Podręcznik dla Szkół Średnich

Wspierający utrzymanie właściwego poziomu bezpieczeństwa informacji Szkoły oraz wspierający edukację i świadomość w obszarze cyberbezpieczeństwa.

Obraz zawierający godło, symbol, odznaka, herb

Opis wygenerowany automatycznie

Spis treści

[Dla kogo 3](#_heading=h.gjdgxs)

[Co znajdziesz w podręczniku? 3](#_heading=h.30j0zll)

[Określenie ról i odpowiedzialności 4](#_heading=h.1fob9te)

[Ustanowienie Systemu Zarzadzania Bezpieczeństwem Informacji 4](#_heading=h.3znysh7)

[Program Budowania Świadomości w obszarze Cyberbezpieczeństwa w Szkole 5](#_heading=h.2et92p0)

[Wykaz załączników 6](#_heading=h.tyjcwt)

[O autorze 6](#_heading=h.3dy6vkm)

**PODRĘCZNIK DLA SZKÓŁ ŚREDNICH**Wspierający utrzymanie właściwego poziomu bezpieczeństwa informacji Szkoły oraz wspierający edukację i świadomość w obszarze cyberbezpieczeństwa

Scenariusz opracowany w ramach projektu „CyberSec EduCheck” – projekt nr. 2023-2-PL01-KA210-VET-000176822

**Autorzy scenariusza:** Mateusz Pękala - Coventry University

**Projekt graficzny:** Karolina Kornecka-Kupiec, Jadwiga Maj – Stowarzyszenie KREA

*Wrocław 2024*

*Publikacja jest rozpowszechniana na zasadach licencji Creative Commons Uznanie autorstwa   
– Użycie niekomercyjne (CC BY-NC) 4.0 Międzynarodowe*

# Dla kogo?

Ten podręcznik jest dla Ciebie, jeśli:

→ Jesteś dyrektorem lub wicedyrektorem szkoły średniej i odpowiadasz za bezpieczeństwo informacji w swojej placówce

→ Zauważasz rosnącą potrzebę wprowadzenia skutecznych działań edukacyjnych w zakresie cyberbezpieczeństwa wśród uczniów i pracowników

→ Chcesz opracować zasady korzystania z technologii, które pomogą zapobiegać cyberprzemocy, dezinformacji oraz innym zagrożeniom cyfrowym

→ Szukasz praktycznych wskazówek, jak budować świadomość cyberzagrożeń w środowisku szkolnym, angażując zarówno uczniów, jak i personel

→ Chcesz, aby Twoja szkoła była przykładem dobrej praktyki w zarządzaniu bezpieczeństwem cyfrowym i ochroną danych

Ten podręcznik został opracowany, aby służyć jako kompleksowy przewodnik mający na celu pomoc dyrektorom szkół w opracowaniu solidnych ram edukacji w zakresie cyberbezpieczeństwa i zarządzania bezpieczeństwem informacji. Odpowiada on na wyzwania związane z zarządzaniem szkołą, a jego celem jest zapobieganie m.in. nieetycznym, niepewnym i ryzykownym zachowaniom wśród młodzieży korzystającej z technologii.

# Co znajdziesz w podręczniku?

Podręcznik dostarcza narzędzi, które pomogą Ci skutecznie wdrożyć program bezpieczeństwa informacji w szkole:

* **Określenie ról i odpowiedzialności** – Dowiesz się, jak jasno przypisać zadania związane z bezpieczeństwem informacji wszystkim pracownikom, od nauczycieli po kadrę zarządzającą.
* **Ustanowienie polityk bezpieczeństwa** – Dowiesz się, jak wdrożyć System Zarządzania Bezpieczeństwem Informacji oraz Politykę Bezpieczeństwa Informacji, co zapewni ochronę danych w Twojej szkole.
* **Program budowania świadomości** – Znajdziesz propozycję działań edukacyjnych, które pomoże zwiększyć świadomość cyberzagrożeń wśród uczniów i pracowników.

W załącznikach do podręcznika znajdziesz szablony dokumentów. Te narzędzia pomogą dostosować zasady bezpieczeństwa do specyfiki Twojej szkoły, budując solidne fundamenty cyfrowego bezpieczeństwa. Przeczytaj podręcznik i wykorzystaj szablony, by skutecznie zarządzać bezpieczeństwem informacji w Twojej placówce.

# Określenie ról i odpowiedzialności

W szkołach, gdzie zasoby są ograniczone i priorytetem jest realizacja programu nauczania oraz opieka nad uczniami, ważne jest jasne określenie ról i odpowiedzialności za bezpieczeństwo informacji. To kluczowy pierwszy krok w budowaniu Systemu Zarządzania Bezpieczeństwem Informacji.

Każdy członek społeczności szkolnej, od nauczycieli, wychowawców i pedagogów po psychologów i dyrekcję, ma swoją rolę w dbaniu o cyberbezpieczeństwo. Wyznaczenie odpowiednich ról i obowiązków zapewnia, że działania związane z bezpieczeństwem informacji będą skutecznie realizowane na wszystkich poziomach szkoły, a ustalone zasady będą przestrzegane.

