



# PRAKTYCZNE BEZPIECZEŃSTWO ORGANIZACJI

OPARTE NA PODEJŚCIU **ISO/IEC 27001**



**CYBERZAGROŻENIA**

Jak chronić organizację w praktyce



Część 1

**FUNDAMENTY**



**DARIUSZ GOŁĘBIOWSKI**

**AUDYTOR WIODĄCY**

Systemu Zarządzania Bezpieczeństwem Informacji  
**ISO 27001**



**LUDZIE**  
świadomość  
i kultura



**PROCESY**  
zasady  
i procedury



**TECHNOLOGIA**  
narzędzia  
i zabezpieczenia



**ZGODNOŚĆ**  
normy  
i regulacje

**poswojsku.pl**

AKADEMIA BEZPIECZEŃSTWA GDDM

Wszelkie prawa do zawartości tej książki są zastrzeżone. Nieautoryzowane przez autora rozpowszechnianie całości lub dowolnego fragmentu niniejszej publikacji w jakiegokolwiek postaci jest zabronione. Wykonanie kopii jakiegokolwiek z dostępnych metod (m.in.: elektroniczną, kserograficzną, fotograficzną) spowoduje naruszenie praw autorskich niniejszego dzieła.

Pamiętaj proszę: bardzo się napracowałem :), uszanuj moje zaangażowanie i godziny pracy spędzone nad napisaniem oraz opracowaniem poradnika: **Praktyczne bezpieczeństwo organizacji oparte na podejściu ISO/IEC 27001 Część 1 Fundamenty**. Poradnik powstał na bazie aktualnych przepisów oraz materiałów doradczo-szkoleniowych GDDM i poswojsku.pl, w tym szkoleń on-line dostępnych na portalu Akademia Bezpieczeństwa GDDM&poswojsku [poswojsku.com.pl](http://poswojsku.com.pl)

**UWAGA – AI!**

***Grafiki umieszczone w poradniku zostały stworzone przez AI – na podstawie opisów przygotowanych przez Autora.***

Autor oraz Wydawnictwo poswojsku.pl

1. dołożyli wszelkich starań, by zawarte w tej książce informacje były kompletne, poprawne oraz rzetelne,
2. nie ponoszą żadnej odpowiedzialności za ewentualne szkody, które mogą wyniknąć z wykorzystania informacji zawartych w tej książce.

Wydawnictwo poswojsku.pl – kontakt:

[www.poswojsku.pl](http://www.poswojsku.pl), [bok@poswojsku.pl](mailto:bok@poswojsku.pl)

ul. Paprocka 86, 98-220 Zduńska Wola

ISBN: 978-83-68360-31-8

Copyright © poswojsku.pl 2026

***Material edukacyjny oparty na podejściu do zarządzania bezpieczeństwem informacji zgodnym z ISO/IEC 27001. Nie jest to dokument certyfikacyjny ani oficjalna publikacja ISO.***

## **Od Autora Kilka słów o formach żeńskich i męskich**

### **Wspaniała Czytelniczko - Drogi Czytelniku**

Zależy mi, aby moje publikacje były przyjazne dla wszystkich osób. Jednocześnie staram się pisać w sposób prosty, naturalny i wygodny w czytaniu.

Dlatego w książce czasami używam form męskich, a czasami żeńskich. Wszystkie odnoszą się do każdej osoby czytającej tę publikację, niezależnie od płci, wieku, pochodzenia, stanowiska czy sposobu, w jaki sama siebie określa.

Nie stosuję konsekwentnie zapisów typu „czytelnik/czytelniczka”, „nauczyciel/nauczycielka” itp., ponieważ utrudniają one płynność czytania.

Jeżeli ktoś zauważy, że liczba końcówek męskich nie zgadza się z liczbą końcówek żeńskich, z góry przepraszam. Nie jest to działanie zamierzone – po prostu jestem autorem książek ;), a nie księgowym końcówek językowych.

