



IQ CONSULTING
SPÓŁKA Z
OGRANICZONĄ
ODPOWIEDZIALNOŚ
CIĄ

★★★★★ 4,9 / 5

8 015 ocen

Szkolenie: Bezpieczeństwo cyfrowe pracowników administracyjnych – cyberhigiena, ochrona danych i reagowanie na incydenty

Numer usługi 2026/09/24/120895/3833215

📍 Poznań

🏢 Usługa szkoleniowa

📄 stacjonarna

👥 Zajęcia grupowe

🕒 27:00 h

📅 26.10.2026 do 29.10.2026

5 350,00 PLN brutto

5 350,00 PLN netto

198,15 PLN brutto/h

198,15 PLN netto/h

261,33 PLN cena rynkowa ⓘ

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Szkolenie przeznaczone jest dla pracowników administracyjno-biurowych, Uczestnik powinien posiadać podstawową umiejętność korzystania z komputera, internetu oraz poczty elektronicznej.
Minimalna liczba uczestników	2
Maksymalna liczba uczestników	30
Data zakończenia rekrutacji	25-10-2026
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 podniesienie poziomu wiedzy i praktycznych umiejętności uczestników w zakresie cyberbezpieczeństwa. Uczestnicy poznają zasady bezpiecznego korzystania z internetu i narzędzi cyfrowych, sposoby ochrony danych oraz metody rozpoznawania zagrożeń. Nauczą się również właściwego reagowania na próby oszustw, phishing i incydenty bezpieczeństwa, zarówno w pracy, jak i w codziennym korzystaniu z sieci.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Wyjaśnia podstawowe zagadnienia dotyczące cyberbezpieczeństwa i bezpiecznego korzystania z internetu, w tym malware, phishing, bezpieczne hasła oraz szyfrowanie danych.	Na podstawie przedstawionych sytuacji prawidłowo rozpoznaje i rozróżnia poszczególne pojęcia.	Test teoretyczny z wynikiem generowanym automatycznie
Rozpoznaje różne rodzaje zagrożeń cyfrowych oraz zna sposoby ich wykrywania.	Wymienia i charakteryzuje minimum trzy rodzaje zagrożeń, podając przykłady oraz metody ich rozpoznawania.	Test teoretyczny z wynikiem generowanym automatycznie
Wyjaśnia rolę aktualizacji oprogramowania w zapewnianiu bezpieczeństwa cyfrowego.	Uzasadnia znaczenie regularnego aktualizowania oprogramowania dla ochrony systemów i danych.	Test teoretyczny z wynikiem generowanym automatycznie
Dobiera odpowiednie zasady tworzenia oraz przechowywania bezpiecznych haseł w sytuacjach związanych z pracą zawodową.	Rozpoznaje cechy silnego hasła lub frazy, wskazuje błędy w sposobie tworzenia haseł oraz zna zastosowanie menedżerów haseł.	Test teoretyczny z wynikiem generowanym automatycznie
Rozpoznaje próby phishingu i inne formy oszustw internetowych oraz właściwie na nie reaguje.	Prawidłowo wskazuje fałszywe wiadomości e-mail i strony internetowe oraz określa właściwe działania podejmowane w przypadku incydentu.	Test teoretyczny z wynikiem generowanym automatycznie
Stosuje zasady bezpiecznego korzystania z sieci publicznych i prywatnych oraz chroni swoją prywatność w internecie.	Rozpoznaje zasady bezpiecznego korzystania z różnych rodzajów sieci i dobiera właściwe praktyki ochrony prywatności.	Test teoretyczny z wynikiem generowanym automatycznie

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

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

TAK

Pytanie 2. Czy dokument lub wyrażnie 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 wyrażnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

Program

Warunki organizacyjne dla przeprowadzenia usługi

Infrastruktura i wyposażenie:

Usługa realizowana jest w sali szkoleniowej spełniającej wymagania BHP, dostosowanej do liczby uczestników. Zapewnione są materiały piśmiennicze oraz warunki do pracy szkoleniowej umożliwiające realizację zajęć teoretycznych i praktycznych.

Materiały szkoleniowe:

Uczestnicy otrzymują komplet materiałów szkoleniowych w formie papierowej i elektronicznej (skrypty, prezentacje, case studies), które stają się ich własnością po zakończeniu usługi.

Materiały są aktualne, zgodne z programem i wspierają osiągnięcie założonych efektów uczenia się.

Kadra dydaktyczna i walidator:

Szkolenie prowadzone jest przez trenera posiadającego udokumentowane doświadczenie zawodowe oraz kompetencje dydaktyczne w obszarze tematycznym usługi.

