

UNIwersytet
GDAŃSKI

Brak ocen dla tego dostawcy

Cyberbezpieczeństwo

Numer usługi 2025/06/06/179368/2800045

799,00 PLN brutto

799,00 PLN netto

133,17 PLN brutto/h

133,17 PLN netto/h

📍 mieszana (zdalna połączona z usługą zdalną w czasie rzeczywistym)

🎓 Usługa szkoleniowa

🕒 6 h

📅 14.10.2025 do 14.10.2025

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Pracownicy biurowi – osoby korzystające na co dzień z komputerów, poczty elektronicznej i systemów firmowych. Kadry zarządzające – menedżerowie i liderzy zespołów, którzy muszą rozumieć ryzyka i podejmować decyzje dotyczące bezpieczeństwa informacji. Działy IT i helpdesk – osoby techniczne, które odpowiadają za infrastrukturę i wsparcie użytkowników. Nowi pracownicy – osoby dopiero wdrażane do organizacji, które powinny poznać zasady bezpiecznej pracy od początku.
Minimalna liczba uczestników	12
Maksymalna liczba uczestników	52
Data zakończenia rekrutacji	24-09-2025
Forma prowadzenia usługi	mieszana (zdalna połączona z usługą zdalną w czasie rzeczywistym)
Liczba godzin usługi	6
Podstawa uzyskania wpisu do BUR	art. 163 ust. 1 ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (t.j. Dz. U. z 2023 r. poz. 742, z późn. zm.)
Zakres uprawnień	Kursy i szkolenia

Cel

Cel edukacyjny

- S (Specific / Konkretny): Rozpoznawanie zagrożeń i stosowanie zasad bezpieczeństwa.
- M (Measurable / Mierzalny): Uczestnicy ukończą zajęcia w czasie 6 godzin.
- A (Achievable / Osiągalny): Szkolenie dostosowane do poziomu uczestników, z praktycznymi przykładami.
- R (Relevant / Istotny): Związany z codzienną pracą i ochroną danych organizacji.
- T (Time-bound / Określony w czasie): Realizacja w ciągu jednego dnia szkoleniowego (np. 6 godzin).

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
◆ Krótkoterminowe (bezpośrednio po szkoleniu): Wzrost świadomości zagrożeń – uczestnicy potrafią rozpoznać phishing, podejrzane załączniki, fałszywe strony logowania. Znajomość dobrych praktyk – np. tworzenie silnych haseł, korzystanie z uwierzytelniania dwuskładnikowego (2FA), bezpieczne korzystanie z Wi-Fi. Zwiększona czujność – pracownicy zgłaszają podejrzane e-maile i incydenty do działu IT. Pozytywne wyniki testów wiedzy – np. 80–100% poprawnych odpowiedzi w quizie końcowym. ◆ Długoterminowe (po kilku tygodniach/miesiącach): Spadek liczby incydentów bezpieczeństwa – mniej przypadków kliknięcia w złośliwe linki, mniej infekcji malware. Lepsze nawyki cyfrowe – regularna zmiana haseł, blokowanie ekranu, nieudostępnianie danych logowania. Zwiększone zaufanie klientów i partnerów – dzięki lepszemu ochronie danych. Zgodność z regulacjami – np. RODO, ISO 27001, NIS2 – organizacja spełnia wymogi prawne i branżowe. ◆ Efekty miękkie: Budowanie kultury bezpieczeństwa – pracownicy czują się współodpowiedzialni za bezpieczeństwo organizacji. Lepsza komunikacja z działem IT – większe zrozumienie procedur i polityk bezpieczeństwa.	Ukończenie zadań.	Wywiad swobodny

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. Cyberbezpieczeństwo – podstawowe pojęcia
2. Uwarunkowania prawne
3. Kategorie informacji i ich wrażliwość
 1. Dane osobowe
 2. Informacja publiczna
 3. Tajemnica przedsiębiorstwa
 4. Własność intelektualna
 5. Informacje niejawne
4. Cyberzagrożenia
 1. Phishing, hacking, cracking
 2. Szkodliwe oprogramowanie
 3. Kradzież danych i tożsamości
 4. Techniki manipulacji
5. Obsługa incydentów
6. Narzędzia, techniki i różne zasady wspierające bezpieczeństwo w sieci
 - Hasła
 - Biometria
 - Oprogramowanie antywirusowe
 - Firewall
 - Kryptografia
 - Usuwanie i przywracanie danych
 - Kopie bezpieczeństwa
 - VPN
 - Anonimowość w sieci

Harmonogram

Liczba przedmiotów/zajęć: 0

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
Brak wyników.					

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	799,00 PLN
Koszt przypadający na 1 uczestnika netto	799,00 PLN
Koszt osobogodziny brutto	133,17 PLN
Koszt osobogodziny netto	133,17 PLN

Prowadzący

Liczba prowadzących: 0

Brak wyników.

Informacje dodatkowe

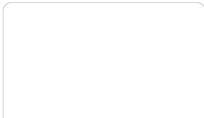
Informacje o materiałach dla uczestników usługi

Materiał zostaną udostępnione w formie elektronicznej.

Warunki techniczne

Należy mieć dostęp do Internetu, poczty elektronicznej.

Kontakt



Rebeka Raczyńska



E-mail rebeka.raczynska@ug.edu.pl

Telefon (+48) 585 233 005