Aby ułatwić ten proces, w załączniku znajdziesz szablon „Role i obowiązki w SZBI” (dokument 02) oraz nadrzędny dokument „Polityka Bezpieczeństwa Informacji” (dokument 01). Oba dokumenty pomogą w skutecznym zarządzaniu bezpieczeństwem informacji w Twojej placówce.

# Ustanowienie Systemu Zarzadzania Bezpieczeństwem Informacji

Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w szkole opiera się na sprawdzonych metodach, które są powszechnie stosowane w biznesie, np. zgodnie z normami bezpieczeństwa ISO 27001. Chociaż szkoły mają inne wyzwania niż firmy, niektóre rozwiązania, takie jak polityki bezpieczeństwa informacji, zasady akceptowalnego użycia zasobów IT czy zarządzanie urządzeniami mobilnymi, mogą zostać skutecznie zaadaptowane do potrzeb placówki oświatowej.

Podstawowym narzędziem w tym procesie jest szablon „Polityka Bezpieczeństwa Informacji” (PBI), który znajdziesz w załączniku podręcznika (dokument 01). Jest to deklaracja, w której szkoła zobowiązuje się do dbania o bezpieczeństwo informacji. PBI określa cele, jakie szkoła chce osiągnąć. Dokument „Zasady Bezpieczeństwa Informacji” (dokument 03) szczegółowo opisuje wdrożenie PBI. Zawiera kilkanaście sekcji, obejmujących m.in. ogólne wytyczne, pracę zdalną, kontrolę dostępu, zarządzanie hasłami, korzystanie z Internetu i poczty oraz BYOD (używanie prywatnych urządzeń). Dokument określa zasady bezpieczeństwa, które muszą przestrzegać nauczyciele i uczniowie, zapewniając ochronę danych w szkole i podczas pracy zdalnej.

Te zasady muszą być przekazane uczniom i pracownikom w ramach Programu Budowania Świadomości w obszarze Cyberbezpieczeństwa, który jest niezbędnym elementem SZBI w szkole.

# Program Budowania Świadomości w obszarze Cyberbezpieczeństwa w Szkole

Jednym z kluczowych elementów Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w szkole jest stworzenie Programu Szkoleniowego, który buduje i utrzymuje świadomość w zakresie cyberbezpieczeństwa. W naturalny sposób edukacja w szkole skupia się na przekazywaniu nowej wiedzy, jednak równie ważne jest regularne przypominanie o obowiązujących zasadach, takich jak reguły bezpieczeństwa czy stosowanie silnych haseł. W tym kontekście szkoła powinna wprowadzić mechanizmy, które zapewnią regularne przypominanie i utrwalanie tych zasad.

Warto pamiętać, że uczniowie nie mają takich obowiązków jak dorośli pracownicy, dlatego program budowania świadomości powinien być dostosowany do specyfiki szkolnej. Obejmuje on całą społeczność szkoły – zarówno pracowników, jak i uczniów – wspólnie stojącą po jednej stronie w walce z cyberzagrożeniami.

Do realizacji tego celu proponujemy szablon „Program Budowania Świadomości w Obszarze Cyberbezpieczeństwa” (dokument 04). Dokument ten wymaga dostosowania do specyfiki danej placówki – nie każda szkoła ma dostęp do takich zasobów jak prelekcje Policji, szkolenia zewnętrzne czy wsparcie rodziców pracujących w branży IT. Jeżeli jednak są takie możliwości, warto je uwzględnić w planie.

Szablon „Program Budowania Świadomości w Obszarze Cyberbezpieczeństwa” (dokument 04) wraz z instrukcjami wypełnienia znajdziesz w załączniku podręcznika.

# Wykaz załączników

1. **Polityka Bezpieczeństwa Informacji (PBI)**  
   Dokument określający ogólne zasady i cele bezpieczeństwa informacji w szkole.
2. **Role i obowiązki w SZBI**  
   Szablon dokumentu definiujący odpowiedzialności i zadania personelu szkolnego (nauczycieli, administracji, dyrekcji) w zakresie bezpieczeństwa informacji.
3. **Zasady bezpieczeństwa informacji**  
   Zasady dotyczące korzystania z zasobów informatycznych, urządzeń mobilnych oraz przestrzegania polityk bezpieczeństwa.
4. **Program Budowania Świadomości w Obszarze Cyberbezpieczeństwa**  
   Szablon programu szkoleniowego dla uczniów i pracowników, który wspiera edukację i utrzymanie świadomości zagrożeń cybernetycznych.

# O autorze

Mateusz Pękala - specjalista w podnoszeniu świadomości bezpieczeństwa informacji, zgodności zabezpieczeń, audytu bezpieczeństwa informacji oraz zarządzaniu ryzykiem. Ma wieloletnie doświadczenie jako audytor, trener i konsultant w obszarze bezpieczeństwa informacji. Jest członkiem organizacji zawodowych, takich jak ISSA Polska i ISACA. Posiada certyfikaty Certified in Risk and Information Systems Control™ (CRISC), Certified Information Security Professional (CISSP), Certified Data Privacy Solutions Engineer™ (CDPSE®) oraz Certified Information Systems Auditor® (CISA), a także certyfikację audytora w zakresie ISO 27001.