



Postępowanie z ryzykiem w bezpieczeństwie informacji. Cele stosowania zabezpieczeń i zabezpieczenia - szkolenie

Numer usługi 2024/06/12/120241/2181102

2 767,50 PLN brutto
2 250,00 PLN netto
184,50 PLN brutto/h
150,00 PLN netto/h

CENTRUM
ZARZĄDZANIA
JAKOŚCIĄ INFOX
SPÓŁKA Z
OGRANICZONĄ
ODPOWIEDZIALNOŚ
CIĄ



📍 Bochnia / stacjonarna
🏠 Usługa szkoleniowa
🕒 15 h
📅 22.08.2024 do 23.08.2024

Informacje podstawowe

Kategoria	Biznes / Zarządzanie przedsiębiorstwem
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Usługa rozwojowa „ Postępowanie z ryzykiem w bezpieczeństwie informacji. Cele stosowania zabezpieczeń i zabezpieczenia - szkolenie ” adresowana jest do: <ol style="list-style-type: none">przedstawicieli kierownictwa odpowiedzialnych za:<ul style="list-style-type: none">zgodność SZBI z wymaganiami ISO/IEC 27001:2022,przedstawianie sprawozdań dla najwyższego kierownictwa w zakresie funkcjonowania SZBI,utrzymanie integralności SZBI podczas planowania i wprowadzania zmian,audytorów wewnętrznych przewidzianych do realizacji audytów w ramach SZBI,menedżerów IT, menedżerów systemów informatycznych, Inspektorów Ochrony Danych,wszystkich organizacji, które przechowują, przetwarzają lub udostępniają poufne informacje - szczególnie ważne jest to dla organizacji z sektorów finansowego, medycznego, IT oraz dla tych, które obsługują duże ilości danych osobowych,wszystkich osób zainteresowanych tematyką i uzyskaniem nowych, przyszłościowych kompetencji zawodowych,
Minimalna liczba uczestników	6
Maksymalna liczba uczestników	20

Data zakończenia rekrutacji	15-08-2024
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	15
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

