Możliwość dofinansowania

Zarządzanie cyberbezpieczeństwem i ryzykiem zgodnie z NIS2, ISO/IEC 27001 i ustawą o KSC - szkolenie

Numer usługi 2026/05/21/18395/3576708

1 900,00 PLN brutto
1 900,00 PLN netto
118,75 PLN brutto/h
118,75 PLN netto/h
261,33 PLN cena rynkowa

Akademia Górniczo-Hutnicza im. Stanisława Staszica w Krakowie

4,6 / 5

45 ocen

Usługa szkoleniowa
zdalna w czasie rzeczywistym
Zajęcia grupowe
16:00 h
18.06.2026 do 19.06.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Kadra kierownicza, właściciele procesów biznesowych i IT, inspektorzy ochrony danych (IOD/DPO), osoby odpowiedzialne za bezpieczeństwo informacji (CISO/BISO), pełnomocnicy ds. systemów zarządzania, specjaliści compliance, audytu i ryzyka oraz przedstawiciele administracji publicznej i przedsiębiorstw, w tym MŚP i dużych organizacji. Przydatne będą: ogólne rozeznanie w procesach biznesowych własnej organizacji oraz podstawowa znajomość pojęć z zakresu IT i bezpieczeństwa informacji.
Minimalna liczba uczestników	8
Maksymalna liczba uczestników	24
Data zakończenia rekrutacji	12-06-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Podstawa uzyskania wpisu do BUR	art. 163 ust. 1 ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (t. j. Dz. U. z 2024 r. poz. 1571, z późn. zm.)
Zakres uprawnień	kształcenie w innych formachkształcenia prowadzonych przez uczelnie

Cel

Cel edukacyjny

Usługa przygotowuje uczestnika do mapowania wymagań NIS2, UKSC i ISO/IEC 27001 na procesy organizacji, przeprowadzania podstawowej oceny ryzyka bezpieczeństwa informacji, projektowania ról i odpowiedzialności w SZBI oraz przygotowania organizacji do audytu zgodności i raportowania incydentów.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Charakteryzuje założenia Systemu Zarządzania Bezpieczeństwem Informacji	omawia cykl PDCA w kontekście SZBI, wskazuje powiązania bezpieczeństwa informacji z procesami biznesowymi, rozróżnia podstawowe elementy dokumentacji SZBI	Test teoretyczny
Przeprowadza podstawową ocenę ryzyka bezpieczeństwa informacji	identyfikuje aktywa, zagrożenia i podatności dla wskazanego procesu, szacuje poziom ryzyka na podstawie przyjętych kryteriów dobiera adekwatną strategię postępowania z ryzykiem	Test teoretyczny
Mapuje wymagania NIS2, UKSC i ISO/IEC 27001 na procesy organizacji	wskazuje wymagania regulacyjne dotyczące przykładowej organizacji, przyporządkowuje wymagania do polityk, procedur i zabezpieczeń, identyfikuje podstawowe luki zgodności	Test teoretyczny
Projektuje podstawowy podział ról i odpowiedzialności w obszarze cyberbezpieczeństwa	opisuje role CISO, właściciela ryzyka i właściciela aktywa, przypisuje odpowiedzialności do zadań w procesie zarządzania bezpieczeństwem, uzasadnia znaczenie odpowiedzialności kierownictwa w kontekście NIS2	Test teoretyczny
Przygotowuje organizację do audytu zgodności i raportowania incydentów	rozróżnia rodzaje audytów związanych z SZBI i cyberbezpieczeństwem, wskazuje dowody i dokumenty potrzebne do audytu, określa podstawowe obowiązki raportowania incydentów do właściwych CSIRT lub organów	Test teoretyczny

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

Zakres tematyczny:

1. Wprowadzenie do Systemu Zarządzania Bezpieczeństwem Informacji: ewolucja podejścia do cyberbezpieczeństwa, model PDCA, powiązanie bezpieczeństwa informacji z procesami biznesowymi.

2. Zarządzanie ryzykiem: metodyki oceny ryzyka, inwentaryzacja i klasyfikacja aktywów, identyfikacja zagrożeń i podatności, strategie postępowania z ryzykiem.

3. ISO/IEC 27001:2022: struktura normy, kontekst organizacji, przywództwo, planowanie, wybrane zabezpieczenia z Załącznika A, podstawowa analiza luk.

4. NIS2 i UKSC: zakres podmiotowy, obowiązki organizacji, odpowiedzialność zarządu, mapowanie wymagań regulacyjnych na polityki i zabezpieczenia ISO 27001.

5. Role i polityki bezpieczeństwa: architektura dokumentacji SZBI, role CISO, właściciela ryzyka i właściciela aktywa, pogodzenie wymagań bezpieczeństwa z celami biznesowymi.

6. Podejście audytowe i zgłaszanie incydentów: rodzaje audytów, przygotowanie organizacji, dowody audytowe, formalne wymagania raportowania incydentów.

Warunki organizacyjne: szkolenie grupowe dla 8–24 uczestników, realizowane na platformie przeznaczonej do pracy zdalnej np. MS Teams. Uczestnicy pracują na materiałach elektronicznych udostępnionych przez prowadzącego. Walidacja ma formę testu końcowego online prowadzonego przez osobę walidującą odrębną od osoby prowadzącej szkolenie.

