Możliwość dofinansowania

CYBERBEZPIECZEŃSTWO - Bezpieczeństwo w pracy zdalnej

Numer usługi 2025/12/01/11913/3183656

1 119,30 PLN brutto
910,00 PLN netto
159,90 PLN brutto/h
130,00 PLN netto/h

Ośrodek Szkolenia "Millenium" - Niepubliczna Placówka Kształcenia Ustawicznego

4,7 / 5

146 ocen

zdalna w czasie rzeczywistym
Usługa szkoleniowa
7 h
08.01.2026 do 08.01.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Pracownicy wykonujący pracę zdalną lub hybrydową, team-leaderzy, HR, IOD **Dlaczego to ważne?** 82% incydentów phishingowych 2024 r. dotykało pracowników spoza biura, a ustawowe przepisy o pracy zdalnej (Kodeks pracy) nakładają na pracodawcę obowiązek zapewnienia bezpiecznych warunków pracy.
Minimalna liczba uczestników	10
Maksymalna liczba uczestników	16
Data zakończenia rekrutacji	04-01-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	7
Podstawa uzyskania wpisu do BUR	Znak Jakości Małopolskich Standardów Usług Edukacyjno-Szkoleniowych (MSUES) - wersja 2.0

Cel

Cel edukacyjny

Po ukończeniu szkolenia uczestnik wymienia min. 8 zagrożeń pracy zdalnej, wskaże podstawowe zabezpieczenia miejsca pracy i sprzętu, zastosuje co najmniej 5 dobrych praktyk higieny cyfrowej oraz 3 techniki dbania o dobrostan psychiczny.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Wiedza charakteryzuje zagrożenia pracy zdalnej (socjotechnika, sieci publiczne, wyciek danych, stres) poprawność opisu zagrożeń test on-line (15 pytań) Umiejętności tworzy 12-znakowe hasło + aktywuje 2FA i szyfrowanie pliku ZIP spełnienie wymogów silnego hasła, poprawny klucz szyfrowania obserwacja instruktora Kompetencje społeczne potrafi zgłosić incydent i wesprzeć współpracowników, a także poszukiwać wsparcia w organizacji i poza nią jasność procedury, empatyczna komunikacja scenka „mini-incydent” + feedback 360°	Wiedza charakteryzuje zagrożenia pracy zdalnej (socjotechnika, sieci publiczne, wyciek danych, stres) poprawność opisu zagrożeń test on-line (15 pytań) Umiejętności tworzy 12-znakowe hasło + aktywuje 2FA i szyfrowanie pliku ZIP spełnienie wymogów silnego hasła, poprawny klucz szyfrowania obserwacja instruktora Kompetencje społeczne potrafi zgłosić incydent i wesprzeć współpracowników, a także poszukiwać wsparcia w organizacji i poza nią jasność procedury, empatyczna komunikacja scenka „mini-incydent” + feedback 360°	Test teoretyczny Obserwacja w warunkach symulowanych

Cel biznesowy

Ograniczenie ryzyka incydentów bezpieczeństwa w trakcie pracy zdalnej, a także naruszeń ochrony danych.

Efekt usługi

Kategoria	Efekt uczenia się (uczestnik…)	Kryteria weryfikacji	Metoda walidacji
Wiedza	charakteryzuje zagrożenia pracy zdalnej (socjotechnika, sieci publiczne, wyciek danych, stres)	poprawność opisu zagrożeń	test on-line (15 pytań)
Umiejętności	tworzy 12-znakowe hasło + aktywuje 2FA i szyfrowanie pliku ZIP	spełnienie wymogów silnego hasła, poprawny klucz szyfrowania	obserwacja instruktora
Kompetencje społeczne	potrafi zgłosić incydent i wesprzeć współpracowników, a także poszukiwać wsparcia w organizacji i poza nią	jasność procedury, empatyczna komunikacja	scenka „mini-incydent” + feedback 360°

