Możliwość dofinansowania

Cyberodporność organizacji: ryzyko, incydenty, backupy i SZBI – dla liderów i IT

Numer usługi 2026/05/12/157622/3553749

2 952,00 PLN brutto
2 400,00 PLN netto
369,00 PLN brutto/h
300,00 PLN netto/h
261,33 PLN cena rynkowa

Grupa WW GovTech sp. z o.o.

4,6 / 5

91 ocen

Bydgoszcz
Usługa szkoleniowa
stacjonarna
Zajęcia grupowe
08:00 h
18.09.2026 do 18.09.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Identyfikatory projektów	Kierunek - Rozwój, Nowy start w Małopolsce z EURESEM, Małopolski Pociąg do kariery, Zachodniopomorskie Bony Szkoleniowe
Grupa docelowa usługi	Szkolenie koncentruje się na **zarządzaniu cyberbezpieczeństwem na poziomie organizacji**, ze szczególnym uwzględnieniem ról decyzyjnych kadry kierowniczej oraz odpowiedzialności zespołów IT. Program obejmuje zarówno aspekty prawno-organizacyjne, jak i techniczne. **Usługa również adresowana dla:** • Uczestników projektu Kierunek-Rozwój • Uczestników projektu Bony rozwojowe • Uczestników Projektu MP oraz dla uczestników projektu NSE • Uczestników Projektu "Małopolski pociąg do kariery i/lub dla Uczestników Projektu "Nowy start w Małopolsce z EURESem". • Uczestników innych Projektów
Minimalna liczba uczestników	10
Maksymalna liczba uczestników	20
Data zakończenia rekrutacji	14-09-2026
Forma prowadzenia usługi	stacjonarna
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 szkolenia jest przygotowanie kadry kierowniczej i IT do planowania i nadzorowania cyberbezpieczeństwa w organizacji: identyfikowania obowiązków (UOKSC/KRI/RODO), priorytetyzacji zagrożeń, wykonywania uproszczonej oceny ryzyka, doboru zasad backupu i ciągłości działania (RTO/RPO), organizacji reagowania na incydenty oraz projektowania podstawowych elementów SZBI.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik wskazuje obowiązki organizacji wynikające z ustawy o krajowym systemie cyberbezpieczeństwa, KRI oraz RODO w kontekście zarządzania bezpieczeństwem informacji.	Poprawnie identyfikuje obowiązki organizacji oraz role odpowiedzialne za bezpieczeństwo informacji.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik rozróżnia najczęstsze zagrożenia cyberbezpieczeństwa występujące w organizacjach oraz wskazuje podstawowe metody ich ograniczania.	Prawidłowo przyporządkowuje przykłady zagrożeń do właściwych obszarów ochrony.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik identyfikuje kluczowe zasoby informacyjne organizacji oraz elementy wpływające na poziom ryzyka bezpieczeństwa informacji.	Poprawnie wskazuje zasoby, zagrożenia i skutki w przykładowych opisach sytuacji.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik definiuje pojęcia RTO i RPO oraz wskazuje zasady planowania kopii zapasowych i ciągłości działania.	Prawidłowo rozróżnia pojęcia RTO i RPO oraz wskazuje właściwe zasady backupu.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik wskazuje podstawowe elementy procedury reagowania na incydenty bezpieczeństwa informacji.	Poprawnie identyfikuje etapy postępowania oraz role w procesie reagowania na incydent.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik wskazuje elementy systemu zarządzania bezpieczeństwem informacji (SZBI) oraz korzyści wynikające z jego wdrożenia.	Prawidłowo identyfikuje elementy SZBI oraz przypisuje im właściwe funkcje organizacyjne.	Test teoretyczny z wynikiem generowanym automatycznie

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem zawierają opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji i zgodnie z zaplanowanymi metodami walidacji?

TAK

Pytanie 3. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Zakres merytoryczny szkolenia

1. Obowiązki organizacji w obszarze cyberbezpieczeństwa

Uczestnicy zapoznają się z kluczowymi obowiązkami wynikającymi z:

- ustawy o krajowym systemie cyberbezpieczeństwa (UOKSC),
- Krajowych Ram Interoperacyjności (KRI),
- RODO w kontekście bezpieczeństwa informacji.

