryzyka w ochronie danych i cyberbezpieczeństwie	2 h	Ćwiczenia, warsztaty
Nowe zagrożenia – AI, deepfake, phishing zaawansowany – rozpoznawanie i przeciwdziałanie	2 h	Prezentacja, ćwiczenia
TEST wyjściowy weryfikacja przyrostu poziomu wiedzy i umiejętności		exit test, monitoring postępów ankieta, test wyboru (online/stacjonarnie)

EFEKTY KSZTAŁCENIA

Uczestnik szkolenia „Cyberbezpieczeństwo z certyfikacją Inspektora Danych Osobowych" nabędzie zaawansowaną wiedzę oraz kluczowe umiejętności niezbędne do efektywnego pełnienia funkcji Inspektora Ochrony Danych (IOD) oraz specjalisty ds. cyberbezpieczeństwa.

Będzie potrafił:

- Identyfikować i analizować przepisy prawne krajowe i unijne dotyczące ochrony danych osobowych, w tym RODO i regulacje sektorowe.
- Rozpoznawać i oceniać ryzyka związane z przetwarzaniem danych osobowych oraz zagrożenia cyberbezpieczeństwa.
- Projektować, wdrażać i utrzymywać polityki bezpieczeństwa informacji w organizacji.
- Prowadzić audyty wewnętrzne oraz dokumentować działania związane z ochroną danych i bezpieczeństwem cyfrowym.
- Wdrażać techniczne i organizacyjne środki ochrony danych, takie jak szyfrowanie, kontrola dostępu, rejestry czynności przetwarzania.
- Reagować na incydenty bezpieczeństwa, w tym prowadzić postępowania wyjaśniające i raportowanie do organów nadzorczych.

- Posługiwać się narzędziami wspierającymi codzienną pracę IOD, np. matrycami ryzyka, checklistami audytowymi, wzorcami dokumentacji.

Szkolenie przygotuje go do:

- Samodzielnego pełnienia funkcji Inspektora Ochrony Danych, zgodnie z wymaganiami prawa krajowego i unijnego.
- Wdrażania i nadzorowania skutecznych systemów zarządzania bezpieczeństwem informacji (ISMS) w organizacjach.
- Efektywnej współpracy z działami IT, compliance i kadr w zakresie ochrony danych i cyberbezpieczeństwa.
- Ubiegania się o certyfikat potwierdzający kwalifikacje zawodowe w zakresie ochrony danych osobowych i bezpieczeństwa cyfrowego.

Ponadto, uczestnik rozwinie umiejętności:

- Praktycznego rozwiązywania problemów w zakresie ochrony danych i cyberbezpieczeństwa.
- Analizowania rzeczywistych przypadków incydentów i projektowania skutecznych działań naprawczych.
- Efektywnego komunikowania się w kontekście bezpieczeństwa danych – zarówno wewnątrz organizacji, jak i w relacji z podmiotami zewnętrznymi.
- Stosowania najnowszych rozwiązań i technologii w zakresie ochrony danych osobowych i systemów informatycznych.

WERYFIKACJA NABYTYCH KOMPETECJI I CERTYFIKAT

Poziom wiedzy i umiejętności UP zostanie zmierzony na początku przystąpienia do projektu poprzez wypełnienie ‘testu wejściowego’.

Poziom wiedzy i kompetencji zostanie zmierzony metodą ankietową na zakończenie szkolenia (‘test wyjściowy’), a dodatkową formą ewaluacji wyników będzie obserwacja uczestników szkolenia przez trenera.

Porównanie – przyrost wiedzy i kompetencji zostanie porównany z ich poziomem przed rozpoczęciem szkolenia, zarówno w sposób ilościowy, jak i jakościowy.

Otrzymanie pozytywnej oceny z testu i obserwacji oraz uzyskanie min. 80% frekwencji na szkoleniu będzie uprawniało UP do otrzymania certyfikatu potwierdzającego nabyte kompetencje oraz zawierającego info o efektach uczenia się i stopnia opanowania ich przez UP.

Walidacja efektów kształcenia przewidziana w każdym zadaniu związanym ze szkoleniami będzie dokonywana przez inną osobę niż trener prowadzący szkolenie – tj. przez koordynatora ds. szkoleń. Podsumowując, proces walidacji będzie przebiegał niezależnie od procesu kształcenia.

Certyfikat będzie wydawany wspólnie przez organizatorów zgodnie ze wzorem obowiązującym w AWSB.