Walidacja efektów uczenia się przeprowadzana jest przez osobę inną niż trener prowadzący (niezależny walidator), co gwarantuje obiektywizm oceny.

Dostępność i zasady horyzontalne:

Miejsce realizacji usługi oraz materiały są dostosowane do potrzeb osób z niepełnosprawnościami, zgodnie z zasadą równego traktowania i niedyskryminacji.

Dostawca zapewnia możliwość skorzystania z mechanizmu racjonalnych usprawnień (np. pętla indukcyjna, tłumacz języka migowego), jeśli zostanie zgłoszone takie zapotrzebowanie

Monitoring i organizacja szkolenia:

W trakcie szkolenia prowadzona jest lista obecności potwierdzająca obecność uczestnika na szkoleniu.

Cel i charakter szkolenia:

Szkolenie trwa 27 godzin zegarowych. Harmonogram uwzględnia dziennie dwie przerwy 30-minutowe, które wliczone są w czas trwania szkolenia.

Podział czasu w ramach 5 dni szkoleniowych przedstawia się następująco:

- zajęcia teoretyczne oraz elementy organizacyjno-teoretyczne
- zajęcia praktyczne, obejmujące warsztaty, ćwiczenia i symulacje
- walidacja efektów uczenia się w formie internetowego testu wiedzy
- przerwy przewidziane w harmonogramie

Łączny czas realizacji usługi wynosi 27 **godzin zegarowych**

2. Sposób prowadzenia zajęć

Szkolenie realizowane jest w formule aktywnej, łączącej przekazywanie wiedzy z praktycznym wykorzystaniem zdobywanych umiejętności. W trakcie zajęć wykorzystywane są m.in. krótkie prezentacje i omówienia prowadzącego, analiza przypadków, zadania wykonywane samodzielnie oraz w zespołach, quizy internetowe, moderowana wymiana doświadczeń, scenki i symulacje sytuacji zawodowych. Uczestnicy pracują również z prostymi checklistami oraz przykładowymi procedurami przydatnymi w codziennej pracy biurowej.

3. Adresaci szkolenia

Szkolenie przeznaczone jest przede wszystkim dla osób wykonujących zadania administracyjne, biurowe i organizacyjne, które w swojej codziennej pracy korzystają z komputerów, poczty elektronicznej, systemów informatycznych oraz przetwarzają informacje służbowe.

W szczególności usługa adresowana jest do:

- pracowników administracyjno-biurowych,
- pracowników sekretariatów i recepcji,
- pracowników działów kadr i księgowości,
- pracowników kancelarii i działów obsługi klienta,
- osób wykonujących zadania back-office,
- pracowników przedsiębiorstw prywatnych,
- pracowników jednostek sektora publicznego,
- osób mających dostęp do danych osobowych i dokumentacji wewnętrznej,
- osób przygotowujących się do podjęcia pracy na stanowiskach administracyjnych.

4. Cel edukacyjny

Celem usługi „Cyberbezpieczeństwo dla pracowników biurowych i administracyjnych – praktyczne szkolenie z cyberhigieny, ochrony danych i reagowania na incydenty” jest rozwinięcie wiedzy i umiejętności uczestników związanych z bezpiecznym funkcjonowaniem w środowisku cyfrowym.

Szkolenie ma przygotować uczestników do świadomego stosowania zasad cyberhigieny, właściwej ochrony danych i informacji oraz rozpoznawania potencjalnych zagrożeń. Szczególny nacisk położony jest na możliwość wykorzystania zdobytej wiedzy w rzeczywistych sytuacjach występujących zarówno w pracy zawodowej, jak i w codziennym korzystaniu z internetu. Uczestnicy poznają również podstawowe zasady zapobiegania incydentom oraz prawidłowego reagowania na sytuacje zagrażające bezpieczeństwu informacji.

5. Walidacja efektów uczenia się

Walidacja szkolenia - W procesie walidacji szkolenia wykorzystano **test teoretyczny generowany automatycznie** skonstruowany tak, by weryfikować efekty uczenia się na trzech poziomach: **wiedzy, umiejętności** oraz **kompetencji społecznych (postaw)**.

