Możliwość dofinansowania

FIRMA HANDLOWO-USŁUGOWA "MIJA" MICHAŁ JAROSZ

4,8 / 5

311 ocen

Zarządzanie bezpieczeństwem informacji i cyberbezpieczeństwem w infrastrukturze IT/OT oraz zapewnienie ciągłości działania w funkcjonowaniu podmiotów kluczowych i ważnych (zgodne z ISO/IEC 27001:2022, IEC 62443 oraz wymaganiami Dyrektywa NIS2 i Ustawą o krajowym systemie cyberbezpieczeństwa).

Numer usługi 2026/03/30/157015/3447498

- Suchedniów
- Usługa szkoleniowa
- stacjonarna
- 18:00 h
- 22.06.2026 do 23.06.2026

5 220,00 PLN brutto
5 220,00 PLN netto
290,00 PLN brutto/h
290,00 PLN netto/h
261,33 PLN cena rynkowa

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Szkolenie ma charakter strategiczno-decyzyjny z elementami warsztatowymi i analizą przypadków. Jest skierowane głównie do kadry kierowniczej w tym: członków zarządu, kierownictwa wyższego i średniego szczebla, osób odpowiedzialnych za strategiczne zarządzanie IT i OT, osób nadzorujących bezpieczeństwo informacji oraz do właścicieli firm i organizacji. Udział w szkoleniu nie wymaga posiadania specjalistycznej wiedzy informatycznej.
Minimalna liczba uczestników	4
Maksymalna liczba uczestników	6
Data zakończenia rekrutacji	21-06-2026
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	18
Podstawa uzyskania wpisu do BUR	Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

Cel

Cel edukacyjny

Celem szkolenia jest przygotowanie kadry kierowniczej do świadomego, skutecznego zarządzania bezpieczeństwem informacji i cyberbezpieczeństwem w organizacji oraz do budowania odporności organizacji na incydenty cyberbezpieczeństwa i zapewnieniu jej ciągłości działania, ze szczególnym uwzględnieniem środowisk IT i OT, zgodnie z podejściem IEC 62443 (Dyrektywa NIS2, Ustawa o krajowym systemie cyberbezpieczeństwa, zapewnienie Systemu Zarządzania Bezpieczeństwem Informacji zgodnego z ISO/I).

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Wiedza: Uczestnik określa i stosuje wymagania regulacyjne oraz przewiduje konsekwencje ich niespełnienia, rozumie znaczenie bezpieczeństwa systemów OT	Uczestnik właściwie odpowiada na pytania dotyczące danego zakresu tematycznego.	Test teoretyczny
	Uczestnik dobiera właściwą formę zabezpieczenia danych w zadanej sytuacji.	Test teoretyczny
		Obserwacja w warunkach symulowanych
Umiejętności: Uczestnik jest przygotowany do działania w sytuacjach kryzysowych, wspiera skuteczne wdrożenie i utrzymanie SZBI	Uczestnik właściwie odpowiada na pytania dotyczące danego zakresu tematycznego.	Test teoretyczny
	Uczestnik rozpoznaje zagrożenie i dobiera odpowiednie działanie zapewniające bezpieczeństwo danych.	Obserwacja w warunkach symulowanych
Kompetencje: Uczestnik uzyskał kompetencje właściwego postępowania zgodnie z wymaganiami z zakresu bezpieczeństwa informacji, w tym działań, jakie należy podjąć w celu zapewnienia bezpieczeństwa informacji, danych osobowych oraz zasobów firmy, organizacji niwelujących wystąpienie cyberzagrożenia.	Uczestnik właściwie odpowiada na pytania dotyczące danego zakresu tematycznego.	Test teoretyczny
	Uczestnik postępuje zgodnie z wymogami dotyczącymi właściwego zabezpieczenia informacji i danych osobowych.	Obserwacja w warunkach symulowanych

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

Brak wymagań co do poziomu wiedzy uczestników, w tym posiadania specjalistycznej wiedzy informatycznej. Szkolenie przeznaczone jest dla właścicieli oraz kadry kierowniczej firm i organizacji.

Szkolenie ma charakter strategiczno-decyzyjny z elementami warsztatowymi i analizą przypadków. Zajęcia teoretyczne i ćwiczenia praktyczne będą realizowane wspólnie dla całej grupy pod kierownictwem prowadzącego szkolenie.

Szkolenie odbywać się będzie w oparciu o miarę godziny lekcyjnej wynoszącej 45 min. Przerwy nie wliczają się w czas trwania usługi. W trakcie szkolenia wykorzystane zostaną liczne przykłady, symulacje i ćwiczenia. Walidacja odbywać się będzie na podstawie testów teoretycznych jednokrotnego wyboru oraz na podstawie obserwacji uczestnika w zasymulowanych sytuacjach.

Dzień 1 Rola zarządu, regulacje i ryzyko - Podstawowe informacje dotyczące szkolenia, pre-test

Moduł 1 – Rola kierownictwa w bezpieczeństwie informacji - wykład

- odpowiedzialność zarządu w SZBI (ISO/IEC 27001 – przywództwo),
- nadzór nad bezpieczeństwem informacji jako element zarządzania organizacją,
- kultura bezpieczeństwa i świadomość organizacyjna.