Usługa rozwojowa przygotowuje do samodzielnego wyboru taktyki postępowania z ryzykami w bezpieczeństwie informacji, określenia niezbędnych zabezpieczeń związanych z realizacją wybranej taktyki, porównywania tych zabezpieczeń z zabezpieczeniami zawartymi w załączniku A do ISO/IEC 27001:2022, opracowania deklaracji stosowania oraz sporządzania planu postępowania z ryzykiem w bezpieczeństwie informacji.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Omawia podstawy postępowania z ryzykiem w bezpieczeństwie informacji.	Omawia zasady stosowania wzorcowego wykazu celów stosowania zabezpieczeń oraz zabezpieczenia stanowiącego załącznik A do ISO/IEC 27001:2022.	Test teoretyczny
	Przedstawia cele stosowania zabezpieczeń oraz zabezpieczenia wyspecyfikowanego w załączniku A do ISO/IEC 27001:2022.	Test teoretyczny
	Przedstawia wytyczne w zakresie realizacji zabezpieczeń – wytyczne ISO/IEC 27002:2022, rozdziały normy, organizacje tekstu normy.	Test teoretyczny
	Charakteryzuje politykę bezpieczeństwa informacji.	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Określa odpowiedzialność w bezpieczeństwie informacji.	Przedstawia podział odpowiedzialności i ról personelu organizacji.	Test teoretyczny
	Przedstawia podział obowiązków członków organizacji.	Test teoretyczny
	Zarządza odpowiedzialnościami.	Analiza dowodów i deklaracji
	Omawia znaczenie łączności z ustawowymi urzędami i specjalnymi grupami interesów.	Test teoretyczny
	Identyfikuje zagrożenia.	Analiza dowodów i deklaracji
Określa rolę informacji.	Inwentaryzuje informacje i inne powiązane aktywa.	Analiza dowodów i deklaracji
	Określa dopuszczalne wykorzystanie informacji i innych powiązanych zasobów.	Test teoretyczny
	Klasyfikuje, etykietuje, przekazuje informacje.	Analiza dowodów i deklaracji
	Kontroluje dostęp, zarządza tożsamością i udziela prawa dostępu.	Analiza dowodów i deklaracji
	Charakteryzuje informacje uwierzytelniające.	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Dba o bezpieczeństwo informacji.	Charakteryzuje bezpieczeństwo informacji w relacjach z dostawcami	Test teoretyczny
	Omawia kwestię bezpieczeństwa informacji w umowach z dostawcami.	Test teoretyczny
	Zarządza bezpieczeństwem informacji w łańcuchu dostaw ICT.	Analiza dowodów i deklaracji
	Monitoruje, przegląda i zarządza zmianami w usługach dostawców.	Analiza dowodów i deklaracji
	Omawia bezpieczeństwo informacji w przypadku korzystania z usług w chmurze.	Test teoretyczny
	Zarządza incydentami związanymi z bezpieczeństwem informacji, planowaniem i przygotowaniem.	Analiza dowodów i deklaracji
	Ocenia i podejmuje decyzje w sprawie zdarzeń związanych z bezpieczeństwem informacji.	Analiza dowodów i deklaracji
	Reaguje na incydenty związane z bezpieczeństwem informacji.	Analiza dowodów i deklaracji
	Wyciąga wnioski z incydentów związanych z bezpieczeństwem informacji i gromadzi dowody.	Analiza dowodów i deklaracji
	Dba o bezpieczeństwo informacji podczas zakłóceń.	Analiza dowodów i deklaracji
Rozwija kompetencje społeczne.	Buduje pozytywną atmosferę bezpieczeństwa i zaufania w kontakcie z innymi ludźmi.	Obserwacja w warunkach rzeczywistych
	Rozwija umiejętności komunikacyjne tj. słucha, zbiera informacje, zadaje pytania, udziela odpowiedzi, bierze udział w dyskusji.	Obserwacja w warunkach rzeczywistych
	Dostrzega, analizuje i rozwiązuje problemy.	Obserwacja w warunkach rzeczywistych

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?

Efekty uczenia się umieszczone są na zaświadczeniu potwierdzającym, że uczestnik ukończył usługę rozwojową.

Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?

Na zaświadczeniu potwierdzającym, że uczestnik ukończył usługę rozwojową umieszczone są efekty uczenia się wraz z kryteriami ich weryfikacji oraz przypisaną do każdego kryterium weryfikacji metodą walidacji.

Pytanie 3. Czy dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

Na zaświadczeniu potwierdzającym, że uczestnik ukończył usługę rozwojową znajduje się adnotacja dotycząca:

- a. Osoby prowadzącej usługę – imię, nazwisko
- b. Osoby walidującej usługę – imię, nazwisko

Program

PROGRAM USŁUGI:

