Możliwość dofinansowania

Cyberbezpieczeństwo i ochrona danych osobistych w przedsiębiorstwie.

Numer usługi 2025/10/16/16236/3082499

2 880,00 PLN brutto
2 880,00 PLN netto
180,00 PLN brutto/h
180,00 PLN netto/h

BIURO RACHUNKOWE BIUREX SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

4,7 / 5

951 ocen

zdalna w czasie rzeczywistym
Usługa szkoleniowa
16 h
28.01.2026 do 29.01.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Szkolenie przeznaczone dla przedsiebiorców i ich pracowników, którzy chcąpoznać zasady ochrony przed cyberprzestępczością, oraz z uwagi na faktzarządzania danymi osobowymi, ochrony tych danych przed atakamihakerów. Szkolenie dedykowane dla kadry zarządzajacej, menagerów,księgowych, kancelarii prawnych. Szkolenie jest dostępne dla wszystkich zainteresowanych - bez względu na poziom doświadczenia w danej dziedzinie. Wierzymy, że każdy uczestnik będzie miał okazję pogłębić swoją wiedzę.
Minimalna liczba uczestników	2
Maksymalna liczba uczestników	22
Data zakończenia rekrutacji	27-01-2026
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

Usługa „ Cyberbezpieczeństwo i ochrona danych osobistych w przedsiębiorstwie."
Przygotowuje uczestników do nabycia wiedzy oraz umiejętności praktycznych dotyczących ochrony przed atakami cyberprzestępców, wirusami, złośliwym oprogramowaniem.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
W ZAKRESIE WIEDZY: Posiada wiedzę z zakresu zagrożeń cyberbezpieczeństwa i metod ochrony danych osobistych.	• rozróżnia rodzaje zagrożeń w cyberprzestrzeni (np. phishing, malware, ransomware, spyware), • charakteryzuje sposoby ataków na systemy operacyjne i sieci komputerowe, • omawia zasady bezpiecznego korzystania z Internetu, poczty e-mail, chmury i mediów społecznościowych, • wskazuje narzędzia i technologie stosowane do ochrony danych (np. fi rewalle, programy antywirusowe, VPN), • opisuje zasady działania metod socjotechnicznych i ich wpływ na bezpieczeństwo informacji	Test teoretyczny
W ZAKRESIE UMIEJĘTNOŚCI Monitoruje i stosuje zasadybezpiecznego korzystania z zasobów sieciowych oraz chroni dane osobowe w praktyce.	• konfiguruje przeglądarkę w trybie prywatnym/incognito i usuwa ślady aktywności w sieci, • tworzy i przywraca kopie zapasowe danych, • identyfikuje sytuacje zwiększonegoryzyka wycieku danych osobowych, • stosuje metody bezpiecznegologowania i uwierzytelniania użytkowników, • posługuje się narzędziami do szyfrowania i zabezpieczania plików oraz folderów.	Obserwacja w warunkach rzeczywistych

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
W ZAKRESIE KOMPETENCJI SPOŁECZNYCH : Stosuje zasady odpowiedzialnego i świadomego zachowania w środowisku cyfrowym.	• rozpoznaje próby wyłudzenia danych i fałszywe komunikaty (np. fałszywe e-maile, linki, aplikacje), • odróżnia legalne działania od nieetycznych praktyk w sieci, • definiuje i omawia pojęcia związane z cyberbezpieczeństwem (np. VPN, trojan, malware, szyfrowanie, incydent bezpieczeństwa), • wykazuje postawę odpowiedzialności za ochronę danych w środowisku pracy, • komunikuje zagrożenia cyfrowe współpracownikom i wspiera ich w stosowaniu zasad bezpieczeństwa.	Obserwacja w warunkach rzeczywistych

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

1 – Część teoretyczna:

- Jak dbać o swoją tożsamość cyfrową. Wirusy, szpiegowanie, rodzaje, sposoby hakowania. Tryb bezpieczny, monitorowanie zachowań w sieci. Rodzaje oraz narzędzia wykorzystywane do ataków hakerskich.
- Zarządzanie i ochrona danych w przedsiębiorstwie e- szyfrowanie danych – kopie bezpieczeństwa - ochrona danych osobowych klientów - po ataku - studium przypadków -incydenty bezpieczeństwa.

