Możliwość dofinansowania

Bezpieczeństwo w świecie cyfrowym – cyberbezpieczeństwo w codziennej pracy

Numer usługi 2026/07/08/157622/3677343

3 321,00 PLN brutto
2 700,00 PLN netto
276,75 PLN brutto/h
225,00 PLN netto/h
284,58 PLN cena rynkowa

Grupa WW GovTech sp. z o.o.

4,6 / 5

91 ocen

- Usługa szkoleniowa
- zdalna w czasie rzeczywistym
- Zajęcia grupowe
- 12:00 h
- 17.09.2026 do 18.09.2026

Informacje podstawowe

Kategoria	Biznes / Zarządzanie przedsiębiorstwem
Identyfikatory projektów	Kierunek - Rozwój, Nowy start w Małopolsce z EURESEM, Małopolski Pociąg do kariery, Zachodniopomorskie Bony Szkoleniowe
Grupa docelowa usługi	Usługa jest skierowana do osób, które w codziennej pracy korzystają z poczty elektronicznej, dokumentów, systemów wewnętrznych, usług online, komunikatorów, chmury lub urządzeń służbowych i mają wpływ na bezpieczeństwo danych oraz informacji w organizacji. W szczególności szkolenie jest przeznaczone dla pracowników administracji publicznej, jednostek samorządu terytorialnego, szkół, uczelni, instytucji kultury, placówek medycznych, organizacji pozarządowych, przedsiębiorstw społecznych oraz firm. Usługa jest odpowiednia także dla osób pracujących z danymi osobowymi, dokumentami, systemami cyfrowymi, ePUAP, systemami dziedzinowymi, chmurą, komunikatorami, urządzeniami mobilnymi oraz dla kadry kierowniczej odpowiedzialnej za organizację pracy i bezpieczeństwo informacji. Nie jest wymagane zaawansowane przygotowanie techniczne. Wymagana jest podstawowa umiejętność obsługi komputera i korzystania z Internetu. **Usługa również adresowana dla uczestników projektów unijnych z dofinansowaniem.**
Minimalna liczba uczestników	2
Maksymalna liczba uczestników	10
Data zakończenia rekrutacji	11-09-2026

Forma prowadzenia usługi	zdalna w czasie rzeczywistym
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 nabycie wiedzy z zakresu cyberbezpieczeństwa w codziennej pracy, rozpoznawania podstawowych cyberzagrożeń, ochrony danych i informacji wrażliwych, zasad bezpiecznego korzystania z poczty, Internetu, komunikatorów, chmury i urządzeń mobilnych, a także zasad reagowania na incydenty bezpieczeństwa oraz ograniczania ryzyka cyfrowego w organizacji i życiu prywatnym.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik rozróżnia podstawowe rodzaje cyberzagrożeń występujących w środowisku cyfrowym.	Identyfikuje cechy phishingu, ransomware, malware, spyware, ataków DDoS i ataków socjotechnicznych oraz przyporządkowuje zagrożenia do opisanych sytuacji.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik rozpoznaje cechy podejrzanej komunikacji elektronicznej.	Wskazuje elementy wiadomości e-mail, SMS, linku, załącznika, domeny lub nadawcy, które mogą świadczyć o próbie oszustwa lub naruszenia bezpieczeństwa.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik wskazuje zasady higieny cyfrowej i zabezpieczania kont użytkowników.	Dobiera właściwe zasady bezpieczeństwa do wskazanych przypadków użycia, w tym silne hasła, uwierzytelnianie dwuskładnikowe, aktualizacje, kopie zapasowe, bezpieczne korzystanie z nośników danych i chmury.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik rozróżnia zasady bezpiecznego korzystania z poczty, Internetu, komunikatorów, wideokonferencji i urządzeń mobilnych.	Identyfikuje dobre praktyki dotyczące przesyłania plików, udostępniania linków, korzystania z publicznych sieci Wi-Fi, VPN, komunikatorów, wideokonferencji i urządzeń służbowych.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik określa działania podejmowane w przypadku incydentu bezpieczeństwa.	Porządkuje podstawowe kroki reagowania na incydent, wskazuje właściwe osoby lub jednostki do powiadomienia oraz rozpoznaje działania, których należy unikać po wykryciu incydentu.	Test teoretyczny z wynikiem generowanym automatycznie

