

ZAKŁAD
DOSKONALENIA
ZAWODOWEGO
KATOWICE**Certyfikowane szkolenie**
"Cyberbezpieczeństwo oraz ochrona
danych osobowych "

Numer usługi 2025/05/26/10510/2772669

5 040,00 PLN brutto
5 040,00 PLN netto
240,00 PLN brutto/h
240,00 PLN netto/hZAKŁAD
DOSKONALENIA
ZAWODOWEGO W
KATOWICACH

★★★★★ 4,6 / 5

1 415 ocen

📍 Gliwice / stacjonarna

🏠 Usługa szkoleniowa

🕒 21 h

📅 24.09.2025 do 26.09.2025

Informacje podstawowe

Kategoria	Prawo i administracja / Prawo pozostałe
Grupa docelowa usługi	Kurs jest skierowany do: • Specjaliści ds. cyberbezpieczeństwa, • Osoby początkujące, • Inspektorzy Ochrony Danych Osobowych, • Wszyscy zainteresowani tematem.
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	5
Data zakończenia rekrutacji	19-09-2025
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	21
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:

•Zdobycie wiedzy na temat cyberbezpieczeństwa i jego praktycznego zastosowania,

- Zdobycie wiedzy na temat podstawowych i zaawansowanych zabezpieczeń,
- Zdobycie wiedzy na temat podstawowych i zaawansowanych metod ataków,
- Zdobycie wiedzy na temat Systemu Zarządzania Bezpieczeństwem Informacji i jego praktycznego zastosowania,
- Zapoznanie się z najnowszym krajobrazem cyberbezpieczeństwa,
- Zdobycie wiedzy nt. ochrony danych osobowych, w aspekcie cyberbezpieczeństwa

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Wyjaśnia znaczenie ochrony informacji i podstawowe zasady bezpieczeństwa informacji.	Identyfikuje i opisuje różne rodzaje zagrożeń oraz ich wpływ na systemy informatyczne.	Test teoretyczny
Rozpoznaje typowe ataki oraz wskazuje sposoby obrony przed nimi.	Rozpoznaje metody inżynierii społecznej i opisuje sposoby ograniczania powierzchni ataku.	Obserwacja w warunkach symulowanych
Zna podstawy prawne ochrony danych osobowych (RODO, UODO).	Stosuje podstawowe zasady ochrony danych i systemów w środowisku pracy.	Test teoretyczny
Rozumie obowiązki administratora, podmiotu przetwarzającego i IOD.	Identyfikuje rodzaje danych osobowych i podstawy ich przetwarzania.	Test teoretyczny
Wyjaśnia prawa osób, których dane są przetwarzane.	Stosuje procedury postępowania w przypadku naruszenia danych.	Test teoretyczny Obserwacja w warunkach symulowanych
Wykazuje się wysoko rozwiniętymi kompetencjami społecznymi na swoim stanowisku pracy.	- organizuje własną pracę w zgodzie z zasadami etyki zawodowej; - współpracuje w zespole zadaniowym; - przyjmuje odpowiedzialność za jakość pracy i rozwój zawodowy.	Test teoretyczny
		Obserwacja w warunkach symulowanych

Kwalifikacje

Inne kwalifikacje

Uznane kwalifikacje

Pytanie 1. Czy wydany dokument jest potwierdzeniem uzyskania kwalifikacji w zawodzie?

TAK

Pytanie 5. Czy dokument jest certyfikatem, dla którego wypracowano system walidacji i certyfikowania efektów uczenia się na poziomie międzynarodowym?

TAK

Informacje

Podstawa prawna dla Podmiotów / kategorii Podmiotów	uprawnione do realizacji procesów walidacji i certyfikowania na mocy innych przepisów prawa
Nazwa Podmiotu prowadzącego walidację	Walidację prowadzi Centrum Egzaminacyjne i Laboratorium Egzaminacyjne akredytowane przez Polskie Towarzystwo Informatyczne
Podmiot prowadzący walidację jest zarejestrowany w BUR	Tak
Nazwa Podmiotu certyfikującego	Polskie Towarzystwo Informatyczne
Podmiot certyfikujący jest zarejestrowany w BUR	Tak

Program

1 godzina zajęć = 45 min (godzina dydaktyczna).

