



Cyberbezpieczeństwo i bezpieczeństwo informacji w urzędach publicznych

SZBI (ISO/IEC 27001) + praktyka urzędu + wymagania KSC/NIS2 – stan na 2026

Czas trwania:

Wariant A – 4 godziny lekcyjne (180 minut) – warsztaty praktyczne (1–2 osoby przy stanowisku)

Wariant B – maks. 4 godziny lekcyjne (180 minut) – forma pokazowa (1 stanowisko + projektor)

Przerwa: 15 minut

Forma: warsztaty + analiza realnych incydentów urzędowych + ćwiczenia decyzyjne

Adresaci: kierownictwo urzędu, kierownicy komórek, pracownicy merytoryczni, BOI, sekretariat, kancelaria, administratorzy informacji / osoby odpowiedzialne za bezpieczeństwo, IT (jako wsparcie)



CEL SZKOLENIA

Po szkoleniu uczestnicy:

- rozumieją, czym jest **bezpieczeństwo informacji** w urzędzie i jak łączy się z cyberbezpieczeństwem,
- rozumieją ideę i praktykę **SZBI – Systemu Zarządzania Bezpieczeństwem Informacji** (w podejściu ISO/IEC 27001),
- potrafią ograniczyć ryzyka: błędy, wycieki, phishing, przejęcia kont, błędne publikacje, utrata danych,
- wiedzą jak reagować na incydent: **kto / co / kiedy** (bez chaosu i zamiatania pod dywan),
- otrzymują proste zasady i zestaw decyzji, które urząd może wdrożyć „od jutra”.



STRUKTURA SZKOLENIA

BLOK I – Bezpieczeństwo informacji w urzędzie: co chronimy i dlaczego

Zakres:

- informacja jako zasób urzędu (dane mieszkańców, rejestry, sprawy, decyzje, pisma),
- triada CIA: poufność–integralność–dostępność w realiach JST,
- gdzie najczęściej „pęka” urząd (ludzie, procesy, narzędzia),

GDDM : Gołębiowski Dariusz Doradztwo Merytoryczne

Twoje partnerstwo w świecie technologii oraz innowacji

- różnica: **incydent** vs „wpadka” vs **naruszenie ochrony danych**.

Ćwiczenie:

- mapa zasobów informacji w urzędzie (3–5 kluczowych obszarów).
-

BLOK II – SZBI (System Zarządzania Bezpieczeństwem Informacji) „po ludzku”

Zakres:

- czym jest **SZBI** i po co go robić w urzędzie (nie dla papieru, tylko dla kontroli i spokoju),
- ISO/IEC 27001 jako filozofia: odpowiedzialność, ryzyko, zasady, ciągłe doskonalenie,
- „minimum SZBI”, które działa: polityka + role + zasady + reagowanie + szkolenia,
- jak nie zrobić „SZBI w segregatorze”, którego nikt nie stosuje.

Efekt praktyczny:

- szkic 10 zasad SZBI dla urzędu (krótko i egzekwowalnie).
-

BLOK III – KSC / NIS2 i urząd: co jest ważne w 2026

Zakres:

- gdzie urząd styka się z wymaganiami cyberbezpieczeństwa (organizacja, dostawcy, procedury),
- rola kierownictwa: odpowiedzialność i decyzje (a nie „to IT”),
- ryzyka wizerunkowe i operacyjne: przerwy w usługach, awarie, kompromitacja urzędu,
- jak rozpoznać obszary największego ryzyka i gdzie zacząć.

(Uwaga: bez „tłuczenia ustawą” – tylko to, co przekłada się na działania.)

PRZERWA – 15 minut

BLOK IV – Najczęstsze cyberzagrożenia w urzędach (2026)

Zakres:

- phishing i podsycia „na przełożonego”, „na dostawcę”, „na fakturę”, „na pismo”,
- przejęcia kont: e-mail, systemy, panele, skrzynki,
- złośliwe załączniki / linki / „dokumenty do podpisu”,
- błędy publikacyjne (BIP, załączniki, dane w plikach),

GDDM : Gołębiowski Dariusz Doradztwo Merytoryczne

Twoje partnerstwo w świecie technologii oraz innowacji

- praca zdalna, pendrive, prywatne urządzenia — realne ryzyka.

Ćwiczenie:

- „Zgłoszenie z BOI: dziwny mail / załącznik / prośba o pilne działanie — co robimy?”
-

BLOK V – Incydent bezpieczeństwa: procedura, która działa

Zakres:

- pierwsze 15 minut po incydencie: co robi pracownik, kierownik, IT,
- zasada: **zabezpiecz, zgłoś, nie pogarszaj**,
- dokumentowanie minimum: co zapisać, aby mieć kontrolę i dowody,
- kiedy to jest naruszenie danych i jak uruchomić właściwy tryb (RODO),
- komunikacja wewnętrzna i zewnętrzna (żeby nie było paniki i plotek).

