Możliwość dofinansowania

Szkolenie: Cyberbezpieczeństwo i ochrona danych osobowych w praktyce — RODO, phishing, social engineering

Numer usługi 2026/06/29/36960/3656675

3 247,20 PLN brutto
2 640,00 PLN netto
202,95 PLN brutto/h
165,00 PLN netto/h
261,33 PLN cena rynkowa

APS Piotr Olgierd Sułkowski

★★★★★ 5,0 / 5

7 853 oceny

- Usługa szkoleniowa
- zdalna w czasie rzeczywistym
- Zajęcia grupowe
- 16:00 h
- 28.08.2026 do 31.08.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Szkolenie adresowane jest do wszystkich pracowników — niezależnie od stanowiska, branży i stażu pracy — którzy w swojej pracy korzystają z urządzeń elektronicznych, poczty e-mail, systemów informatycznych lub przetwarzają dane osobowe. Obowiązki wynikające z RODO dotyczą każdego pracownika przetwarzającego jakiekolwiek dane osobowe, a zagrożenia takie jak phishing czy social engineering mogą dotknąć każdego użytkownika systemu informatycznego organizacji.
Minimalna liczba uczestników	2
Maksymalna liczba uczestników	25
Data zakończenia rekrutacji	22-08-2026
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 przygotowuje uczestnika do identyfikowania zagrożeń z zakresu cyberbezpieczeństwa występujących w środowisku pracy, rozpoznawania i reagowania na próby phishingu oraz social engineeringu, stosowania zasad ochrony danych osobowych zgodnie z RODO, bezpiecznego korzystania z urządzeń, systemów i sieci informatycznych oraz podejmowania działań ograniczających ryzyko incydentów bezpieczeństwa w organizacji.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik identyfikuje zagrożenia z zakresu cyberbezpieczeństwa oraz wyjaśnia mechanizmy ich działania i potencjalne skutki dla organizacji	Wskazuje minimum 6 rodzajów zagrożeń cyfrowych oraz opisuje ich mechanizmy działania i potencjalne skutki dla organizacji.	Test teoretyczny
Uczestnik analizuje próby phishingu i social engineeringu oraz dobiera właściwy sposób reagowania na incydent bezpieczeństwa.	Analizuje minimum 5 scenariuszy zagrożeń (e-mail, SMS, telefon, strona internetowa) oraz wskazuje cechy charakterystyczne ataku i prawidłowy sposób postępowania.	Obserwacja w warunkach symulowanych
Uczestnik stosuje zasady ochrony danych osobowych zgodnie z RODO w codziennej pracy zawodowej.	Wskazuje obowiązki pracownika wynikające z RODO, rozpoznaje sytuacje mogące prowadzić do naruszenia ochrony danych oraz określa prawidłowy sposób postępowania w minimum 4 scenariuszach dotyczących przetwarzania danych osobowych.	Test teoretyczny
Uczestnik stosuje zasady bezpiecznego korzystania z urządzeń, systemów i sieci informatycznych.	Wykonuje zadania obejmujące stosowanie minimum 8 zasad bezpiecznej pracy z urządzeniami, systemami i siecią, w tym dotyczące haseł, uwierzytelniania, korzystania z poczty elektronicznej, sieci Wi-Fi oraz pracy zdalnej. organizacji.	Obserwacja w warunkach symulowanych

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: Krajobraz zagrożeń cyfrowych (3h)

- Rodzaje cyberataków: phishing, spear phishing, ransomware, malware, Man-in-the-Middle
- Social engineering — psychologiczne mechanizmy manipulacji cyfrowej
- Skala problemu: statystyki incydentów w polskich firmach i organizacjach
- Słabe ogniwo: dlaczego człowiek, nie technologia, jest głównym celem ataku
- Ćwiczenia: identyfikacja zagrożeń w przedstawionych scenariuszach

Moduł 2: Phishing i social engineering — rozpoznawanie i reagowanie (4h)