Omówione zostaną role i odpowiedzialności kadry kierowniczej oraz IT, konsekwencje braku zgodności oraz znaczenie dokumentacji i nadzoru nad procesami bezpieczeństwa.

2. Krajobraz zagrożeń i priorytety ochrony

Moduł poświęcony jest identyfikacji **najczęstszych zagrożeń cyberbezpieczeństwa** występujących w organizacjach, w tym:

- incydentów związanych z pocztą elektroniczną i kontami użytkowników,
- zagrożeń wynikających z braku kontroli dostępu,
- podatności infrastrukturalnych i organizacyjnych.

Uczestnicy uczą się **ustalać priorytety zabezpieczeń** w oparciu o realne ryzyko, a nie wyłącznie dostępne technologie.

3. Zarządzanie ryzykiem w bezpieczeństwie informacji

W tej części szkolenia uczestnicy poznają uproszczone, praktyczne podejście do:

- identyfikacji kluczowych zasobów informacyjnych,
- przypisywania zagrożeń i skutków,
- doboru adekwatnych zabezpieczeń organizacyjnych i technicznych.

Moduł koncentruje się na **matrycy ryzyka** jako narzędziu wspierającym decyzje zarządcze i planowanie działań ochronnych.

4. Kopie zapasowe i ciągłość działania

Uczestnicy zapoznają się z zasadami ochrony danych poprzez:

- planowanie kopii zapasowych (backup),
- zasady 3-2-1,
- pojęcia RTO i RPO,
- znaczenie testów odtwarzania danych.

Moduł podkreśla rolę backupów jako elementu **ciągłości działania organizacji**, a nie wyłącznie rozwiązania technicznego.

5. Reagowanie na incydenty i komunikacja kryzysowa

W tej części omawiane są:

- role i odpowiedzialności w procesie reagowania na incydenty,
- podstawowe procedury postępowania w przypadku naruszenia bezpieczeństwa informacji,
- znaczenie komunikacji wewnętrznej i zewnętrznej w sytuacjach kryzysowych.

Uczestnicy poznają elementy, które powinna zawierać procedura reagowania na incydenty z perspektywy organizacyjnej i decyzyjnej.

6. System Zarządzania Bezpieczeństwem Informacji (SZBI)

Moduł poświęcony jest:

- celom i korzyściom wdrożenia SZBI,
- kluczowym elementom systemu (polityki, procedury, role, nadzór),
- organizacji procesu wdrożenia SZBI w organizacji,
- identyfikacji tzw. „quick wins", czyli działań możliwych do szybkiego wdrożenia.

Uczestnicy uzyskują wiedzę pozwalającą **projektować podstawowe elementy SZBI** adekwatnie do skali i potrzeb organizacji.

Metody dydaktyczne

- analiza przypadków (case study),
- warsztat decyzyjny (ryzyko i priorytety),
- praca na checklistach i przykładach dokumentów,
- moderowana dyskusja,
- sesja pytań i odpowiedzi.

Harmonogram

Liczba pozycji harmonogramu: 10

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 10 Obowiązki organizacji w cyberbezpieczeństwie (UOKSC, KRI, RODO)	Zajęcia	BARTOSZ LEŚNIAK	18-09-2026	08:00	08:30	00:30
2 z 10 Krajobraz zagrożeń cyberbezpieczeństwa i priorytety ochrony	Zajęcia	BARTOSZ LEŚNIAK	18-09-2026	08:30	09:30	01:00
3 z 10 Zarządzanie ryzykiem w bezpieczeństwie informacji	Zajęcia	BARTOSZ LEŚNIAK	18-09-2026	09:30	10:45	01:15
4 z 10 -	Przerwa	-	18-09-2026	10:45	11:15	00:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
5 z 10 Kopie zapasowe i ciągłość działania (backup, RTO, RPO)	Zajęcia	BARTOSZ LEŚNIAK	18-09-2026	11:15	12:30	01:15
6 z 10 Reagowanie na incydenty i komunikacja kryzysowa	Zajęcia	BARTOSZ LEŚNIAK	18-09-2026	12:30	13:45	01:15
7 z 10 -	Przerwa	-	18-09-2026	13:45	14:15	00:30
8 z 10 System Zarządzania Bezpieczeństwem Informacji – SZBI	Zajęcia	BARTOSZ LEŚNIAK	18-09-2026	14:15	15:15	01:00
9 z 10 Podsumowanie + Q&A	Zajęcia	BARTOSZ LEŚNIAK	18-09-2026	15:15	15:30	00:15
10 z 10 -	Walidacja	BARTOSZ LEŚNIAK	18-09-2026	15:30	16:00	00:30