Metoda potwierdzenia osiągnięcia efektu usługi

Metoda walidacji
test on-line (15 pytań)

obserwacja instruktora
scenka „mini-incydent” + feedback 360°

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

Godz.	Moduł / Treści kluczowe	Metody
09:00 – 09:45	**1. Co i dlaczego chronić w pracy zdalnej** • krajobraz współczesnych cyberzagrożeń (ENISA, CERT-PL) • obowiązki pracodawcy/pracownika wg Kodeksu Pracy • Ćwiczenie: mapa ryzyka home-office	mini-wykład + ćwiczenie
09:45 – 11:15	**2. Przeciwdziałanie zagrożeniom** • bezpieczna sieć, VPN, aktualizacje • hasła i menedżery haseł – warsztat tworzenia haseł, szyfrowanie plików, kopie zapasowe	case study + ćwiczenie
11:30 – 12:30	**3. Sytuacje trudne i kryzysowe** • phishing, deepfake’y głosowe • Ćw.: rozpoznawanie phishingu (quiz Kahoot) • procedura reagowania	symulacja + dyskusja, ćwiczenia
12:30 – 13:15	**4. Ochrona prywatności online** • inwigilacja, cookies, fingerprinting • media społecznościowe – ustawienia prywatności • dobre praktyki	prezentacja + burza mózgów
13:15 – 14:45	**5. Higiena cyfrowa & dobrostan** • wypalenie, ergonomia, izolacja – wg WHO 2023 • Ćw.: mikronawyki i przerwy aktywne • sieci wsparcia wewnątrz firmy, • techniki radzenia sobie ze stresem cyfrowym	ćwiczenie + moderowana dyskusja
14:45 – 15:15	**6. Walidacja** • test wiedzy • prezentacja planu działań jakie uczestnik zamierza wdrożyć po szkoleniu	test + obserwacja

Harmonogram

Liczba przedmiotów/zajęć: 1

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 1 Cyberbezpieczeństwo	Dawid Mrowiec	08-01-2026	10:00	16:00	06:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	1 119,30 PLN
Koszt przypadający na 1 uczestnika netto	910,00 PLN
Koszt osobogodziny brutto	159,90 PLN
Koszt osobogodziny netto	130,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Dawid Mrowiec

Dawid Mrowiec - specjalista w zakresie bezpieczeństwa, zarządzania ryzykiem i compliance. Audytor, doradca i trener. Absolwent psychologii w zarządzaniu oraz bezpieczeństwa narodowego na UJ, a także studiów podyplomowych Corporate Governance, Risk and Compliance Management na SGH. W pracy bazuje na interdyscyplinarnej wiedzy, łącząc doświadczenia zawodowe z aktywnością naukową.

Posiadacz licznych certyfikatów specjalistycznych, w tym m.in. Approved Compliance Expert (ACE), Regulatory Compliance (University of Pennsylvania), Risk Management Specialization (New York Institute of Finance), audytora wiodącego normy ISO 27001 (system zarządzania bezpieczeństwem informacji), audytora wewnętrznego norm ISO 22301 (system zarządzania ciągłością działania) i ISO 27701 (system zarządzania informacjami o prywatności), a także wdrożeniowca ISO 42001 (system zarządzania sztuczną inteligencją).

Jest członkiem czterech organizacji branżowych: SABI – Stowarzyszenie Inspektorów Ochrony

Danych, IIA Polska, ACFE Poland Chapter oraz Stowarzyszenia Managerów i Audytorów Systemów Zarządzania SMASZ.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

- e-skrypt „Bezpieczny Home-Office” (PDF)
- check-lista bezpiecznej pracy zdalnej
- infografika dotycząca zarządzania hasłami
- szablon procedury zgłaszania incydentu (docx)
- linki do wartościowych źródeł wiedzy na temat bezpieczeństwa w pracy zdalnej

Warunki uczestnictwa

podstawowa biegłość komputerowa; brak wymogu wiedzy technicznej

Warunki techniczne

Platforma MS Teams / Zoom; kamera, mikrofon, łącze ≥ 10 Mbps; aktualna przeglądarka.

Kontakt

Dominika Kaczmarczyk-Żółciak

E-mail biuro@millenium.edu.pl

Telefon (+48) 731 200 001