Możliwość dofinansowania

QMSSolutions
Aneta Gaik

Brak ocen dla tego dostawcy

Cyberbezpieczeństwo w organizacji – ochrona informacji i danych zgodnie z ISO/IEC 27001 i TISAX

Numer usługi 2025/08/18/159760/2945576

zdalna w czasie rzeczywistym
Usługa szkoleniowa
16 h
25.09.2025 do 26.09.2025

5 000,00 PLN brutto
5 000,00 PLN netto
312,50 PLN brutto/h
312,50 PLN netto/h

Informacje podstawowe

Kategoria	Biznes / Zarządzanie przedsiębiorstwem
Identyfikatory projektów	Regionalny Fundusz Szkoleniowy II
Grupa docelowa usługi	• Pracownicy administracyjni i operacyjni • Osoby przetwarzające dane osobowe i informacje wrażliwe • Kadra kierownicza i menedżerska • Pracownicy IT i administratorzy systemów • Pełnomocnicy ds. bezpieczeństwa informacji i RODO • Osoby zaangażowane w realizację wymagań ISO 27001, TISAX i RODO
Minimalna liczba uczestników	3
Maksymalna liczba uczestników	25
Data zakończenia rekrutacji	24-09-2025
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

Podniesienie świadomości uczestników w zakresie zagrożeń cybernetycznych, utrwalenie praktycznych umiejętności rozpoznawania i reagowania na incydenty oraz zrozumienie roli użytkownika w systemie zarządzania bezpieczeństwem informacji.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Po ukończeniu szkolenia uczestnicy będą: 1. Wiedza: Rozumieć podstawowe pojęcia związane z cyberbezpieczeństwem, takie jak zagrożenia, podatności i ryzyka. Znać strukturę i wymagania norm ISO 27001 i TISAX w zakresie ochrony informacji. Rozumieć procesy zarządzania ryzykiem związanym z cyberbezpieczeństwem. Znać kluczowe elementy polityki bezpieczeństwa informacji. Rozumieć zasady ochrony danych osobowych (RODO) i ich związek z cyberbezpieczeństwem. Znać najlepsze praktyki w zakresie ochrony przed atakami phishingowymi, malware i innymi zagrożeniami. Znać podstawy kryptografii i jej zastosowanie w ochronie danych. Znać wymagania dotyczące bezpieczeństwa w chmurze i zarządzania dostępem.	1. Wiedza: Kryteria: Uczestnik potrafi poprawnie zdefiniować kluczowe pojęcia z zakresu cyberbezpieczeństwa (np. zagrożenie, podatność, ryzyko). Uczestnik potrafi wymienić i omówić główne elementy norm ISO 27001 i TISAX. Uczestnik potrafi zidentyfikować i wyjaśnić etapy procesu zarządzania ryzykiem. Uczestnik potrafi zdefiniować cele i elementy polityki bezpieczeństwa informacji. Uczestnik potrafi wymienić i wyjaśnić zasady ochrony danych osobowych (RODO). Uczestnik potrafi wskazać przykłady zagrożeń i skutecznych metod ochrony przed nimi (phishing, malware). Uczestnik potrafi wyjaśnić podstawowe pojęcia kryptografii i jej zastosowanie. Uczestnik potrafi wymienić i omówić kluczowe aspekty bezpieczeństwa w chmurze i zarządzania dostępem. Co Uczestnik Powinien Zrobić/Powiedzieć/Pokazać Trenerowi: Powiedzieć: Poprawnie zdefiniować pojęcia na pytania trenera, zacytować odpowiednie fragmenty norm. Zrobić: Uczestniczyć aktywnie w dyskusjach, odpowiadać na pytania testowe i quizy. Pokazać: Prezentować w praktyce zrozumienie pojęć na podstawie analizy case studies.	Test teoretyczny z wynikiem generowanym automatycznie

