Możliwość dofinansowania

Cyber Security Foundation (S_52140)

Numer usługi 2026/03/07/7629/3388107

2 632,20 PLN brutto
2 140,00 PLN netto
101,24 PLN brutto/h
82,31 PLN netto/h
261,33 PLN cena rynkowa

ASSECO DATA SYSTEMS SPÓŁKA AKCYJNA

4,4 / 5

157 ocen

Usługa szkoleniowa
zdalna w czasie rzeczywistym
Zajęcia grupowe
26:00 h
22.07.2026 do 24.07.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	• Pracownicy działów IT • Szefowie i pracownicy działów bezpieczeństwa (CISO /CSO) • Audytorzy bezpieczeństwa IT • Osoby odpowiedzialne za administrowanie sieciami i systemami IT • Eksperci odpowiedzialni za ciągłość działania i zarządzanie kryzysowe • Szefowie działów audytu • Konsultanci i eksperci bezpieczeństwa informacji • Menedżerowie i specjaliści z działów zarządzania ryzykiem • Menedżerowie i dyrektorzy IT • Eksperci IT Governance.
Minimalna liczba uczestników	3
Maksymalna liczba uczestników	20
Data zakończenia rekrutacji	15-07-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	26
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 zapoznanie uczestników z podstawami zarządzania cyberbezpieczeństwem w organizacji, w tym z głównymi zagrożeniami, metodami cyberataków, technikami cyberobrony oraz podstawowymi regulacjami w obszarze bezpieczeństwa informacji. Uczestnicy poznają zasady organizacji systemu cyberbezpieczeństwa oraz rolę zarządzania ryzykiem i reagowania na incydenty w kontekście wymagań regulacyjnych i dobrych praktyk.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
WIEDZA: Uczestnik opisuje podstawowe pojęcia z zakresu cyberbezpieczeństwa oraz współczesne zagrożenia i techniki cyberataków.	Wyjaśnia pojęcia związane z cyberbezpieczeństwem (np. incydent, podatność, zagrożenie) Rozpoznaje podstawowe typy cyberataków Wskazuje przykłady zagrożeń dla systemów informatycznych i danych	Test teoretyczny
WIEDZA: Uczestnik wyjaśnia zasady zarządzania cyberbezpieczeństwem w organizacji oraz rolę regulacji i standardów w tym obszarze.	Opisuje podstawowe elementy SZBI Wskazuje rolę zarządzania ryzykiem i reagowania na incydenty Identyfikuje przykłady regulacji i dobrych praktyk w obszarze cyberbezpieczeństwa	Test teoretyczny
UMIEJĘTNOŚCI: Uczestnik identyfikuje podstawowe zagrożenia cyberbezpieczeństwa w organizacji.	Analizuje przykładowe scenariusze zagrożeń cybernetycznych Wskazuje potencjalne podatności w systemach lub procesach Określa możliwe skutki incydentów bezpieczeństwa	Test teoretyczny
UMIEJĘTNOŚCI: Uczestnik wskazuje podstawowe działania służące zapobieganiu incydentom cyberbezpieczeństwa. KOMPETECJE SPOŁECZNE: Uczestnik dostrzega znaczenie cyberbezpieczeństwa dla funkcjonowania organizacji.	Proponuje działania ograniczające ryzyko cyberzagrożeń Wskazuje przykłady środków organizacyjnych i technicznych zwiększających bezpieczeństwo Omawia podstawowe zasady reagowania na incydenty Wskazuje wpływ incydentów cyberbezpieczeństwa na działalność organizacji Uzasadnia potrzebę stosowania zasad bezpieczeństwa informacji Identyfikuje rolę pracowników w budowaniu bezpieczeństwa cyfrowego	Test teoretyczny Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
KOMPETECJE SPOŁECZNE: Uczestnik wykazuje odpowiedzialność za stosowanie zasad bezpieczeństwa informacji w swojej pracy.	Stosuje podstawowe zasady bezpiecznego korzystania z systemów informatycznych Identyfikuje sytuacje mogące prowadzić do naruszenia bezpieczeństwa informacji Proponuje działania wspierające budowanie kultury cyberbezpieczeństwa w organizacji	Test teoretyczny

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

- Wprowadzenie do kursu
- Podstawowe terminy stosowane w zarządzaniu cyberbezpieczeństwem
- Zarządzanie ryzykiem, zgodnością (compliance)
- Zapewnienie ciągłości działania i odtwarzanie po awarii
- Zarządzanie bezpieczeństwem zasobów i danych
- Bezpieczeństwo sieci i komunikacji
- Zarządzanie tożsamością i użytkownikami
- Kryptografia i PKI
- Malware i bezpieczeństwo stacji końcowej (end-point security)
- Zarządzanie podatnościami (Vulnerability management)
- Bezpieczeństwo fizyczne i regulacyjne
- Polityki, procedury, standardy i rekomendacje bezpieczeństwa
- Szkolenia i podnoszenie świadomości cyberbezpieczeństwa
- Ataki i inżynieria socjalna (social engineering)

- Bezpieczeństwo urządzeń mobilnych
- Podsumowanie szkolenia

Szkolenie trwa **3 dni**. Łącznie realizowanych jest **26 godzin dydaktycznych** (45 min) wraz z przerwami.

