



Cyberbezpieczeństwo i higiena cyfrowa: ochrona przed zagrożeniami online z elementami zielonych kompetencji w pracy z danymi

Numer usługi 2025/12/19/30963/3222843

2 000,00 PLN brutto
2 000,00 PLN netto
125,00 PLN brutto/h
125,00 PLN netto/h

OŚRODEK
SZKOLENIA
DOKSZTAŁCANIA I
DOSKONALENIA
KADR KURSÓR
SPÓŁKA Z
OGRANICZONĄ
ODPOWIEDZIALNOŚ
CIĄ

★★★★★ 4,6 / 5

536 ocen

📍 zdalna w czasie rzeczywistym

📄 Usługa szkoleniowa

🕒 16 h

📅 26.02.2026 do 06.03.2026

Informacje podstawowe

Kategoria

Informatyka i telekomunikacja / Bezpieczeństwo IT

Grupa docelowa usługi

- osoby początkujące – bez doświadczenia w cyberbezpieczeństwie, chcące zdobyć podstawową wiedzę o ochronie danych w sieci
- entuzjaści technologii – zainteresowani IT i bezpieczeństwem online
- studenci kierunków informatycznych i pokrewnych – poszerzający kompetencje w zakresie zabezpieczeń
- profesjonaliści IT i osoby pracujące z informacją – aktualizujący wiedzę o zagrożeniach i dobrych praktykach
- osoby pracujące zdalnie i hybrydowo, przetwarzające dane osobowe lub poufne w środowisku cyfrowym

Usługa jest dostępna dla wszystkich zainteresowanych – zarówno osób indywidualnych, jak i kierowanych przez urzędy, firmy, instytucje oraz wszystkich operatorów.

Mogą w niej uczestniczyć także osoby z programów regionalnych, w tym m.in.

- Kierunek - Rozwój WUP Toruń
- Usługi rozwojowe województwa śląskiego
- Małopolski pociąg do kariery – sezon 1,
- Nowy start w Małopolsce z EURESem

Minimalna liczba uczestników

5

Maksymalna liczba uczestników

20

Data zakończenia rekrutacji

24-02-2026

Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	16
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 przygotowuje do identyfikacji i ograniczania zagrożeń online oraz do organizacji bezpiecznej pracy z informacją zgodnie z dobrymi praktykami i podejściem ISO/IEC 27001. Uczestnik planuje działania prewencyjne i reakcję na incydent w pracy zdalnej oraz stosuje zasady higieny cyfrowej i zielonych kompetencji w obiegu danych (minimalizacja, porządek, 6R, ograniczanie zbędnego transferu i przechowywania).

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Wiedza: Definiuje pojęcia cyberbezpieczeństwa i klasyfikuje typowe zagrożenia online.	rozdziela phishing/smishing/vishing, malware, wyciek danych; przypisuje zagrożenie do kanału (e-mail, WWW, komunikator, chmura)	Test teoretyczny z wynikiem generowanym automatycznie
Wiedza: Charakteryzuje podejście do zarządzania bezpieczeństwem informacji wg ISO/IEC 27001 na poziomie ogólnym.	wskazuje elementy podejścia (ryzyko, zabezpieczenia, role, doskonalenie); dobiera przykład zabezpieczenia do wskazanego ryzyka	Test teoretyczny z wynikiem generowanym automatycznie
Wiedza: Opisuje zasady ochrony danych osobowych i poufności informacji w pracy cyfrowej i zdalnej.	rozdziela dane osobowe/poufne; identyfikuje błędy w udostępnianiu; uzasadnia potrzebę ograniczenia dostępu	Test teoretyczny z wynikiem generowanym automatycznie
Wiedza: Wyjaśnia wpływ działań cyfrowych na środowisko oraz charakteryzuje zielone praktyki w obiegu danych.	wskazuje źródła wpływu (energia urządzeń, przechowywanie i transfer danych); definiuje 6R w pracy cyfrowej; dobiera praktykę ograniczającą wpływ bez obniżania bezpieczeństwa	Test teoretyczny z wynikiem generowanym automatycznie
Umiejętności: Ocenia wiarygodność komunikacji online i identyfikuje symptomy socjotechniki.	ocenia przykładowe treści pod kątem „czerwonych flag”; wskazuje poprawne działania weryfikacyjne	Test teoretyczny z wynikiem generowanym automatycznie
Umiejętności: Dobiera podstawowe zabezpieczenia kont i urządzeń dla pracy z informacją.	dobiera zasady haseł, 2FA, aktualizacji i kopii zapasowych; wskazuje właściwe ustawienia prywatności i uprawnień	Test teoretyczny z wynikiem generowanym automatycznie