- Anatomia ataku phishingowego — jak wygląda i jak go rozpoznać
- Phishing e-mailowy, SMS (smishing), telefoniczny (vishing), strony www
- Red flags: fałszywe adresy, pilność, linki, załączniki, prośby o dane
- Procedura reagowania: co zrobić gdy kliknąłeś, gdy podałeś dane, gdy widzisz podejrzaną wiadomość
- Ćwiczenia: analiza rzeczywistych przykładów ataków phishingowych

Moduł 3: RODO w praktyce pracowniczej (4h)

- Podstawy RODO — co to są dane osobowe i kiedy je przetwarzamy
- Obowiązki pracownika: podstawy prawne przetwarzania, minimalizacja danych, dostęp do danych
- Naruszenie ochrony danych — jak je rozpoznać i jak postępować
- Dane szczególnie chronione — kategorie i zasady postępowania
- Ćwiczenia: analiza scenariuszy przetwarzania danych w środowisku pracy

Moduł 4: Bezpieczna praca z urządzeniami i systemami (4h)

- Hasła i uwierzytelnianie: silne hasła, 2FA, menedżery haseł
- Bezpieczne korzystanie z sieci: firmowa sieć Wi-Fi, VPN, publiczne sieci
- Urządzenia mobilne i praca zdalna — specyficzne zagrożenia i zabezpieczenia
- Aktualizacje, kopie zapasowe, szyfrowanie danych
- Polityka czystego biurka i czystego ekranu
- Ćwiczenia: symulowane scenariusze incydentów bezpieczeństwa

Moduł 5: Walidacja

Walidacja efektów uczenia się

- test teoretyczny,
- obserwacja w warunkach symulowanych.

Warunki organizacyjne:

W celu osiągnięcia maksymalizacji efektów szkolenia grupa uczestników powinna wynosić minimum 2 osoby. Realizacja zadań i ćwiczeń prowadzona jest w sposób stopniowo zwiększający poziom trudności, umożliwiający uczestnikom praktyczne zastosowanie zasad cyberbezpieczeństwa oraz ochrony danych osobowych w środowisku pracy.

Szkolenie przewiduje pracę całej grupy, pracę indywidualną oraz pracę w podgrupach. Zajęcia realizowane są metodami interaktywnymi i aktywizującymi, umożliwiającymi uczenie się przez doświadczenie. Uczestnicy wykonują ćwiczenia praktyczne, analizują studia przypadków, uczestniczą w symulacjach incydentów bezpieczeństwa oraz opracowują propozycje działań możliwych do wdrożenia w organizacji.

Zajęcia teoretyczne obejmują 8 godzin, natomiast zajęcia praktyczne 8 godzin.

Po zakończeniu udziału w usłudze rozwojowej uczestnik otrzymuje zaświadczenie o ukończeniu szkolenia.

Szkolenie adresowane jest do:

- przedsiębiorców,
- kadry zarządzającej,
- liderów zespołów,
- pracowników.

Warunkiem uzyskania zaświadczenia jest uczestnictwo w 100% zajęć usługi rozwojowej oraz uzyskanie pozytywnego wyniku walidacji efektów uczenia się.

Walidacja efektów uczenia się realizowana jest jako odrębny etap procesu usługi rozwojowej, niezależny od procesu kształcenia, bez elementów dydaktycznych oraz bez udzielania wskazówek uczestnikom.

Walidacja obejmuje:

1. Test teoretyczny weryfikujący efekty wiedzy.
2. Zadanie praktyczne realizowane w formule obserwacji w warunkach symulowanych.

a) Opis symulacji i przedmiotu obserwacji

W ramach zadania praktycznego uczestnik analizuje sytuację zawodową dotyczącą zagrożenia cyberbezpieczeństwa, próby phishingu, naruszenia ochrony danych osobowych lub incydentu bezpieczeństwa informacji oraz opracowuje sposób prawidłowego postępowania.