2 – Część praktyczna:

- Jak dbać o swoją tożsamość cyfrową. Wirusy, szpiegowanie, rodzaje, sposoby hakowania. Tryb bezpieczny, monitorowanie zachowań w sieci.Rodzaje oraz narzędzia wykorzystywane do ataków hakerskich.
- Zarządzanie i ochrona danych w przedsiębiorstwie e- szyfrowanie danych – kopie bezpieczeństwa - ochrona danych osobowych klientów - po ataku - studium przypadków -incydenty bezpieczeństwa.
- Walidacja

Szkolenie kierowane jest : dla wszystkich zainteresowanych - bez względu na poziom doświadczenia w danej dziedzinie. Wierzymy, że każdy uczestnik będzie miał okazję pogłębić swoją wiedzę.

Warunki organizacyjne: każdy uczestnik pracuje indywidualnie przy samodzielnym stanowisku komputerowym.

W harmonogramie uwzględniono godziny zegarowe, natomiast kurs opiera się na 45-minutowych godzinach lekcyjnych- stąd rozbieżność pomiędzy liczbą godzin w harmonogramie a ogólną liczbą godzin kursu.

1 godzina= 45 minut (godzina szkoleniowa)

Szkolenie obejmuje łącznie 16 godzin dydaktycznych, co przekłada się na 12 godzin zegarowych. Szkolenie obejmuje 1:30 przerwy. 12 godzin dydaktycznych to część teoretyczna zaś 4 godziny dydaktyczne obejmuje część praktyczna.

Podczas ostatnich 30 minut szkolenia zostanie przeprowadzona walidacja.

Przerwy nie są wliczane w czas szkolenia.

Szkolenie będzie realizowane w formie zdalnej za pomocą platformy ClickMeeting.

Całość nagrania zostanie zarchiwizowana i umieszczona na dysku zewnętrznym w celu kontroli i audytu.

1. Prezentacja powerpoint celem utrwalenia informacji przekazanych w trakcie szkolenia drogą mailową.

2. E-materiały w formacie PDF.

Szkolenie w formie zdalnej będzie odbywało się w czasie rzeczywistym. W zależności od czasu potrzeb będą wykorzystywane różne elementy : ćwiczenia, testy, ankiety, udostępnianie ekranu i inne. Całe szkolenie jest rejestrowane w celach kontroli/audytu. Wykorzystanie nagrania w innym celu niż kontrola/audyt wymaga zgody Trenera i Uczestników

Harmonogram

Liczba przedmiotów/zajęć: 15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 15 **Jak dbać o swoją tożsamość cyfrową. Wirusy, szpiegowanie, rodzaje, sposoby hakowania. Tryb bezpieczny, monitorowanie zachowań w sieci. Rodzaje oraz narzędzia wykorzystywane do ataków hakerskich.**	Rafał Tomaszewski	28-01-2026	09:00	10:30	01:30
2 z 15 przerwa	Rafał Tomaszewski	28-01-2026	10:30	10:45	00:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
3 z 15 Jak dbać o swoją tożsamość cyfrową. Wirusy, szpiegowanie, rodzaje, sposoby hakowania. Tryb bezpieczny, monitorowanie zachowań w sieci. Rodzaje oraz narzędzia wykorzystywane do ataków hakerskich.	Rafał Tomaszewski	28-01-2026	10:45	12:15	01:30
4 z 15 przerwa	Rafał Tomaszewski	28-01-2026	12:15	12:30	00:15
5 z 15 Jak dbać o swoją tożsamość cyfrową. Wirusy, szpiegowanie, rodzaje, sposoby hakowania. Tryb bezpieczny, monitorowanie zachowań w sieci. Rodzaje oraz narzędzia wykorzystywane do ataków hakerskich.	Rafał Tomaszewski	28-01-2026	12:30	14:00	01:30
6 z 15 przerwa	Rafał Tomaszewski	28-01-2026	14:00	14:15	00:15
7 z 15 Jak dbać o swoją tożsamość cyfrową. Wirusy, szpiegowanie, rodzaje, sposoby hakowania. Tryb bezpieczny, monitorowanie zachowań w sieci. Rodzaje oraz narzędzia wykorzystywane do ataków hakerskich.	Rafał Tomaszewski	28-01-2026	14:15	15:45	01:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
8 z 15 Zarządzanie i ochrona danych w przedsiębiorstwie- szyfrowanie danych - kopie bezpieczeństwa - ochrona danych osobowych klientów - po ataku - studium przypadków - incydenty bezpieczeństwa	Rafał Tomaszewski	29-01-2026	09:00	10:30	01:30
9 z 15 przerwa	Rafał Tomaszewski	29-01-2026	10:30	10:45	00:15
10 z 15 Zarządzanie i ochrona danych w przedsiębiorstwie- szyfrowanie danych - kopie bezpieczeństwa - ochrona danych osobowych klientów - po ataku - studium przypadków - incydenty bezpieczeństwa	Rafał Tomaszewski	29-01-2026	10:45	12:15	01:30
11 z 15 przerwa	Rafał Tomaszewski	29-01-2026	12:15	12:30	00:15
12 z 15 Zarządzanie i ochrona danych w przedsiębiorstwie- szyfrowanie danych - kopie bezpieczeństwa - ochrona danych osobowych klientów - po ataku - studium przypadków - incydenty bezpieczeństw	Rafał Tomaszewski	29-01-2026	12:30	14:00	01:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
13 z 15 przerwa	Rafał Tomaszewski	29-01-2026	14:00	14:15	00:15
14 z 15 Zarządzanie i ochrona danych w przedsiębiorstwie- szyfrowanie danych - kopie bezpieczeństwa - ochrona danych osobowych klientów - po ataku - studium przypadków - incydenty bezpieczeństwa	Rafał Tomaszewski	29-01-2026	14:15	15:15	01:00
15 z 15 Walidacja	Rafał Tomaszewski	29-01-2026	15:15	15:45	00:30