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Umiejętności: Planuje reakcję na incydent bezpieczeństwa informacji w pracy zdalnej.	układa kolejność działań (zabezpieczenie, ograniczenie szkód, zgłoszenie, analiza); identyfikuje role i kanały raportowania	Test teoretyczny z wynikiem generowanym automatycznie
Umiejętności: Analizuje ryzyko w typowych scenariuszach przetwarzania informacji.	identyfikuje aktywa i zagrożenia; ocenia skutki; dobiera adekwatne zabezpieczenia organizacyjne i techniczne	Test teoretyczny z wynikiem generowanym automatycznie
Umiejętności: Organizuje obieg informacji w sposób bezpieczny i zgodny z zielonym podejściem.	planuje minimalizację danych, porządek wersji, ograniczanie duplikatów; wskazuje kiedy stosować link zamiast załącznika; uzasadnia retencję i bezpieczne usuwanie danych	Test teoretyczny z wynikiem generowanym automatycznie
Kompetencje społeczne: Organizuje komunikację zespołową wokół zasad bezpieczeństwa informacji.	formułuje jasne reguły udostępniania i uprawnień; argumentuje wybór zasad w zależności od odbiorcy	Test teoretyczny z wynikiem generowanym automatycznie
Kompetencje społeczne: Uzasadnia potrzebę przestrzegania procedur bezpieczeństwa i konsekwencje ich naruszenia.	wskazuje skutki organizacyjne i prawne; ocenia ryzyko wynikające z nieprzestrzegania zasad	Test teoretyczny z wynikiem generowanym automatycznie
Kompetencje społeczne: Promuje odpowiedzialne, w tym środowiskowo, korzystanie z technologii w obiegu danych.	uzasadnia zielone praktyki (6R, redukcja transferu, porządek danych) i pokazuje ich związek ze spadkiem ryzyka cyber (mniej kopii = mniejsza powierzchnia ataku)	Test teoretyczny z wynikiem generowanym automatycznie

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

Kurs Cyberbezpieczeństwo to kompleksowy program szkoleniowy przeznaczony dla osób pragnących rozwijać swoje umiejętności w zakresie ochrony danych i zarządzania ryzykiem w obszarze IT. Szkolenie odbywa się w formie zdalnej, umożliwiając bezpośrednią interakcję z prowadzącymi i innymi uczestnikami.

Dlaczego warto skorzystać z naszej usługi:

Kompleksowa wiedza teoretyczna i praktyczna:

- Szkolenie obejmuje wszystkie kluczowe aspekty związane z zarządzaniem bezpieczeństwem informacji. Uczestnicy poznają zarówno podstawowe, jak i zaawansowane techniki ochrony danych, w tym identyfikację zagrożeń, analizę ryzyka oraz wdrażanie procedur zabezpieczeń.

Praktyczne umiejętności:

- Program szkolenia nastawiony jest na praktyczne przykłady i case studies, co pozwala uczestnikom na natychmiastowe zastosowanie zdobytej wiedzy w praktyce. Praktyczne podejście gwarantuje, że uczestnicy będą gotowi do efektywnego zarządzania bezpieczeństwem informacji od razu po ukończeniu szkolenia.