1. Zasady stosowania wzorcowego wykazu celów stosowania zabezpieczeń oraz zabezpieczenia stanowiącego załącznik A do ISO/IEC 27001:2022.
2. Cele stosowania zabezpieczeń oraz zabezpieczenia wyspecyfikowanego w załączniku A do ISO/IEC 27001:2022.
3. Wprowadzenie do wytycznych w zakresie realizacji zabezpieczeń – wytyczne ISO/IEC 27002:2022, rozdziały normy, organizacja tekstu normy.
4. Polityka bezpieczeństwa informacji.
5. Podział odpowiedzialności i ról personelu organizacji.
6. Podział obowiązków członków organizacji.
7. Zarządzanie odpowiedzialnościami.
8. Łączność z ustawowymi urzędami.
9. Łączność ze specjalnymi grupami interesów.
10. Identyfikacja zagrożeń.
11. Inwentaryzacja informacji i innych powiązanych aktywów.
12. Dopuszczalne wykorzystanie informacji i innych powiązanych zasobów.
13. Zwrot aktywów.
14. Klasyfikacja informacji.
15. Etykietowanie informacji.
16. Przekazywanie informacji.
17. Kontrola dostępu.
18. Zarządzanie tożsamością.
19. Informacje uwierzytelniające.
20. Prawa dostępu.
21. Bezpieczeństwo informacji w relacjach z dostawcami.
22. Kwestia bezpieczeństwa informacji w umowach z dostawcami.
23. Zarządzanie bezpieczeństwem informacji w łańcuchu dostaw ICT.
24. Monitorowanie, przegląd i zarządzanie zmianami w usługach dostawców.
25. Bezpieczeństwo informacji w przypadku korzystania z usług w chmurze.
26. Zarządzanie incydentami związanymi z bezpieczeństwem informacji, planowanie i przygotowanie.
27. Ocena i podejmowanie decyzji w sprawie zdarzeń związanych z bezpieczeństwem informacji.
28. Reagowanie na incydenty związane z bezpieczeństwem informacji.
29. Wyciąganie wniosków z incydentów związanych z bezpieczeństwem informacji.
30. Gromadzenie dowodów.
31. Bezpieczeństwo informacji podczas zakłóceń.
32. Gotowość ICT do zapewnienia ciągłości działania.
33. Wymogi prawne, ustawowe, regulacyjne i umowne.
34. Prawa własności intelektualnej.
35. Ochrona dokumentacji.
36. Prywatność i ochrona informacji umożliwiających ustalenie tożsamości.
37. Niezależny przegląd bezpieczeństwa informacji.
38. Zgodność z politykami, zasadami i standardami bezpieczeństwa informacji.
39. Udokumentowane procedury operacyjne.
40. Fizyczne granice bezpieczeństwa.
41. Zabezpieczanie biur, pomieszczeń i obiektów.
42. Monitorowanie bezpieczeństwa fizycznego.
43. Ochrona przed zagrożeniami fizycznymi i środowiskowymi.
44. Praca w bezpiecznych miejscach.
45. Przejrzyste biurko i wyraźny ekran.
46. Lokalizacja i ochrona sprzętu.
47. Bezpieczeństwo aktywów poza lokalem przedsiębiorstwa.
48. Nośniki pamięci.
49. Narzędzia pomocnicze.
50. Bezpieczeństwo okablowania.
51. Konserwacja sprzętu.
52. Bezpieczna utylizacja lub ponowne użycie sprzętu.
53. Urządzenia końcowe użytkownika.
54. Bezpieczne uwierzytelnianie.
55. Zarządzanie pojemnością.

56. Ochrona przed złośliwym oprogramowaniem.
57. Zarządzanie lukami technicznymi.
58. Zarządzanie konfiguracją.
59. Usuwanie informacji.
60. Maskowanie danych.
61. Zapobieganie wyciekom danych.
62. Kopia zapasowa informacji.
63. Redundancja urządzeń do przetwarzania informacji.
64. Logowanie.
65. Działania monitorujące.
66. Synchronizacja zegara.
67. Korzystanie z uprzywilejowanych programów narzędziowych.
68. Instalacja oprogramowania w systemach operacyjnych.
69. Bezpieczeństwo sieci.
70. Bezpieczeństwo usług sieciowych.
71. Segregacja sieci.
72. Filtrowanie stron internetowych.
73. Wykorzystanie kryptografii.
74. Bezpieczny cykl życia programowania.
75. Wymagania bezpieczeństwa aplikacji.
76. Bezpieczna architektura systemu i zasady inżynieryjne.
77. Bezpieczne kodowanie.
78. Testy bezpieczeństwa w fazie rozwoju i akceptacji.
79. Outsourcing kodowanie (tworzenia oprogramowania).
80. Oddzielenie środowisk tworzenia, testów i produkcji.
81. Zarządzanie zmianami oprogramowania.
82. Informacja o testach.
83. Ochrona systemów i informatycznych w czasie testowania.