Szkolenie zostanie utrzymane w ofercie Akademii WSB jako szkolenie komercyjne. Informacja o nim znajdzie się na stronie www i w przypadku zebrania grupy chętnych szkolenie zostanie przeprowadzone odpłatnie. Utrzymana zostanie współpraca z partnerami, którzy będą uczestniczyć w aktualizacji programów i realizacji szkoleń.

KADRA

Osoby prowadzące szkolenie, będą spełniać co najmniej następujące warunki:

- tytuł min. Mgr,
- Trener/ wykładowca od min. 5 lat,
- wiedza praktyczna i teoretyczna z zakresu przedmiotowego szkolenia - doświadczenie min. 5 lat jako np. biegły sądowy z zakresu informatyki śledczej lub ekspert Biura Ekspertyz Sadowych w zakresie informatyki lub Ekspert w zakresie przestępczości teleinformatycznej

Podczas szkoleń „CYBEZBEZPIECZŃSTWO Z CERTYFIKACJĄ INSPEKTORA DANYCH OSOBOWYCH" przeszkolone zostaną osoby w wieku 18-64 lata, zamieszkałe na terenie Polski. Kurs kierowany jest głównie do osób, dla których pogłębienie wiedzy, uzupełnienie luk kompetencyjnych, przekwalifikowanie będzie przepustką do wejścia/ powrotu/ utrzymania się na rynku pracy.

Informacja o rekrutacji i Kryteria obowiązkowe – szczegółowe informacje w Regulaminie.

Oferta ma charakter otwarty, nie jest zawężona do konkretnej grupy osób, jednakże wskazano priorytety rekrutacji, dla osób w trudniejszej sytuacji społeczno-gospodarczej.
Kryteria premiujące dla osób dorosłych (1 pkt za każde):

- osób biernych zawodowo,
- bezrobotnych,
- osób poniżej 35 r.ż.,
- osób w wieku 50+,
- osób z niepełnosprawnościami,

- osób pełniących funkcje opiekuńcze,
- kobiet.

ORGANIZACJA

Niektóre Szkolenia stacjonarne będą odbywały się w Akademii WSB zlokalizowanej w Dąbrowie Górniczej przy ul. Cieplaka 1C. W przypadku pozostałych szkoleń informacja o miejscu jego odbywania zostanie podana na etapie rekrutacji.

PROMOCJA

Działania informacyjne i rekrutacyjne prowadzone będą aktywnie na terenie całej Polski z zastosowaniem różnych form. Na strategię promocji i informacji będą składały się skoordynowane działania wszystkich podmiotów tworzących grupę partnerską. Informacje będą kierowane bezpośrednio do odbiorców wsparcia (grupy docelowej), ale również do ogółu społeczeństwa.

Główną osią promocyjno-informacyjną będzie strona internetowa partnerów projektu (komunikaty i informacje) oraz oficjalne profile w najbardziej popularnych mediach społecznościowych tj. Facebook, Instagram.

EWALUACJA

W ramach projektu prowadzony będzie systematyczny monitoring zapotrzebowania rynku, aby lepiej dostosowywać program szkoleń.

Ewaluacja realizowanego programu szkoleniowego będzie kluczowym elementem procesu zarządzania szkoleniami. W pierwszej kolejności ewaluacja umożliwi ocenę, czy cele szkoleniowe są osiągane, a to pozwoli na bieżąco monitorować, czy realizowane szkolenia przynoszą oczekiwane rezultaty i czy uczestnicy nabierają potrzebnych umiejętności. Pomoże zidentyfikować, które elementy szkolenia były najbardziej skuteczne, co umożliwia zoptymalizowanie alokacji zasobów. Proces ewaluacji pełnić będzie zatem rolę narzędzia kontroli jakości szkoleń., co pozwoli zapewnić, że szkolenia są zgodne z oczekiwaniami i spełniają ustalone standardy. Ewaluacja nie tylko koncentruje się na wynikach końcowych, ale także na samym procesie szkoleniowym. To pozwala na stałe doskonalenie metod nauczania, dostosowanie do zmieniających się potrzeb i skuteczne reagowanie na nowe wyzwania. Ewaluacja będzie ważnym instrumentem zarzadzania ryzykiem ponieważ pozwala identyfikować

potencjalne problemy i ryzyka związane z programami szkoleniowymi, umożliwiając wcześniejsze działania korygujące. Podsumowując, ewaluacja projektu szkoleniowego jest kluczowym narzędziem do ciągłego doskonalenia programów, zapewnienia skuteczności działań oraz dostosowania szkoleń do zmieniających się potrzeb organizacji i otoczenia.