**Życzę przyjemnej lektury wszystkim osobom  
czytającym tę książkę.**

# **Praktyczne bezpieczeństwo organizacji oparte na ISO 27001 Część 1 Fundamenty**

Poradnik powstał na bazie wewnętrznych materiałów szkoleniowych i doradczych właściciela firmy GDDM [www.gddm.com.pl](http://www.gddm.com.pl) będącego certyfikowanym Audytorem Wiodącym Systemu Zarządzania Bezpieczeństwem Informacji ISO 27001



## **Spis treści**

### **WPROWADZENIE: DLACZEGO CZYTASZ TĘ KSIĄŻKĘ?..... 13**

Dlaczego napisałem tę książkę: Misja walki z mitem „bezpieczeństwa jako kosztu”.....	15
Dla kogo jest ta książka?.....	17
Krajobraz regulacyjny w UE: Dlaczego „teraz” jest kluczowe?.....	19
Główna teza: Więcej porządku, a nie więcej „bezpieczeństwa”.....	20

### **Co to jest ISO 27001?..... 22**

1. ISO 27001 to „Plan Budowy Bezpiecznego Domu”.....	23
2. ISO 27001 to „System Zarządzania” (a nie - jednorazowa akcja).....	24
3. ISO 27001 to „Certyfikat Zaufania”.....	26

*Praktyczne bezpieczeństwo organizacji oparte na ISO 27001*

Czym ISO 27001 NIE jest? (Najczęstsze mity).....27  
Podsumowując:.....28

**ROZDZIAŁ 1: DLACZEGO ORGANIZACJE  
WPADAJĄ W KŁOPOTY.....30**

Scenariusz A: Paraliż urzędowy (Ransomware).....34  
Scenariusz B: „Wysyłka do wszystkich” (Wyciek danych)  
..... 36  
Scenariusz C: „Ups, nie chciałem” (Błąd ludzki).....38  
Scenariusz D: Syndrom „Starego Marka” (Odejście  
kluczowego pracownika).....39  
Scenariusz E: Klasyk gatunku (Phishing).....41  
Analiza wspólnego mianownika.....42  
Technologia vs. Organizacja.....43  
Podsumowanie rozdziału.....44  
DODATEK DO ROZDZIAŁU 1: Dlaczego organizacje  
wpadają w kłopoty.....45

**ROZDZIAŁ 2: CZYM NAPRAWDĘ JEST  
BEZPIECZEŃSTWO ORGANIZACJI.....47**

Bezpieczeństwo jako zdolność do działania.....51  
1. Ciągłość działania (Continuity) – „Biznes musi żyć”  
.....52

2. Odporność (Resilience) – „Zdolność do powrotu”....	52
3. Zgodność (Compliance) – „Prawo do działania”.....	53
4. Klasyczna Triada CIA – „Składniki bezpieczeństwa” .....	54
Przykład z życia: Szpital vs. Sklep internetowy.....	55
Bezpieczeństwo jako Enabler (Umożliwiacz).....	57
Podsumowanie rozdziału.....	61
DODATEK DO ROZDZIAŁU 2: Czym naprawdę jest bezpieczeństwo organizacji.....	62
<b>ROZDZIAŁ 3: Informacja jest aktywem - Myślenie ISO.....</b>	<b>64</b>
Zmiana paradygmatu: Informacja jako paliwo biznesowe.	69
Katalog Aktywów – Przykłady sektorowe.....	70
Koncepcja Właścicielstwa Aktywów: Kluczowy punkt ISO .....	72
Klasyfikacja informacji – Oddzielanie „szumu” od „diamentów”.....	74
Podsumowanie i konkluzja rozdziału.....	76
DODATEK DO ROZDZIAŁU 3: Informacja jest aktywem .....	77
<b>ROZDZIAŁ 4: RYZYKO – NAJWAŻNIEJSZE SŁOWO W BEZPIECZEŃSTWIE.....</b>	<b>79</b>

Co to właściwie jest ryzyko? (Definicja zrozumiała dla większości ludzi).....	83
Iluzja 100% bezpieczeństwa.....	85
Skutki, które bolą (Typologia skutków).....	87
Apetyt na ryzyko – jak podejmować rozsądne decyzje?....	89
Zarządzanie zamiast paniki – cztery drogi reakcji.....	91
Podsumowanie rozdziału.....	93
<b>ROZDZIAŁ 5: LUDZIE, PROCESY I TECHNOLOGIA (ZŁOTY TRÓJKĄT).....</b>	<b>96</b>
Wstęp: Pułapka „Magicznego Pudełka”.....	99
Koncepcja Złotego Trójkąta.....	101
Filar 1: Ludzie (Świadomość i Kultura).....	103
Filar 2: Procesy (Zasady Gry).....	106
Filar 3: Technologia (Narzędzia i Automatyzacja).....	108
Synergia w praktyce – Przykład „Nowego Pracownika”. ..	110
Podsumowanie i konkluzja rozdziału.....	113
DODATEK DO ROZDZIAŁU 5: LUDZIE, PROCESY I TECHNOLOGIA (ZŁOTY TRÓJKĄT).....	114
<b>ROZDZIAŁ 6: CZYM JEST ISO 27001?.....</b>	<b>116</b>
ISO jako mapa, a nie cel podróży.....	121
Serce normy: Podejście oparte na ryzyku (Risk-based approach).....	123