Sposób weryfikacji efektów uczenia się:

Efekty uczenia się, osiągnięte dzięki udziałowi uczestników w usłudze rozwojowej „**Postępowanie z ryzykiem w bezpieczeństwie informacji. Cele stosowania zabezpieczeń i zabezpieczenia - szkolenie**” zostaną zweryfikowane poprzez:

- **WIEDZA** - przeprowadzenie przez Osobę prowadzącą usługę testu wśród uczestników. Test zostanie przeprowadzony w pierwszym dniu usługi rozwojowej (PRE TEST) w celu sprawdzenia poziomu wiedzy uczestników przed udziałem w usłudze rozwojowej. W dniu zakończenia usługi rozwojowej, jako jej podsumowanie zostanie przeprowadzony test (POST TEST) mający na celu sprawdzenie poziomu wiedzy uczestników po zakończeniu udziału w usłudze rozwojowej.

Dowód: PRE TEST + POST TEST

Przygotowanie, przeprowadzenie testu: Osoba prowadząca usługę

Walidacja: Osoba walidująca usługę

- **UMIEJĘTNOŚCI** – analiza dowodów przez Osobę walidującą usługę. Osoba walidująca usługę na podstawie stworzonego przez Osobę prowadzącą usługę case study (studium przypadku) ocenia umiejętności uczestników w rzeczywistych sytuacjach, które mogą wystąpić.

Dowód: case study

Przygotowanie, przeprowadzenie case study: Osoba prowadząca usługę

Walidacja: Osoba walidująca usługę

- **KOMPETENCJE SPOŁECZNE** – obserwacja uczestników przez Osobę prowadzącą usługę oraz Osobę walidującą w warunkach rzeczywistych tj. podczas usługi rozwojowej. Analiza działań uczestników w zakresie kryteriów weryfikacji określonych w efekcie uczenia się „*Rozwija kompetencje społeczne*” w warunkach rzeczywistych, tj. podczas usługi rozwojowej.

Dodatkowo: wywiad Osoby walidującej usługę z Osobą prowadzącą usługę

Dowód: protokół z obserwacji i wywiadu

Walidacja: Osoba walidująca usługę

- Dodatkowo, osiągnięcie efektów uczenia się, w tym kryteriów weryfikacji zostanie zweryfikowane poprzez ankietę ewaluacyjną po zakończeniu usługi rozwojowej, mającą na celu indywidualne potwierdzenie przez każdego uczestnika usługi rozwojowej stopnia osiągnięcia przez niego danego efektu uczenia się w tym kryteriów weryfikacji.

Dowód: ankieta ewaluacyjna

Przeprowadzenie ankiety: Osoba prowadząca usługę

Walidacja: Osoba walidująca usługę

Warunki organizacyjne:

Usługa rozwojowa „**Postępowanie z ryzykiem w bezpieczeństwie informacji. Cele stosowania zabezpieczeń i zabezpieczenia - szkolenie**” realizowana będzie bez podziału na grupy. Usługa rozwojowa nie wymaga dostępu do indywidualnych stanowisk komputerowych. Sala w której będzie realizowana usługa rozwojowa będzie wyposażona w rzutnik, ekran do projektora. Na sali będzie dostęp do Internetu.

Czas trwania:

Usługa rozwojowa „**Postępowanie z ryzykiem w bezpieczeństwie informacji. Cele stosowania zabezpieczeń i zabezpieczenia - szkolenie**” trwa 15 godzin zegarowych, gdzie 1 godzina szkolenia trwa 60 minut.

Przerwy podczas usługi rozwojowej:

Dzień 1: 22.08.2024 r.

Przerwa nr 1: 11:00 – 11:15

Przerwa nr 2: 14:15 – 14:30

Dzień 2: 23.08.2024 r.