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	2 880,00 PLN
Koszt przypadający na 1 uczestnika netto	2 880,00 PLN
Koszt osobogodziny brutto	180,00 PLN
Koszt osobogodziny netto	180,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Rafał Tomaszewski

Rafał Tomaszewski to doświadczony trener, który od lat specjalizuje się w wspieraniu przedsiębiorców w prowadzeniu działalności gospodarczej. Jego wszechstronne wykształcenie oraz bogate doświadczenie zawodowe stanowią solidną podstawę dla oferowanych przez niego usług.

Posiadając wykształcenie wyższe ekonomiczne, ze specjalnością w rachunkowości, Rafał Tomaszewski rozpoczął swoją karierę zawodową w 2010 roku. Od tego czasu aktywnie wykorzystuje swoją wiedzę i umiejętności w obszarze zarządzania finansami oraz prowadzenia rachunkowości w firmach.Aktualnie, jest certyfikowanym Audytorem Wiodącym Systemu Zarządzania Bezpieczeństwem Informacji zgodnie z normą ISO 27001, co świadczy o jego zaawansowanych umiejętnościach w zakresie zarządzania ryzykiem i ochrony informacji w firmach. Ponadto, jest absolwentem studiów podyplomowych z zakresu Zarządzania Cyberbezpieczeństwem, co dodatkowo podkreśla jego specjalizację w obszarze bezpieczeństwa IT. Rafał Tomaszewski wyróżnia się profesjonalizmem, zaangażowaniem oraz umiejętnością dostosowywania się do zmieniających się warunków rynkowych i technologicznych. Jego głównym celem jest pomaganie przedsiębiorcom w osiągnięciu sukcesu poprzez efektywne zarządzanie finansami, procesami oraz bezpieczeństwem informacji.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnicy otrzymają nagranie ze szkolenia oraz prezentację Power Point przygotowane przez Trenera wysłane na adres e-mail.

Informacje dodatkowe

Uwaga:

Usługa jest zwolniona z podatku VAT w przypadku, kiedy przedsiębiorstwo zwolnione jest z podatku VAT lub dofinansowanie wynosi co najmniej70%. W innej sytuacji do ceny netto doliczany jest podatek VAT w wysokości 23%.

Podstawa: §3 ust. 1 pkt. 14 rozporządzenia Ministra Finansów z dnia 20.12.2013 r. w sprawie zwolnień od podatku od towarów i usług orazszczegółowych warunków stosowania tych zwolnień (Dz.U. z 2018 r., poz. 701).

Całe szkolenie jest rejestrowane w celach kontroli/audytu. Wykorzystanie nagrania w innym celu niż kontrola/audyt wymaga zgody Trenera iUczestników.

Uczestnicy otrzymają zaświadczenie, potwierdzające że ukończyli szkolenie.

Forma świadczenia usługi :

Zdalna w czasie rzeczywistym - prowadzona na żywo.

Warunki techniczne

Warunki techniczne

Oto wymagania techniczne dotyczące uczestnictwa w szkoleniu za pomocą platformy ClickMeeting:

1.