Standard globalny – Twój „paszport” w biznesie.....	125
ISO 27001 jako „szablon porządku” .....	127
Podsumowanie dla Zarządu – Dlaczego w ogóle to robimy? .....	129
DODATEK DO ROZDZIAŁU 6: CZYM JEST ISO 27001? .....	131

## ROZDZIAŁ 7: Czym jest SZBI (System Zarządzania Bezpieczeństwem Informacji) ..... 133

Architektura SZBI: To nie jest program komputerowy!..	136
Kluczowe komponenty SZBI (Filarowe elementy układanki).....	138
1. Polityka Bezpieczeństwa czyli Zasady gry.....	138
2. Role i Odpowiedzialności czyli Kto trzyma “czujkę dymu”?.....	139
3. Analiza Ryzyka czyli Co widzimy?.....	140
4. Zarządzanie Incydentami czyli Co robimy, gdy coś pójdzie nie tak?.....	141
5. Doskonalenie czyli magiczny Cykl PDCA – Planuj, Wykonaj, Sprawdź, Działaj.....	142
SZBI jako żywy organizm.....	143
Podsumowanie – SZBI w pigułce dla lidera:.....	144

DODATEK DO ROZDZIAŁU 7: Czym jest SZBI (System Zarządzania Bezpieczeństwem Informacji).....	145
<b>ROZDZIAŁ 8: ODPOWIEDZIALNOŚĆ KIEROWNICTWA.....</b>	<b>147</b>
Kto trzyma klucze? Dlaczego bezpieczeństwo nie jest „problemem IT” .....	150
Podział ról: Kto robi co?.....	152
Rola Zarządu (Decyzje, zasoby, kultura).....	152
Rola CISO / Specjalisty (Rady, implementacja, nadzór) .....	153
Czego nie można delegować? (Hard Truths).....	154
Scenariusz „Kto odpowiada za wyciek?” – Analiza konsekwencji.....	156
Podsumowanie dla Zarządu – Twoja lista kontrolna:.....	158
DODATEK DO ROZDZIAŁU 8: Odpowiedzialność Kierownictwa.....	160
<b>ROZDZIAŁ 9: Pierwsze 30 dni budowy bezpieczeństwa (Checklista).....</b>	<b>162</b>
Tydzień 1: Inwentaryzacja i Świadomość (Poznaj swoje aktywa).....	165
Tydzień 2: Struktura i Ludzie (Określenie ról).....	167


*Praktyczne bezpieczeństwo organizacji oparte na ISO 27001*


Tydzień 3: Diagnoza Ryzyka (Wykazanie zagrożeń).....	169
Tydzień 4: Plan Działań (Quick Wins i Priorytety).....	171
Złota Zasada: Nie próbuj naprawić wszystkiego naraz!...	173
Checklist: Twoje pierwsze 30 dni.....	174
DODATEK DO ROZDZIAŁU 9: Pierwsze 30 dni budowy bezpieczeństwa.....	176
<b>ROZDZIAŁ 10: Twoja droga dalej.....</b>	<b>178</b>
Bezpieczeństwo to maraton, nie sprint.....	181
Twoja mapa drogowa: Co dalej?.....	182
Część 2 Analiza ryzyka w praktyce.....	182
Część 3 Kontrolki i zabezpieczenia techniczne.....	182
Część 3 Dokumentacja SZBI (Szablony i praktyka)...	183
Część 4 Audyt wewnętrzny IS 27001.....	183
Część 5 Kontekst regulacyjny: NIS2, KSC, RODO....	183
Słowo końcowe: Twoja nowa rola.....	184
DODATEK DO ROZDZIAŁU 10: Droga dalej.....	185
<b>Epilog: Architektura Zaufania – Twoja Nowa Rola.....</b>	<b>186</b>
Od „Gaszenia Pożarów” do „Budowania Fundamentów” .....	188
Twoje pierwsze 24 godziny.....	189
Słowo końcowe.....	190


*Praktyczne bezpieczeństwo organizacji oparte na ISO 27001*

Co będzie w kolejnych częściach poradnika: Praktyczne  
bezpieczeństwo organizacji oparte na ISO 27001?.....191

ZAPROSZENIE.....193

 Poznaj inne książki poswojsku.pl.....195

 Szkolenia i Webinary.....199

 Zostańmy w kontakcie!.....201



**WPROWADZENIE:  
DLACZEGO CZYTASZ TĘ  
KSIĄŻKĘ?**

W tej sekundzie, w Twoim biurze, zaczyna się chaos. Informatycy biegną do serwerowni, prawnice zaczynają nerwowo przeszukiwać akta dotyczące RODO, a Ty – osoba odpowiedzialna za bezpieczeństwo zastanawiasz się, czy ta sytuacja jest wynikiem wielomiesięcznego planowania napastnika, czy może po prostu dlatego, że pracownik z działu marketingu kliknął w link z „darmową promocją na pizzę”?

