Możliwość dofinansowania

Podstawy cyberbezpieczeństwa - szkolenie zakończone certyfikatem CISCO

Numer usługi 2025/06/13/181485/2814832

2 800,00 PLN brutto
2 800,00 PLN netto
233,33 PLN brutto/h
233,33 PLN netto/h

PAŃSTWOWA AKADEMIA NAUK STOSOWANYCH W GŁOGOWIE

Brak ocen dla tego dostawcy

Głogów / stacjonarna
Usługa szkoleniowa
12 h
17.10.2025 do 18.10.2025

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Osoby dorosłe zainteresowane tematyką bezpieczeństwa cyfrowego, w szczególności pracownicy sektora edukacyjnego, administracji publicznej, instytucji kultury oraz osoby planujące rozwój kompetencji IT. Nie są wymagane wcześniejsze kompetencje techniczne.
Minimalna liczba uczestników	6
Maksymalna liczba uczestników	12
Data zakończenia rekrutacji	30-09-2025
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	12
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 2023 r. poz. 742, z późn. zm.)
Zakres uprawnień	Prowadzenie szkoleń i kursów w zakresie i obszarach objętych zgodami na prowadzenie kierunków studiów wyższych

Cel

Cel edukacyjny

Uczestnik szkolenia zdobędzie wiedzę do samodzielnego korzystania z zakresu cyberbezpieczeństwa, ochrony danych oraz stosowania technik bezpieczeństwa cyfrowego w środowisku zawodowym i prywatnym. Szkolenie przygotuje do

swobodnego korzystania z narzędzi ochrony i do stosowania rozwiązań zgodnych z przepisami NIS2 (Network and Information Systems Directive 2 -cyberbezpieczeństwa w sektorach kluczowych), PSD2 (Payment Services Directive - regulacji i bezpieczeństwa usług płatniczych w UE).

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
1. Podstawowe pojęcia i terminologia cyberbezpieczeństwa	1. Uczestnik poprawnie definiuje podstawowe pojęcia związane z cyberbezpieczeństwem.	Test teoretyczny
2. Rodzaje zagrożeń i źródła ryzyka w sieci	2. Uczestnik identyfikuje i klasyfikuje podstawowe zagrożenia występujące w cyberprzestrzeni	Test teoretyczny
3. Znaczenie cyberbezpieczeństwa w życiu prywatnym i zawodowym	3. Uczestnik opisuje wpływ cyberbezpieczeństwa na bezpieczeństwo osobiste i organizacyjne.	Wywiad swobodny
4. Najczęstsze typy ataków (phishing, malware, ransomware)	4. Uczestnik rozpoznaje charakterystyczne cechy ataków i wskazuje sposoby ich wykrywania.	Obserwacja w warunkach symulowanych
5. Techniki inżynierii społecznej	5. Uczestnik wyjaśnia mechanizmy manipulacji stosowane w inżynierii społecznej i wskazuje przykłady ich użycia.	Wywiad ustrukturyzowany
6. Wykrywanie i zapobieganie atakom	6. Uczestnik przedstawia metody detekcji ataków i zapobiegania ich skutkom.	Obserwacja w warunkach symulowanych
7. Ochrona danych osobowych (RODO)	7. Uczestnik wskazuje podstawowe obowiązki wynikające z RODO w kontekście cyberbezpieczeństwa.	Test teoretyczny
8. Bezpieczne przechowywanie i przesyłanie informacji	8. Uczestnik prezentuje zasady bezpiecznego przechowywania i szyfrowania danych.	Obserwacja w warunkach symulowanych
9. Zarządzanie hasłami i tożsamością cyfrową	9. Uczestnik stosuje zalecenia dotyczące tworzenia i ochrony haseł oraz zarządzania tożsamością cyfrową.	Obserwacja w warunkach symulowanych
10. Tworzenie polityk bezpieczeństwa	10. Uczestnik wskazuje podstawowe elementy polityki bezpieczeństwa w organizacji.	Prezentacja
11. Zarządzanie incydentami i plan ciągłości działania	11. Uczestnik opisuje procedury reagowania na incydenty i tworzenia planów ciągłości działania.	Obserwacja w warunkach symulowanych

