Możliwość dofinansowania

Bezpieczeństwo w świecie cyfrowym – cyberbezpieczeństwo w codziennej pracy urzędnika

Numer usługi 2026/07/08/157622/3677452

2 952,00 PLN brutto
2 400,00 PLN netto
246,00 PLN brutto/h
200,00 PLN netto/h
261,33 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
24.09.2026 do 25.09.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Usługa jest skierowana do pracowników administracji publicznej, jednostek samorządu terytorialnego, jednostek organizacyjnych JST, szkół, uczelni, instytucji kultury, placówek medycznych, organizacji pozarządowych oraz firm, które w codziennej pracy korzystają z narzędzi cyfrowych, poczty elektronicznej, systemów wewnętrznych, e-usług, dokumentów elektronicznych, komunikatorów, chmury lub urządzeń mobilnych. Szkolenie jest przeznaczone zarówno dla osób nietechnicznych, jak i dla pracowników administracyjnych, merytorycznych oraz kierowniczych, którzy chcą zwiększyć bezpieczeństwo pracy z danymi, dokumentami i systemami cyfrowymi.
Minimalna liczba uczestników	2
Maksymalna liczba uczestników	10
Data zakończenia rekrutacji	18-09-2026
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

Usługa prowadzi do nabycia wiedzy i kompetencji z zakresu bezpiecznego korzystania z zasobów cyfrowych w codziennej pracy, rozpoznawania podstawowych cyberzagrożeń, ochrony danych i informacji, stosowania zasad higieny cyfrowej oraz właściwego reagowania na incydenty bezpieczeństwa.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik rozróżnia podstawowe pojęcia związane z cyberbezpieczeństwem i bezpieczeństwem informacji	Wskazuje znaczenie cyberbezpieczeństwa w pracy organizacji oraz rozpoznaje podstawowe pojęcia dotyczące ochrony danych, systemów i użytkowników.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik rozpoznaje podstawowe rodzaje cyberzagrożeń.	Przyporządkowuje phishing, ransomware, malware, spyware, DDoS i ataki socjotechniczne do właściwych opisów lub przykładów sytuacji.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik identyfikuje cechy podejrzanych wiadomości, linków i załączników.	Wskazuje sygnały ostrzegawcze, takie jak podejrzany nadawca, presja czasu, nietypowy link, załącznik lub prośba o dane.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik wskazuje zasady higieny cyfrowej w codziennej pracy.	Rozpoznaje zasady dotyczące silnych haseł, uwierzytelniania dwuskładnikowego, aktualizacji, backupu, nośników danych, chmury i urządzeń służbowych.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik rozróżnia zasady bezpiecznego korzystania z poczty, Internetu, komunikatorów i urządzeń mobilnych.	Dobiera właściwe działania do sytuacji związanych z pocztą elektroniczną, wideokonferencjami, publicznym Wi-Fi, VPN, udostępnianiem plików i pracą mobilną.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik określa zasady reagowania na incydenty bezpieczeństwa.	Porządkuje podstawowe działania po zauważeniu incydentu oraz wskazuje, kogo powiadomić, jakich działań unikać i jakie informacje przygotować.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik rozpoznaje zasady ochrony danych osobowych i informacji wrażliwych w kontekście cyberzagrożeń.	Identyfikuje sytuacje mogące prowadzić do naruszenia ochrony danych oraz wskazuje działania ograniczające ryzyko ujawnienia informacji.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik wskazuje rolę polityk bezpieczeństwa informacji i zarządzania ryzykiem w organizacji	Przyporządkowuje podstawowe działania bezpieczeństwa do obszarów odpowiedzialności pracownika, przełożonego, działu IT i organizacji.	Test teoretyczny z wynikiem generowanym automatycznie

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik identyfikuje zagrożenia cyfrowe występujące w życiu prywatnym.	Rozpoznaje ryzyka związane z bankowością elektroniczną, zakupami online, mediami społecznościowymi, ochroną tożsamości i śladem cyfrowym.	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 szkolenia