Każdego dnia jest przewidziana 1 dłuższa przerwa na lunch (30 minut) oraz 2 krótsze przerwy kawowe (po 15 minut każda). Przerwy zostały wliczone w harmonogramie usługi.

Ramowy program szkolenia

1. Podstawowe terminy stosowane w zarządzaniu cyberbezpieczeństwem
2. Zarządzanie ryzykiem, zgodnością (compliance)
3. Zapewnienie ciągłości działania i odtwarzanie po awarii
4. Zarządzanie bezpieczeństwem zasobów i danych
5. Bezpieczeństwo sieci i komunikacji
6. Zarządzanie tożsamością i użytkownikami
7. Kryptografia i PKI
8. Malware i bezpieczeństwo stacji końcowej (end-point security)
9. Zarządzanie podatnościami (Vulnerability management)
10. Bezpieczeństwo fizyczne i regulacyjne
11. Polityki, procedury, standardy i rekomendacje bezpieczeństwa
12. Szkolenia i podnoszenie świadomości cyberbezpieczeństwa
13. Ataki i inżynieria socjalna (social engineering)
14. Bezpieczeństwo urządzeń mobilnych
15. Podsumowanie szkolenia

Wszystkie punkty agendy obejmują zarówno zagadnienia teoretyczne, jak i praktyczne. **Łącznie w szkoleniu przewidziano 3 godziny dydaktyczne na część praktyczną. Część teoretyczna obejmuje 23 godziny dydaktyczne.**

Szkolenie rozpoczyna się i kończy odpowiednio pre- i post-testem walidującym efekty kształcenia. Jest to test teoretyczny z wynikiem generowanym automatycznie.

Harmonogram

Liczba pozycji harmonogramu: 26

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 26 Pre-test	-	22-07-2026	09:00	09:15	00:15
2 z 26 Podstawowe terminy stosowane w zarządzaniu cyberbezpieczeństwem	-	22-07-2026	09:15	10:15	01:00
3 z 26 Przerwa kawowa	-	22-07-2026	10:15	10:30	00:15
4 z 26 Zarządzanie ryzykiem, zgodnością (compliance)	-	22-07-2026	10:30	11:30	01:00

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
5 z 26 Zapewnienie ciągłości działania i odtwarzanie po awarii	-	22-07-2026	11:30	12:30	01:00
6 z 26 Przerwa na lunch	-	22-07-2026	12:30	13:00	00:30
7 z 26 Zarządzanie bezpieczeństwem zasobów i danych	-	22-07-2026	13:00	14:00	01:00
8 z 26 Przerwa kawowa	-	22-07-2026	14:00	14:15	00:15
9 z 26 Bezpieczeństwo sieci i komunikacji	-	22-07-2026	14:15	15:30	01:15
10 z 26 Zarządzanie tożsamością i użytkownikami	-	23-07-2026	09:00	10:15	01:15
11 z 26 Przerwa kawowa	-	23-07-2026	10:15	10:30	00:15
12 z 26 Kryptografia i PKI	-	23-07-2026	10:30	11:30	01:00
13 z 26 Malware i bezpieczeństwo stacji końcowej (end-point security)	-	23-07-2026	11:30	12:30	01:00
14 z 26 Przerwa na lunch	-	23-07-2026	12:30	13:00	00:30
15 z 26 Zarządzanie podatnościami (Vulnerability management)	-	23-07-2026	13:00	14:00	01:00
16 z 26 Przerwa kawowa	-	23-07-2026	14:00	14:15	00:15

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
17 z 26 Bezpieczeństwo fizyczne i regulacyjne	-	23-07-2026	14:15	15:30	01:15
18 z 26 Polityki, procedury, standardy i rekomendacje bezpieczeństwa	-	24-07-2026	09:00	10:15	01:15
19 z 26 Przerwa kawowa	-	24-07-2026	10:15	10:30	00:15
20 z 26 Szkolenia i podnoszenie świadomości cyberbezpieczeństwa	-	24-07-2026	10:30	11:30	01:00
21 z 26 Ataki i inżynieria socjalna (social engineering)	-	24-07-2026	11:30	12:30	01:00
22 z 26 Przerwa na lunch	-	24-07-2026	12:30	13:00	00:30
23 z 26 Bezpieczeństwo urządzeń mobilnych	-	24-07-2026	13:00	14:00	01:00
24 z 26 Przerwa kawowa	-	24-07-2026	14:00	14:15	00:15
25 z 26 Podsumowanie szkolenia	-	24-07-2026	14:15	15:15	01:00
26 z 26 Post-test (walidacja efektów kształcenia)	-	24-07-2026	15:15	15:30	00:15

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	2 632,20 PLN
Koszt przypadający na 1 uczestnika netto	2 140,00 PLN
Koszt osobogodziny brutto	101,24 PLN
Koszt osobogodziny netto	82,31 PLN

Prowadzący

Liczba prowadzących: 0

Brak wyników.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

W cenie uczestnik otrzymuje

- Udział w 3-dniowym szkoleniu #cyberSecurity Foundation prowadzonym zdalnie w czasie na żywo przez trenera eksperta ds. cyberbezpieczeństwa
- Komplet materiałów szkoleniowych #cyberSecurity Foundation w wersji elektronicznej
- Zaświadczenie Asseco Academy o ukończeniu szkolenia.