Interaktywna forma zdalna:

- Szkolenie odbywa się w formie zdalnej, w czasie rzeczywistym, za pomocą platformy Zoom. Umożliwia to uczestnictwo z dowolnego miejsca, oszczędzając czas i koszty związane z dojazdami. Interaktywne sesje wideo, współdzielenie ekranu i chat pozwalają na aktywny udział i bieżącą komunikację z prowadzącymi oraz innymi uczestnikami.

Godziny realizacji szkolenia:

- Szkolenie obejmuje 16 godzin edukacyjnych tj. 12 godzin zegarowych. (12 teoria/4 praktyka)
- Każda godzina szkolenia obejmuje 45 minut.
- walidacja wliczona jest w czas trwania usługi - czas trwania 15 minut w formie testu z wynikiem generowanym automatycznie.

Przerwy:

- Przerwy nie są wliczone w czas trwania usługi.

Metody pracy:

- Zajęcia prowadzone są metodą ćwiczeniową, połączoną z rozmową na żywo oraz współdzieleniem ekranu. Warunkiem niezbędnym do osiągnięcia celu szkolenia jest samodzielne wykonanie wszystkich ćwiczeń zadanych przez trenera.

Doświadczeni prowadzący:

- Informacje o osobach prowadzących szkolenie, w tym imiona, nazwiska, kwalifikacje oraz doświadczenie, zostaną podane na 6 dni przed rozpoczęciem szkolenia, zgodnie z wymogami regulaminu BUR. Trenera prowadzący usługę oraz osoba walidująca będzie posiadała doświadczenie zawodowe zdobyte nie wcześniej niż 5 lat lub kwalifikacje nabyte nie wcześniej niż 5 lat przed datą wprowadzenia szczegółowych danych dotyczących oferowanej usługi.

Certyfikat ukończenia:

- zaświadczenie wydane na podstawie § 23 ust. 4 rozporządzenia Ministra Edukacji i Nauki z dnia 6 października 2023 r. w sprawie kształcenia ustawicznego w formach pozaszkolnych (Dz. U. poz. 2175).
- w/w zaświadczenie zgodne z § 14 ust. 3 Rozporządzenia Ministra Funduszy i Polityki Regionalnej z dnia 28 lipca 2023 r. w sprawie rejestru podmiotów świadczących usługi rozwojowe (Dz.U. 2023 poz. 1686)

Harmonogram szkolenia:

Szczegółowy harmonogram zajęć, uwzględniający podział na dni i godziny oraz przerwy, zostanie ustalony i uzupełniony na 6 dni przed rozpoczęciem szkolenia, zgodnie z regulaminem BUR. Będzie on dostosowany do preferencji czasowych uczestników.

Osoby zainteresowane udziałem w szkoleniu prosimy o kontakt w celu określenia preferowanych godzin szkolenia

- Szkolenie może być realizowane zarówno raz jak i kilka razy w tygodniu w trybie dziennym, umożliwiając intensywną naukę i skoncentrowane zajęcia lub popołudniowym, co pozwala uczestnikom z innymi obowiązkami dostęp do wartościowej edukacji.
- Dodatkowo, istnieje opcja organizacji zajęć w formie weekendowej, co sprawia, że szkolenie staje się bardziej elastyczne i dostosowane do różnych harmonogramów życia.