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik rozpoznaje zasady ochrony danych osobowych i informacji wrażliwych.	Wskazuje przykłady ryzyk związanych z ujawnieniem danych, rozpoznaje sytuacje mogące prowadzić do naruszenia ochrony danych oraz identyfikuje podstawowe działania ograniczające skutki takiego zdarzenia.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik wskazuje elementy polityki bezpieczeństwa informacji w organizacji.	Przyporządkowuje role, odpowiedzialności, procedury i działania minimalizujące ryzyko do podstawowych obszarów bezpieczeństwa informacji w organizacji.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik identyfikuje zasady cyberbezpieczeństwa przy korzystaniu z usług cyfrowych w życiu prywatnym.	Rozpoznaje ryzyka związane z bankowością elektroniczną, zakupami online, mediami społecznościowymi, ochroną tożsamości i śladem cyfrowym oraz wskazuje działania ograniczające te ryzyka.	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

Moduł 1. Wprowadzenie do cyberbezpieczeństwa w codziennej pracy

• rola użytkownika w ochronie danych i ciągłości działania organizacji

• cyberbezpieczeństwo jako element codziennej odpowiedzialności pracownika

• najczęstsze obszary ryzyka w pracy administracyjnej, biurowej, edukacyjnej, medycznej i organizacyjnej

Moduł 2. Rodzaje zagrożeń cybernetycznych

• phishing, ransomware, malware, spyware, DDoS i ataki socjotechniczne

• przykłady incydentów w administracji publicznej, instytucjach, organizacjach i firmach

• mechanizmy manipulacji wykorzystywane w atakach cyfrowych

Moduł 3. Bezpieczna komunikacja i korzystanie z Internetu

• poczta elektroniczna, linki, załączniki i domeny

• komunikatory, wideokonferencje, udostępnianie plików i linków

• VPN, publiczne Wi-Fi, urządzenia mobilne i praca zdalna

Moduł 4. Higiena cyfrowa w codziennej pracy

• silne hasła i menedżery haseł

• uwierzytelnianie dwuskładnikowe

• aktualizacje, kopie zapasowe, nośniki danych, chmura i bezpieczne nawyki użytkownika

Moduł 5. Reagowanie na incydenty bezpieczeństwa

• podstawowe rodzaje incydentów bezpieczeństwa

• kolejność działań po wykryciu incydentu

• zgłaszanie incydentów, dokumentowanie zdarzenia i błędy, których należy unikać

Moduł 6. Bezpieczeństwo systemów, oprogramowania i kont użytkowników

• aktualizacje i łatki bezpieczeństwa

• oprogramowanie antywirusowe i ochrona urządzeń

• uprawnienia użytkowników, zarządzanie kontami i zasada ograniczonego dostępu

Moduł 7. Ochrona danych osobowych i informacji wrażliwych

• cyberzagrożenia a dane osobowe

• przykłady naruszeń ochrony danych

• postępowanie po przypadkowym ujawnieniu danych lub wysłaniu informacji do niewłaściwego odbiorcy

Moduł 8. Polityka bezpieczeństwa informacji w organizacji

• podstawowe zasady polityki bezpieczeństwa informacji

• role i odpowiedzialności pracowników i kadry kierowniczej

• zarządzanie ryzykiem i działania ograniczające ryzyko organizacyjne

Moduł 9. Cyberbezpieczeństwo w życiu prywatnym

• bankowość elektroniczna i zakupy online

• media społecznościowe, ochrona tożsamości i ślad cyfrowy

• zasady ograniczania ryzyka cyfrowego poza miejscem pracy

Moduł 10. Podsumowanie i walidacja

• powtórzenie najważniejszych pojęć i zasad

• omówienie najczęstszych błędów użytkowników

• test teoretyczny z wynikiem generowanym automatycznie

Metody szkoleniowe

• prezentacja ekspercka

• wykład interaktywny

• analiza przypadków

• omówienie przykładów wiadomości, linków i sytuacji ryzykownych

• dyskusja moderowana

• checklisty bezpieczeństwa

• demonstracja dobrych i złych praktyk

• pytania kontrolne utrwalające wiedzę

Walidacja - test teoretyczny z wynikiem generowanym automatycznie.

