Możliwość dofinansowania

Cyberbezpieczeństwo w codziennej pracy — ochrona danych, hasła, phishing i bezpieczna praca zdalna

Numer usługi 2026/01/13/30963/3255054

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 KURSOR SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

4,5 / 5

697 ocen

Usługa szkoleniowa
zdalna w czasie rzeczywistym
16:00 h
01.06.2026 do 02.06.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Szkolenie skierowane jest do: • pracowników wszystkich działów organizacji, którzy na co dzień korzystają z komputera, poczty e-mail, systemów firmowych i przetwarzają informacje lub dane • osób pracujących zdalnie i hybrydowo oraz użytkowników urządzeń mobilnych w środowisku służbowym • kadry kierowniczej i liderów zespołów odpowiedzialnych za organizację pracy i egzekwowanie zasad bezpieczeństwa • pracowników administracji, finansów, HR, sprzedaży, obsługi klienta oraz innych stanowisk szczególnie narażonych na phishing i socjotechnikę • osób odpowiedzialnych za obieg dokumentów i przetwarzanie danych osobowych oraz informacji poufnych • nowych pracowników oraz osób wymagających ujednolicenia wiedzy i dobrych praktyk w zakresie cyberbezpieczeństwa
Minimalna liczba uczestników	5
Maksymalna liczba uczestników	20
Data zakończenia rekrutacji	25-05-2026
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

Celem edukacyjnym szkolenia jest podniesienie świadomości cyberbezpieczeństwa oraz rozwinięcie umiejętności rozpoznawania zagrożeń (np. phishing, malware) i właściwego reagowania na incydenty. Uczestnicy nauczą się bezpiecznej pracy z danymi i systemami, stosowania dobrych praktyk (hasła, MFA, praca zdalna) oraz przestrzegania procedur i zasad ochrony informacji w organizacji.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Rozumie podstawowe zagrożenia cybernetyczne i potrafi je identyfikować	poprawnie rozpoznaje typy ataków (phishing, ransomware, malware, socjotechnika) na przykładach oraz wskazuje cechy podejrzanych wiadomości w teście/ćwiczeniu.	Test teoretyczny
Zna zasady bezpiecznej pracy z danymi i informacjami	wskazuje poprawne sposoby przetwarzania i ochrony danych (w tym osobowych i poufnych) oraz unika typowych błędów w zadaniu scenariuszowym.	Test teoretyczny z wynikiem generowanym automatycznie
Potrafi stosować dobre praktyki cyberbezpieczeństwa w codziennej pracy	demonstruje prawidłowe nawyki: silne hasła, MFA, bezpieczne korzystanie z poczty i internetu, aktualizacje, praca z dokumentami; potwierdzone checklistą lub zadaniem praktycznym.	Test teoretyczny z wynikiem generowanym automatycznie
Zna podstawy normy ISO/IEC 27001	wyjaśnia, czym jest SZBI, jakie są role polityk i procedur oraz wskazuje przykłady zastosowania w organizacji w krótkim teście lub dyskusji.	Test teoretyczny z wynikiem generowanym automatycznie
Wie, jak reagować na incydenty bezpieczeństwa	poprawnie opisuje kroki postępowania, kanały zgłaszania i działania po incydencie na podstawie case study lub symulacji.	Test teoretyczny z wynikiem generowanym automatycznie
Zwiększa świadomość zagrożeń w środowisku cyfrowym	identyfikuje ryzyka w codziennych sytuacjach (praca zdalna, Wi-Fi, urządzenia mobilne), proponuje działania zapobiegawcze oraz uzyskuje wymagany wynik w teście końcowym.	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

Celem szkolenia jest zwiększenie świadomości cyberbezpieczeństwa pracowników oraz przygotowanie ich do bezpiecznego i odpowiedzialnego korzystania z danych, systemów i narzędzi cyfrowych. Szkolenie rozwija umiejętność identyfikowania zagrożeń, stosowania dobrych praktyk ochrony informacji oraz właściwego reagowania na incydenty bezpieczeństwa w codziennej pracy organizacji.

