Możliwość dofinansowania

REA Sp. z o.o.

Brak ocen dla tego dostawcy

"Cyberbezpieczeństwo w organizacji aspekt prawny i praktyczny"

Numer usługi 2024/12/02/162530/2444839

1 000,00 PLN brutto
1 000,00 PLN netto
100,00 PLN brutto/h
100,00 PLN netto/h

zdalna w czasie rzeczywistym
Usługa szkoleniowa
10 h
18.03.2025 do 18.03.2025

Informacje podstawowe

Kategoria	Prawo i administracja / Administracja publiczna
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Grupa docelowa dla usługi "Cyberbezpieczeństwo w organizacji: aspekt prawny i praktyczny" obejmuje pracowników firm i organizacji na różnych szczeblach, od operacyjnych po menedżerskie, którzy mają kontakt z technologią i danymi. Szkolenie jest również dedykowane specjalistom IT i administracji systemami, odpowiedzialnym za zarządzanie bezpieczeństwem infrastruktury. Kadra zarządzająca i właściciele firm, a także osoby odpowiedzialne za ochronę danych osobowych (np. inspektorzy ochrony danych), również skorzystają z kursu. Działy compliance i audytów wewnętrznych, odpowiedzialne za przestrzeganie regulacji, także są grupą docelową. Szkolenie jest także odpowiednie dla freelancerów i osób pracujących zdalnie, które muszą dbać o bezpieczeństwo swoich urządzeń i danych.
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	8
Data zakończenia rekrutacji	11-03-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	10
Podstawa uzyskania wpisu do BUR	Certyfikat ICVC - SURE (Standard Usług Rozwojowych w Edukacji): Norma zarządzania jakością w zakresie świadczenia usług rozwojowych

Cel

Cel edukacyjny

Celem szkolenia jest podniesienie świadomości uczestników na temat zagrożeń cybernetycznych oraz metod ochrony, takich jak zarządzanie hasłami i rozpoznawanie phishingu. Uczestnicy poznają także przepisy prawne, takie jak RODO, oraz procedury reagowania na incydenty bezpieczeństwa. Szkolenie ma na celu wyposażenie pracowników w praktyczne umiejętności wdrażania zasad cyberbezpieczeństwa w organizacji, minimalizując ryzyko ataków.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Rozpoznawanie i reagowanie na zagrożenia cybernetyczne, takie jak phishing i ransomware.	Sprawdzian wiedzy uczestników na temat zagrożeń cybernetycznych i metod ochrony (np. phishing, ransomware).	Wywiad swobodny
Umiejętność tworzenia i zarządzania silnymi hasłami oraz korzystania z menedżerów haseł.	Wykonanie symulacji ataków phishingowych i prawidłowe rozpoznanie zagrożeń.	Debata swobodna
Zastosowanie zasad bezpiecznego korzystania z urządzeń mobilnych, komputerów i Wi-Fi.	Tworzenie silnych haseł i poprawne korzystanie z menedżera haseł.	Debata swobodna
Wiedza na temat przepisów prawnych związanych z ochroną danych osobowych (np. RODO).	Ocena reakcji uczestników na incydenty cyberbezpieczeństwa w organizacji.	Wywiad swobodny
Umiejętność reagowania na incydenty cyberbezpieczeństwa w organizacji.	Sprawdzanie zgodności działań uczestników z zasadami bezpiecznego korzystania z technologii.	Wywiad swobodny
Zastosowanie polityk i procedur bezpieczeństwa IT w codziennej pracy organizacji.	Sprawdzenie umiejętności uczestników w zakresie tworzenia i wdrażania polityk bezpieczeństwa IT.	Wywiad swobodny

Cel biznesowy

Celem biznesowym jest przeprowadzenie szkolenia z zakresu cyberbezpieczeństwa, które ma na celu poprawę poziomu bezpieczeństwa w organizacji. Szkolenie powinno przyczynić się do zmniejszenia liczby incydentów związanych z cyberzagrożeniami. Cel jest szczegółowy i mierzalny poprzez ocenę liczby incydentów przed i po szkoleniu. Zrealizowanie celu jest realistyczne, biorąc pod uwagę dostępne zasoby i wsparcie organizacji. Sukces będzie mierzony na podstawie poprawy wyników związanych z bezpieczeństwem w organizacji.

Efekt usługi

Po zakończeniu szkolenia uczestnicy będą w stanie skutecznie rozpoznawać zagrożenia cybernetyczne, stosować zasady bezpiecznego korzystania z technologii oraz wdrażać procedury ochrony danych i reagowania na incydenty w organizacji.

Kryteria weryfikacji:

1. **Sprawdzenie wiedzy** – Sprawdzian wiedzy uczestników na temat zagrożeń cybernetycznych i metod ochrony (np. phishing, ransomware).
2. **Ćwiczenia praktyczne** – Wykonanie symulacji ataków phishingowych i prawidłowe rozpoznanie zagrożeń przez uczestników.
3. **Analiza haseł** – Ocenienie umiejętności uczestników w tworzeniu silnych haseł i korzystaniu z menedżera haseł.
4. **Studium przypadku** – Ocena reakcji uczestników na incydenty cyberbezpieczeństwa w organizacji.
5. **Ocena przestrzegania procedur** – Sprawdzenie, czy uczestnicy wdrażają procedury ochrony danych i reagowania na incydenty.
6. **Ocena implementacji polityk bezpieczeństwa** – Weryfikacja umiejętności uczestników w zakresie tworzenia i wdrażania polityk bezpieczeństwa IT w organizacji.