Harmonogram

Liczba pozycji harmonogramu: 15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 15 Wprowadzenie do cyberbezpieczeństwa w codziennej pracy	Zajęcia	Adrian Ślęzak	17-09-2026	09:00	10:00	01:00
2 z 15 Rodzaje zagrożeń cybernetycznych	Zajęcia	Adrian Ślęzak	17-09-2026	10:00	11:00	01:00
3 z 15 -	Przerwa	-	17-09-2026	11:00	11:30	00:30
4 z 15 Higiena cyfrowa w codziennej pracy	Zajęcia	Adrian Ślęzak	17-09-2026	11:30	12:30	01:00
5 z 15 Bezpieczna komunikacja i korzystanie z Internetu	Zajęcia	Adrian Ślęzak	17-09-2026	12:30	13:30	01:00

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
6 z 15 -	Przerwa	-	17-09-2026	13:30	14:00	00:30
7 z 15 Reagowanie na incydenty bezpieczeństwa	Zajęcia	Adrian Ślęzak	17-09-2026	14:00	15:00	01:00
8 z 15 Bezpieczeństwo systemów, oprogramowania i kont użytkowników	Zajęcia	Adrian Ślęzak	18-09-2026	09:00	10:00	01:00
9 z 15 Ochrona danych osobowych i informacji wrażliwych	Zajęcia	Adrian Ślęzak	18-09-2026	10:00	11:00	01:00
10 z 15 -	Przerwa	-	18-09-2026	11:00	11:30	00:30
11 z 15 Polityka bezpieczeństwa informacji w organizacji	Zajęcia	Adrian Ślęzak	18-09-2026	11:30	12:30	01:00
12 z 15 Cyberbezpieczeństwo w życiu prywatnym	Zajęcia	Adrian Ślęzak	18-09-2026	12:30	13:30	01:00
13 z 15 -	Przerwa	-	18-09-2026	13:30	14:00	00:30
14 z 15 Powtórzenie i podsumowanie najważniejszych zasad	Zajęcia	Adrian Ślęzak	18-09-2026	14:00	14:30	00:30
15 z 15 -	Walidacja	Adrian Ślęzak	18-09-2026	14:30	15:00	00:30

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	12:00
w tym suma godzin zajęć	09:30
w tym suma godzin walidacji	00:30
w tym suma przerw	02:00
Suma godzin dydaktycznych bez przerw	13:15

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	3 321,00 PLN
Koszt przypadający na 1 uczestnika netto	2 700,00 PLN
Koszt osobogodziny brutto	276,75 PLN
Koszt osobogodziny netto	225,00 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	12:00

Prowadzący

Liczba prowadzących: 1

1 z 1

Adrian Ślęzak

Specjalizuje się w tworzeniu i audytowaniu rozwiązań cyfrowych zgodnych ze standardami WCAG 2.0, 2.1 i 2.2. Od 2021 roku współpracuje z firmami, instytucjami publicznymi, uczelniami, jednostkami samorządu terytorialnego oraz organizacjami pozarządowymi, wspierając je w projektowaniu bezpiecznych, dostępnych i użytecznych serwisów, aplikacji oraz dokumentów cyfrowych.
Jako trener i audytor prowadzi szkolenia oraz prelekcje dla programistów, redaktorów, pracowników administracji publicznej, instytucji edukacyjnych i organizacji. Jego doświadczenie obejmuje zarówno zagadnienia techniczne, w tym HTML, CMS-y, aplikacje i dokumenty cyfrowe, jak również praktyczne aspekty bezpieczeństwa użytkownika w środowisku cyfrowym, ochrony danych, prywatności, higieny cyfrowej oraz świadomego korzystania z usług online.
W pracy szkoleniowej łączy wiedzę z zakresu dostępności cyfrowej, bezpieczeństwa informacji, ochrony prywatności i edukacji cyfrowej. Wspiera uczestników w rozpoznawaniu ryzyk, bezpiecznym korzystaniu z narzędzi cyfrowych oraz wdrażaniu dobrych praktyk ograniczających zagrożenia w codziennej pracy. Posiada doświadczenie obejmujące ponad 150 godzin doświadczenia szkoleniowego.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnicy otrzymują:

- prezentacja ze szkolenia
- checklista bezpieczeństwa stanowiska pracy
- checklista bezpiecznej poczty elektronicznej
- zestaw dobrych praktyk cyberbezpieczeństwa
- zestaw przykładowych pytań kontrolnych
- 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 o ukończeniu szkolenia jest uczestnictwo w co najmniej 80% - 100% (w zależności od programu dofinansowania i podpisanej umowy z Operatorem) zajęć usługi rozwojowej oraz pozytywnej oceny z walidacji.
- 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%.

Warunki techniczne

Uczestnik powinien posiadać:

- komputer lub laptop,
- stabilne połączenie z Internetem,
- kamerę i mikrofon,
- dostęp do przeglądarki internetowej,
- możliwość pracy z dokumentami biurowymi,
- możliwość korzystania z platformy szkoleniowej wskazanej przez organizatora.

Kontakt

ELŻBIETA RACHTAN

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