Industry 4.0 Upskilling For SMEs

Co-funded by the European Union

SZKOLENIA DLA KADRY ZARZĄDZAJĄCEJ I PRACOWNIKÓW MAŁYCH I ŚREDNICH PRZEDSIĘBIORSTW

MODUŁ 2

BEZPIECZEŃSTWO DANYCH

30H
Godziny nauki

Hybrydowa
Forma szkolenia

Mikro-poświadczenia
Certyfikacja

BEZPŁATNE SZKOLENIE

OPIS MODUŁU

Moduł ten zawiera podstawowe wskazówki dotyczące ustanawiania, wdrażania, utrzymywania i ciągłego doskonalenia bezpieczeństwa informacji. Celem jest zapewnienie pracownikom zrozumienia typowych zagrożeń bezpieczeństwa oraz sposobów unikania ryzyka i postępowania w przypadku incydentów związanych z bezpieczeństwem. Świadomość jest kluczem do bezpieczeństwa informacji w organizacji. Próby phishingu i oszustw są podejmowane codziennie, dlatego ważne jest, aby zidentyfikować złośliwych aktorów.

Po ukończeniu tego modułu będziesz w stanie zrozumieć zasady i instrukcje bezpieczeństwa swojej firmy, rozpoznawać próby phishingu, mieć podstawową wiedzę na temat przepisów dotyczących ochrony danych i uczestniczyć w rozwijaniu bezpieczeństwa informacji w swojej organizacji.

SKONTAKTUJ SIĘ Z NAMI

i4u.project@ui1.es

i4u.eu

ceei BURGOS · Universidad Isabel I · OLEMISEN BALANSSIA RY · SIEA SLOVAK INNOVATION AND ENERGY AGENCY · WSEI University · RASEKO · Prios

Industry 4.0 Upskilling For SMEs

Co-funded by the European Union

SZKOLENIA DLA KADRY ZARZĄDZAJĄCEJ I PRACOWNIKÓW MAŁYCH I ŚREDNICH PRZEDSIĘBIORSTW

MODUŁ 2

BEZPIECZEŃSTWO DANYCH

Bezpieczeństwo informacji i danych to praktyka ochrony informacji poprzez zmniejszenie ryzyka związanego z informacjami i ochronę informacji cyfrowych przed nieautoryzowanym użyciem, uszkodzeniem lub kradzieżą przez cały cykl ich życia. Informacje są najcenniejszym zasobem organizacji.

DEFINICJA BEZPIECZEŃSTWA INFORMACJI

- **Poufność**
- **Niezaprzeczalność**
- **Dostępność**
- **Integralność**
- **Kontrola dostępu**

WARSZTATY DOTYCZĄCE BEZPIECZEŃSTWA DANYCH

- **Warsztat pracownika biurowego**
- **Warsztat dla profesjonalistów IT**
- **Warsztaty dla kierownictwa**

OCHRONA DANYCH

Ochrona danych to szerokie pojęcie, które obejmuje różnorodne praktyki, technologie i strategie mające na celu ochronę poufnych informacji przed uszkodzeniem, utratą lub zniszczeniem.

- Zagrożenia dla poufności ze strony sztucznej inteligencji
- Prawa krajowe
- PIR (pasywna podczerwień)
- EGDPR
- Wymagania biznesowe

Typowe zagrożenia bezpieczeństwa danych

- **Phishing**
- **Słabe hasła**
- **Naruszenie danych**
- **Utrata danych**
- **Złośliwe oprogramowanie**
- **Aktywność hakerów**
- **Wrażliwość**
- **Niewłaściwa obsługa**
- **Problemy ze sprzętem**
- **Ataki na usługi**

ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI

Rola kierownictwa jest kluczowa w zarządzaniu bezpieczeństwem danych. Ważne jest, aby kierownictwo rozumiało aktualny stan bezpieczeństwa informacji i identyfikowało potencjalne zagrożenia bezpieczeństwa.

ceei BURGOS · Universidad Isabel I · OLEMISEN BALANSSIA RY · SIEA SLOVAK INNOVATION AND ENERGY AGENCY · WSEI University · RASEKO · Prios