

BEZPIECZEŃSTWO INFORMACJI

CYBER AI KSC SZBI ISO 27001



OCHRONA
INFORMACJI



TECHNOLOGIA
I AI



LUDZIE
I PROCESY



ZGODNOŚĆ
I NORMY



BEZPIECZNA
ORGANIZACJA



PODEJŚCIE
ISO/IEC 27001



Moduł 1

PODSTAWY

GOŁĘBIOWSKI DARIUSZ

Audytór Wiodący Systemu Zarządzania
Bezpieczeństwem Informacji ISO 27001



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 jakąkolwiek z dostępnych metod (m.in.: elektroniczną, kserograficzną, fotograficzną) spowoduje naruszenie praw autorskich niniejszego dzieła.

Pamiętaj proszę: napracowałem się, uszanuj moje zaangażowanie i godziny pracy spędzone nad napisaniem i opracowaniem poradnika:

BEZPIECZEŃSTWO INFORMACJI CYBER AI KSC SZBI ISO 27001 Moduł 1 Podstawy. Poradnik powstał na bazie Modułu szkolenia on-line dostępnego na portalu Akademia Bezpieczeństwa GDDM&poswojsku poswojsku.com.pl

Czytaj tylko legalnie kupione egzemplarze.

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, bok@poswojsku.pl

ul. Paprocka 86, 98-220 Zduńska Wola

ISBN: 978-83-68360-29-5

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.

BEZPIECZEŃSTWO INFORMACJI CYBER AI KSC SZBI ISO 27001 Moduł 1 PODSTAWY

Poradnik powstał na bazie szkolenia on-line na portalu www.poswojsku.com.pl . Gdy ukończysz w.w szkolenie - możesz otrzymać certyfikat:

Audytor Wewnętrzny.

Drugim sposobem uzyskania w.w. Certyfikatu jest egzamin, który przygotowany został na bazie tej serii poradników.





Szczegóły – prosimy o kontakt:

bok@poswojsku.pl



Spis treści




Lekcja 1.1 Dlaczego bezpieczeństwo informacji to nie jest temat IT.....	10
Wprowadzenie – obalamy pierwszy mit.....	14
Kto naprawdę „dotyka” informacji?.....	16
Skąd biorą się realne incydenty?.....	17
Przykład 1 – „To tylko mail...”.....	18
Przykład 2 – „Przecież wszyscy sobie ufamy”.....	19
Przykład 3 – „Tylko na chwilę wyszedłem”.....	20
Co z tego wynika?.....	21
Nowe spojrzenie – ISO.....	22
Ćwiczenie 1 szybka refleksja (2–3 min).....	23
Ćwiczenie 2 „kto ma dostęp?” (mini-analiza).....	24
Wyjaśnienie do Ćwiczenie 2.....	25
Podsumowanie punktu 1.1.....	36

Punkt 1.1 – dopasowanie do przykładowych grup odbiorców.....	37
 WERSJA A: DYREKTORZY / KADRA ZARZĄDZAJĄCA.....	38
Przykład poswojsku.....	39
Mini-ćwiczenie.....	40
 WERSJA B: PODMIOTY MEDYCZNE.....	41
 WERSJA C: NAUCZYCIELE/ NAUCZYCIELKI - SZKOŁY.....	43
 WERSJA D: URZĘDY / ADMINISTRACJA PUBLICZNA.....	45
Finalna myśl do punktu 1.1 - uniwersalna.....	47
Most do kolejnego punktu.....	47
Lekcja 1.2 Czym jest informacja i dlaczego jest zasobem.....	48
Cel tej lekcji.....	50
Wprowadzenie – zmiana perspektywy.....	51
Kluczowa myśl do zapamiętania.....	54
Jakie formy ma informacja?.....	55

Rodzaje informacji – nie wszystko jest takie samo.....	56
Przykład z życia – „to przecież nic ważnego” ..	57
Ćwiczenie.....	58
Dlaczego informacja „boli” dopiero po incydencie?.....	63
Puenta.....	65
„Most” do kolejnej porcji informacji.....	66
1.3 Trójkąt bezpieczeństwa informacji (CIA)....	67
Trójkąt bezpieczeństwa – tzw. Triada Bezpieczeństwa.....	68
Cel tej porcji wiedzy.....	71
Wprowadzenie – trzy pytania, które zawsze wracają.....	72
Kluczowa myśl - do zapamiętania.....	73

Element 1: Poufność (Confidentiality).....	74
Element 2: Integralność (Integrity).....	75
Element 3: Dostępność (Availability).....	76
Praktyczne przykłady.....	77
Dlaczego równowaga jest ważna?.....	78
Ćwiczenie.....	79
Puenta tej lekcji.....	80
Most do kolejnej porcji wiedzy.....	81
Lekcja 1.4 Bezpieczeństwo informacji w codziennej pracy.....	82
Cel tej lekcji.....	83
O czym naprawdę jest ta lekcja?.....	84
Typowe sytuacje ryzykowne (wszyscy je znamy).....	85
⚠️ Case Study: „5 minut nieuwagi, 5 lat problemów”.....	86
Ćwiczenie.....	91
Puenta 1.4.....	91
Lekcja 1.5 Najczęstsze błędy organizacji (i ludzi)	92