Harmonogram

Liczba pozycji harmonogramu: 31

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 31 Bezpieczne środowisko pracy – wprowadzenie do cyberbezpieczeństwa	Zajęcia	DOMINIK HAMERA	26-10-2026	09:00	10:00	01:00
2 z 31 Ocena ryzyka na własnym stanowisku pracy	Zajęcia	DOMINIK HAMERA	26-10-2026	10:00	11:00	01:00
3 z 31 -	Przerwa	-	26-10-2026	11:00	11:30	00:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
4 z 31 Najczęstsze cyberzagrożenia – jak dochodzi do ataku?	Zajęcia	DOMINIK HAMERA	26-10-2026	11:30	12:30	01:00
5 z 31 Fałszywe wiadomości i manipulacja użytkownikami	Zajęcia	DOMINIK HAMERA	26-10-2026	12:30	13:30	01:00
6 z 31 -	Przerwa	-	26-10-2026	13:30	14:00	00:30
7 z 31 Oszustwa biznesowe i wyłudzenia finansowe	Zajęcia	DOMINIK HAMERA	26-10-2026	14:00	15:00	01:00
8 z 31 Podsumowanie dnia – reagowanie na zagrożenia	Zajęcia	DOMINIK HAMERA	26-10-2026	15:00	16:00	01:00
9 z 31 Silne uwierzytelnianie – jak zabezpieczać dostęp do kont?	Zajęcia	DOMINIK HAMERA	27-10-2026	09:00	10:00	01:00
10 z 31 Menedżery haseł i uwierzytelnianie wieloskładnikowe	Zajęcia	DOMINIK HAMERA	27-10-2026	10:00	11:00	01:00
11 z 31 -	Przerwa	-	27-10-2026	11:00	11:30	00:30
12 z 31 Ochrona danych osobowych w codziennej pracy	Zajęcia	DOMINIK HAMERA	27-10-2026	11:30	12:30	01:00

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
13 z 31 Bezpieczne dokumenty i wymiana informacji	Zajęcia	DOMINIK HAMERA	27-10-2026	12:30	13:30	01:00
14 z 31 -	Przerwa	-	27-10-2026	13:30	14:00	00:30
15 z 31 Kopie zapasowe – ochrona przed utratą danych	Zajęcia	DOMINIK HAMERA	27-10-2026	14:00	15:00	01:00
16 z 31 Warsztat: bezpieczne zarządzanie informacją	Zajęcia	DOMINIK HAMERA	27-10-2026	15:00	16:00	01:00
17 z 31 Aktualizacje, zabezpieczenia i ochrona urządzeń	Zajęcia	DOMINIK HAMERA	28-10-2026	09:00	10:00	01:00
18 z 31 Prywatność podczas korzystania z internetu	Zajęcia	DOMINIK HAMERA	28-10-2026	10:00	11:00	01:00
19 z 31 -	Przerwa	-	28-10-2026	11:00	11:30	00:30
20 z 31 Bezpieczne korzystanie z usług chmurowych	Zajęcia	DOMINIK HAMERA	28-10-2026	11:30	12:30	01:00
21 z 31 -	Przerwa	-	28-10-2026	13:30	14:00	00:30
22 z 31 Socjotechnika – człowiek jako element systemu bezpieczeństwa	Zajęcia	DOMINIK HAMERA	28-10-2026	14:00	15:00	01:00

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
23 z 31 Ćwiczenie: czy można zaufać temu komunikatowi ?	Zajęcia	DOMINIK HAMERA	28-10-2026	15:00	16:00	01:00
24 z 31 Co zrobić, gdy wydarzy się incydent?	Zajęcia	DOMINIK HAMERA	29-10-2026	09:00	10:00	01:00
25 z 31 Warsztat reagowania na incydenty	Zajęcia	DOMINIK HAMERA	29-10-2026	10:00	11:00	01:00
26 z 31 -	Przerwa	-	29-10-2026	11:00	11:30	00:30
27 z 31 Kultura bezpieczeńst wa w organizacji	Zajęcia	DOMINIK HAMERA	29-10-2026	11:30	12:30	01:00
28 z 31 Symulacja incydentu cyberbezpiec zeństwa	Zajęcia	DOMINIK HAMERA	29-10-2026	12:30	13:30	01:00
29 z 31 -	Przerwa	-	29-10-2026	13:30	14:00	00:30
30 z 31 Przegląd najważniejszy ch zasad bezpiecznej pracy	Zajęcia	DOMINIK HAMERA	29-10-2026	14:00	15:00	01:00
31 z 31 -	Walidacja	DOMINIK HAMERA	29-10-2026	15:00	16:00	01:00

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	27:00
w tym suma godzin zajęć	22:00

Rodzaj godzin	Liczba godzin
w tym suma godzin walidacji	01:00
w tym suma przerw	04:00
Suma godzin dydaktycznych bez przerw	30:30