Efekt:

- prosty „schemat reagowania” dla urzędu (do powieszenia na ścianie / intranecie).
-

BLOK VI – Dobre praktyki i zasady SZBI do wdrożenia od razu

Zakres:

- cyberhygiena urzędowa: hasła, MFA, poczta, dokumenty, dostęp,
- minimalne standardy: uprawnienia, kopie, aktualizacje, obieg dokumentów,
- zasady pracy z informacją: klasyfikacja, udostępnianie, publikowanie,
- jak budować kulturę bezpieczeństwa (bez straszenia i bez paraliżu).

Efekt końcowy warsztatów:

- wspólnie wypracowane zasady **SZBI dla urzędu** (wersja prosta, do wdrożenia),
 - rekomendacje „TOP 10 zmian” (quick wins) dla kierownictwa.
-

EFEKTY SZKOLENIA

Po szkoleniu urząd:

- ma jasność „kto za co odpowiada” w bezpieczeństwie informacji,
- ma fundament **SZBI** (Systemu Zarządzania Bezpieczeństwem Informacji) – w wersji realistycznej,
- zmniejsza ryzyko incydentów, skarg i kompromitacji urzędu,

GDDM : Gołębiowski Dariusz Doradztwo Merytoryczne

Twoje partnerstwo w świecie technologii oraz innowacji

- reaguje szybciej i spokojniej na incydenty,
- podnosi świadomość pracowników bez tworzenia strachu.



Prowadzący szkolenie

Szkolenie prowadzi **Audytór Wiodący Systemu Zarządzania Bezpieczeństwem Informacji ISO/IEC 27001**, z doświadczeniem w:

- audytach i wdrożeniach systemów bezpieczeństwa informacji,
- pracy z podmiotami publicznymi i prywatnymi,
- doradztwie w obszarze RODO, cyberbezpieczeństwa i zarządzania ryzykiem,
- przekładaniu przepisów i norm na **praktyczne działania organizacyjne**.

Szkolenie prowadzone jest z **perspektywy audytora**, a nie sprzedawcy rozwiązań IT.



Forma szkolenia

- szkolenie stacjonarne lub on-line,
- forma warsztatowa lub pokazowa,
- zakres dopasowywany do wielkości i charakteru placówki.

Jeżeli masz jakiegokolwiek pytania lub też chciałbyś/abyś dopasować szkolenie do potrzeb Twojej organizacji – serdecznie zapraszam do kontaktu – porozmawiajmy :): 509 869 388.

GDDM : Gołębiowski Dariusz Doradztwo Merytoryczne

Twoje partnerstwo w świecie technologii oraz innowacji

SZKOLENIA I WEBINARY przykłady zrealizowanych tematów

Jeśli chcesz pogłębić wiedzę, zdobyć praktyczne umiejętności i od razu wprowadzić je w życie – zapraszam Cię na moje szkolenia i webinaria. 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 on-line i webinarów - znajdziesz na stronie:  poswojsku.pl

A na www.gddm.com.pl – dowiesz się więcej o mnie i moich szkoleniach tradycyjnych

SERDECZNIE ZAPRASZAM DO WSPÓŁPRACY – DARIUSZ GOŁĘBIOWSKI :)

GDDM : Gołębiowski Dariusz Doradztwo Merytoryczne

Twoje partnerstwo w świecie technologii oraz innowacji

POZNAJ MOJE KSIĄŻKI

Jeśli tematyka tego szkolenia Ciebie zainteresowała, to poza profesjonalnymi kursami – możemy wspólnie uczyć się także z moich ebooków: wiedza o cyberbezpieczeństwie, technologii i świadomym korzystaniu z internetu. Każda z moich książek 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: Cyberhygiena

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 cyberhygiena 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.


GDDM : Gołębiowski Dariusz Doradztwo Merytoryczne

Twoje partnerstwo w świecie technologii oraz innowacji

SAGA CYBERJESTESTWA – seria książek fantazy

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 poradniki i inne ebooki - możesz nabyć na:

-  stronie wydawnictwa cyfrowego poswojsku.pl
-

ZOSTAŃMY W KONTAKCIE!

Jeśli chcesz być na bieżąco z nowymi książkami, szkoleniami i inspiracjami o cyberbezpieczeństwie, technologii i AI – zapraszam Ciebie 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 zbudujemy bezpieczniejszy i bardziej świadomy świat cyfrowy!