Cel.....	92
Ważne na start.....	93
Najczęstsze błędy (bez oceniania).....	93
Przykład „wszyscy wiedzą, jak jest”.....	94
Mini-checklista.....	95
Puenta 1.5.....	99
Lekcja 1.6 Rola człowieka w systemie	
bezpieczeństwa.....	100
Cel lekcji.....	101
Człowiek – najsłabsze ogniwo?.....	102
Cena Milczenia: Dlaczego strach to największy wróg	
uKSC/NIS2?.....	104
Psychologia Błędu: Dlaczego Twój mózg Cię oszukuje?	107
Świadomość zamiast strachu (Zmiana paradygmatu).....	109
Ćwiczenie refleksyjne: Test „Niewidzialnego Pracownika”	
.....	111
Plan działania dla Lidera - Jak budować Human Firewall?	
.....	113
Puenta 1.6.....	114
Lekcja 1.7 Podsumowanie MODUŁU 1 i	
przygotowanie do dalszej drogi.....	115
Cel tej lekcji.....	116
Co już wiesz po MODUŁ 1?.....	117
Dlaczego nie zaczynamy od narzędzi?.....	120
Co zmieniło się w Twoim spojrzeniu?.....	122
Jedno zdanie, które warto zapamiętać.....	123
Domknięcie MODUŁU 1.....	124

Most do MODUŁU 2 – naturalny krok dalej.	125
Co będzie w MODUŁE 2?.....	126
ZAPROSZENIE.....	127
 Poznaj inne książki poswojsku.pl.....	129
 Szkolenia i Webinary.....	133
 Zostańmy w kontakcie!.....	135



Lekcja 1.1

Dlaczego

bezpieczeństwo

informacji to nie

jest temat IT

Informacja to najcenniejszy zasób każdej organizacji.

**Bezpieczeństwo informacji to ochrona procesów
biznesowych i wartości organizacji (w tym
czynnika ludzkiego), a nie tylko konfiguracja
firewalli czy aktualizacja systemów.**

**Skuteczna odporność organizacji na zagrożenia
zależy od:**

ludzi,

procedur,

odpowiedzialności zarządu,

**ponieważ technologia jest jedynie narzędziem w
służbie zarządzania ryzykiem.**

Cel tej części poradnika:

złamanie mitu, że cyber = informatyk

Musisz sobie uzmysłowić, że:

- bezpieczeństwo informacji ≠ cyberbezpieczeństwo,
- każdy/a pracownik/pracownica jest „użytkownikiem informacji”,
- incydenty nie zaczynają się zwykle w serwerowni,
- postępowanie typu: „przecież tylko wysłałem/am maila...” czy „to było tylko jedno kliknięcie w link” – może doprowadzić do katastrofy Twojego pracodawcę.

Mini-refleksja:

Wskaż proszę - kto w Twojej organizacji ma dostęp do informacji? Podziel te osoby na dwie grupy:

A. pracujące przy komputerze,

B. nie używające komputera w codziennej pracy.

Przemyślenia koniecznie zapisz w pliku tekstowym lub na papierze, aby móc do nich sięgnąć ponownie, po przejściu przez kolejne części tego poradnika.

Wprowadzenie – obalamy pierwszy mit

Gdy pada hasło „**bezpieczeństwo informacji**”,
większość osób myśli:

- hasła,
- serwery,
- firewalle,
- informatyk/informatyczka „gdzieś tam na zapleczu”.

To naturalne. Ale... **to nieprawda** :).

Bezpieczeństwo informacji **zaczyna się dużo wcześniej:**

- przy biurku,
- przy telefonie,
- w mailu,
- na czacie.
- w rozmowie,
- w decyzji „komu to wysłać”.

Kluczowa myśl do zapamiętania

Jeśli pracujesz z informacją – jesteś częścią systemu bezpieczeństwa.

Niezależnie od stanowiska, działu czy wykształcenia.

**IT dba o systemy,
ludzie decydują, co z informacją robią.**

Kto naprawdę „dotyka” informacji?

Nie tylko dział IT czy księgowość. Informacje mają w rękach m.in.:

- sekretariat,
- kadry,
- księgowość,
- nauczyciele (w placówkach edukacyjnych),
- dyrekcja,
- handlowcy,
- pracownicy administracji,
- stażyści,
- pracownicy/pracownice ochrony,
- osoby sprzątające (tak, one też ;)).

Skąd biorą się realne incydenty?