Moduł 2 – Wymagania prawne i odpowiedzialność - wykład

- obowiązki wynikające z Dyrektywa NIS2 (zarządzanie ryzykiem, raportowanie incydentów, odpowiedzialność kierownictwa),
- obowiązki wynikające z Ustawa o krajowym systemie cyberbezpieczeństwa,
- konsekwencje braku zgodności (organizacyjne, finansowe, reputacyjne).

Moduł 3 – Zarządzanie ryzykiem na poziomie strategicznym - wykład połączony z ćwiczeniami

- rola zarządu w zatwierdzaniu ryzyka,
- podejmowanie decyzji na podstawie analizy ryzyka,
- akceptacja, redukcja, transfer i unikanie ryzyka,
- przykłady ryzyk krytycznych (IT i OT).

Moduł 4 – Cyberzagrożenia i ich wpływ na organizację - wykład

- ransomware i jego skutki biznesowe,
- phishing jako główny wektor ataku,
- wycieki danych i odpowiedzialność organizacji,
- wpływ incydentów na ciągłość działania.

Moduł 5 – Specyfika bezpieczeństwa OT (IEC 62443) - wykład

- różnice między IT a OT,
- zagrożenia dla infrastruktury przemysłowej,
- znaczenie segmentacji i separacji sieci,

Dzień 2 – Decyzje, incydenty i ciągłość działania

Moduł 6 – Nadzór nad środkami bezpieczeństwa - wykład połączony z ćwiczeniami

- kluczowe środki techniczne (MFA, SIEM, backup, segmentacja),

- środki organizacyjne (polityki, procedury, audyty),
- jak zarząd powinien oceniać skuteczność zabezpieczeń.

Moduł 7 – Zarządzanie incydentami (poziom zarządczy) - wykład

- rola kierownictwa w sytuacji incydentu,
- decyzje kryzysowe i komunikacja,
- raportowanie incydentów zgodnie z NIS2 i KSC,
- współpraca z CSIRT.

Moduł 8 – Ciągłość działania i odporność organizacji - wykład

- znaczenie BIA dla zarządu,
- parametry RTO i RPO w decyzjach biznesowych,
- odpowiedzialność za zapewnienie ciągłości działania,
- testowanie planów i gotowość organizacji.

Moduł 9 – Warsztaty decyzyjne dla kadry kierowniczej - ćwiczenia

- symulacja incydentu (np. ransomware / atak na OT),
- podejmowanie decyzji strategicznych,
- zarządzanie kryzysowe,
- analiza konsekwencji decyzji.

Moduł 10 – Podsumowanie i wnioski

- kluczowe obowiązki zarządu,
- najczęstsze błędy organizacji,
- rekomendacje działań dla organizacji.
- podsumowanie szkolenia, post-test

Harmonogram

Liczba pozycji harmonogramu: 0

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
Brak wyników.					

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	5 220,00 PLN
Podmiot uprawniony do zwolnienia z VAT na podstawie art. 43 ust. 1 ustawy o VAT	
Koszt przypadający na 1 uczestnika netto	5 220,00 PLN
Koszt osobogodziny brutto	290,00 PLN

Koszt osobogodziny netto	290,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

MARIUSZ PISKORCZYK

Audytor wiodący ISO/IEC 27001 i ISO 9001. Wdrażanie i szkolenia w zakresie Systemów Zarządzania Bezpieczeństwem Informacji. Specjalista w zakresie "Ochrony Danych Osobowych" - Inspektor Ochrony Danych Osobowych. Administrator Systemów Informatycznych. 20 letnie doświadczenie na stanowisko informatyka w Administracji publicznej, potem jako audytor systemów bezpieczeństwa informacji i IOD. Audyty w zakresie wymagań Krajowych Systemów Cyberbezpieczeństwa, przeprowadzanie testów podatności i zagrożeń. Administrator Systemów Serwerowych Windows Serwer, administrator sieci i urządzeń klasy UTM. Ukończone studia na kierunku Zarządzania Systemami Informatycznymi na WSEiP w Kielcach. Członek ISSA Polska. Właściciel podmiotu zajmującego się wdrażaniem i szkoleniem ISO/IEC 27001, ISO 9001 i ISO 22301. Szkolenia podmiotów administracji publicznej oraz służby zdrowia w zakresie standardów bezpieczeństwa i cyberbezpieczeństwa oraz zarządzania bezpieczeństwem informacji. Współpracujący z podmiotami z sektora cyberbezpieczeństwa IT. Opracowanie bezpłatnych poradników w zakresie ataków cybernetycznych Ransomware, bezpieczeństwa informacji i norm ISO. Publikacja artykułów w zakresie cyberbezpieczeństwa.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Prezentacja powerpoint, celem utrwalenia informacji przekazanych w trakcie szkolenia, przesłana będzie drogą mailową.

Warunki uczestnictwa

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

Informacje dodatkowe

Po zakończeniu usługi uczestnik otrzyma certyfikat. Usługa szkoleniowa podzielona jest na godziny dydaktyczne (1 godzina dydaktyczna = 45 minut).

Usługa jest zwolniona z podatku VAT w przypadku, kiedy przedsiębiorstwo zwolnione jest z podatku VAT lub dofi nansowanie wynosi conajmniej 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 iusługoraz szczegółowych warunków stosowania tych zwolnień (Dz.U. z 2018 r., poz. 701).

Adres

Suchedniów
Suchedniów
woj. świętokrzyskie

Sala wykładowa

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi

Kontakt

ELŻBIETA LUDWIKOWSKA

E-mail e.ludwikowska.mija@gmail.com
Telefon (+48) 609 718 185