Większość organizacji reaguje na takie sytuacje jak na klęskę przeznaczenia. Jednak jako ekspert bezpieczeństwa powiem właśnie Tobie coś, co może być nieprzyjemne dla niektórych:

**To nie był wypadek. To był brak systemu. Kto zawalił? Dział IT? Czyżby? Tak uważasz?**

**Szefostwo powinno wiedzieć – za bezpieczeństwo nie odpowiada IT, tylko .. osoby zarządzające organizacją. Hmm, czyli być może .. Ty?**

**Właśnie powyższe idee oparte na metodologii ISO 27001 - przyświecają powstaniu tego poradnika.**

## **Dlaczego napisałem tę książkę: Misja walki z mitem „bezpieczeństwa jako kosztu”**

W świecie korporacyjnym i administracyjnym panuje powszechny mit: bezpieczeństwo IT to „podatek”, który trzeba płacić. To czarna dziura w budżecie, w której pieniądze znikają na drodze firewalle, których nikt nie rozumie i oprogramowanie, które tylko spowalnia pracę pracowników, a nawet pracownic ;). Wyobraź sobie taką scenę:

Jest czwartek, godzina 15:45. Telefon Twojego dyrektora generalnego dzwoni, wyświetla się nieznany numer. Po drugiej stronie słychać spokojny, niemal uprzejmy głos:

*„Dzień dobry, mamy dostęp do Państwa bazy danych klientów oraz systemów księgowych. Chcemy porozmawiać o warunkach odblokowania danych”.*

**Moim zadaniem jest zburzenie wyżej wymienionego mitu.**

Chcę Ci pokazać, że bezpieczeństwo nie jest kosztem. Bezpieczeństwo jest **fundamentem ciągłości biznesowej**. Jeśli porównamy organizację do samochodu, bezpieczeństwo nie jest hamulcem, który ma nas zatrzymać. Hamulec jest po to, abyśmy mogli jechać *szybciej i bezpieczniej*. Bez hamulców nikt nie odważyłby się wjechać na autostradę z prędkością 120 km/h.

Ta książka powstała z frustracji obserwowani organizacji, które kupują najdroższe „zamki” do drzwi, zostawiając jednocześnie okna otwarte na oścież. Piszę ją, aby przenieść ciężar dyskusji z „**ile wydamy na nowe narzędzia**” na „**jak zbudujemy odporną organizację**”.

## **Dla kogo jest ta książka?**

Ten poradnik nie jest przeznaczony wyłącznie dla „technicznych świrów”. Wręcz przeciwnie – jest stworzony dla każdego, kto ma udział w sukcesie organizacji:

- **Dla Kadry Zarządzającej (C-level):**

Jeśli potrzebujesz zrozumieć ryzyko biznesowe, sposób na uniknięcie kar regulacyjnych i sposób na budowanie zaufania klientów poprzez bezpieczne procesy.

- **Dla Oficerów Bezpieczeństwa (CISO):**

Jeśli szukasz konkretnej mapy drogowej, jak wdrożyć ISO 27001 bez „marnowania czasu” na biurokrację, która nie ma przełożenia na rzeczywiste zabezpieczenia.

- **Dla Menedżerów:**

Jeśli chcesz wiedzieć, jak zabezpieczyć swoje zespoły, jakie procedury wprowadzić w pracy i jak nie być „wąskim gardłem” w procesie wdrażania zmian.

- **Dla Pracowników (szczególnie pragnących rozpocząć karierę w cyberbezpieczeństwie):**

Jeśli chcesz zrozumieć, dlaczego Twoje hasło jest ważne, dlaczego procedury istnieją i jak stać się „żywą tarczą” organizacji, a nie jej najsłabszym ogniwem.