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	5 350,00 PLN
Podmiot uprawniony do zwolnienia z VAT na podstawie art. 43 ust. 1 ustawy o VAT	
Koszt przypadający na 1 uczestnika netto	5 350,00 PLN
Koszt osobogodziny brutto	198,15 PLN
Koszt osobogodziny netto	198,15 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	27:00

Prowadzący

Liczba prowadzących: 1



1 z 1

DOMINIK HAMERA

Dominik Hamera posiada aktualne i udokumentowane doświadczenie trenerskie z ostatnich 5 lat w obszarze cyberbezpieczeństwa, cyberhigieny, ochrony danych i informacji oraz bezpiecznego korzystania z narzędzi cyfrowych. W 2025 r. przeprowadził łącznie 560 godzin szkoleń z cyberbezpieczeństwa w ramach projektów KPO: 320 h dla mieszkańców woj. śląskiego, 160 h dla mieszkańców woj. wielkopolskiego oraz 80 h dla nauczycieli przedszkoli z woj. kujawsko-pomorskiego. W 2026 r. zrealizował kolejne 240 h szkoleń KPO dla mieszkańców woj. wielkopolskiego. Ponadto przeprowadził ponad 300 h szkoleń dla klientów indywidualnych i firm. Łącznie w latach 2025–2026 zrealizował ponad 1100 h szkoleń związanych z

cyberbezpieczeństwem. Zakres obejmował m.in. ochronę danych, phishing, cyberoszustwa, reagowanie na incydenty oraz bezpieczne stosowanie haseł, MFA, backupu, VPN i narzędzi cyfrowych.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnicy szkolenia otrzymają materiały dydaktyczne w formie papierowej i elektronicznej przygotowane w oparciu o tematykę szkolenia oraz zgodnie z wymaganiami prawnymi określonymi w prawie polskim oraz UE.

Materiały dla uczestników usługi:

- pliki dokumentów przygotowanych w formacie .doc, .pdf,
- prezentacja multimedialna,

Uczestnicy szkolenia otrzymają zaświadczenie o ukończeniu szkolenia potwierdzające nabyte umiejętności w zakresie przygotowania przedsiębiorstwa do zielonej transformacji oraz zarządzania zmianą organizacyjną przy wdrażaniu rozwiązań proekologicznych.

Czas walidacji oraz jej cena są integralną częścią usługi.

Warunki uczestnictwa

Uczestnikiem może zostać osoba, która spełnia następujące warunki:

- jest osobą pełnoletnią,
- zatrudnienie w przedsiębiorstwie na stanowisku związanym z wykonywaniem czynności administracyjno-biurowych lub współpraca z nim,
- brak przeciwwskazań do udziału w szkoleniu o charakterze warsztatowym (praca umysłowa, praca w grupie)

Szkolenie przeznaczone jest dla pracowników administracyjno-biurowych, którzy w codziennej pracy funkcjonują w dynamicznym środowisku zawodowym wymagającym współpracy zespołowej, sprawnej komunikacji, odpowiedzialności za realizowane zadania oraz umiejętności adaptacji do zmian.

Poziom frekwencji na szkoleniu pozwalający na wydanie zaświadczenia o ukończeniu szkolenia powinien wynosić 100%.

W przypadku uczestnictwa w usłudze osoby z niepełnosprawnością dostawca usługi zapewni realizację usługi rozwojowej uwzględniając potrzeby osób z niepełnosprawnościami

Informacje dodatkowe

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. Usługa rozwojowa nie obejmuje wzajemnego świadczenia usług w projekcie o zbliżonej tematyce przez Dostawców usług, którzy delegują na usługi siebie oraz swoich pracowników i korzystają z dofinansowania, a następnie świadczą usługi w zakresie tej samej tematyki dla Przedsiębiorcy, który wcześniej występował w roli Dostawcy tych usług. Cena usługi nie obejmuje kosztów niezwiązanych bezpośrednio z usługą rozwojową, w szczególności kosztów środków trwałych przekazywanych Przedsiębiorcom lub Pracownikom przedsiębiorcy, kosztów dojazdu oraz zakwaterowania. Koszt przeprowadzenia walidacji jest uwzględniony w cenie szkolenia.

Koszt przeprowadzenia walidacji jest uwzględniony w cenie szkolenia

Adres

ul. Opolska 51/15
61-433 Poznań

woj. wielkopolskie

Udogodnienia w miejscu realizacji usługi

- Wi-fi

Kontakt



Anna Wasilewska

E-mail anna.wasilewska@iq-consulting.pl

Telefon (+48) 575 429 403