Harmonogram

Liczba pozycji harmonogramu: 11

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 11 Wprowadzenie do SZBI: cyberbezpieczeństwo od IT do biznesu, PDCA, integracja z BPM. Forma: wykład ekspercki, rozmowa na żywo, współdzielenie ekranu.	Zajęcia	dr inż. Jarosław Homa	18-06-2026	08:00	10:00	02:00
2 z 11 -	Przerwa	-	18-06-2026	10:00	10:15	00:15
3 z 11 Zarządzanie ryzykiem: aktywa, zagrożenia, podatności, szacowanie ryzyka. Forma: warsztat online, case study, praca na arkuszu ćwiczeniowym, dyskusja moderowana.	Zajęcia	dr inż. Jarosław Homa	18-06-2026	10:15	13:15	03:00
4 z 11 -	Przerwa	-	18-06-2026	13:15	14:00	00:45
5 z 11 Standard ISO/IEC 27001:2022: struktura normy, kontekst organizacji, przywództwo, planowanie, Załącznik A, podstawowa analiza luk. Forma: wykład, współdzielenie ekranu, ćwiczenie warsztatowe.	Zajęcia	dr inż. Jarosław Homa	18-06-2026	14:00	16:00	02:00

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
6 z 11 ISO/IEC 27001:2022 – kontynuacja analizy luk i podsumowanie ćwiczenia. Forma: warsztat online, omówienie wyników.	Zajęcia	dr inż. Jarosław Homa	19-06-2026	08:00	09:00	01:00
7 z 11 Krajobraz regulacyjny NIS2 i UKSC: zakres podmiotowy, wymagania, odpowiedzialność zarządu, mapowanie wymagań na ISO 27001. Forma: wykład, case study, dyskusja moderowana.	Zajęcia	dr inż. Jarosław Homa	19-06-2026	09:00	12:00	03:00
8 z 11 -	Przerwa	-	19-06-2026	12:00	13:00	01:00
9 z 11 Role i polityki bezpieczeństwa: dokumentacja SZBI, role CISO, właściciel ryzyka, właściciel aktywa, specyfika podmiotów komercyjnych. Forma: wykład, ćwiczenie, rozmowa na żywo.	Zajęcia	dr inż. Jarosław Homa	19-06-2026	13:00	14:30	01:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
10 z 11 Podejście audytowe i zgłaszanie incydentów: audyty, przygotowanie organizacji, wymogi raportowania do CSIRT i organów właściwych. Forma: wykład, case study, współdzielenie ekranu.	Zajęcia	dr inż. Jarosław Homa	19-06-2026	14:30	15:30	01:00
11 z 11 -	Walidacja	-	19-06-2026	15:30	16:00	00:30

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	16:00
w tym suma godzin zajęć	13:30
w tym suma godzin walidacji	00:30
w tym suma przerw	02:00
Suma godzin dydaktycznych bez przerw	18:30

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	1 900,00 PLN
Podmiot uprawniony do zwolnienia z VAT na podstawie art. 43 ust. 1 ustawy o VAT	
Koszt przypadający na 1 uczestnika netto	1 900,00 PLN

Koszt osobogodziny brutto	118,75 PLN
Koszt osobogodziny netto	118,75 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	16:00

Prowadzący

Liczba prowadzących: 1

1 z 1

dr inż. Jarosław Homa

Pełnomocnik Rektora ds. Cyberbezpieczeństwa oraz Wicedyrektor Centrum Cyberbezpieczeństwa Politechniki Śląskiej. Menedżer zarządzania cyberbezpieczeństwem, architekt IT i cyberbezpieczeństwa, wykładowca akademicki prowadzący zajęcia m.in. na studiach MBA, podyplomowych oraz kierunkach informatycznych. Ekspert w obszarze systemów IT i OT, audytor wiodący ISO/IEC 27001 oraz ISO 22301, posiadacz certyfikatów PRINCE2, ITIL, AgilePM i Cisco CCNA. Projektuje i wdraża rozwiązania z zakresu cyberbezpieczeństwa, w tym SOC, z uwzględnieniem wymagań NIS2, UKSC i NIST.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnicy otrzymają materiały bezpośrednio związane z realizowaną usługą: prezentację szkoleniową w formacie PDF, zestaw ćwiczeń warsztatowych, oraz dokument potwierdzający udział/ukończenie szkolenia po spełnieniu warunków organizacyjnych i podejściu do testu końcowego.

Warunki techniczne

1. Sprzęt komputerowy

Uczestnik zobowiązany jest do korzystania z komputera lub laptopa wyposażonego w:

- system operacyjny Windows 10/11, macOS lub Linux,
- procesor klasy **Intel i5 / Ryzen 5** lub równoważny,
- minimum **8 GB RAM** (zalecane 16 GB),
- co najmniej **10 GB wolnej przestrzeni dyskowej**,
- stabilne łącze internetowe o przepustowości **min. 10 Mbps**,
- aktualną przeglądarkę internetową: Chrome, Edge lub Firefox.

2. Wyposażenie audiowizualne

Uczestnik musi posiadać:

- **sprawną kamerę** (wbudowaną lub zewnętrzną), umożliwiającą udział w zajęciach, ćwiczeniach oraz interakcję z prowadzącym,
- **sprawny głośnik i mikrofon** (wbudowany lub zewnętrzny), niezbędny do komunikacji podczas zajęć.Zaleca się korzystanie z **słuchawek z mikrofonem** w celu poprawy jakości dźwięku i redukcji zakłóceń.

3. Środowisko szkoleniowe

Szkolenie realizowane jest z wykorzystaniem platformy umożliwiającej:

- **udostępnianie ekranu** przez prowadzącego i uczestników,
- **komunikację audio-wideo oraz czat** w celu zapewnienia interaktywnego udziału w zajęciach,
- **współdzielenie materiałów i plików** niezbędnych do realizacji programu szkolenia,
- **interaktywną prezentację kodu i analiz danych**, w tym wykonywanie ćwiczeń praktycznych w czasie rzeczywistym.

Kontakt

Agata Rzepka

E-mail rzepka@agh.edu.pl

Telefon (+48) 12 3283 414