Korzyści dla uczestników szkolenia:

- zwiększenie świadomości zagrożeń cybernetycznych i ich wpływu na pracę oraz bezpieczeństwo organizacji
- umiejętność rozpoznawania prób phishingu, ataków socjotechnicznych i innych zagrożeń cyfrowych
- nabycie praktycznych nawyków bezpiecznej pracy z danymi i informacjami
- lepsze zrozumienie odpowiedzialności pracownika w zakresie ochrony danych i bezpieczeństwa informacji
- znajomość podstawowych zasad reagowania na incydenty bezpieczeństwa
- większa pewność w korzystaniu z narzędzi cyfrowych, pracy zdalnej i urządzeń mobilnych
- ograniczenie ryzyka błędów użytkownika prowadzących do naruszeń bezpieczeństwa

Interaktywna forma zdalna:

Szkolenie prowadzone jest w formule zdalnej, w czasie rzeczywistym, za pośrednictwem platformy Zoom. Taka forma umożliwia uczestnictwo z dowolnego miejsca, redukując koszty oraz czas związany z dojazdem. Zajęcia mają charakter interaktywny – uczestnicy mają dostęp do funkcji wideokonferencji, współdzielenia ekranu oraz czatu, co sprzyja bieżącej komunikacji z prowadzącym i innymi uczestnikami szkolenia.

Godziny realizacji szkolenia:

- Szkolenie obejmuje 16 godzin edukacyjnych tj. 12 godzin zegarowych.
- Każda godzina szkolenia obejmuje 45 minut.
- Przerwy nie są wliczone w czas trwania usługi.

Metody pracy:

Zajęcia w ramach kursu realizowane są w formie interaktywnych wykładów z elementami prezentacji na żywo oraz współdzielenia ekranu. Uczestnicy biorą aktywny udział zarówno w pracy indywidualnej, jak i zespołowej, wykonując ćwiczenia praktyczne oparte na rzeczywistych przypadkach projektowych. Istotnym elementem procesu dydaktycznego jest uczestnictwo w dyskusjach oraz samodzielna analiza materiałów, co umożliwia skuteczne przyswojenie wiedzy i rozwój praktycznych umiejętności.

Dostosowanie kursu do potrzeb osób ze szczególnymi wymaganiami

- **Pomoc techniczna**: Uczestnicy, którzy napotykają trudności z korzystaniem z platformy szkoleniowej lub dostępem do materiałów, mogą liczyć na wsparcie techniczne.

- **Interaktywne sesje pytań i odpowiedzi**: Organizujemy spotkania Q&A, w trakcie których uczestnicy mogą zadawać pytania na żywo – również za pośrednictwem czatu tekstowego, co jest szczególnie przydatne dla osób mających trudności z komunikacją werbalną.
- **Szkolenie na platformie ZOOM**: Szkolenie odbywa się na platformie ZOOM, która spełnia międzynarodowe standardy dostępności, w tym wytyczne WCAG 2.1.
- **Indywidualne tempo nauki**: Program szkolenia uwzględnia elastyczny harmonogram, co pozwala dostosować tempo pracy do indywidualnych potrzeb uczestników.

Certyfikat ukończenia:

Certyfikat ukończenia kursu - 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).

Weryfikacja efektów uczenia się:

Ocena efektów uczenia się odbywa się poprzez test wiedzy przeprowadzany dwukrotnie – na początku oraz na zakończenie szkolenia. Umożliwia to zmierzenie postępów uczestników oraz sprawdzenie stopnia przyswojenia wiedzy i umiejętności. Taka forma weryfikacji potwierdza gotowość do praktycznego wykorzystania zdobytych kompetencji.

Program szkolenia:

Moduł 1. Wprowadzenie do cyberbezpieczeństwa i bezpieczeństwa informacji

- podstawowe pojęcia z zakresu cyberbezpieczeństwa
- cyberbezpieczeństwo a bezpieczeństwo informacji
- aktualne trendy i zagrożenia w środowisku cyfrowym
- odpowiedzialność pracowników i organizacji za ochronę danych

Moduł 2. Zagrożenia cybernetyczne w praktyce

- rodzaje ataków cybernetycznych (phishing, ransomware, malware, ataki socjotechniczne)
- identyfikacja podejrzanych wiadomości i prób wyłudzeń
- analiza rzeczywistych przykładów incydentów bezpieczeństwa
- najczęstsze błędy użytkowników prowadzące do naruszeń bezpieczeństwa

Moduł 3. Ochrona danych i informacji w organizacji

- zasady bezpiecznego przetwarzania danych
- ochrona danych osobowych i poufnych informacji
- dobre praktyki w zakresie pracy z dokumentami elektronicznymi
- bezpieczeństwo informacji w systemach informatycznych

Moduł 4. Zarządzanie ryzykiem w cyberbezpieczeństwie

- identyfikacja i analiza ryzyk związanych z bezpieczeństwem informacji
- ocena skutków incydentów bezpieczeństwa
- metody minimalizacji ryzyka
- rola pracowników w procesie zarządzania ryzykiem

Moduł 5. Standardy i normy bezpieczeństwa informacji

- wprowadzenie do normy ISO/IEC 27001
- system zarządzania bezpieczeństwem informacji (SZBI)
- polityki bezpieczeństwa i procedury
- dobre praktyki wdrażania standardów w organizacji