- **w związku z powyższym nie wskazano szczegółowego harmonogramu** - jesteśmy gotowi dostosować się do potrzeb całej grupy zapisanych osób, tworząc harmonogram, który uwzględni zróżnicowane preferencje czasowe uczestników.
- Harmonogram szkolenia może ulegać nieznacznemu przesunięciu czasowemu, zależnie od czasu potrzebnego na wykonanie poszczególnych ćwiczeń i zdolności przyswajania materiału przez uczestników, zgodnie z ich indywidualnym tempem nauki

Dostępność kurs do potrzeb osób ze szczególnymi potrzebami

- Wsparcie techniczne: Zapewniamy wsparcie techniczne dla uczestników, którzy mogą potrzebować pomocy w obsłudze platformy
- szkoleniowej lub dostępu do materiałów.
- Sesje Q&A: sesje pytań i odpowiedzi, gdzie uczestnicy mogą zadawać pytania w czasie rzeczywistym, również poprzez czat tekstowy,
- co jest pomocne dla osób, które mogą mieć trudności z komunikacją werbalną.
- platforma ZOOM, na której prowadzone jest szkolenie, jest zgodna z międzynarodowymi standardami dostępności,
- takimi jak WCAG 2.1.
- elastyczny harmonogram szkolenia, aby dostosować tempo nauki do indywidualnych możliwości uczestników.

Program:

1. **Wprowadzenie do cyberzagrożeń i cyberhigieny** - rodzaje zagrożeń, schematy ataków, błędy użytkowników, przykłady sytuacji z życia zawodowego (e-mail, komunikator, fałszywe logowania).
2. **Dane prawnie chronione i odpowiedzialność w obiegu informacji** - poufność, udostępnianie danych, minimalizacja dostępu, konsekwencje naruszeń, logika „kto i po co ma dostęp”.
3. **Identyfikacja i klasyfikacja ryzyk w bezpieczeństwie informacji** - źródła ryzyk, aktywa, zagrożenia, skutki dla organizacji, omówienie scenariuszy ryzyka w pracy zdalnej.
4. **Zarządzanie ryzykiem i podejście ISO/IEC 27001 - ujęcie ogólne** - SZBI jako sposób porządkowania zasad, ról i zabezpieczeń; przykłady działań prewencyjnych.
5. **Najlepsze praktyki zabezpieczeń w pracy cyfrowej** - urządzenia i nośniki, aktualizacje, hasła, 2FA, kopie zapasowe, bezpieczne udostępnianie i uprawnienia.
6. **Nowe technologie a bezpieczeństwo informacji (AI, biometria) – ryzyka i zasady ostrożności** - ryzyka ujawniania danych, zasady korzystania z narzędzi, odpowiedzialność użytkownika.
7. **Praca zdalna: zasady, błędy, reakcja na incydent** - procedury reagowania, komunikacja, raportowanie, najczęstsze błędy i ich ograniczanie.
8. **Kompetencje cyfrowe: higiena pracy z kontami i danymi** - pojęcia (konto, uprawnienia, chmura, wersje), porządkowanie informacji, bezpieczne udostępnianie, ograniczanie „chaosu plików” jako czynnika ryzyka. (Przykład omawiany: „10 wersji dokumentu w mailach” vs „jedna wersja z kontrolą dostępu”).
9. **Zielone kompetencje w pracy cyfrowej i cyberbezpieczeństwie**
 - • • • • Wpływ działań cyfrowych na środowisko: energia urządzeń, transfer danych, przechowywanie (dlaczego duże pliki i duplikaty mają koszt).
 - 6R w wersji „cyfrowej”: ograniczaj zbędne dane, używaj ponownie (szablony), porządkuj i archiwizuj, usuwaj bezpiecznie to, co niepotrzebne (retencja).
 - „Zielone” praktyki, które wspierają bezpieczeństwo: minimalizacja danych i kopii = mniej miejsc wycieku; jasne zasady retencji = mniejsze ryzyko przetrzymywania danych bez potrzeby.
 - Optymalizacja obiegu informacji: kiedy stosować link zamiast ciężkich załączników, jak ograniczać duplikaty i „śmieci cyfrowe”, jak planować repozytoria/zasoby, by były i bezpieczne, i oszczędne.
10. **Case study (w formule omówienia): incydent + wnioski** - omówienie przykładowego incydentu, wskazanie działań prewencyjnych, naprawczych i „zielonych” (porządek danych, ograniczenie kopii, retencja).