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Po ukończeniu szkolenia uczestnicy będą: 2. Umiejętności: Identyfikować i oceniać ryzyko związane z cyberbezpieczeństwem w swojej organizacji. Opracowywać i wdrażać polityki i procedury bezpieczeństwa informacji. Wdrażać środki techniczne i organizacyjne chroniące dane i systemy. Przeprowadzać audyty wewnętrzne w zakresie cyberbezpieczeństwa. Reagować na incydenty związane z bezpieczeństwem informacji. Szkolić pracowników w zakresie cyberbezpieczeństwa. Korzystać z narzędzi i technologii do ochrony danych. Oceniać zgodność z normami ISO 27001 i TISAX.	2. Umiejętności: Kryteria: Uczestnik potrafi zidentyfikować i ocenić ryzyko cyberbezpieczeństwa w symulowanym scenariuszu. Potrafi opracować fragment polityki bezpieczeństwa informacji dla danego przypadku. Potrafi wskazać i omówić środki techniczne i organizacyjne, które można zastosować w celu ochrony danych. Potrafi przeprowadzić symulację audytu wewnętrznego dla wybranego obszaru. Potrafi opisać procedurę reagowania na incydent bezpieczeństwa w symulowanym przypadku. Uczestnik potrafi przygotować krótkie szkolenie dla pracowników w zakresie bezpieczeństwa. Uczestnik potrafi zidentyfikować potencjalne luki w zabezpieczeniach w symulowanym środowisku. Uczestnik potrafi ocenić zgodność z wybranymi wymaganiami ISO 27001 lub TISAX w symulowanym scenariuszu.	Test teoretyczny z wynikiem generowanym automatycznie

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Po ukończeniu szkolenia uczestnicy będą: 3. Kompetencje Społeczne: Zwiększona świadomość zagrożeń związanych z cyberbezpieczeństwem i ich wpływu na organizację. Umiejętność współpracy w zespole w zakresie wdrażania i utrzymywania systemów bezpieczeństwa. Umiejętność komunikowania się na temat cyberbezpieczeństwa z różnymi grupami interesariuszy. Umiejętność promowania kultury bezpieczeństwa w organizacji. Odpowiedzialność za ochronę danych i informacji. Kreatywne podejście do rozwiązywania problemów związanych z cyberbezpieczeństwem. Gotowość do ciągłego uczenia się i doskonalenia w obszarze cyberbezpieczeństwa. Etyczne podejście do kwestii ochrony danych i prywatności.	3. Kompetencje Społeczne: Kryteria: Uczestnik wykazuje świadomość zagrożeń i ich wpływu na organizację. Uczestnik potrafi efektywnie współpracować z innymi uczestnikami w grupowych ćwiczeniach. Uczestnik potrafi jasno i zrozumiale komunikować się na tematy związane z cyberbezpieczeństwem. Uczestnik przejawia proaktywną postawę w kwestiach bezpieczeństwa. Uczestnik wykazuje odpowiedzialność za ochronę danych i informacji. Uczestnik wykazuje się kreatywnością w rozwiązywaniu problemów. Uczestnik wyraża chęć do dalszego uczenia się i doskonalenia. Uczestnik respektuje zasady etyki w zakresie ochrony danych. Co Uczestnik Powinien Zrobić/Powiedzieć/Pokazać Trenerowi: Powiedzieć: Aktywnie uczestniczyć w dyskusjach, wyrażać swoje opinie, zadawać pytania. Zrobić: Współpracować w grupie, brać aktywny udział w ćwiczeniach, prezentować wyniki pracy zespołowej. Pokazać: Wykazać się zaangażowaniem w trakcie szkolenia, dbać o rzetelność wykonywanych zadań, wykazywać szacunek dla innych uczestników.	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

Program szkolenia:

Wprowadzenie do cyberbezpieczeństwa

• Definicje, podstawowe pojęcia i zagrożenia

• Znaczenie cyberbezpieczeństwa dla organizacji

• Powiązania z ISO/IEC 27001, TISAX i RODO

Zagrożenia cybernetyczne i typy ataków

• Malware (wirusy, trojany, ransomware, spyware)

• Phishing, smishing, vishing

• Inżynieria społeczna i manipulacja psychologiczna

• DDoS, MITM (Man-in-the-Middle), kradzież tożsamości

Zasady bezpiecznego korzystania z systemów i danych

• Zarządzanie hasłami (MFA, SSO, menedżery haseł)

• Szyfrowanie danych – podstawy

• Przechowywanie i przesyłanie danych (VPN, e-mail, chmura)

• Zasady ochrony danych osobowych (RODO a cyberbezpieczeństwo)

Środki bezpieczeństwa w codziennej pracy

• Cyberhigiena: e-maile, linki, pliki, aktualizacje

• Urządzenia służbowe i prywatne (BYOD)

• Mobilne zagrożenia (smartfony, tablety)