- Komputer o następujących parametrach:
- Procesor dwurdzeniowy 2 GHz lub lepszy (zalecany czterordzeniowy).
- 2 GB pamięci RAM (zalecane 4 GB lub więcej).
- System operacyjny: Windows 8 (zalecany Windows 10), Mac OS wersja 10.13 (zalecana najnowsza wersja), Linux, Chrome OS.
- Aktualna wersja jednej z następujących przeglądarek: Google Chrome, Mozilla Firefox, Safari, Edge lub Opera.

2.

Kamera:

- ClickMeeting współpracuje z wbudowanymi kamerami w laptopach oraz większością kamer internetowych.
- Jeśli korzystasz z bardziej zaawansowanej lub profesjonalnej kamery, może być konieczne zainstalowanie dodatkowego oprogramowania lub sprzętu.

3.

Urządzenia mobilne:

- Jeśli korzystasz z urządzenia mobilnego, może być konieczne pobranie odpowiedniej aplikacji z iTunes App Store lub Google Play Store.
- Aby pełnić funkcje dźwięku i obrazu podczas konferencji, wymagane jest posiadanie zestawu słuchawkowego lub głośnikówpodłączonych do urządzenia. Upewnij się, że są one rozpoznane przez Twoje urządzenie i nie są jednocześnie używane przez inneaplikacje.

4.

Dostęp do internetu:

- Minimalne wymagania dotyczące prędkości łącza internetowego:
- Dźwięk: 512 kbps.
- Dźwięk + obraz w jakości SD: 512 kbps + 1 Mbps.
- Dźwięk + obraz w jakości HD: 512 kbps + 2 Mbps.
- Współdzielenie ekranu w trybie LiteQ: 2 Mbps.
- Współdzielenie ekranu w trybie HighQ: 2-5 Mbps.
- Współdzielenie ekranu oparte na przeglądarce: 1-4 Mbps.
- Upewnij się, że masz zainstalowaną najnowszą wersję przeglądarki internetowej.

5.

Okres ważności linku:

- Link do szkolenia będzie ważny w dniach i godzinach określonych w harmonogramie usługi.
- Podczas szkolenia online możesz oczekiwać:
- Wygodnej formy szkolenia, gdzie wystarczy dostęp do urządzenia z internetem (komputer, tablet, telefon), słuchawki lub głośniki.
- Szkolenie odbywa się w wirtualnym pokoju konferencyjnym, w niewielkiej grupie uczestników.
- Uczestnictwa w pełnowartościowym szkoleniu, gdzie trener prowadzi zajęcia "na żywo", widzisz i słyszysz trenera.
- Na ekranie swojego komputera w czasie rzeczywistym będziesz widzieć prezentacje, ankiety i ćwiczenia, które będą pokazywane podczas szkolenia. Podsumowując, aby uczestniczyć w szkoleniu za pomocą platformy ClickMeeting, musisz spełnić następujące wymagania techniczne:
- Komputer z dwurdzeniowym procesorem 2 GHz lub lepszym (zalecany czterordzeniowy).
- Minimum 2 GB pamięci RAM (zalecane 4 GB lub więcej).
- System operacyjny: Windows 8 (zalecany Windows 10), Mac OS wersja 10.13 (zalecana najnowsza wersja), Linux, Chrome OS.
- Najnowsza wersja przeglądarki internetowej: Google Chrome, Mozilla Firefox, Safari, Edge lub Opera.
- Kamera internetowa (wbudowana lub zewnętrzna).
- Głośniki lub słuchawki.
- Mikrofon (wbudowany lub zewnętrzny).
- Klawiatura (wbudowana lub zewnętrzna).
- Mysz lub touchpad.
- Dodatkowo, aby uzyskać pełny dostęp do funkcji dźwięku i obrazu podczas konferencji, zaleca się posiadanie zestawu słuchawkowego lub głośników, które nie są jednocześnie używane przez inne aplikacje.
- Upewnij się, że masz również stabilne połączenie internetowe, które spełnia minimalne wymagane prędkości dla różnych trybów transmisji audio-wideo.
- Szkolenie będzie prowadzone w formie zdalnej, w wirtualnym pokoju konferencyjnym, gdzie będziesz mógł aktywnie uczestniczyć, oglądając prezentacje i ćwiczenia oraz słuchając trenera.

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

Kontakt

Jolanta Cadera

E-mail jolanta.cadera@biurex.pl
Telefon (+48) 887 689 878