CYBERSEC
EDUCHECK

PODRĘCZNIK DLA SZKÓŁ ŚREDNICH

WSPIERAJĄCY UTRZYMANIE WŁAŚCIWEGO POZIOMU BEZPIECZEŃSTWA INFORMACJI SZKOŁY ORAZ WSPIERAJĄCY EDUKACJĘ I ŚWIADOMOŚĆ W OBSZARZE CYBERBEZPIECZEŃSTWA

Przygotowane przez:
Mateusz Pękala

PROJEKT NR 2023-2-PL01-KA210-VET-000176822

Dofinansowane przez Unię Europejską

LIDER:
Research Institute Europe | Coventry University

PARTNERZY:
KREA STOWARZYSZENIE KREATYWNI DLA BIZNESU
EUROPEAN CENTRE FOR CAREER EDUCATION

Spis treści

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 Zarządzania 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.

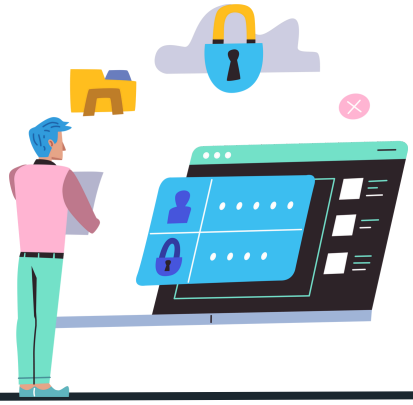
PBI określa cele, jakie szkoła chce osiągnąć. Dokument ***„Zasady Bezpieczeństwa Informacji”*** **(dokument 03)** szczegółowo opisuje wdrożenie PBI. Zawiera kilkanaście sekcji, obejmujących m.in. ogólne wytyczne, pracę zdalną, kontrolę dostępu, zarządzanie hasłami, korzystanie z Internetu i poczty oraz 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

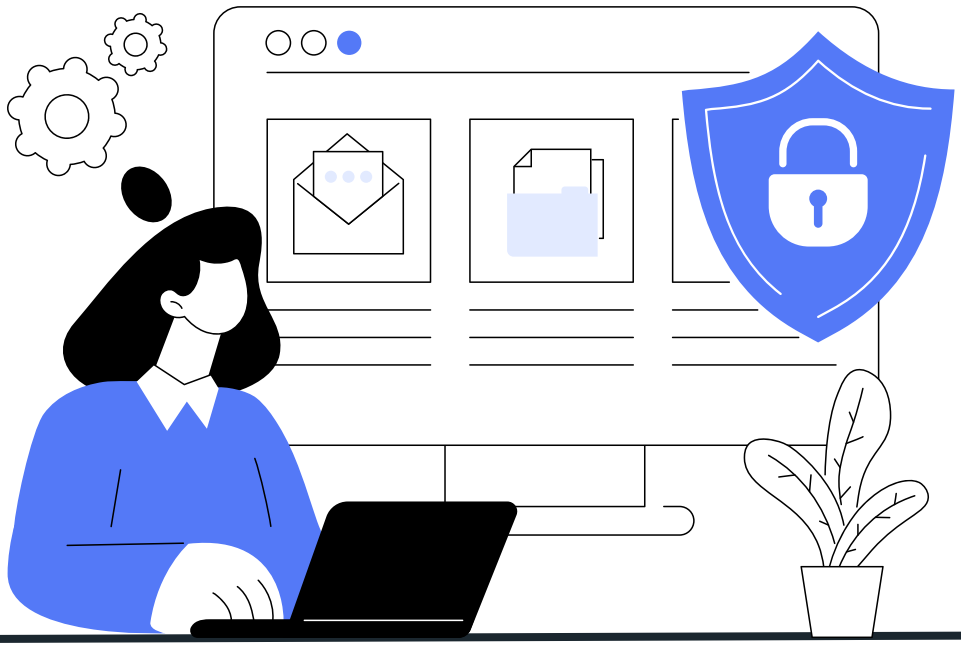
Szablon dokumentu definiujący odpowiedzialności i zadania personelu szkolnego (nauczycieli, administracji, dyrekcji) w zakresie bezpieczeństwa informacji.