**Serdecznie zapraszam na kolejne strony mojego poradnika :) o bezpieczeństwie organizacji,**

**Autor: Dariusz Gołębiowski**

**Audytor Wiodący Systemu Zarządzania  
Bezpieczeństwem Informacji ISO 27001**

**strona domowa: [www.gddm.com.pl](http://www.gddm.com.pl)**

## **Krajobraz regulacyjny w UE: Dlaczego „teraz” jest kluczowe?**

Jeśli myślisz, że „moim małym biznesem/organizacją nikt się nie zainteresuje”, to czas na małą korektę planów. Unia Europejska właśnie „podkręciła śrubę”.

Wchodzimy w erę **dyrektywy NIS2**. To już nie jest tylko opcjonalny „dobryton”. To zestaw twardych wymagań dotyczących odporności cyfrowej, raportowania incydentów i łańcucha dostaw dla szerokiego spektrum sektorów – od energetyki po administrację publiczną i medycynę.

Łącząc to z RODO oraz rosnącymi wymaganiami w obszarze cyberbezpieczeństwa, stajemy przed faktem: **bezpieczeństwo staje się warunkiem koniecznym do prowadzenia działalności**. Niezapewnione bezpieczeństwo to ryzyko prawne, finansowe i

wizerunkowe, które może wykluczyć organizację z rynku w jeden dzień.

## **Główna teza: Więcej porządku, a nie więcej „bezpieczeństwa”**

Oto najważniejsza lekcja, jaką wyciągniesz z tej książki: **Większość organizacji nie potrzebuje „więcej cyberbezpieczeństwa”.**

**Potrzebuje więcej porządku.**

Wielu liderów myśli, że rozwiązaniem problemu jest kupno kolejnego systemu detekcji zagrożeń. To tak, jakbyś chciał ***ugasić pożar w kuchni, kupując dodatkowe wiadra z wodą, zamiast wyłączyć palnik.***

**Chaos vs. Proces** Większość organizacji działa w trybie „gaszenia pożarów” (reaktywne podejście). Ktoś zgubił laptopa? Panika. Ktoś dostał phishing? Kryzys. Ktoś zmienił komputer? Dane zostały na starym dysku. To jest chaos.

Moja teza jest prosta:

**ISO 27001 to nie jest lista technicznych wymagań.**

**To system zarządzania porządkiem.**

- Zamiast „masz być bezpieczny”, ISO pyta: „Gdzie masz swoje dane? Kto ma do nich dostęp? Co się stanie, jeśli je zgubisz? Jak to naprawi?”.
- Zamiast „kupujemy nowy firewall”, ISO pyta: „Jaki jest nasz apetyt na ryzyko i czy ten proces jest powtarzalny?”.

W tej książce nauczysz się, jak przejść z trybu „czekamy, aż nas zhakują” do trybu

***„budujemy system, który jest odporny na ataki, zgodny z prawem i wspiera nasz rozwój”.***

**Zaczynamy.**

**Czas porzucić chaos na rzecz procesu.**

## **Co to jest ISO 27001?**

Jeśli usłyszałeś, że Twoja firma powinna wdrażać ISO 27001 albo SZBI oparte na metodologii ISO 27001, a Twoją pierwszą myślą było: *„Czy to oznacza, że muszę kupić jeszcze więcej drogich programów i zatrudnić armię informatyków?”* – mam dla Ciebie dobrą wiadomość. **Nie.**

Najprostsza definicja brzmi:

**ISO 27001 to światowy standard zarządzania bezpieczeństwem informacji.**

Ale co to oznacza w praktyce, jeśli nie jesteś ekspertem? Pozwól, że użyję trzech prostych porównań.

# 1. ISO 27001 to „Plan Budowy Bezpiecznego Domu”

Wyobraź sobie, że budujesz dom. Możesz kupić najdroższe drzwi, ale jeśli nie zaplanowałaś, gdzie wpuścisz gości, a okna zostawisz na parterze, drzwi nic nie znaczą.

ISO 27001 nie mówi Ci, jaką konkretnie markę zamka masz kupić. Zamiast tego daje Tobie i Twojej organizacji **kompletny plan**:

- Gdzie masz najcenniejsze rzeczy (pieniądze, dokumenty)?
- Kto ma do nich klucz i dlaczego?
- Co zrobisz, jeśli ktoś spróbuje włamać się w nocy?
- Jak często sprawdzasz, czy zamki nadal działają?

## **2. ISO 27001 to „System Zarządzania” (a nie - jednorazowa akcja)**

Wielu ludzi myśli, że bezpieczeństwo to „instalacja antywirusa” albo nie wyłączenie firewall. ISO 27001 mówi:

„Nie, bezpieczeństwo to **system**”.