Przerwa nr 1: 11:00 – 11:15

Przerwa nr 2: 14:15 – 14:30

Informacje dodatkowe:

Usługa rozwojowa „**Postępowanie z ryzykiem w bezpieczeństwie informacji. Cele stosowania zabezpieczeń i zabezpieczenia - szkolenie**”:

- może zostać przeprowadzona w formie zdalnej w czasie rzeczywistym,
- może zostać przeprowadzona dla zamkniętej grupy uczestników – szkolenie indywidualne, zamknięte,
- może zostać zrealizowana w innym, dogodnym terminie,

W celu ustalenia szczegółów realizacji zapraszamy do kontaktu mailowego.

Harmonogram

Liczba przedmiotów/zajęć: 30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 30 Zasady stosowania wzorcowego wykazu celów stosowania zabezpieczeń oraz zabezpieczenia stanowiącego załącznik A do ISO/IEC 27001:2022.	Eligiusz Myśliwy	22-08-2024	08:00	08:30	00:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<p>2 z 30 Cele stosowania zabezpieczeń oraz zabezpieczenia wyspecyfikowanego w załączniku A do ISO/IEC 27001:2022.</p>	Eligiusz Myśliwy	22-08-2024	08:30	09:00	00:30
<p>3 z 30 Wprowadzenie do wytycznych w zakresie realizacji zabezpieczeń – wytyczne ISO/IEC 27002:2022, rozdziały normy, organizacja tekstu normy.</p>	Eligiusz Myśliwy	22-08-2024	09:00	09:30	00:30
<p>4 z 30 Polityka bezpieczeństwa informacji. Podział odpowiedzialności i ról personelu organizacji. Podział obowiązków członków organizacji. Zarządzanie odpowiedzialnościami.</p>	Eligiusz Myśliwy	22-08-2024	09:30	10:00	00:30
<p>5 z 30 Łączność z ustawowymi urzędami. Łączność ze specjalnymi grupami interesów. Identyfikacja zagrożeń. Inwentaryzacja informacji i innych powiązanych aktywów.</p>	Eligiusz Myśliwy	22-08-2024	10:00	10:30	00:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<p>6 z 30</p> <p>Dopuszczalne wykorzystanie informacji i innych powiązanych zasobów. Zwrot aktywów. Klasyfikacja informacji. Etykietowanie informacji. Przekazywanie informacji.</p>	Eligiusz Myśliwy	22-08-2024	10:30	11:00	00:30
<p>7 z 30</p> <p>Kontrola dostępu. Zarządzanie tożsamością. Informacje uwierzytelniające. Prawa dostępu. Bezpieczeństwo informacji w relacjach z dostawcami. Kwestia bezpieczeństwa informacji w umowach z dostawcami.</p>	Eligiusz Myśliwy	22-08-2024	11:15	11:45	00:30
<p>8 z 30</p> <p>Zarządzanie bezpieczeństwem informacji w łańcuchu dostaw ICT. Monitorowanie, przegląd i zarządzanie zmianami w usługach dostawców. Bezpieczeństwo informacji w przypadku korzystania z usług w chmurze.</p>	Eligiusz Myśliwy	22-08-2024	11:45	12:15	00:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<p>9 z 30</p> <p>Zarządzanie incydentami związanymi z bezpieczeństwem informacji, planowanie i przygotowanie. Ocena i podejmowanie decyzji w sprawie zdarzeń związanych z bezpieczeństwem informacji.</p>	Eligiusz Myśliwy	22-08-2024	12:15	12:45	00:30
<p>10 z 30</p> <p>Reagowanie na incydenty związane z bezpieczeństwem informacji. Wyciąganie wniosków z incydentów związanych z bezpieczeństwem informacji. Gromadzenie dowodów.</p>	Eligiusz Myśliwy	22-08-2024	12:45	13:15	00:30
<p>11 z 30</p> <p>Bezpieczeństwo informacji podczas zakłóceń. Gotowość ICT do zapewnienia ciągłości działania.</p>	Eligiusz Myśliwy	22-08-2024	13:15	13:45	00:30
