



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

Numer usługi 2026/05/20/11918/3573417

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

★★★★★ 4,6 / 5  
406 ocen

📄 Usługa szkoleniowa  
📺 zdalna  
🕒 05:40 h  
📅 10.07.2026 do 10.07.2026

## Informacje podstawowe

<b>Kategoria</b>	Informatyka i telekomunikacja / Bezpieczeństwo IT
<b>Grupa docelowa usługi</b>	<ul style="list-style-type: none"><li>właścicielka/właściciel firmy, zarząd, dyrekcja,</li><li>menedżerowie i kierownicy działów,</li><li>pracownicy biurowi, administracja, back office,</li><li>sprzedaż, obsługa klienta, HR, jakość,</li><li>osoby odpowiedzialne za dokumentację, dane i procesy.</li></ul> <p>Szkolenie jest <b>przeznaczone dla decydentów i pracowników</b>, którzy na co dzień przetwarzają informacje i podejmują decyzje.</p>
<b>Minimalna liczba uczestników</b>	10
<b>Maksymalna liczba uczestników</b>	20
<b>Data zakończenia rekrutacji</b>	09-07-2026
<b>Forma prowadzenia usługi</b>	zdalna
<b>Podstawa uzyskania wpisu do BUR</b>	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"><li>- omawia zasady poufności, integralności i dostępności informacji,</li><li>- rozróżnia elementy SZBI,</li><li>- wskazuje podstawowe wymagania KSC/NIS2 dla organizacji</li></ul>	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik identyfikuje zagrożenia cyberbezpieczeństwa oraz dobiera działania ograniczające ryzyko w organizacji	<ul style="list-style-type: none"><li>- rozpoznaje przykłady phishingu i prób wyłudzeń,</li><li>- wskazuje działania ograniczające ryzyko incydentów,</li><li>- dobiera podstawowe zasady cyberhigieny w środowisku pracy</li></ul>	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik stosuje podstawowe zasady reagowania na incydenty bezpieczeństwa informacji	<ul style="list-style-type: none"><li>- wskazuje działania podejmowane po wykryciu incydentu,</li><li>- rozróżnia zasady zgłaszania i dokumentowania incydentów,</li><li>- identyfikuje błędy w reagowaniu na incydenty</li></ul>	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"><li>- wskazuje znaczenie współpracy w obszarze bezpieczeństwa informacji,</li><li>- rozróżnia role pracowników i kadry zarządzającej w SZBI,</li><li>- identyfikuje znaczenie kultury bezpieczeństwa w organizacji</li></ul>	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.

## 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 z 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, jeżeli 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	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

# Informacje dodatkowe

## Informacje o materiałach dla uczestników usługi

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

## Warunki techniczne

Wymagany dostęp do komputera ze stabilnym łączem internetowym oraz aplikacja Zoom.

## Kontakt



**Ilona Pawłowska**

**E-mail** [ilona.pawlowska@formatrix.pl](mailto:ilona.pawlowska@formatrix.pl)

**Telefon** (+48) 502 702 435