Metoda potwierdzenia osiągnięcia efektu usługi

Metoda potwierdzenia osiągnięcia efektu usługi:

1. **Egzamin końcowy** – Przeprowadzenie sprawdzianu wiedzy, który oceni zrozumienie przez uczestników zagrożeń cybernetycznych, metod ochrony danych, zasad bezpiecznego korzystania z technologii oraz procedur reagowania na incydenty.
2. **Symulacje praktyczne** – Zorganizowanie symulacji phishingu oraz innych scenariuszy cyberzagrożeń, które pozwolą ocenić zdolność uczestników do prawidłowego rozpoznawania zagrożeń i reagowania na nie w czasie rzeczywistym.
3. **Analiza wdrożonych polityk bezpieczeństwa** – Ocena dokumentacji i procedur opracowanych przez uczestników, aby potwierdzić, że potrafią wdrożyć zasady bezpieczeństwa w swojej organizacji.
4. **Feedback i ocena ze strony przełożonych** – Zbieranie opinii od menedżerów lub liderów zespołów na temat poprawy zachowań związanych z bezpieczeństwem cyfrowym po zakończeniu szkolenia.

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?

Tak, dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się.

Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?

Tak, dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji.

Pytanie 3. Czy dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

Tak, dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji.

Program

Program szkolenia:

1. Wprowadzenie do Cyberbezpieczeństwa

• Co to jest cyberbezpieczeństwo?

• Definicja i znaczenie w kontekście organizacji.

• Przykłady zagrożeń cybernetycznych: phishing, ransomware, ataki DDoS.

• Koszty naruszeń bezpieczeństwa:

• Straty finansowe, wizerunkowe i prawne.

• Przykłady rzeczywistych incydentów.

2. Najczęstsze Zagrożenia i Metody Ochrony

• Phishing i socjotechnika:

• Rozpoznawanie podejrzanych e-maili, linków i załączników.

• Przykłady ataków opartych na manipulacji ludźmi.

• Bezpieczne korzystanie z Internetu:

• Rozpoznawanie fałszywych stron internetowych.

• Zasady ochrony tożsamości w sieci.

• Bezpieczne hasła:

• Tworzenie i zarządzanie silnymi hasłami.

• Wprowadzenie do menedżerów haseł.

• Zagrożenia wewnętrzne:

• Przypadkowe działania pracowników.

• Celowe działania osób z wewnątrz organizacji.

3. Zasady Bezpiecznego Korzystania z Technologii IT

• Urządzenia służbowe i prywatne:

• Bezpieczne korzystanie z urządzeń mobilnych i laptopów.

• Zasady pracy zdalnej i korzystania z Wi-Fi.

• Oprogramowanie i aktualizacje:

• Znaczenie regularnych aktualizacji systemów i aplikacji.

• Zagrożenia wynikające z korzystania z nieautoryzowanego oprogramowania.

• Ochrona danych organizacji:

• Klasyfikacja i zasady przetwarzania danych wrażliwych.

• Szyfrowanie i kopie zapasowe.

4. Symulacje i Warsztaty Praktyczne

• Symulacje phishingu:

• Praktyczne ćwiczenia w rozpoznawaniu podejrzanych e-maili i zachowania w przypadku ich otrzymania.

• Testowanie haseł:

• Warsztat tworzenia silnych haseł i nauka korzystania z menedżerów haseł.

• Symulacja incydentu:

• Ćwiczenia z reagowania na potencjalny atak (np. włamanie do systemu, zgubiony laptop).

• Wprowadzenie do podstawowych narzędzi IT:

• Szyfrowanie e-maili.

• Użycie VPN.

5. Polityki Cyberbezpieczeństwa w Organizacji

• Omówienie polityk organizacji:

• Procedury zgłaszania incydentów.

• Zasady użytkowania urządzeń firmowych i systemów IT.

• Przestrzeganie przepisów prawnych:

• GDPR/RODO i inne przepisy dotyczące ochrony danych.

6. Podsumowanie i Sesja Pytań

• Powtórzenie kluczowych zasad.

• Pytania uczestników i dyskusja.

• Przekazanie materiałów szkoleniowych i checklisty bezpieczeństwa.

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	1 000,00 PLN
Koszt przypadający na 1 uczestnika netto	1 000,00 PLN
Koszt osobogodziny brutto	100,00 PLN
Koszt osobogodziny netto	100,00 PLN

Prowadzący

Liczba prowadzących: 0

Brak wyników.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały dydaktyczne będą mieć formę:

- papierową w formie skryptu oraz notatek
- prezentacji multimedialnej
- certyfikat ukończenia szkolenia

Warunki uczestnictwa

Warunkiem niezbędnym do spełnienia przez uczestników, aby realizacja usługi pozwoliła na osiągnięcie głównego celu jest aktywność oraz obecność na szkoleniu.

Warunki techniczne

Szkolenie prowadzone będzie na pltformie Clickmeeting. Prezenterzy oraz uczestnicy nie muszą tworzyć konta, aby dołączyć do szkolenia. Mogą zostać zaproszeni do wydarzenia poprzez e-mail z linkiem przekierowującym do pokoju edukacyjnego. Platforma oparta jest na przeglądarce, wymagane zatem jest korzystanie z Google Chrome, Mozilla Firefox, Safari, Edge (Chromium), Yandex lub Opera.Platforma współpracuje z wszystkimi wbudowanymi w laptopy kamerami oraz większością kamer internetowych.

Kontakt

Małgorzata Bucka

E-mail rea.biurozarzadu@gmail.com

Telefon (+48) 789 574 344