PRAKTYCZNE BEZPIECZEŃSTWO ORGANIZACJI

OPARTE NA ISO 27001

BEZPIECZEŃSTWO INFORMACJI | TECHNOLOGIA I AI | LUDZIE I PROCESY | ZGODNOŚĆ I NORMY | BEZPIECZNA ORGANIZACJA

CYBERZAGROŻENIA

Jak chronić organizację w praktyce

GOŁĘBIOWSKI DARIUSZ

AUDYTOR WIODĄCY

SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

ISO 27001

PRAKTYKA Z ORGANIZACJI | SPRAWDZONE METODY | JASNE WYJAŚNIENIA | REALNE KORZYŚCI

poswojsku.pl

AKADEMIA BEZPIECZEŃSTWA GDDM

Pamiętaj proszę:

napracowałem się, uszanuj moje zaangażowanie i godziny pracy spędzone nad napisaniem i opracowaniem poradnika: ***Praktyczne bezpieczeństwo organizacji oparte na ISO 27001***. 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

Czytaj tylko legalnie kupione egzemplarze.

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: 978-83-68360-31-8

Praktyczne bezpieczeństwo organizacji oparte na ISO 27001

Poradnik powstał na bazie wewnętrznych materiałów szkoleniowych i doradczych właściciela firmy GDDM www.gddm.com.pl będącego certyfikowanym Audytor Wiodącym Systemu Zarządzania Bezpieczeństwem Informacji ISO 27001

Spis treści

✨

WPROWADZENIE: DLACZEGO CZYTASZ TĘ KSIĄŻKĘ?

W tej sekundzie, w biurze, zaczyna się chaos. Informatycy biegną do serwerowni, prawnicy zaczynają nerwowo przeszukiwać akta dotyczące RODO, a Ty zastanawiasz się, czy ta sytuacja jest wynikiem wielomiesięcznego planowania napastnika, czy może po prostu dlatego, że pracownik z działu marketingu kliknął w link z „darmowym voucherem na pizzę".

Większość organizacji reaguje na takie sytuacje jak na klęskę przeznaczenia. Jednak jako ekspert bezpieczeństwa powiem Ci coś, co może być nieprzyjemne dla niektórych: **To nie był wypadek. To był brak systemu.**

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 czerny dziurę w budżecie, w której pieniądze znikają na drogie firewalle, których nikt nie rozumie, i oprogramowanie, które tylko spowalnia pracę pracowników.Wyobraź sobie taką scenę: Jest czwartek, godzina 15:45. Telefon Twojego dyrektora generalnego dzwoni, a na ekranie wyświetla się numer, którego nie rozpoznaje. 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 tego 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 obserwowaniem firm, 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:** Jeśli chcesz zrozumieć, dlaczego Twoje hasło jest ważne, dlaczego procedury istnieją i jak stać się „żywą tarczą" organizacji, a nie jej najsłabszym ogniwem.

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, 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. 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 phishinga? Kryzys. Ktoś odebrał stanowisko? 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 naprawisz?”.
- 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”.

Zaczynajmy. Czas porzucić chaos na rzecz procesu.

Co to jest ISO 27001?

Jeśli usłyszałeś, że Twoja firma powinna „wdrażać 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 zaplanowałeś, 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 Ci **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” (Nie jednorazowa akcja)

Wielu ludzi myśli, że bezpieczeństwo to „instalacja antywirusa”. ISO 27001 mówi: „Nie, bezpieczeństwo to **system**”. To różnica między kupieniem gaśnicy (jednorazowe działanie), a posiadaniem 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 Ci magicznie, że nigdy nas nie zhakują (bo nikt nie może tego zagwarantować). Ale obiecuję Ci, że mamy profesjonalny system, który identyfikuje zagrożenia, chroni Twoje dane zgodnie z najlepszymi światowymi standardami i potrafi zareagować, gdy coś pójdzie nie tak”.*

Czego ISO 27001 NIE jest? (Najczęstsze mity)

- **Nie jest listą „technicznych zabawliwek”:** To nie jest lista kontrolna „czy masz firewall”. To

lista pytań o zarządzanie: „czy wiesz, co robisz, gdy firewall zawiedzie?”.