Zadanie polega na:

- identyfikacji rodzaju zagrożenia i jego potencjalnych skutków dla organizacji;
- rozpoznaniu cech charakterystycznych ataku phishingowego lub działań z zakresu social engineeringu;
- wskazaniu ryzyk związanych z przetwarzaniem danych osobowych;
- określeniu właściwego sposobu reagowania na incydent bezpieczeństwa;
- zaproponowaniu działań zapobiegających podobnym zdarzeniom w przyszłości;
- wskazaniu zasad bezpiecznego korzystania z urządzeń, systemów i sieci informatycznych.

Przedmiotem obserwacji jest faktyczne działanie uczestnika, w szczególności:

- sposób analizy przedstawionej sytuacji,
- poprawność identyfikacji zagrożeń cyberbezpieczeństwa,
- trafność proponowanych działań ograniczających ryzyko incydentu,
- umiejętność zastosowania zasad ochrony danych osobowych i cyberbezpieczeństwa,
- sposób prezentacji i uzasadnienia proponowanych rozwiązań.

b) Sposób realizacji walidacji i dowody walidacyjne

Zadanie realizowane jest na podstawie studium przypadku lub scenariusza sytuacji zawodowej odnoszącej się do bezpieczeństwa informacji, ochrony danych osobowych lub incydentów cyberbezpieczeństwa.

Dowodami walidacyjnymi są:

- arkusz oceny zadania praktycznego,
- protokół walidacji podpisany przez walidatora,
- test teoretyczny,
- dokumentacja walidacyjna sporządzona przez osobę walidującą.

c) Progi zaliczenia

Test teoretyczny:

- minimum 60% poprawnych odpowiedzi.

Zadanie praktyczne:

- minimum 60% punktów w arkuszu oceny obejmującym kryteria:
  - poprawność identyfikacji zagrożeń cyberbezpieczeństwa,
  - trafność analizy ryzyk dla organizacji,
  - adekwatność proponowanych działań związanych z reagowaniem na incydent,
  - poprawność zastosowania zasad ochrony danych osobowych i bezpiecznej pracy z systemami informatycznymi,
  - jakość uzasadnienia proponowanych rozwiązań.

d) Odrębność etapu walidacji

Walidacja realizowana jest jako oddzielny moduł usługi, bez elementów szkoleniowych, bez omawiania odpowiedzi i bez informacji zwrotnej o charakterze dydaktycznym.

Proces walidacji przeprowadzany jest wyłącznie przez osobę walidującą, inną niż trener prowadzący szkolenie.

Trener nie uczestniczy w procesie walidacji – nie ocenia, nie komentuje, nie udziela wskazówek ani nie bierze udziału w podejmowaniu decyzji o zaliczeniu.

Wyniki walidacji dokumentowane są w formie:

- arkuszy ocen,
- protokołu walidacji,
- testów teoretycznych,
- dokumentacji podpisanej przez osobę walidującą.

Efekty o charakterze wiedzy weryfikowane są testem teoretycznym.

Efekty o charakterze umiejętności weryfikowane są zadaniem praktycznym realizowanym w warunkach symulowanych.

Każdy efekt uczenia się został przypisany do konkretnego elementu walidacji, co zapewnia jednoznaczne potwierdzenie osiągnięcia zakładanych efektów uczenia się.

Warunkiem ukończenia usługi rozwojowej jest:

- udział w 100% zajęć,
- uzyskanie pozytywnego wyniku walidacji efektów uczenia się.

Zaświadczenie o ukończeniu usługi wydawane jest po spełnieniu obu powyższych warunków.

W przypadku niezaliczenia walidacji uczestnik nie uzyskuje potwierdzenia kompetencji, niezależnie od spełnienia wymogu frekwencji.