Najczęstsze źródła problemów to:

- mail wysłany **do złej osoby**,
- załącznik otwarty „bo wyglądał normalnie”,
- link kliknięty, bo sprawiał wrażenie, że przyszedł od szefa (wójta, burmistrzynie, prezesa, kierowniczkę),
- dokument zostawiony na drukarce,
- rozmowa prowadzona „przy obcych”,
- zdjęcie ekranu wysłane na prywatny komunikator czy adres email,
- pendrive „znaleziony na biurku”.

! Żaden system IT tego **nie zatrzyma**.

Przykład 1 – „To tylko mail...”

Pracownik/ca wysła listę danych (uczniów, klientów, pacjentów) do osoby o podobnym nazwisku, co pierwotny cel wysyłki.

Efekt:

- naruszenie poufności,
- stres,
- procedura,
- czas,
- możliwe konsekwencje prawne.

Technicznie wszystko działało poprawnie.

Problemem była **ludzka decyzja.**

Przykład 2 – „Przecież wszyscy sobie ufamy”

Hasło do systemu zna kilka osób, „bo tak szybciej”.

W rzeczywistości jest mniej skomplikowanie, ale dużo bardziej niebezpiecznie.

Efekt:

- brak rozliczalności,
- brak kontroli,
- chaos przy incydencie („kto to zrobił?”).

To **nie jest zła wola**, zwykle, choć i tego nie można tak zupełnie wykluczyć. To **brak świadomości**, czyli zapewne brak odpowiednich szkoleń z tzw. komponentem warsztatowym.

Przykład 3 – „Tylko na chwilę wyszedłem”

Otwarty komputer, działający system,
ktoś przechodzi obok. Pełen dostęp!

Nieuwaga, lekkomyślność, a może
jeszcze coś gorszego?

Efekt:

- dostęp do danych,
- możliwość skopiowania, zmiany, zrobienia zdjęcia.

System był bezpieczny.

Zachowanie – niestety nie było.

Co z tego wynika?

Bezpieczeństwo informacji:

- **✗** nie zaczyna się od jakichkolwiek cyfrowych narzędzi,
- **✗** nie kończy się na IT, a nawet nie zaczyna od IT,
- **✓** zaczyna się od **myślenia każdej osoby w organizacji,**
- **✓** trwa w **codziennych, drobnych decyzjach**
– w naszych działaniach i ich braku.

Nowe spojrzenie – ISO

W filozofii ISO:

- informacja = **zasób**
- człowiek = **kluczowy element systemu**
- procedury mają pomagać, nie - straszyć

Nie chodzi o:

- karanie,
- podejrzliwość,
- kontrolę „dla kontroli”.

Chodzi o:

- świadomość,
- przewidywanie skutków,
- odpowiedzialność,
- zdrowy rozsądek.

Ćwiczenie 1 szybka refleksja (2–3 min)

Odpowiedz sobie (na kartce lub w głowie):

1. Z jakimi informacjami **pracuję codziennie**?
2. Które z nich byłyby problemem, gdyby trafiły „nie tam gdzie trzeba”?
3. W którym momencie dnia **najłatwiej o błąd**?

Nie oceniaj.

Rozważ przynajmniej kilka możliwych opcji.

Najlepiej spisz wszystkie spostrzeżenia i refleksje. Zachowaj te dane do dalszej analizy.

Ćwiczenie 2 „kto ma dostęp?” (mini-analiza)

Wypisz:

- jedną informację,
- kto ma do niej dostęp **oficjalnie**,
- kto ma do niej dostęp **w praktyce**.

Różnice bywają bardzo ciekawe.

Wyjaśnienie do Ćwiczenie 2

...

Serdecznie dziękuję za to, że poświęciłeś/aś swój czas na zapoznanie się z początkową częścią mojego poradnika.

Zapraszam do skorzystania z pełnej wersji ebooka:

***BEZPIECZEŃSTWO INFORMACJI CYBER AI KSC SZBI
ISO 27001 Moduł 1 PODSTAWY***

**Szczegóły oferty znajdziesz na stronie firmy
Wydawnictwo Cyfrowe poswojsku.pl**

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

**B. szkolenia elearnig zakończonego certyfikatem
Audytora Wewnętrznego na portalu Akademia
Bezpieczeństwa GDDM - 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***

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

**B. szkolenia elearnig zakończonego certyfikatem
Audytora Wewnętrznego na portalu Akademia
Bezpieczeństwa GDDM - 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 dotyczące 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

a webinarów: 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
- ◆ Facebook  facebook.com/poswojsku
- ◆ YouTube  youtube.com/@poswojsku
- ◆ LinkedIn  linkedin.com/in/golebiowski-dariusz
- ◆ Instagram  instagram.com/poswojsku
- ◆ Threads  threads.com/@poswojsku
- ◆ TikTok  tiktok.com/@astilus
- ◆ Amazon Author Page 
amazon.com/author/dariuszgolebiowski
- ◆ Goodreads  goodreads.com/dariuszgolebiowski

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