• Sieci Wi-Fi i praca zdalna – jak chronić organizację

Odpowiedzialność użytkownika i organizacji

• Zakres odpowiedzialności pracownika a pracodawcy

• Rola działu IT i Inspektora Ochrony Danych

• Konsekwencje naruszenia bezpieczeństwa – dyscyplinarne i prawne

• Polityki bezpieczeństwa i instrukcje wewnętrzne

Audyty, oceny ryzyka i reagowanie na incydenty

• Ocena ryzyka (DPIA, ISO 27005)

• Zgłaszanie incydentów i reagowanie

• Scenariusze incydentów – ransomware, phishing

• Ćwiczenia zespołowe: analiza fałszywego e-maila, ryzyko BYOD

Normy i wymagania formalne

• ISO/IEC 27001:2022 – kontekst, wymagania i zabezpieczenia (Załącznik A)

• TISAX – wymagania branży automotive

• RODO – przetwarzanie danych w kontekście cyberzagrożeń

Podsumowanie i wnioski praktyczne

• Dobre praktyki i lista kontrolna

• Narzędzia wspierające bezpieczeństwo

• Rekomendacje dla uczestników po szkoleniu

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	5 000,00 PLN
Koszt przypadający na 1 uczestnika netto	5 000,00 PLN
Koszt osobogodziny brutto	312,50 PLN
Koszt osobogodziny netto	312,50 PLN

Prowadzący

Liczba prowadzących: 0

Brak wyników.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały szkoleniowe w wersji PDF, wydanie e-certyfikatu w formie elektronicznej.

Cena usługi nie obejmuje kosztów niezwiązanych bezpośrednio z usługa rozwojową, w szczególności kosztów środków trwałych przekazywanych Uczestnikom/-czkom projektu, kosztów dojazdu i zakwaterowania.

Usługa rozwojowa nie jest świadczona przez podmiot pełniący funkcję Operatora lub Partnera Operatora w danym projekcie PSF lub w którymkolwiek Regionalnym Programie lub FERS albo przez podmiot powiązany z Operatorem lub Partnerem kapitałowo lub osobowo.

Warunki uczestnictwa

Warunki uczestnictwa

Warunkiem uczestnictwa jest zakwalifikowanie się do programu oraz podpisanie umowy z operatorem i otrzymanie nr ID wsparcia.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały szkoleniowe w wersji PDF, wydanie e-certyfikatu w formie elektronicznej.

Cena usługi nie obejmuje kosztów niezwiązanych bezpośrednio z usługa rozwojową, w szczególności kosztów środków trwałych przekazywanych Uczestnikom/-czkom projektu, kosztów dojazdu i zakwaterowania.

Usługa rozwojowa nie jest świadczona przez podmiot pełniący funkcję Operatora lub Partnera Operatora w danym projekcie PSF lub w którymkolwiek Regionalnym Programie lub FERS albo przez podmiot powiązany z Operatorem lub Partnerem kapitałowo lub osobowo.

Warunki techniczne

Usługa zdalna w czasie rzeczywistym.

Warunki techniczne niezbędne do udziału w usłudze:

1. przed szkoleniem uczestnik otrzymuje linki, które pozwolą dołączyć do szkolenia w aplikacji TEAMS
2. sprzęt - komputer z łączem internetowym;
3. minimalne wymagania systemowe - macOS X z systemem macOS 10.7 lub nowszym lub Windows XP lub nowszy;
4. minimalne wymagania dotyczące parametrów łącza sieciowego - szerokopasmowe przewodowe lub bezprzewodowe (3G lub 4G/LTE);
5. wymagania urządzeń audio/wideo

- głośniki i mikrofon (wbudowane lub podłączane na USB lub bezprzewodowe bluetooth)
- kamera internetowa lub kamera internetowa HD (wbudowana lub podłączana na USB lub, kamera video HD lub HD z kartą przechwytywania wideo);

1. zalecane przeglądarki - Microsoft Edge 38.14393.0.0 lub wyższa lub Google Chrome 53.0.2785 lub wyższa;

Okres ważności linku rozpoczyna się na 15 min. przed rozpoczęciem spotkania online i trwa do 15 min. ponad ramowy czas spotkania.

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

Kontakt

Ryszard Budniok

E-mail qmssolutions24@gmail.com

Telefon (+48) 600 831 005