• cele, agenda i zasady pracy podczas szkolenia

• znaczenie cyberbezpieczeństwa w codziennej pracy urzędnika

• rola użytkownika w ograniczaniu ryzyka cyfrowego

Moduł 2. Rodzaje zagrożeń cybernetycznych

• phishing, ransomware, malware, spyware, DDoS

• socjotechnika i inżynieria społeczna

• przykłady incydentów w administracji publicznej i organizacjach

Moduł 3. Higiena cyfrowa – zachowania zapobiegające zagrożeniom

• bezpieczne hasła i uwierzytelnianie dwuskładnikowe

• zasady korzystania z urządzeń służbowych

• backup, nośniki danych, chmura i aktualizacje

Moduł 4. Bezpieczna komunikacja i korzystanie z Internetu

• poczta elektroniczna i rozpoznawanie phishingu

• komunikatory, wideokonferencje, udostępnianie linków i plików

• VPN, publiczne Wi-Fi i urządzenia mobilne

Moduł 5. Reagowanie na incydenty bezpieczeństwa

• pierwsze działania po wykryciu incydentu

• procedury zgłaszania i powiadamiania

• podstawy dokumentowania zdarzenia i najczęstsze błędy użytkowników

Moduł 6. Bezpieczeństwo systemów i oprogramowania

• aktualizacje i łatki bezpieczeństwa

• oprogramowanie antywirusowe

• uprawnienia użytkowników i zarządzanie kontami

Moduł 7. Ochrona danych osobowych i RODO w praktyce

• dane osobowe a cyberzagrożenia

• obowiązki pracownika w zakresie ochrony informacji

• przykłady naruszeń i działania ograniczające ryzyko

Moduł 8. Polityki bezpieczeństwa informacji w organizacji

• podstawowe zasady polityki bezpieczeństwa

• role i odpowiedzialności w organizacji

• zarządzanie ryzykiem i dobre praktyki organizacyjne

Moduł 9. Cyberbezpieczeństwo w życiu prywatnym

• bankowość elektroniczna i zakupy online

• ochrona tożsamości w sieci

• media społecznościowe i ślad cyfrowy

Moduł 10. Podsumowanie i walidacja

• powtórzenie kluczowych zasad

• test teoretyczny z wynikiem generowanym automatycznie

• omówienie dalszych działań wspierających bezpieczeństwo cyfrowe

8. Metody szkoleniowe

• prezentacja ekspercka

• mini wykład

• dyskusja moderowana

• analiza przykładów

• omówienie dobrych i złych praktyk

• praca z checklistą

• pytania kontrolne w trakcie szkolenia

9. Walidacja - prowadzona jest w formie testu teoretycznego z wynikiem generowanym automatycznie.

Harmonogram

Liczba pozycji harmonogramu: 13

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 13 Wprowadzenie do szkolenia. Rodzaje zagrożeń cybernetycznych	Zajęcia	Adrian Ślęzak	24-09-2026	09:00	10:30	01:30
2 z 13 -	Przerwa	-	24-09-2026	10:30	11:00	00:30
3 z 13 Higiena cyfrowa – zachowania zapobiegające zagrożeniom	Zajęcia	Adrian Ślęzak	24-09-2026	11:00	12:30	01:30
4 z 13 -	Przerwa	-	24-09-2026	12:30	13:00	00:30
5 z 13 Bezpieczna komunikacja i korzystanie z Internetu	Zajęcia	Adrian Ślęzak	24-09-2026	13:00	14:15	01:15
6 z 13 Reagowanie na incydenty bezpieczeństwa	Zajęcia	Adrian Ślęzak	24-09-2026	14:15	15:00	00:45
7 z 13 Bezpieczeństwo systemów i oprogramowania	Zajęcia	Adrian Ślęzak	25-09-2026	09:00	10:30	01:30
8 z 13 -	Przerwa	-	25-09-2026	10:30	11:00	00:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
9 z 13 Ochrona danych osobowych i RODO w praktyce	Zajęcia	Adrian Ślęzak	25-09-2026	11:00	12:30	01:30
10 z 13 -	Przerwa	-	25-09-2026	12:30	13:00	00:30
11 z 13 Polityki bezpieczeństwa informacji w organizacji	Zajęcia	Adrian Ślęzak	25-09-2026	13:00	14:00	01:00
12 z 13 Cyberbezpieczeństwo w życiu prywatnym	Zajęcia	Adrian Ślęzak	25-09-2026	14:00	14:30	00:30
13 z 13 -	Walidacja	Adrian Ślęzak	25-09-2026	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	2 952,00 PLN
Koszt przypadający na 1 uczestnika netto	2 400,00 PLN
Koszt osobogodziny brutto	246,00 PLN
Koszt osobogodziny netto	200,00 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 dydaktycznych.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnicy otrzymują:

- prezentacja szkoleniowa
- materiały podsumowujące
- checklista bezpieczeństwa stanowiska pracy
- checklista bezpieczeństwa poczty elektronicznej
- zestaw dobrych praktyk z zakresu higieny cyfrowej
- 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.

Warunki techniczne

Warunki techniczne

• komputer lub laptop z dostępem do Internetu

• aktualna przeglądarka internetowa

• mikrofon i kamera

• dostęp do platformy szkoleniowej wskazanej przez organizatora

• możliwość korzystania z poczty elektronicznej i podstawowych narzędzi biurowych

Kontakt

ELŻBIETA RACHTAN

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