- **Nie jest „papierologią dla samej papierologii”:** Jeśli dokumenty nie mają przełożenia na to, jak pracują ludzie i jak działają systemy, to wdrożenie ISO jest błędne.
- **Nie jest celem samym w sobie:** Celem ISO nie jest zdobycie certyfikatu na ścianę. Celem jest **odporność organizacji** na ataki, wycieki danych i błędy ludzkie.

Podsumowując:

ISO 27001 to przejście z trybu **„Mamy nadzieję, że nas nie zhakują”** do trybu **„Wiemy, co może pójść nie tak, i wiemy dokładnie, jak na to zareagować”**. To przejście od chaosu do uporządkowanego procesu, który chroni Twoje pieniądze, Twoich klientów i Twoją reputację.

ROZDZIAŁ 1: DLACZEGO ORGANIZACJE WPADAJĄ W KŁOPOTY

Plan Rozdziału

1. **Wstęp: Anatomia porażki** – Krótkie wprowadzenie w to, że cyberbezpieczeństwo to nie tylko „hakerzy w kapturach", ale realne ryzyka biznesowe.
2. **Scenariusze z życia wzięte (Autopsje):**
    1. *Scenariusz A: Paraliż urzędowy (Ransomware)* – Jak jeden klik może zatrzymać usługi publiczne.
    2. *Scenariusz B: „Wysyłka do wszystkich" (Wyciek danych)* – Koszty utraty zaufania i kary regulacyjne.
    3. *Scenariusz C: „Ups, nie chciałem" (Błąd ludzki)* – Przypadkowe usunięcie danych jako cichy zabójca ciągłości.

4. *Scenariusz D*: *Syndrom „Nieznajomego Marka" (Odejście kluczowego pracownika)* – Ryzyko utraty wiedzy.
5. *Scenariusz E*: *Klasyk gatunku (Phishing)* – Dlaczego najprostsza metoda wciąż działa.

3. **Analiza wspólnego mianownika** – Przejście od „co się stało" do „dlaczego to się stało".
4. **Technologia vs. Organizacja** – Dlaczego lepsze zabezpieczenia nie rozwiązują problemu braku procesów.
5. **Podsumowanie i konkluzja rozdziału – Fundament serii.**

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

Zapraszam do skorzystania z pełnej wersji ebooka:

Praktyczne bezpieczeństwo organizacji oparte na ISO 27001 Część 1 Fundamenty

Szczegóły oferty znajdziesz na stronie firmy Wydawnictwo Cyfrowe poswojsku.pl

ZAPRASZAM DO ZAKUPU PEŁNEJ WERSJI KSIĄŻKI

Co będzie w Części 2?

Część 1 – Fundamenty

Część 2 – Analiza ryzyka w praktyce

Część 3 – Kontrolki ISO 27001 bez bólu

Część 4 – Dokumentacja SZBI

Część 5 – Audyt wewnętrzny ISO 27001

Część 6 – NIS2, KSC i ISO 27001

Jeżeli chcesz szybki dostęp do Części 2 poradnika napisz maila do Wydawnictwa Cyfrowego poswojsku bok@poswojsku.pl a jak tylko będzie dostępny – dostarczymy stosowną informację :).

W następnej części:

- nauczysz się **tworzyć SYSTEM ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI (SZBI)**,
- przykładowe – wzorcowe dokumenty związane z wdrożeniem uKSC 2026 i NIS2,
- mnóstwo niezbędnej fachowej wiedzy podanej w przystępny, zrozumiały sposób.

SERDECZNIE ZAPRASZAM CIEBIE

AUTOR Audytor Wiodący Systemu Zarządzania Bezpieczeństwem Informacji ISO 27001

Dariusz Gołębiowski

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 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

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 budujmy bezpieczniejszy i bardziej świadomy świat cyfrowy!