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.



1.Polityka Bezpieczeństwa Informacji (PBI)

Właściwości dokumentu

Nazwa	**Polityka Bezpieczeństwa Informacji**
Zatwierdzanie i nadzór	Dyrektor Szkoły
Recenzja	Oficer Bezpieczeństwa Informacji w Szkole
Częstotliwość przeglądu	Raz w roku lub po każdej znaczącej zmianie w procesie
Lokalizacja przechowywania	Intranet / dedykowany folder na dysku sieciowym

Historia wersji

Wersja	Data	Autor	Opis zmian
0.1	01.10.2024	Coventry University	Przygotowanie projektu szablonu

Spis treści

Wprowadzenie

Odpowiedzialność za bezpieczeństwo informacji spoczywa na wszystkich pracownikach, pracownikach tymczasowych i zewnętrznych (kontrahentach) oraz kierownictwie Szkoły.

Uczniowie odpowiadają za przestrzeganie wytycznych dotyczących bezpieczeństwa informacji przekazywanym im przez Dyrekcję Szkoły i Nauczycieli.
Szkoła prowadzi działalność edukacyjną w sposób, który chroni pracowników, kontrahentów, uczniów i rodziców przed niepożądanymi zdarzeniami bezpieczeństwa, które wpływają na poufność, integralność i / lub dostępność przetwarzanych informacji.

Celem dokumentu jest ustanowienie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w Szkole, w tym definicja odpowiedzialności za jego funkcjonowanie i określenie ram ustalania konkretnych celów w zakresie bezpieczeństwa.
Kierownictwo Szkoły zapewnia, że bezpieczeństwo informacji jest ważnym aspektem działalności Szkoły i deklaruje pełne zaangażowanie we wdrażanie i zarządzanie SZBI m.in. poprzez zapewnienie odpowiednich zasobów organizacyjnych i finansowych.

Polityka Bezpieczeństwa Informacji

• Cel

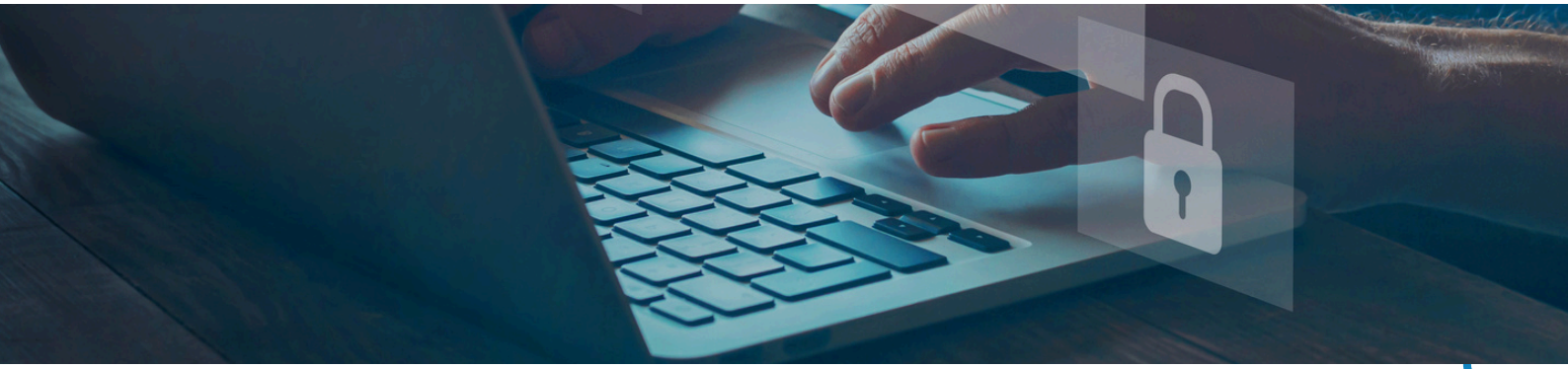
Celem SZBI jest zapewnienie bezpieczeństwa informacji zgodnie ze zidentyfikowanymi potrzebami i oczekiwaniami Dyrekcji, Pracowników, Uczniów, Rodziców i innych interesariuszy Szkoły.