I. Zrozumienie podstawowych zasad bezpieczeństwa i zagrożeń bezpieczeństwa (4 godziny, w tym 1 godzina zajęć praktycznych)

1. Co to jest informacja i dlaczego należy ją chronić?
2. Poufność; integralność; dostępność; wpływ zagrożenia i ryzyka;
3. Zasada najmniejszego przywileju; Inżynieria społeczna; analiza powierzchni ataku; modelowanie zagrożeń

4. Zrozumienie bezpieczeństwa fizycznego

- Bezpieczeństwo obiektu;
- Bezpieczeństwo komputera;
- Wymienne urządzenia i dyski;
- Kontrola dostępu;
- Bezpieczeństwo urządzeń mobilnych;
- Keyloggery

5. Zrozumienie bezpieczeństwa w Internecie

- Ustawienia bezpieczeństwa przeglądarki;
- Bezpieczne strony internetowe

6. Szyfrowanie i podpisywanie poczty mail oraz inne zastosowania; wirtualna sieć prywatna (VPN);

- Klucz publiczny / klucz prywatny;
- Algorytmy szyfrowania; właściwości certyfikatu;
- Infrastruktura PKI / usługi certyfikacyjne;
- Tokeny sprzętowe, ograniczenie urządzeń, aby uruchamiały tylko zaufane aplikacje

7. Rodzaje ataków

- Phishing
- Spoofing
- Smishing
- Vishing
- Ataki przez pocztę elektroniczną
- Deepfake
- Kradzieże tożsamości
- Ransomware
- Malware
- Kradzieże i wyludzenia informacji
- Ataki kierowane przez media społecznościowe

8. Metody obrony i przeciwdziałania

- Zabezpieczenie sprzętu i nośników danych
- Klucze sprzętowe

- Zarządzanie hasłami i dostępem do danych
- Weryfikacja dwuetapowa 2FA
- Polityka haseł
- Hasła – tworzenie bezpiecznych haseł
- Menadżer haseł
- Monitorowanie systemów i sieci
- Procedury bezpieczeństwa i polityki organizacyjne
- Szkolenia z zakresu bezpieczeństwa i edukacja pracowników
- Ochrona danych w czasie ich przesyłania i przechowywania
- Regularne aktualizacje i ochrona przed złośliwym oprogramowaniem
- Tworzenie kopii zapasowych i odzyskiwanie danych
- Segregacja danych i klasyfikacja informacji
- Wdrożenie i przestrzeganie standardów ochrony poczty elektronicznej

II. Krajobraz cyberbezpieczeństwa (5 godzin w tym 1 godzina zajęć praktycznych)

1. Stan cyberbezpieczeństwa w roku 2024

- Raporty NIK
- Raporty CERT Polska
- Raporty CSIRT NASK

2. Główne zagrożenia

3. Metody ataków

4. Jak się chronić?

5. Zarządzanie bezpieczeństwem informacji

- System Zarządzania Bezpieczeństwem informacji (SZBI)
- Identyfikacja ryzyk związanych z prywatnością i ich konsekwencje prawne
- Zasady szacowania ryzyka i ocena wpływu zastosowania określonych rozwiązań w zakresie
- Skuteczności zarządzania bezpieczeństwem
- Jak rozumieć i stosować podejście oparte na ryzyku – praktyczne wypełnienie szablonu Analizy Ryzyka
- Zarządzanie cyklem życia danych osobowych
- Omówienie wymagań normy ISO 27001
- Wytyczne normy ISO 27002:2017 jako wykaz dobrych praktyk z zakresu bezpieczeństwa danych i informacji
- Kontrola dostępu,
- Kryptografia,
- Bezpieczeństwo fizyczne,
- Bezpieczna eksploatacja, w tym kopie zapasowe,
- Bezpieczeństwo komunikacji,
- Pozyskiwanie, rozwój i utrzymywanie systemów,
- Zarządzanie incydentami bezpieczeństwa danych i informacji,
- Zarządzanie ciągłością działania,
- Zgodność z przepisami prawa.
- Rola, zadania i uprawnienia Data Security Officer;
- Auditowanie systemów bezpieczeństwa danych i informacji,
- Cyberhigiena.

