



Cyberbezpieczeństwo i bezpieczeństwo informacji w firmie. SZBI (ISO/IEC 27001), praktyka biznesowa i wymagania KSC/NIS2 w 2026 roku.

Numer usługi 2026/05/08/11918/3546631

1 291,50 PLN brutto
1 050,00 PLN netto
227,91 PLN brutto/h
185,29 PLN netto/h
261,33 PLN cena rynkowa ⓘ

FIRMA
SZKOLENIOWA
FORMATRIX
MARCIN
FILIPOWSKI

📍 Katowice
🏠 Usługa szkoleniowa
📄 stacjonarna
👥 Zajęcia grupowe

★★★★★ 4,6 / 5
406 ocen

🕒 05:40 h
📅 21.08.2026 do 21.08.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	<ul style="list-style-type: none">• właścicielka/właściciel firmy, zarząd, dyrekcja,• menedżerowie i kierownicy działów,• pracownicy biurowi, administracja, back office,• sprzedaż, obsługa klienta, HR, jakość,• osoby odpowiedzialne za dokumentację, dane i procesy. <p>Szkolenie jest przeznaczone dla decydentów i pracowników, którzy na co dzień przetwarzają informacje i podejmują decyzje.</p>
Minimalna liczba uczestników	10
Maksymalna liczba uczestników	20
Data zakończenia rekrutacji	19-08-2026
Forma prowadzenia usługi	stacjonarna
Podstawa uzyskania wpisu do BUR	Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

Cel

Cel edukacyjny

Celem szkolenia jest zdobycie przez uczestników wiedzy i praktycznych umiejętności z zakresu cyberbezpieczeństwa i bezpieczeństwa informacji w organizacji, w tym zasad SZBI zgodnego z ISO/IEC 27001 oraz wymagań KSC/NIS2. Uczestnicy nauczą się rozpoznawać zagrożenia, reagować na incydenty oraz wdrażać podstawowe rozwiązania zwiększające bezpieczeństwo informacji w firmie.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik charakteryzuje zasady bezpieczeństwa informacji, podstawy SZBI ISO/IEC 27001 oraz wymagania KSC/NIS2	<ul style="list-style-type: none">- omawia zasady poufności, integralności i dostępności informacji,- rozróżnia elementy SZBI,- wskazuje podstawowe wymagania KSC/NIS2 dla organizacji	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik identyfikuje zagrożenia cyberbezpieczeństwa oraz dobiera działania ograniczające ryzyko w organizacji	<ul style="list-style-type: none">- rozpoznaje przykłady phishingu i prób wyłudzeń,- wskazuje działania ograniczające ryzyko incydentów,- dobiera podstawowe zasady cyberhigieny w środowisku pracy	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik stosuje podstawowe zasady reagowania na incydenty bezpieczeństwa informacji	<ul style="list-style-type: none">- wskazuje działania podejmowane po wykryciu incydentu,- rozróżnia zasady zgłaszania i dokumentowania incydentów,- identyfikuje błędy w reagowaniu na incydenty	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik uzasadnia znaczenie odpowiedzialności pracowników i kadry zarządzającej za bezpieczeństwo informacji w organizacji	<ul style="list-style-type: none">- wskazuje znaczenie współpracy w obszarze bezpieczeństwa informacji,- rozróżnia role pracowników i kadry zarządzającej w SZBI,- identyfikuje znaczenie kultury bezpieczeństwa w organizacji	Test teoretyczny z wynikiem generowanym automatycznie

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 rozdzielanie procesów kształcenia i szkolenia od walidacji?

TAK

Program

BLOK I – Bezpieczeństwo informacji jako element zarządzania firmą

Zakres tematyczny:

- informacja jako kluczowy zasób biznesowy,
- triada CIA (poufność, integralność, dostępność) w realiach firmy,
- gdzie firmy tracą dane, pieniądze i reputację,
- ludzie, procesy i technologia – wspólna odpowiedzialność.

Ćwiczenie:

- identyfikacja kluczowych informacji i procesów w firmie.

BLOK II – SZBI (System Zarządzania Bezpieczeństwem Informacji) po biznesowemu

Zakres tematyczny:

- czym jest **SZBI** i po co firmie ISO/IEC 27001,
- podejście oparte na ryzyku zamiast „odhaczania dokumentów”,
- minimalny, sensowny SZBI: polityka, role, zasady, reakcja, szkolenia,
- najczęstsze błędy firm przy „wdrażaniu bezpieczeństwa”.

Efekt:

- zarys praktycznego SZBI dopasowanego do wielkości firmy.

