BEZPIECZEŃSTWO INFORMACJI

CYBER AI KSC SZBI ISO 27001

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

Moduł 1

PODSTAWY

GOŁĘBIOWSKI DARIUSZ
Audytor Wiodący Systemu Zarządzania
Bezpieczeństwem Informacji ISO 27001

poswojsku.pl
AKADEMIA BEZPIECZEŃSTWA GDDM

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.

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

BEZPIECZEŃSTWO INFORMACJI CYBER AI KSC SZBI ISO 27001 Moduł 1 PODSTAWY

Poradnik powstał na bazie szkolenia on-line na portalu www.poswojsku.com.pl , z którego możesz otrzymać certyfikat:

Audytor Wewnętrzny

✨

Spis treści

✨

BEZPIECZEŃSTWO INFORMACJI CYBER AI KSC SZBI ISO 27001 PODSTAWY

Informacja jako najcenniejszy zasób każdej organizacji zasób.

Lekcja 1.1 Dlaczego bezpieczeństwo informacji to nie jest temat IT

Bezpieczeństwo informacji to ochrona procesów biznesowych i wartości organizacji, a nie tylko konfiguracja firewalli czy aktualizacja systemów.

Skuteczna odporność zależy od ludzi, procedur i odpowiedzialności zarządu, ponieważ technologia jest jedynie narzędziem w służbie zarządzania ryzykiem.

Cel:

złamanie mitu, że cyber = informatyk

- bezpieczeństwo informacji ≠ cyberbezpieczeństwo
- każdy pracownik jest „użytkownikiem informacji”

- gdzie naprawdę zaczynają się incydenty (nie w serwerowni)
- **case poswojsku**: „przecież tylko wysłałem/am maila…”

***Mini-refleksja*:**

Wskaż proszę - kto w Twojej organizacji ma dostęp do informacji, nawet jeśli nie ma komputera? Przemyślenia koniecznie zapisz, aby móc do nich sięgnąć w przyszłości.

Wprowadzenie – obalamy pierwszy mit

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

- hasła,
- serwery,
- firewalle,
- informatyków „gdzieś tam na zapleczu”.

To naturalne.
Ale… **to nieprawda**.

👉 Bezpieczeństwo informacji **zaczyna się dużo wcześniej** –
przy biurku, przy telefonie, w mailu, 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. Informacje mają w rękach m.in.:

- sekretariat,
- kadry,
- księgowość,
- nauczyciele,
- dyrekcja,
- handlowcy,
- pracownicy administracji,
- stażyści,
- osoby sprzątające (tak, one też – dokumenty na biurku).

Skąd biorą się realne incydenty?

Najczęstsze źródła problemów to:

- mail wysłany **do złej osoby**,
- załącznik otwarty „bo wyglądał normalnie”,
- dokument zostawiony na drukarce,
- rozmowa prowadzona „przy obcych”,
- zdjęcie ekranu wysłane na prywatny komunikator czy adres email,
- pendrive „znaleziony na biurku”.

❗ Żaden firewall tego **nie zatrzyma**.

Przykład 1 – „To tylko mail…”

Pracownik/ca wysyła 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, otwarty 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.

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

Przykłady informacji podlegających ochronie zgodnie z normą ISO 27001 i System Zarządzania Bezpieczeństwem Informacji (SZBI). Ważne jest zrozumienie, że informacja w kontekście SZBI to nie tylko dane cyfrowe, ale wszystko, co ma wartość dla organizacji i wymaga ochrony.

Oto kilka przykładów informacji z wyjaśnieniami, podzielone na kategorie, aby lepiej zobrazować różnorodność. Pamiętaj, że konkretne informacje wymagające ochrony będą zależeć od specyfiki działalności Twojej organizacji.

ZAPROSZENIE

Do zakupu pełnej wersji eBooka :)

i/lub szkolenia on-line na portalu

www.poswojsku.com.pl ,

z którego możesz otrzymać certyfikat:

Audytor Wewnętrzny Systemu Bezpieczeństwa Informacji i Cyberbezpieczeństwa

AUTOR: Dariusz Gołębiowski

Audytor Wiodący Systemu Zarządzania Bezpieczeństwem Informacji ISO 27001

📚 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!