• Wspierane cele Szkoły

SZBI wspiera następujące cele Organizacji:

- Demonstrowanie zaangażowania i wsparcia Kierownictwa Szkoły dla bezpieczeństwa informacji.
- Ustanowienie odpowiednich zabezpieczeń w oparciu o zidentyfikowane ryzyko.
- Zgodność z wewnętrznymi i zewnętrznymi zobowiązaniami.
- Zgodność z wymaganiami Organów Nadzorczych Szkoły i umownymi zobowiązaniami w zakresie bezpieczeństwa informacji.
- Zgodność zobowiązującymi wymogami dotyczącymi prywatności danych, w tym wymogom RODO.

Niniejsza Polityka Bezpieczeństwa Informacji jest wspierana i uzupełniana przez inne polityki, procedury oraz pozostałą dokumentację SZBI oraz Polityki RODO.



• Zakres SZBI

Niniejsza Polityka ma zastosowanie dla wszystkich zarządzanych przez Szkołę w tym procesów i informacji a także usług chmurowych, oprogramowania, urządzeń, personału i pomieszczeń.

• Role i obowiązki w SZBI

Mając na uwadze konieczność integracji procesów związanych z bezpieczeństwem informacji z bieżącą działalnością Szkoły, a także obowiązki operacyjne i sprawozdawcze Kierownictwo Szkoły określi odpowiednią strukturę ról i obowiązków, biorąc pod uwagę konieczność przypisania odpowiedzialności za całościowe działanie Systemu Zarządzania Bezpieczeństwem Informacji.
Oficer Bezpieczeństwa Informacji w Szkole jest odpowiedzialny za utrzymanie Polityki Bezpieczeństwa Informacji, wspieranie jej celów i doradztwo w zakresie jej wdrażania.
Kadra (Nauczyciele, Wychowawcy, Pedagodzy) będzie odpowiedzialna za wdrożenie i realizację zapisów Polityki Bezpieczeństwa Informacji wraz z dokumentami towarzyszącymi w swoich obszarach.
Uczniowie muszą być informowani o swoich obowiązkach w zakresie bezpieczeństwa informacji.

2. Role i obowiązki w SZBI

Właściwości dokumentu

Nazwa	Role i obowiązki w SZBI
Zatwierdzanie i nadzór	Dyrektor Szkoły
Recenzja	Oficer Bezpieczeństwa Informacji w Szkole
Częstotliwość przeglądu	Raz w roku lub po każdej znaczącej zmianie w procesie
Lokalizacja przechowywania	Intranet / dedykowany folder na dysku sieciowym

Historia wersji

Wersja	Data	Autor	Opis zmian
0.1	01.10.2024	Coventry University	Przygotowanie projektu szablonu

Spis treści

CEL

Celem dokumentu jest zdefiniowanie ról i obowiązków, które są istotne dla efektywnego działania Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).

SZBI Role i obowiązki

Szkoła zidentyfikowała role i obowiązki w ramach SZBI.
Role w SZBI mogą być łączone i wykonywane przez te same osoby, zgodnie z możliwościami Szkoły.

- **Dyrektor Szkoły**

Dyrektor Szkoły zapewnia wizję, wspiera wdrożenie i funkcjonowanie SZBI oraz zapewnia ogólne wytyczne, kierunek i wsparcie dla funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji w Szkole.

Do obowiązków Dyrektora Szkoły należy:

- Akceptacja celów i zakresu SZBI, z uwzględnieniem celów Szkoły i wymagań prawnych
- Wyznaczanie ról i zatwierdzanie zmian organizacyjnych związanych z SZBI,
- Zatwierdzenie Polityki Bezpieczeństwa Informacji,
- Zatwierdzanie dokumentów SZBI wynikających z Polityki Bezpieczeństwa Informacji,
- Zatwierdzanie akceptowalnego poziomu ryzyka, wyników analizy ryzyka i planów postępowania z ryzykiem w procesach objętych SZBI,
- Zatwierdzanie budżetu związanego z SZBI,
- Zatwierdzanie wyników audytów i przeglądów SZBI,
- Podejmowanie decyzji w procesie zarządzania kryzysowego.