Harmonogram

Liczba pozycji harmonogramu: 16

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 16 Moduł 1: Krajobraz zagrożeń cyfrowych (cz. 1) (chat, współdzielenie ekranu, wykład, ćwiczenia, rozmowa)	Zajęcia	MICHAŁ POSTEK	28-08-2026	08:00	09:30	01:30
2 z 16 -	Przerwa	-	28-08-2026	09:30	09:45	00:15
3 z 16 Moduł 1: Krajobraz zagrożeń (cz. 2 — zakończenie) (chat, współdzielenie ekranu, wykład, ćwiczenia, rozmowa)	Zajęcia	MICHAŁ POSTEK	28-08-2026	09:45	11:15	01:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
4 z 16 -	Przerwa	-	28-08-2026	11:15	12:00	00:45
5 z 16 Moduł 2: Phishing i social engineering (cz. 1)(chat, współdzielenie ekranu, wykład, ćwiczenia, rozmowa)	Zajęcia	MICHAŁ POSTEK	28-08-2026	12:00	13:30	01:30
6 z 16 -	Przerwa	-	28-08-2026	13:30	13:45	00:15
7 z 16 Moduł 2: Phishing i social engineering (cz. 2 — zakończenie) (chat, współdzielenie ekranu, wykład, ćwiczenia, rozmowa)	Zajęcia	MICHAŁ POSTEK	28-08-2026	13:45	15:15	01:30
8 z 16 Podsumowanie dnia	Zajęcia	MICHAŁ POSTEK	28-08-2026	15:15	16:00	00:45
9 z 16 Moduł 3: RODO w praktyce pracowniczej (cz. 1)(chat, współdzielenie ekranu, wykład, ćwiczenia, rozmowa)	Zajęcia	MICHAŁ POSTEK	31-08-2026	08:00	09:30	01:30
10 z 16 -	Przerwa	-	31-08-2026	09:30	09:45	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
11 z 16 Moduł 3: RODO (cz. 2 — zakończenie) (chat, współdzielenie ekranu, wykład, ćwiczenia, rozmowa)	Zajęcia	MICHAŁ POSTEK	31-08-2026	09:45	11:15	01:30
12 z 16 -	Przerwa	-	31-08-2026	11:15	12:00	00:45
13 z 16 Moduł 4: Bezpieczna praca z urządzeniami i systemami (cz. 1)(chat, współdzielenie ekranu, wykład, ćwiczenia, rozmowa)	Zajęcia	MICHAŁ POSTEK	31-08-2026	12:00	13:30	01:30
14 z 16 -	Przerwa	-	31-08-2026	13:30	13:45	00:15
15 z 16 Moduł 4: Bezpieczna praca (cz. 2 — zakończenie) (chat, współdzielenie ekranu, wykład, ćwiczenia, rozmowa)	Zajęcia	MICHAŁ POSTEK	31-08-2026	13:45	14:30	00:45
16 z 16 -	Walidacja	-	31-08-2026	14:30	16:00	01:30

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	16:00
w tym suma godzin zajęć	12:00
w tym suma godzin walidacji	01:30
w tym suma przerw	02:30

Rodzaj godzin	Liczba godzin
Suma godzin dydaktycznych bez przerw	18:00

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	3 247,20 PLN
Koszt przypadający na 1 uczestnika netto	2 640,00 PLN
Koszt osobogodziny brutto	202,95 PLN
Koszt osobogodziny netto	165,00 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	16:00

Prowadzący

Liczba prowadzących: 1

1 z 1

MICHAŁ POSTEK

Specjalista informatyki i administrator sieci z wieloletnim doświadczeniem w pracy akademickiej i edukacyjnej. Od lat związany z Politechniką Koszalińską oraz Zespołem Szkół Nr 9 w Koszalinie, gdzie odpowiada za rozwój i utrzymanie nowoczesnych systemów informatycznych. Specjalizuje się w cyfryzacji procesów, wdrażaniu nowych technologii i zarządzaniu infrastrukturą IT. Łączy wiedzę

techniczną z praktyką w obszarze zielonych kompetencji — m.in. optymalizacji zużycia energii przez systemy informatyczne, zrównoważonego rozwoju cyfrowego oraz wykorzystania nowoczesnych narzędzi do wspierania transformacji ekologicznej organizacji. Ukończył szkolenia z zakresu ESG, gospodarki obiegu zamkniętego (GOZ) oraz efektywności energetycznej w przedsiębiorstwach (2024–2025).