III. Podstawowe zasady przetwarzania danych osobowych (10 godzin, w tym 2 godziny zajęć praktycznych)

1. Podstawy Ochrony

- RODO - podstawowe informacje oraz definicje - wybrane zagadnienia
- Dane osobowe
- Przetwarzanie danych osobowych
- Podstawy prawne przetwarzania danych osobowych
- Obowiązki administratora
- Obowiązki Podmiotu przetwarzającego
- Prawa osób, których dane są przetwarzane
- Administracyjne kary pieniężne
- Obowiązki Inspektora Ochrony Danych Osobowych
- Postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych
- Odpowiedzialność cywilna, karna i administracyjna
- Przesłanki dopuszczalności przetwarzania danych osobowych (zwykłych i szczególnie chronionych)
- Ocena skutków dla ochrony danych
- Ochrona danych w fazie projektowania

- Domyślna ochrona danych
- Podstawy prawne przekazywania danych osobowych do państwa trzeciego
- Ochrona danych osobowych w stosunkach pracy
- Zasady przetwarzania danych osobowych na stanowiskach pracy

IV. Egzamin 1 godzina

Egzamin 1 godzina jest wliczony w czas usługi rozwojowej.

1 godzina zajęć = 45 min (godzina dydaktyczna).

Przerwy są wliczone w czas usługi rozwojowej.

Egzamin:

Organizator w ramach usługi szkolenia pokrywa koszt przystąpienia do pierwszego egzaminu z modułu Egzamin S3 IT Security. Egzamin przeprowadzony zostanie w pracowni komputerowej w OKZ Pyskowice, ul. Powstańców Śląskich 7

Ocena umiejętności Kandydata dokonywana jest na podstawie wyniku testu, który polega na rozwiązywaniu zadań praktycznych, łącznie co najmniej 32 zadania. Test ma formę elektroniczną i trwa 45 minut. Test składa się z zadań, które należy wykonać w określonej kolejności i zgodnie z instrukcjami. Zadania mogą dotyczyć dowolnych tematów z zakresu sylabusu modułu. Każde zadanie jest oceniane punktowo, przy czym część punktów może być przyznana za poprawność wykonania poszczególnych kroków. Aby zaliczyć test, Kandydat musi uzyskać co najmniej 75% punktów.

Harmonogram

Liczba przedmiotów/zajęć: 9

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 9 Zrozumienie podstawowych zasad bezpieczeństwa i zagrożeń bezpieczeństwa	Jacek Żywczok	24-09-2025	08:00	11:45	03:45
2 z 9 Przerwa	Jacek Żywczok	24-09-2025	11:45	12:00	00:15
3 z 9 Krajobraz cyberbezpieczeństwa	Jacek Żywczok	24-09-2025	12:00	15:45	03:45
4 z 9 Podstawowe zasady przetwarzania danych osobowych	Małgorzata Będkowska	25-09-2025	15:00	17:15	02:15
5 z 9 Przerwa	Małgorzata Będkowska	25-09-2025	17:15	17:30	00:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
6 z 9 Podstawowe zasady przetwarzania danych osobowych	Małgorzata Będkowska	25-09-2025	17:30	20:30	03:00
7 z 9 Podstawowe zasady przetwarzania danych osobowych	Małgorzata Będkowska	26-09-2025	15:00	17:15	02:15
8 z 9 Przerwa	Małgorzata Będkowska	26-09-2025	17:15	17:30	00:15
9 z 9 Egzamin	-	26-09-2025	17:30	18:15	00:45

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	5 040,00 PLN
Koszt przypadający na 1 uczestnika netto	5 040,00 PLN
Koszt osobogodziny brutto	240,00 PLN
Koszt osobogodziny netto	240,00 PLN
W tym koszt walidacji brutto	40,00 PLN
W tym koszt walidacji netto	40,00 PLN
W tym koszt certyfikowania brutto	233,70 PLN
W tym koszt certyfikowania netto	233,70 PLN