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
12. Bezpieczeństwo sieci i urządzeń w firmie	12. Uczestnik wymienia podstawowe środki zabezpieczania sieci i urządzeń końcowych.	Test teoretyczny
13. Role i kompetencje specjalistów ds. bezpieczeństwa	13. Uczestnik charakteryzuje główne stanowiska i kompetencje wymagane w obszarze cyberbezpieczeństwa.	Prezentacja
14. Możliwości certyfikacji i rozwoju zawodowego	14. Uczestnik wskazuje główne certyfikaty i ścieżki rozwoju w dziedzinie cyberbezpieczeństwa.	Wywiad swobodny
15. Etyka w zawodzie specjalisty cyberbezpieczeństwa	15. Uczestnik rozstrzyga przykładowe dylematy etyczne związane z zawodem specjalisty bezpieczeństwa.	Wywiad ustrukturyzowany
16. Podstawy prawne ochrony informacji i cyberbezpieczeństwa w Polsce i UE	16. Uczestnik identyfikuje kluczowe akty prawne regulujące ochronę informacji i cyberbezpieczeństwa.	Test teoretyczny
17. Zastosowanie podpisu elektronicznego i e-doręczeń	17. Uczestnik opisuje zasady używania podpisu elektronicznego i e-doręczeń w obrocie prawnym.	Obserwacja w warunkach symulowanych
18. Obowiązki administratorów danych i użytkowników	18. Uczestnik określa podstawowe obowiązki administratorów i użytkowników w zakresie bezpieczeństwa danych.	Test teoretyczny

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

DZIEŃ 1 (6 godzin):

Moduł 1: Wprowadzenie do cyberbezpieczeństwa

1. Podstawowe pojęcia i terminologia cyberbezpieczeństwa
2. Rodzaje zagrożeń i źródła ryzyka w sieci
3. Znaczenie cyberbezpieczeństwa w życiu prywatnym i zawodowym

Moduł 2: Ataki i techniki infiltracji

1. Najczęstsze typy ataków (phishing, malware, ransomware)
2. Techniki inżynierii społecznej
3. Wykrywanie i zapobieganie atakom

Moduł 3: Prywatność i bezpieczeństwo danych

1. Ochrona danych osobowych (RODO)
2. Bezpieczne przechowywanie i przesyłanie informacji
3. Zarządzanie hasłami i tożsamością cyfrową

DZIEŃ 2 (6 godzin) :

Moduł 4: Bezpieczeństwo organizacji

1. Tworzenie polityk bezpieczeństwa
2. Zarządzanie incydentami i plan ciągłości działania
3. Bezpieczeństwo sieci i urządzeń w firmie

Moduł 5: Kariera w cyberbezpieczeństwie

1. Role i kompetencje specjalistów ds. bezpieczeństwa
2. Możliwości certyfikacji i rozwoju zawodowego
3. Etyka w zawodzie specjalisty cyberbezpieczeństwa

Moduł 6: Akty prawne, podpis elektroniczny

1. Podstawy prawne ochrony informacji i cyberbezpieczeństwa w Polsce i UE
2. Zastosowanie podpisu elektronicznego i e-doręczeń
3. Obowiązki administratorów danych i użytkowników

Moduł 7: Egzamin wewnętrzny

Test wiedzy teoretycznej

Harmonogram

Liczba przedmiotów/zajęć: 23

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 23 Podstawowe pojęcia i terminologia cyberbezpieczeństwa	Bartłomiej Sulikowski	17-10-2025	09:00	09:15	00:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
2 z 23 Rodzaje zagrożeń i źródła ryzyka w sieci	Bartłomiej Sulikowski	17-10-2025	09:15	10:00	00:45
3 z 23 Znaczenie cyberbezpieczeństwa w życiu prywatnym i zawodowym	Bartłomiej Sulikowski	17-10-2025	10:00	10:30	00:30
4 z 23 Przerwa organizacyjna	Bartłomiej Sulikowski	17-10-2025	10:30	10:40	00:10
5 z 23 Najczęstsze typy ataków (phishing, malware, ransomware)	Bartłomiej Sulikowski	17-10-2025	10:40	11:20	00:40
6 z 23 Techniki inżynierii społecznej	Bartłomiej Sulikowski	17-10-2025	11:20	12:20	01:00
7 z 23 Wykrywanie i zapobieganie atakom	Bartłomiej Sulikowski	17-10-2025	12:20	13:20	01:00
8 z 23 Przerwa organizacyjna	Bartłomiej Sulikowski	17-10-2025	13:20	13:30	00:10
9 z 23 Ochrona danych osobowych (RODO)	Bartłomiej Sulikowski	17-10-2025	13:30	14:00	00:30
10 z 23 Bezpieczne przechowywanie i przesyłanie informacji	Bartłomiej Sulikowski	17-10-2025	14:00	14:30	00:30
11 z 23 Zarządzanie hasłami i tożsamością cyfrową	Bartłomiej Sulikowski	17-10-2025	14:30	15:00	00:30
12 z 23 Tworzenie polityk bezpieczeństwa	Bartłomiej Sulikowski	18-10-2025	09:00	09:15	00:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
13 z 23 Zarządzanie incydentami i plan ciągłości działania	Bartłomiej Sulikowski	18-10-2025	09:15	10:00	00:45
14 z 23 Bezpieczeństwo sieci i urządzeń w firmie	Bartłomiej Sulikowski	18-10-2025	10:00	10:30	00:30
15 z 23 Przerwa organizacyjna	Bartłomiej Sulikowski	18-10-2025	10:30	10:40	00:10
16 z 23 Role i kompetencje specjalistów ds. bezpieczeństwa	Bartłomiej Sulikowski	18-10-2025	10:40	11:20	00:40
17 z 23 Możliwości certyfikacji i rozwoju zawodowego	Bartłomiej Sulikowski	18-10-2025	11:20	12:20	01:00
18 z 23 Etyka w zawodzie specjalisty cyberbezpieczeństwa	Bartłomiej Sulikowski	18-10-2025	12:20	13:20	01:00
19 z 23 Przerwa organizacyjna	Bartłomiej Sulikowski	18-10-2025	13:20	13:30	00:10
20 z 23 Podstawy prawne ochrony informacji i cyberbezpieczeństwa w Polsce i UE	Bartłomiej Sulikowski	18-10-2025	13:30	14:00	00:30
21 z 23 Zastosowanie podpisu elektronicznego i e-doręczeń	Bartłomiej Sulikowski	18-10-2025	14:00	14:30	00:30
22 z 23 Obowiązki administratorów danych i użytkowników	Bartłomiej Sulikowski	18-10-2025	14:30	14:50	00:20