<p>12 z 30</p> <p>Wymogi prawne, ustawowe, regulacyjne i umowne. Prawa własności intelektualnej. Ochrona dokumentacji.</p>	Eligiusz Myśliwy	22-08-2024	13:45	14:15	00:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<p>13 z 30</p> <p>Prywatność i ochrona informacji umożliwiających ustalenie tożsamości.</p>	Eligiusz Myśliwy	22-08-2024	14:30	15:00	00:30
<p>14 z 30</p> <p>Niezależny przegląd bezpieczeństwa informacji. Zgodność z politykami, zasadami i standardami bezpieczeństwa informacji.</p>	Eligiusz Myśliwy	22-08-2024	15:00	15:30	00:30
<p>15 z 30</p> <p>Udokumentowane procedury operacyjne. Fizyczne granice bezpieczeństwa. Zabezpieczanie biur, pomieszczeń i obiektów. Monitorowanie bezpieczeństwa fizycznego.</p>	Eligiusz Myśliwy	22-08-2024	15:30	16:00	00:30
<p>16 z 30</p> <p>Ochrona przed zagrożeniami fizycznymi i środowiskowymi. Praca w bezpiecznych miejscach. Przejrzyste biurko i wyraźny ekran. Lokalizacja i ochrona sprzętu.</p>	Eligiusz Myśliwy	23-08-2024	08:00	08:30	00:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
17 z 30 Bezpieczeństwo aktywów poza lokalem przedsiębiorstwa . Nośniki pamięci. Narzędzia pomocnicze.	Eligiusz Myśliwy	23-08-2024	08:30	09:00	00:30
18 z 30 Bezpieczeństwo okablowania. Konserwacja sprzętu. Bezpieczna utylizacja lub ponowne użycie sprzętu.	Eligiusz Myśliwy	23-08-2024	09:00	09:30	00:30
19 z 30 Urządzenia końcowe użytkownika. Bezpieczne uwierzytelnianie. Zarządzanie pojemnością.	Eligiusz Myśliwy	23-08-2024	09:30	10:00	00:30
20 z 30 Ochrona przed złośliwym oprogramowaniem. Zarządzanie lukami technicznymi. Zarządzanie konfiguracją.	Eligiusz Myśliwy	23-08-2024	10:00	10:30	00:30
21 z 30 Usuwanie informacji. Maskowanie danych. Zapobieganie wyciekom danych. Kopia zapasowa informacji.	Eligiusz Myśliwy	23-08-2024	10:30	11:00	00:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<p>22 z 30</p> <p>Redundancja urządzeń do przetwarzania informacji. Logowanie. Działania monitorujące.</p>	Eligiusz Myśliwy	23-08-2024	11:15	11:45	00:30
<p>23 z 30</p> <p>Synchronizacja zegara. Korzystanie z uprzywilejowanych programów narzędziowych.</p>	Eligiusz Myśliwy	23-08-2024	11:45	12:15	00:30
<p>24 z 30</p> <p>Instalacja oprogramowania w systemach operacyjnych. Bezpieczeństwo sieci. Bezpieczeństwo usług sieciowych.</p>	Eligiusz Myśliwy	23-08-2024	12:15	12:45	00:30
<p>25 z 30</p> <p>Segregacja sieci. Filtrowanie stron internetowych. Wykorzystanie kryptografii.</p>	Eligiusz Myśliwy	23-08-2024	12:45	13:15	00:30
<p>26 z 30</p> <p>Bezpieczny cykl życia programowania. Wymagania bezpieczeństwa aplikacji.</p>	Eligiusz Myśliwy	23-08-2024	13:15	13:45	00:30
<p>27 z 30</p> <p>Bezpieczna architektura systemu i zasady inżyneryjne. Bezpieczne kodowanie.</p>	Eligiusz Myśliwy	23-08-2024	13:45	14:15	00:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
28 z 30 Testy bezpieczeństwa w fazie rozwoju i akceptacji. Outsourcing kodowanie (tworzenia oprogramowania).	Eligiusz Myśliwy	23-08-2024	14:30	15:00	00:30
29 z 30 Oddzielenie środowisk tworzenia, testów i produkcji. Zarządzanie zmianami oprogramowania.	Eligiusz Myśliwy	23-08-2024	15:00	15:30	00:30
30 z 30 Informacja o testach. Ochrona systemów i informatycznych w czasie testowania.	Eligiusz Myśliwy	23-08-2024	15:30	16:00	00:30