To różnica między kupieniem gaśnicy (jednorazowe działanie), a posiadaniem kompleksowego systemu przeciwpożarowego, który obejmuje:

- **Szkolenie** ludzi, jak nie wywołać pożaru.
- **Procedury** ewakuacyjne.
- **Regularne przeglądy** instalacji.
- **Analizę ryzyka** (czy np. kuchnia nie jest zbyt blisko magazynu paliw?).

W języku ISO nazywamy to **SZBI (System Zarządzania Bezpieczeństwem Informacji)**. To „instrukcja obsługi” Twojej firmy, która pilnuje, by bezpieczeństwo było stałym elementem codziennej pracy, a nie projektem, który robi się raz w roku.

### **3. ISO 27001 to „Certyfikat Zaufania”**

Na rynku globalnym ISO 27001 działa jak „paszport” dla Twojej firmy. Kiedy pokazujesz klientowi certyfikat ISO 27001, mówisz mu:

*„Nie obiecuję Tobie magicznie, że nigdy nas nie zhakują (bo przy obecnym poziomie technologii - nikt nie może tego zagwarantować).*

*Ale obiecuję Tobie,, że mamy profesjonalny system, który identyfikuje zagrożenia, chroni Twoje dane zgodnie z najlepszymi światowymi standardami i potrafi zareagować, gdy coś pójdzie nie tak”.*

**ISO 27001 to system mający zapewnić tzw. “ciągłość działania”.**

## **Czym ISO 27001 NIE jest? (Najczęstsze mity)**

...

**SERDECZNIE DZIĘKUJĘ,  
ŻE ZAINTERESOWAŁEŚ/AŚ SIĘ MOIM  
PORADNIKIEM :)**

„Wiedza to dopiero początek – czas na działanie. Masz już fundamenty, teraz czas zbudować bezpieczną twierdzę. Przejdź do pełnej wersji poradnika, aby otrzymać gotowe checklisty, szablony i mapę drogową, która zmieni Twoje podejście do bezpieczeństwa z 'gaszenia pożarów' na realną kontrolę.”

**KUP PEŁNĄ WERSJĘ PORADNIKA**

[www.poswojsku.pl](http://www.poswojsku.pl)

**SERDECZNIE DZIĘKUJĘ,  
ŻE ZAINTERESOWAŁEŚ/AŚ SIĘ MOIM  
PORADNIKIEM :)**

**„Wiedza to dopiero początek – czas na działanie. Masz już fundamenty, teraz czas zbudować bezpieczną twierdzę. Przejdź do pełnej wersji poradnika, aby otrzymać gotowe checklisty, szablony i mapę drogową, która zmieni Twoje podejście do bezpieczeństwa z 'gaszenia pożarów' na realną kontrolę.”**

**KUP PEŁNĄ WERSJĘ PORADNIKA**

**[www.poswojsku.pl](http://www.poswojsku.pl)**

**Co będzie w kolejnych  
częściach poradnika:  
Praktyczne bezpieczeństwo  
organizacji oparte na ISO  
27001?**

**Seria główna (PL + EN)**

**Część 2 Analiza ryzyka w praktyce**

**Część 3 Zabezpieczenia i kontrolki**

**Część 4 Dokumentacja SZBI**

**Część 5 Audyt wewnętrzny ISO 27001**

**Część 6 NIS2 kontra ISO 27001**

**Autor: Dariusz Gołębiowski**

**Audyt Wiodący Systemu Zarządzania  
Bezpieczeństwem Informacji ISO 27001**

**strona domowa: [www.gddm.com.pl](http://www.gddm.com.pl)**

**Seria rozszerzona (tylko PL)**

**KSC kontra ISO 27001**

**SZBI dla szkoły publicznej (już w sprzedaży)**

**SZBI dla JST**

**SZBI dla małej firmy**

**szukasz poradnika?**

**napisz maila do Wydawnictwa Cyfrowego poswojsku**

**[bok@poswojsku.pl](mailto:bok@poswojsku.pl)**

**a jak tylko będzie dostępny**

**dostarczymy stosowną informację :).**

# **ZAPROSZENIE**

**Seria wydawnicza:**

**BEZPIECZEŃSTWO INFORMACJI CYBER AI KSC SZBI  
ISO 27001**

**Moduł 1 PODSTAWY**

**a już wkrótce kolejne moduły.**

**MODUŁ 2 Ryzyko i myślenie audytowe**

**MODUŁ 3 Dokumentacja, która ma sens**

**MODUŁ 4 Wdrożenie w praktyce**

**MODUŁ 5 Audyt wewnętrzny i doskonalenie**

**MODUŁ 6 Podsumowanie i dojrzałość**

**Poradniki – materiały edukacyjne dostępne  
będą w postaci:**

**A. ebooków dostępnych na [poswojsku.pl](http://poswojsku.pl)**

**B. szkolenia elearnig zakończonego certyfikatem  
Audytora Wewnętrznego na portalu Akademia  
Bezpieczeństwa GDDM - [poswojsku.com.pl](http://poswojsku.com.pl)**