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
23 z 23 Test wiedzy teoretycznej	-	18-10-2025	14:50	15:00	00:10

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	2 800,00 PLN
Koszt przypadający na 1 uczestnika netto	2 800,00 PLN
Koszt osobogodziny brutto	233,33 PLN
Koszt osobogodziny netto	233,33 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Bartłomiej Sulikowski

Certyfikat szkoleniowca Akademii Cisco.
II.2021 - do chwili obecnej, profesor uczelni, Instytut Sterowania i Systemów Informatycznych,Wydział Elektrotechniki, Informatyki i Telekomunikacji, Uniwersytet Zielonogórski,
X.2024 - do chwili obecnej, wykładowca, Państwowa Akademia Nauk Stosowanych w Głogowie,
II.2021 - do chwili obecnej, wykładowca, Uczelnia Jana Wyżykowskiego w Polkowicach,
IV.2006 - I. 2 021, adiunkt, Instytut Sterowania i Systemow Informatycznych, Wydział Elektrotechniki,Informatyki i Telekomunikacji, Uniwersytet Zielonogorski,
X.2011 - IX.2017, starszy wykładowca, Instytut Politechniczny, Państwowa Wyższa Szkoła Zawodowa w Głogowie,
IV.2017 - do chwili obecnej, trener w projekcie: „Program podnoszenia kompetencji studentówkierunku Informatyka Uniwersytetu Zielonogorskiego”,
nr umowy: POWR.03.01.00-00-K045/16-00, PO Wiedza Edukacja Rozwoj, Oś priorytetowa:Szkolnictwo wyższe dla gospodarki i rozwoju, Działania 3.1: Kompetencje w szkolnictwie wyższym,Benefi ncjent: Uniwersytet Zielonogorski
V.2005 - do chwili obecnej, certyfi kowany instruktor Akademii Sieci Komputerowych CISCO, InstytutSterowania i Systemow Informatycznych, Wydział Elektrotechniki, Informatyki i Telekomunikacji,Uniwersytet Zielonogorski, szkolenia: CCNA, FWL, CCNP, ITE, Cybersecurity Essentials, NetworkSecurity, Introduction to cybersecurity

II.2009 - VIII.2010, kierownik, trener i autor wniosku o dofi nansowanie projektu EFS „Zrobmy Coś Razem”

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Osoba biorąca udział w szkoleniu uzyska:

- dostęp do pełnych materiałów CISCO w j. polskim
- autorskie prezentacje
- instrukcje ćwiczeniowe
- dostęp do platformy egzaminacyjnej online (CISCO NetAcad)

Adres

ul. Piotra Skargi 5

67-200 Głogów

woj. dolnośląskie

Szkolenie odbędzie się w budynkach Uczelni - Państwowej Akademii Nauk Stosowanych w Głogowie.
Pomieszczenie do szkolenia z cyberbezpieczeństwa będzie dobrze wyposażone technicznie, przestronne, zapewniające komfort uczestników i prowadzącego.
Technologie takie jak komputery, Wi-Fi, projektor, oraz odpowiednie zabezpieczenie sieci to kluczowe elementy, które jako organizatorzy zapewniamy.
Komfort fizyczny uczestników (wentylacja, wygodne siedzenie, przerwy) jest gwarantowany.

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi
- Laboratorium komputerowe
- Komputery Terminale Projektor Ekran Głośniki Mikrofon Zabezpieczone sieci

Kontakt

Jarosław Hermaszewski

E-mail j.hermaszewski@pans.glogow.pl

Telefon (+48) 517 157 106