Harmonogram

Liczba przedmiotów/zajęć: 0

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

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	2 000,00 PLN
Koszt przypadający na 1 uczestnika netto	2 000,00 PLN
Koszt osobogodziny brutto	125,00 PLN
Koszt osobogodziny netto	125,00 PLN

Prowadzący

Liczba prowadzących: 0

Brak wyników.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

uczestnicy otrzymają materiały dydaktyczne w formie elektronicznej. Zostaną one przesłane w postaci plików i dokumentów (np. PDF, prezentacje, arkusze informacyjne, linków, inne)

Warunki uczestnictwa

Obowiązek uczestnictwa w co najmniej 80% zajęć – czas zalogowania w platformie Zoom.

Podczas szkolenia **obowiązkowe jest korzystanie z kamery internetowej przez uczestników.**

Informacje dodatkowe

Podstawą do rozliczenia usługi jest wygenerowanie z systemu raportu, umożliwiającego identyfikację wszystkich uczestników oraz zastosowanego narzędzia.

Zawarto umowę WUP w Toruniu w ramach Projektu Kierunek - Rozwój

Regulamin współpracy i rozliczenia usług z wykorzystaniem elektronicznym bonów szkoleniowych w ramach projektu „Małopolski pociąg do kariery – sezon 1” i projektu „Nowy start w Małopolsce z EURESem” został obustronnie podpisany.

Ośrodek Szkolenia Doksztalcania i Doskonalenia Kadr Kursor Spółka z ograniczoną odpowiedzialnością świadczy usługi zwolnione z podatku od towarów i usług na podstawie Art. 43., ust. 1. Ustawy o podatku od towarów i usług z dnia 11 marca 2004 r.

Warunki techniczne

Warunki techniczne szkolenia na platformie Zoom:

1. Sprzęt komputerowy:

- Wymagany komputer PC lub Mac z dostępem do internetu.
- Zalecana kamera internetowa oraz mikrofon dla udziału w sesjach wideo.

2. Przeglądarka internetowa:

- Zalecane przeglądarki: Google Chrome, Mozilla Firefox, Safari.
- Wymagane zaktualizowane wersje przeglądarek dla optymalnej wydajności.

3. Stabilne połączenie internetowe:

- Minimalna prędkość łącza: 2 Mbps dla udziału w sesjach wideo.
- Zalecane połączenie kablowe dla stabilności.

4. Platforma Zoom:

- Konieczne pobranie i zainstalowanie najnowszej wersji aplikacji Zoom przed szkoleniem.
- Aktywne konto Zoom (możliwość utworzenia bezpłatnego konta).

5. System operacyjny:

- Kompatybilność z systemem Windows lub macOS.

6. Oprogramowanie dodatkowe:

- Zalecane zainstalowanie najnowszych wersji programów, takich jak przeglądarka, Java, Flash itp.

7. Dźwięk i słuchawki:

- Zalecane użycie słuchawek z mikrofonem dla lepszej jakości dźwięku.
- Sprawdzenie działania dźwięku przed rozpoczęciem szkolenia.

8. Przygotowanie przed sesją:

- Testowanie sprzętu i połączenia przed planowanym szkoleniem.
- Zapewnienie cichego miejsca pracy dla minimalizacji zakłóceń.

9. Wsparcie techniczne:

- Zapewnienie kontaktu z pomocą techniczną w razie problemów podczas sesji.

Zapewnienie powyższych warunków technicznych umożliwi płynny przebieg szkolenia na platformie Zoom, zminimalizuje zakłócenia i zagwarantuje efektywną interakcję między prowadzącym a uczestnikami.

Kontakt



Jolanta Krzak

E-mail szkolenia.zamosc@kursor.edu.pl

Telefon (+48) 500 177 049