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	2 767,50 PLN
Koszt przypadający na 1 uczestnika netto	2 250,00 PLN
Koszt osobogodziny brutto	184,50 PLN
Koszt osobogodziny netto	150,00 PLN

Prowadzący

Liczba prowadzących: 1



1 z 1



Eligiusz Myśliwy

Certyfikowany Audytor Wewnętrzny (CIA – Certified Internal Auditor), Audytor Wiodący Systemu Zarządzania Bezpieczeństwem Informacji.

Ekspert w dziedzinie Zarządzania Jakością, trener, konsultant i pełnomocnik ds. jakości, specjalista w zakresie zarządzania ciągłością działania.

Doświadczony trener i wykładowca realizujący szkolenia i doradztwo z zakresu systemów zarządzania jakością w organizacjach.

Prowadzi konsultacje i szkolenia w dziedzinie ochrony danych osobowych, zarządzania ryzykiem, bezpieczeństwem informacji. Planuje audyty wewnętrzne w organizacjach klientów oraz realizuje zadania audytowe. Wdraża i doskonali Systemy Zarządzania Jakością w samorządach lokalnych, prywatnych przedsiębiorstwach.

Wdrożył systemy zarządzania w ponad 1,5 tys. przedsiębiorstw. Przeszkolił ponad 3 tysiące osób.

Posiada 20-letnie doświadczenie we wdrażaniu i doskonaleniu Systemów Zarządzania.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Każdy z uczestników otrzymuje komplet materiałów w wersji papierowej i/lub elektronicznej.

Każdy z uczestników otrzymuje prezentację multimedialną w wersji papierowej i/lub elektronicznej i/lub konspekt w wersji papierowej i/lub elektronicznej.

Dodatkowo, uczestnicy usługi rozwojowej otrzymają wykaz materiałów (książek, artykułów, stron internetowych, czasopism, rejestrów, ogólnodostępnych prezentacji ppt., materiałów audiovideo, e-podręczników, e-booków, itp.) umożliwiających utrwalenie efektów uczenia się, zdobytych w trakcie udziału w usłudze rozwojowej oraz umożliwiających samokształcenie się po zakończeniu usługi rozwojowej.

Uczestnicy otrzymają certyfikat i zaświadczenie, potwierdzające, że ukończyli usługę rozwojową.

Informacje dodatkowe

Usługa rozwojowa, która dla uczestnika ma charakter usługi kształcenia zawodowego / przekwalifikowania zawodowego i jest finansowana ze środków publicznych w co najmniej 70% jest zwolniona z podatku VAT na podstawie §3 ust.1 pkt 14 rozporządzenia Ministra Finansów z dn. 20 grudnia 2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień (Dz.U.2018.701)).

Cena usługi rozwojowej dla 1 uczestnika, który uzyskał dofinansowanie w co najmniej 70% wynosi **2 250,00 zł netto/brutto**.

Cena usługi rozwojowej dla uczestników, którzy uzyskali dofinansowanie ze środków publicznych poniżej 70% oraz dla uczestników, którzy nie uzyskali takiego dofinansowania lub usługa rozwojowa nie ma charakteru usługi kształcenia zawodowego / przekwalifikowania zawodowego jest powiększona o podatek VAT (23%).

Cena usługi rozwojowej dla pozostałych (wyżej opisanych) uczestników to **2 250,00 zł netto + 517,50 zł 23%VAT = 2 767,50 zł/osoba brutto**.

Adres

ul. Brzeska 95
32-700 Bochnia
woj. małopolskie

Kontakt



Magdalena Polek

E-mail sekretariat@czj-infox.pl

Telefon (+48) 518 925 841