Język

- Język szkolenia: polski
- Język materiałów: polski

Metody interaktywne i aktywizujące prowadzenia usługi m.in.: dyskusje, quizy, odpowiadanie na pytania testowe, praca z tablicą interaktywną, ćwiczenia do samodzielnego wykonania lub w grupach 3-4 osobowych.

Link do szkolenia: https://academy.asseco.pl/szkolenie/cyber-security-foundation/

Warunki uczestnictwa

Warunki organizacyjne: Szkolenie realizowane jest w formie zdalnej w czasie rzeczywistym. Uczestnik powinien posiadać dostęp do komputera z kamerą i mikrofonem, spełniające minimalne wymagania opisane w sekcji: Warunki techniczne. Uczestnik bierze udział w szkoleniu wraz z całą grupą szkoleniową, zarówno w części teoretycznej, jak i praktycznej, zgodnie z programem.

Wymagana frekwencja: min. 80%. Podstawą weryfikacji są listy obecności tworzona na podstawie rzeczywistego czasu zalogowania w sesji szkoleniowej. Brak wymaganej frekwencji skutkuje nieuznaniem usługi za zrealizowaną i brakiem możliwości rozliczenia dofinansowania w systemie BUR.

Informacje dodatkowe

Dla usług z dofinansowaniem powyżej 70% istnieje możliwość wystawienia faktury ZW VAT. Prosimy o kontakt z Biurem Asseco Academy academy@assecods.pl Natomiast w przypadku dofinansowania usługi poniżej 70% ze środków publicznych, usługa nie jest zwolniona z podatku VAT. Należy wówczas doliczyć do usługi szkoleniowej należny VAT w wysokości 23%. Podstawa prawna zwolnienia z VAT: art. 43 ust. 1 pkt. 29 lit. c ustawy o podatku od towarów i usług z dnia 11 marca 2004r. (Dz.U. Nr 54, poz. 535 ze zm.) oraz zgodnie z § 3 ust. 1 pkt. 14 Rozporządzenia Ministra Finansów z dnia 20.12.2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień (Dz.U. z 2015, poz. 736 ze zm.).

Warunki techniczne

Szkolenie prowadzone jest w formie zdalnej na żywo za pośrednictwem aplikacji Webex Meeting. Aby wziąć udział, konieczne jest posiadanie urządzenia takiego jak komputer stacjonarny lub laptop wyposażonego w stabilne połączenie internetowe oraz mikrofon i kamerę. Przed rozpoczęciem szkolenia uczestnicy będą mieli możliwość przetestowania swojego sprzętu podczas sesji próbnej, aby upewnić się, że połączenie internetowe, mikrofon i kamera/słuchawki działają poprawnie.

Minimalne wymagania sprzętowo-systemowe

- Komputer PC z systemem Windows 7 lub nowszym, Max OX 10.13 lub nowszym. Istnieje możliwość korzystania z innych systemów, w tym Linux. Szczegółowe informacje można uzyskać pod adresem: https://help.webex.com/en-us/nki3xrq/Webex-Meetings-Suite-SystemRequirements.
- Przeglądarka internetowa (zalecamy korzystanie z Chrome lub Firefox).
- Karta LAN: min. 100 MBPS lub stabilne połączenie WiFi (zalecamy połączenie do sieci „kablem”). Nie dopuszcza się udziału w szkoleniu za pośrednictwem łączy GSM/LTE. Zalecane pasmo, to przynajmniej 2 MB/s (download i upload). W przypadku spadku przepustowości łącza poniżej 1,2 MB/s należy liczyć się z istotnym obniżeniem jakości połączenia.
- Mikrofon i głośniki (zalecamy korzystanie z zestawu typu headset).
- Kamera internetowa.

Przed szkoleniem każdy uczestnik otrzyma na podany adres email link do platformy, gdzie odbędzie się szkolenie. Uczestnictwo w szkoleniu umożliwia aktywne uczestnictwo w zajęciach, w tym komunikację z trenerem oraz pozostałymi uczestnikami. Umożliwia to wymianę doświadczeń oraz aktywny kontakt zarówno z grupą, jak i prowadzącym. Dodatkowo, uczestnicy mają dostęp do funkcji czatu online, co jeszcze bardziej ułatwia interakcję.

Kontakt

Alicja Kozłowska

E-mail bur-szkolenia@assecods.pl
Telefon (+48) 801 303 030