BLOK III – KSC / NIS2 a firmy (2026)

Zakres tematyczny:

- kiedy firma wchodzi w obszar wymagań cyberbezpieczeństwa,
- odpowiedzialność zarządu i kadry kierowniczej,
- ryzyka kontraktowe, finansowe i wizerunkowe,
- bezpieczeństwo łańcucha dostaw i dostawców IT.

(Bez straszenia – tylko to, co ma przełożenie na decyzje biznesowe.)

BLOK IV – Najczęstsze cyberzagrożenia w firmach

Zakres tematyczny:

- phishing, podszycia i fałszywe faktury,
- przejęcia kont e-mail i systemów,
- ransomware i utrata dostępności,
- błędy pracowników i „dobre intencje”,
- praca zdalna, prywatne urządzenia, pendrive'y.

Ćwiczenie:

- „mail od kontrahenta z pilną prośbą” – analiza i decyzje.

BLOK V – Incydent bezpieczeństwa: jak reagować bez chaosu

Zakres tematyczny:

- czym jest incydent bezpieczeństwa informacji,
- pierwsze minuty i godziny po wykryciu,
- zabezpieczenie, zgłoszenie, dokumentowanie,
- kiedy uruchamia się tryb RODO,
- komunikacja wewnętrzna i zewnętrzna.

Efekt:

- • prosty schemat reagowania dla firmy.

BLOK VI – Dobre praktyki i zasady SZBI do wdrożenia od razu

Zakres tematyczny:

- • cyberhigiena firmowa: hasła, MFA, poczta, dostęp,
- zasady pracy z dokumentami i danymi klientów,
- minimalne standardy organizacyjne,
- budowanie kultury bezpieczeństwa bez paraliżu.

Efekt końcowy warsztatów:

- • firmowy zestaw zasad **SZBI** (krótki, zrozumiały),
- lista „TOP 10 quick wins” dla zarządu i zespołów.

Harmonogram

Liczba pozycji harmonogramu: 10

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 10 BLOK I – Bezpieczeństwo informacji jako element zarządzania firmą	Zajęcia	MARCIN FILIPOWSKI	21-08-2026	09:00	09:45	00:45
2 z 10 BLOK II – SZBI (System Zarządzania Bezpieczeństwem Informacji) po biznesowemu	Zajęcia	MARCIN FILIPOWSKI	21-08-2026	09:45	10:30	00:45
3 z 10 -	Przerwa	-	21-08-2026	10:30	10:50	00:20
4 z 10 BLOK III – KSC / NIS2 a firmy (2026)	Zajęcia	MARCIN FILIPOWSKI	21-08-2026	10:50	11:30	00:40
5 z 10 BLOK IV – Najczęstsze cyberzagrożenia w firmach	Zajęcia	MARCIN FILIPOWSKI	21-08-2026	11:30	12:15	00:45
6 z 10 -	Przerwa	-	21-08-2026	12:15	12:35	00:20

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
7 z 10 BLOK V – Incydent bezpieczeństwa: jak reagować bez chaosu	Zajęcia	MARCIN FILIPOWSKI	21-08-2026	12:35	13:15	00:40
8 z 10 BLOK VI – Dobre praktyki i zasady SZBI do wdrożenia od razu + podsumowanie	Zajęcia	MARCIN FILIPOWSKI	21-08-2026	13:15	14:00	00:45
9 z 10 -	Przerwa	-	21-08-2026	14:00	14:20	00:20
10 z 10 -	Walidacja	MARCIN FILIPOWSKI	21-08-2026	14:20	14:40	00:20

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	05:40
w tym suma godzin zajęć	04:20
w tym suma godzin walidacji	00:20
w tym suma przerw	01:00
Suma godzin dydaktycznych bez przerw	06:10

Cennik

Jeżeli korzystasz z dofinansowania w wysokości co najmniej 70% przysługuje Tobie zwolnienie z podatku VAT

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	1 291,50 PLN

Koszt przypadający na 1 uczestnika netto	1 050,00 PLN
--	--------------

Koszt osobogodziny brutto	227,91 PLN
---------------------------	------------

Koszt osobogodziny netto	185,29 PLN
--------------------------	------------

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
---------------	---------------

Liczba godzin zegarowych usługi	05:40
---------------------------------	-------

Prowadzący

Liczba prowadzących: 1



1 z 1

MARCIN FILIPOWSKI

Audytor Wiodący Systemu Zarządzania Bezpieczeństwem Informacji ISO/IEC 27001, z doświadczeniem w audytach, doradztwie i szkoleniach dla firm z sektora przemysłowego i usługowego.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Każdy uczestnik otrzymuje certyfikat, materiały w formie elektronicznej, notes, długopis.

Adres

Katowice
Katowice
woj. śląskie

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi

Kontakt

 Ilona Pawłowska



E-mail ilona.pawlowska@formatrix.pl

Telefon (+48) 502 702 435