Prowadzący

Liczba prowadzących: 2



1 z 2

Jacek Żywczok

Od 5 lat wykładowca i trener specjalizujący się w kursach o tematyce informatycznej, w szczególności cyberbezpieczeństwa, ochrony danych osobowych oraz z zakresu obsługi programów komputerowych MS Excel – w pełnym zakresie obejmującym m.in. pracę z arkuszem kalkulacyjnym, formuły i funkcje, grafikę i wykresy, formatowanie oraz raportowanie danych. Prowadzi również szkolenia i kursy rozwijające zielone kompetencje, w tym wykorzystanie narzędzi cyfrowych do controllingu środowiskowego, optymalizacji procesów energetycznych i materiałowych oraz raportowania zrównoważonego rozwoju.

Absolwent Uniwersytetu Śląskiego, Wydział Techniki (magister informacji naukowo-technicznej). Nauczyciel akademicki prowadzący zajęcia praktyczne, laboratoryjne i wykłady w Wyższej Szkole Technologii Informatycznej w Katowicach. Jako kierownik i koordynator posiada kwalifikacje do prowadzenia praktyk zawodowych w WSTI.

Posiada szerokie kompetencje w zakresie obsługi pakietów biurowych (MS Office, Open Office), systemów operacyjnych (Windows), baz danych (DBase, Access), grafiki komputerowej oraz zarządzania sieciami. Zna języki programowania HTML i Java. Dysponuje praktyczną wiedzą dotyczącą sprzętu komputerowego, urządzeń biurowych i technologii telekomunikacyjnych.



2 z 2

Małgorzata Będowska

Od 5 lat wykładowca i trener specjalizujący się w kursach o tematyce informatycznej, w szczególności cyberbezpieczeństwa, ochrony danych osobowych oraz z zakresu obsługi programów komputerowych.

Absolwentka Akademii WSB – specjalizacja „Zarządzanie cyberbezpieczeństwem”. Wykładowca, prowadzący zajęcia praktyczne oraz wykłady. Czynny egzaminator PTI – ECDL. Menager oraz współwłaściciel firmy szkoleniowo – doradczej.

Posiada szerokie kompetencje w zakresie cyberbezpieczeństwa, ochrony danych osobowych oraz obsługi pakietów biurowych (MS Office, Open Office), systemów operacyjnych (Windows), baz danych (DBase, Access), grafiki komputerowej oraz zarządzania sieciami.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały opracowane przez wykładowców - skrypty, notes, długopis

Informacje dodatkowe

Egzamin 1 godzina jest wliczona w czas usługi rozwojowej.

1 godzina zajęć = 45 min (godzina dydaktyczna).

Przerwy są wliczone w czas usługi rozwojowej.

Cena szkolenia została skalkulowana dla grupy minimum 2 osobowej i obejmuje jedno podejście do egzaminu ECDL S3 IT Security (233,70zł/os.)

Termin realizacji usługi obejmuje również egzamin zewnętrzny z zakresu IT Security S3

Uczestnik szkolenia po zdaniu egzaminu otrzymuje zaświadczenie o ukończeniu szkolenia oraz certyfikat ECDL S3 - IT Security w wersji elektronicznej. Certyfikat nie ma określonego terminu ważności.

Informujemy, że w Zakład Doskonalenia Zawodowego w Katowicach jest zwolniony z podatku VAT, w związku z tym koszt szkolenia netto brutto jest identyczny (zwolniona z podatku VAT na podstawie art. 43, ust. 1, pkt. 26, lit. Ustawy o VAT)

Adres

ul. Prymasa Stefana Wyszyńskiego 11

44-100 Gliwice

woj. śląskie

CKZ Gliwice mieści się w budynku Fluor -PrzoiPrzem

Parking przy ul. Dworcowej

Egzamin przeprowadzony zostanie w pracowni komputerowej w Ośrodku Kształcenia Zawodowego w Pyskowicach, ul. Powstańców Śląskich 7

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi
- Laboratorium komputerowe
- Obiekt w pełni przystosowany do wymogów osób niepełnosprawnych ruchowo

Kontakt



Anna Grzegoszczyk

E-mail a.grzegoszczyk@zdz.katowice.pl

Telefon (+48) 502 793 398