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnikom zostaną przekazane materiały dydaktyczne w postaci prezentacji PowerPoint.

Materiały zgodne ze standardem WCAG 2.1.

Warunki uczestnictwa

Szkolenie skierowane jest do osób pełnoletnich zainteresowanych podnoszeniem kompetencji w zakresie cyberbezpieczeństwa, ochrony danych osobowych oraz bezpiecznego korzystania z technologii informatycznych w środowisku pracy.

Uczestnikami mogą być w szczególności przedsiębiorcy, kadra zarządzająca, liderzy zespołów oraz pracownicy, którzy w swojej pracy korzystają z urządzeń elektronicznych, poczty elektronicznej, systemów informatycznych lub przetwarzają dane osobowe.

Nie jest wymagane posiadanie specjalistycznej wiedzy z zakresu informatyki, cyberbezpieczeństwa ani ochrony danych osobowych. Od uczestników oczekuje się podstawowych umiejętności obsługi komputera oraz gotowości do aktywnego udziału w ćwiczeniach, analizach przypadków i symulacjach realizowanych podczas szkolenia.

Informacje dodatkowe

W przypadku osób z dofinansowaniem powyżej 70% usługa zwolniona z VAT na podstawie art. 43 ust. 1 pkt 29 litera a) ustawy o VAT i § 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 (tekst jednolity Dz.U. z 2025r., poz. 832)

Organizator zapewnia dostępność osobom ze szczególnymi potrzebami podczas realizacji usług rozwojowych zgodnie z Ustawą z dnia 19 lipca 2019 r. o zapewnianiu dostępności osobom ze szczególnymi potrzebami (Dz.U. 2022 poz. 2240) oraz „Standardami dostępności dla polityki spójności 2021-2027”.

W przypadku potrzeby zapewnienia specjalnych udogodnień prosimy o kontakt pod numerem 500 026 554 lub mailem na psulkowski@gmail.com przed zapisem na usługę!

Warunki techniczne

Forma zdalna usługi. Szkolenie prowadzone jest za pośrednictwem platformy ZOOM.US.

1. W celu prawidłowego i pełnego korzystania z usługi, uczestnik powinien dysponować: urządzeniem mającym dostęp do sieci Internet (komputer, smartfon, tablet), zdolnym do odbioru dźwięku (głośniki, słuchawki), zdolnym do przekazywania dźwięku (mikrofon) w celu interakcji pomiędzy trenerem a uczestnikiem, przeglądarką Windows: IE 11+, Edge 12+, Firefox 27+, Chrome 30+, Mac: Safari 7+, Firefox 27+, Chrome 30+.

2. Minimalna wymagana szybkość połączenia internetowego w celu korzystania z webinariów wynosi 2 Mb/s (zalecane połączenie szerokopasmowe).

3. Dołączenie następuje poprzez kliknięcie w indywidualny link wysłany mailem do uczestnika przed analizą oraz wpisanie imienia i nazwiska.

Ważność linku - od rozpoczęcia szkolenia do jego zakończenia zgodnie z harmonogramem w karcie.

Warunki techniczne niezbędne do udziału w usłudze znajdują się pod tym linkiem: https://support.zoom.us/hc/en-us/articles/201362023-System-Requirements-for-PC-Mac-and-Linux

Kontakt

PIOTR SUŁKOWSKI

E-mail psulkowski@gmail.com
Telefon (+48) 500 026 554