Moduł 6. Bezpieczna praca zdalna i mobilna

- zagrożenia związane z pracą zdalną i hybrydową
- bezpieczne korzystanie z sieci Wi-Fi i urządzeń mobilnych
- ochrona danych poza siedzibą firmy
- dobre praktyki pracy zdalnej z punktu widzenia cyberbezpieczeństwa

Moduł 7. Hasła, dostęp i uwierzytelnianie

- zasady tworzenia i zarządzania silnymi hasłami
- uwierzytelnianie wieloskładnikowe (MFA)
- zarządzanie dostępami i uprawnieniami

- ochrona kont użytkowników

Moduł 8. Reagowanie na incydenty bezpieczeństwa

- czym jest incydent bezpieczeństwa
- procedury reagowania na incydenty
- zgłaszanie naruszeń i podejrzanych zdarzeń
- działania po incydencie i zapobieganie podobnym sytuacjom w przyszłości

Moduł 9. Świadomość bezpieczeństwa i dobre praktyki użytkownika

- budowanie świadomości cyberbezpieczeństwa w organizacji
- odpowiedzialne korzystanie z technologii cyfrowych
- rola człowieka jako najsłabszego i jednocześnie kluczowego ogniwa bezpieczeństwa
- kształtowanie bezpiecznych nawyków w pracy z danymi

Moduł 10. Warsztaty praktyczne i podsumowanie

- analiza studiów przypadków
- ćwiczenia praktyczne z identyfikacji zagrożeń
- omówienie dobrych i złych praktyk
- podsumowanie szkolenia i rekomendacje do wdrożenia w organizacji

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	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

W ramach przygotowania do szkolenia uczestnicy otrzymają materiały dydaktyczne w formie elektronicznej. Zostaną one przesłane w postaci plików i dokumentów (np. PDF, prezentacje, arkusze informacyjne) przed rozpoczęciem szkolenia, aby umożliwić wcześniejsze zapoznanie się z treściami.

Celem udostępnienia materiałów przed szkoleniem jest:

- ułatwienie wstępnego zrozumienia omawianych zagadnień,
- zwiększenie efektywności udziału w szkoleniu,
- umożliwienie uczestnikom przygotowania ewentualnych pytań lub refleksji,
- zapewnienie dostępu do niezbędnych materiałów również po zakończeniu spotkania.

Materiały będą wysyłane na podane wcześniej adresy e-mail uczestników. Prosimy o upewnienie się, że wiadomości nie trafiają do folderu SPAM oraz o zapisanie plików na własnych urządzeniach przed szkoleniem.

Informacje dodatkowe

Kluczowe elementy organizacyjne oraz etapy uczestnictwa w kursie:

- **Dostęp do platformy e-learningowej** – każdy uczestnik otrzyma indywidualny dostęp do zasobów szkoleniowych dostępnych online.
- **Test wstępny** – szkolenie rozpocznie się od krótkiego testu diagnozującego poziom wiedzy uczestników, co umożliwi lepsze dostosowanie treści i tempa nauki.
- **Prezentacje na żywo** – trener prowadzi interaktywne sesje online, w trakcie których omawia kluczowe zagadnienia i odpowiada na pytania uczestników.
- **Zadania praktyczne** – uczestnicy realizują ćwiczenia związane z tematyką szkolenia; każde zadanie jest oceniane przez prowadzącego.
- **Egzamin końcowy** – po zakończeniu wszystkich modułów uczestnicy przystępują do testu końcowego weryfikującego poziom opanowania materiału.

Warunki techniczne

Szkolenie odbędzie się na platforma zoom.

Warunki techniczne szkolenia na platformie Zoom:

1. Sprzęt komputerowy:
   - Wymagany komputer z dostępem do internetu wraz z kamerą oraz kamerą.
2. Przeglądarka internetowa
   - Zalecane przeglądarki: Google Chrome, Mozilla Firefox, Safari.
3. Stabilne połączenie internetowe:
4. Platforma Zoom:
   - Konieczne pobranie i zainstalowanie najnowszej wersji aplikacji Zoom przed szkoleniem.
   - Aktywne konto Zoom (możliwość utworzenia bezpłatnego konta).
5. Dźwięk i słuchawki:
   - Zalecane użycie słuchawek z mikrofonem dla lepszej jakości dźwięku.
   - Sprawdzenie działania dźwięku przed rozpoczęciem szkolenia.
6. Przygotowanie przed sesją:
   - Testowanie sprzętu i połączenia przed planowanym szkoleniem.
   - Zapewnienie cichego miejsca pracy dla minimalizacji zakłóceń.

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

Kontakt

Anna Mirosław

E-mail szkolenia.lublin@kursor.edu.pl
Telefon (+48) 531 191 181