**Serdecznie zapraszam do dalszego zgłębiania Twojej  
wiedzy i podnoszenia kompetencji w zakresie  
bezpieczeństwa informacji i cyberbezpieczeństwa.**

***AUTOR: Dariusz Gołębiowski***

***Audytor Wiodący Systemu Zarządzania  
Bezpieczeństwem Informacji ISO 27001***

***szkolę, doradzam, audytuję, wdrażam i porządkuję  
obszary: bezpieczeństwo informacji,  
cyberbezpieczeństwo, RODO i ryzyko informacyjne***

## **Poznaj inne książki poswojsku.pl**

Jeśli spodobał się Tobie ten poradnik i chcesz dalej rozwijać swoją wiedzę o cyberbezpieczeństwie, technologii i świadomym korzystaniu z internetu, oto moje inne książki, które mogą w tym pomóc. Każda z nich powstała z myślą o osobach, które szukają praktycznych wskazówek, konkretnych przykładów i języka zrozumiałego dla każdego.

### **Twoje bezpieczeństwo w świecie cyber i sztucznej inteligencji – Część 1: Wprowadzenie**

Kompleksowy wstęp do tematyki ochrony danych, prywatności i bezpiecznego korzystania z sieci. To książka dla tych, którzy chcą szybko zrozumieć, na czym polegają najważniejsze zagrożenia i jak zacząć się przed nimi skutecznie bronić – bez skomplikowanego żargonu. Znajdziesz tu przykłady z życia i proste instrukcje krok po kroku.

## **Twoje bezpieczeństwo w świecie cyber i sztucznej inteligencji – Część 2: Cyberhigiena**

Praktyczny przewodnik po codziennych nawykach, które realnie zwiększają Twoje bezpieczeństwo. Dowiesz się, jak tworzyć silne hasła, chronić urządzenia, wykrywać próby oszustw i przygotować swoją rodzinę na zagrożenia cyfrowe. To pozycja obowiązkowa, jeśli chcesz, żeby cyberhigiena była naturalną częścią Twojego życia.

## **Twoje bezpieczeństwo w świecie cyber i sztucznej inteligencji – Część 3: Dziecko i Ty**

Poradnik stworzony specjalnie dla rodziców i opiekunów, którzy chcą wprowadzać dzieci w cyfrowy świat z rozsądkiem i spokojem. Znajdziesz tu nie tylko zasady i rekomendacje, ale też gotowe sposoby rozmowy o bezpieczeństwie i budowania zaufania. Ta książka pomoże Ci chronić najmłodszych bez straszenia i nadmiernej kontroli.

## **AI w edukacji – Część 1: Praktyczny poradnik nie tylko dla nauczycieli**

Sztuczna inteligencja to nie tylko moda, ale i realne narzędzie, które może usprawnić naukę i pracę. W tej książce pokazuję, jak korzystać z AI w prosty sposób – od generowania treści, przez wspieranie kreatywności, po automatyzację codziennych zadań. Idealna dla edukatorek/edukatorów i osób, które chcą poznać podstawy nowoczesnych technologii.

## **AI w edukacji – Część 2: Praktyczne pomysły na kreatywną edukację**

Kontynuacja pierwszej części – pełna inspiracji, scenariuszy zajęć i ćwiczeń. Dowiesz się, jak prowadzić warsztaty i lekcje, które łączą AI z rozwojem kompetencji cyfrowych, logicznego myślenia i twórczego podejścia do nauki. Świetna pozycja dla wszystkich, którzy szukają konkretnych narzędzi i gotowych rozwiązań.

## **Stwórz Grę Mobilną**


Praktyczny przewodnik dla osób, które marzą o stworzeniu własnej gry na smartfon. Od absolutnych podstaw programowania w JavaScript i React Native, przez projektowanie rozgrywki, aż po publikację gry. Jeśli chcesz uczyć się kodowania w sposób ciekawy i namacalny, to ta książka będzie Twoim drogowskazem.