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	08:00
w tym suma godzin zajęć	06:30
w tym suma godzin walidacji	00:30
w tym suma przerw	01:00
Suma godzin dydaktycznych bez przerw	09:15

Cennik

Jeżeli korzystasz z dofinansowania i usługa stanowi usługę kształcenia zawodowego lub przekwalifikowania zawodowego wraz z usługą lub dostawą towarów ściśle związaną z usługami kształcenia zawodowego lub przekwalifikowania zawodowego to możesz mieć możliwość skorzystania za zwolnienia z podatku VAT na

podstawie art. 43 ust. 1 pkt 29 lit. c ustawy z dnia 11 marca 2024 r. o podatku od towarów i usług, jeśli usługa w całości jest finansowana ze środków publicznych lub § 3 ust. 1 pkt 14 rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień w przypadku, gdy usługa jest finansowana w co najmniej 70% ze środków publicznych.

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	2 952,00 PLN
Koszt przypadający na 1 uczestnika netto	2 400,00 PLN
Koszt osobogodziny brutto	369,00 PLN
Koszt osobogodziny netto	300,00 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	08:00

Prowadzący

Liczba prowadzących: 1

1 z 1

BARTOSZ LEŚNIAK

Specjalista od zabezpieczeń systemów i sieci komputerowych od ponad 20 lat. Konsultant, szkoleniowiec z cyberbezpieczeństwa. Posiadam uprawnienia audytora wewnętrznego normy ISO27001 i ukończoną specjalizację Cyberbezpieczeństwa i Systemów Zarządzania Bezpieczeństwem Informacji na AGH w Krakowie.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnicy otrzymują:

- prezentację ze szkolenia,
- zaświadczenie o ukończeniu szkolenia.

Warunki uczestnictwa

Wymogi unijne związane z realizacją szkolenia z dofinansowaniem:

- Logowanie się pełnym imieniem i nazwiskiem
- Włączona kamera oraz dostęp do mikrofonu

Niespełnienie powyższych może skutkować brakiem dofinansowania

- Warunkiem uzyskania zaświadczenia jest uczestnictwo w co najmniej 80%- 100% (w zależności od programu dofinansowania i podpisanej umowy z Operatorem) zajęć usługi rozwojowej
- W ramach realizacji usług szkoleniowych, Organizator utrwala wizerunek Uczestników w formie nagrań wideo, fotografii lub innych materiałów audiowizualnych wyłącznie w celach archiwizacyjnych, kontrolnych oraz dokumentacyjnych związanych z projektem dofinansowanym.
- Uczestnik zapisując się na szkolenie wyraża zgodę na utrwalenie i wykorzystanie jego wizerunku w wyżej wymienionych celach.
- Organizator nie udostępnia nagrań Uczestnikom po szkoleniu.

Informacje dodatkowe

Zawarto Umowę z UP Toruń w ramach projektu Kierunek Rozwój

Podstawa zwolnienia z VAT:

1. art. 43 ust. 1 pkt 29 lit. c ustawy o VAT – dofinansowanie 100%,
2. § 3 ust. 1 pkt 14 rozporządzenia MF – dofinansowanie min. 70%,
3. przy dofinansowaniu poniżej 70% do ceny doliczany jest VAT 23%.

Adres

Bydgoszcz 4/-
85-031 Bydgoszcz
woj. kujawsko-pomorskie

Kontakt

ELŻBIETA RACHTAN

E-mail e.rachtan@grupaww.dev
Telefon (+48) 793 123 470