---

## **Saga CyberJestestwa**

Powieść science fiction dla tych, którzy chcą oderwać się od codzienności i zanurzyć w refleksyjnej historii o sensie istnienia, wolności i relacjach w obliczu zmian. To opowieść o ludziach i technologii, o wyborach i konsekwencjach – dla miłośniczek/miłośników literatury, którzy cenią głębsze przesłanie i oryginalny klimat.

Wszystkie moje ebooki możesz nabyć na:

 stronie wydawnictwa cyfrowego **poswojsku.pl**

## **Szkolenia i Webinary**

Jeśli chcesz pogłębić wiedzę, zdobyć praktyczne umiejętności i od razu wprowadzić je w życie – zapraszam Cię na moje szkolenia i webinary. Każde z nich zostało przygotowane tak, aby w przystępny sposób przekazać konkretne rozwiązania i pomóc Ci działać od zaraz.

### **Bezpieczni w sieci – Jak chronić siebie i rodzinę przed cyberzagrożeniami**

Szkolenie, w którym krok po kroku omawiam zagrożenia najczęściej dotykające rodziny – od fałszywych wiadomości i wyłudzeń danych, po ochronę urządzeń domowych i zabezpieczanie dzieci w internecie. Idealne dla rodziców, opiekunów i osób, które chcą działać świadomie.

### **Cyberbezpieczeństwo dla małych organizacji i firm**


Praktyczny warsztat dla właścicieli firm, fundacji i urzędów, którzy chcą nauczyć się chronić dane pracowników i klientów bez kosztownych wdrożeń. Omawiam darmowe narzędzia, procedury bezpieczeństwa i sposoby budowania kultury cyberhigieny w zespole.

### **AI w życiu codziennym – od podstaw**

Webinar pokazujący, jak sztuczna inteligencja może ułatwić pracę, naukę i organizację codziennych spraw. Dowiesz się, jak korzystać z AI do tworzenia treści, automatyzacji zadań i rozwijania nowych umiejętności – nawet jeśli nie masz doświadczenia technicznego.

### **Szyfrowanie danych – dyski, pliki, poczta**

Szkolenie wprowadzające w świat szyfrowania, pokazujące krok po kroku, jak zabezpieczyć swoje dane prywatne i firmowe za pomocą bezpłatnych narzędzi. Idealne dla każdego, kto chce uniknąć utraty poufnych informacji.

 **Cyfrowe bezpieczeństwo dziecka – jak mądrze wspierać młodych użytkowników internetu**

Spotkanie dla rodziców i nauczycieli, którzy chcą dowiedzieć się, jak rozmawiać z dziećmi o zagrożeniach online, jak ustawiać kontrolę rodzicielską i jak budować zaufanie w cyfrowym świecie.

**Aktualne terminy szkoleń i webinarów** znajdziesz na










stronie:  [poswojsku.pl](https://poswojsku.pl)

a webinarów: [www.poswojsku.com.pl](https://www.poswojsku.com.pl)

Zapraszam również do kontaktu – chętnie pomogę dobrać szkolenie odpowiednie dla Twoich potrzeb.

 **Zostańmy w kontakcie!**

**Jeśli chcesz być na bieżąco z nowymi książkami, szkoleniami i inspiracjami o cyberbezpieczeństwie, technologii i AI – zapraszam Cię do obserwowania moich profili. Dzięki temu nie przegapisz premier, promocji i wartościowych materiałów które tworzę: często, prosto, przystępnie i z humorem.**

- ◆ Strona internetowa  [poswojsku.pl](https://poswojsku.pl)
- ◆ Facebook  [facebook.com/poswojsku](https://facebook.com/poswojsku)
- ◆ YouTube  [youtube.com/@poswojsku](https://youtube.com/@poswojsku)
- ◆ LinkedIn  [linkedin.com/in/golebiowski-dariusz](https://linkedin.com/in/golebiowski-dariusz)
- ◆ Instagram  [instagram.com/poswojsku](https://instagram.com/poswojsku)
- ◆ Threads  [threads.com/@poswojsku](https://threads.com/@poswojsku)
- ◆ TikTok  [tiktok.com/@astilus](https://tiktok.com/@astilus)
- ◆ Amazon Author Page   
[amazon.com/author/dariuszgolebiowski](https://amazon.com/author/dariuszgolebiowski)
- ◆ Goodreads  [goodreads.com/dariuszgolebiowski](https://goodreads.com/dariuszgolebiowski)

**Proszę, dołącz do mnie – razem budujmy  
bezpieczniejszy i bardziej świadomy świat cyfrowy!**