- **Oficer Bezpieczeństwa Informacji w Szkole**

Oficer Bezpieczeństwa Informacji w Szkole jest odpowiedzialny za działanie SZBI oraz przygotowanie wytycznych i nadzór nad bezpieczeństwem informacji.

Do obowiązków Oficera należą:

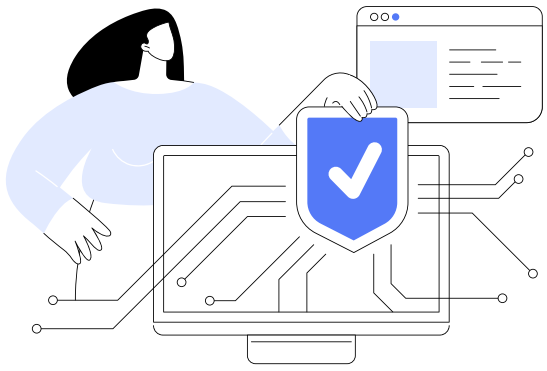
1. Wprowadzanie zmian i nadzór nad spójnością dokumentacji SZBI oraz przeprowadzanie jej cyklicznych przeglądów i aktualizacji,
2. Podnoszenie świadomości pracowników i uczniów w zakresie zagadnień bezpieczeństwa informacji, w szczególności nadzór nad Programem Budowania Świadomości w Obszarze Cyberbezpieczeństwa w Szkole,
3. Wdrażanie i nadzór nad przestrzeganiem zasad i mechanizmów związanych z bezpieczeństwem informacji,
4. Ocena skuteczności realizacji wymagań wynikających z przepisów bezpieczeństwa informacji.

- **Inspektor Ochrony Danych osobowych (IOD)**

Szkoły dysponujące już dokumentacją w obszarze ochrony danych osobowych (RODO) mogą nawiązać do tych zapisów i nie definiować ponownie obowiązków IODa. Istotne jest by dokumentacja SZBI i Polityki dotyczące ochrony danych osobowych były ze sobą zintegrowane. W rzeczywistości zgodność z RODO to jeden z celów SZBI.

IOD pomaga personelowi Szkoły we wszystkich kwestiach związanych z ochroną danych osobowych. Do obowiązków IODa należą:

- Informowanie i doradzanie Dyrekcji Szkoły oraz pracownikom, o ich obowiązkach wynikających z prawa o ochronie danych osobowych,
- Monitorowanie zgodności ze wszystkimi przepisami dotyczącymi ochrony danych, w tym w zakresie audytów, działań uświadamiających, a także szkolenia personelu zaangażowanego w operacje przetwarzania,
- Udzielanie porad w przypadku przeprowadzenia DPIA i monitorowanie jego wydajności,
- Działanie jako punkt kontaktowy dla wniosków od osób fizycznych dotyczących przetwarzania ich danych osobowych i wykonywania ich praw,
- Współpraca z organami ochrony danych i pełnienie funkcji punktu kontaktowego dla organów ochrony danych w kwestiach związanych z przetwarzaniem danych osobowych,
- Wsparcie prac związanych z utrzymaniem i doskonaleniem SZBI w obszarze ochrony danych osobowych,
- Wsparcie w doborze środków ochrony odpowiednich do ilości i zakresu przetwarzania danych osobowych,
- Wsparcie prac projektowych nad systemami przetwarzającymi dane osobowe,
- Klasyfikacja operacji przetwarzania danych osobowych według ilości, rodzaju i celu przetwarzania,
- Prowadzenie ewidencji operacji przetwarzania danych osobowych.



- **Nauczyciel/Pracownik**

Wszyscy Pracownicy, którzy mają dostęp do zasobów informacyjnych Szkoły, w tym pracownicy, kontrahenci, stażyści i zewnętrzni dostawcy usług mają obowiązek:

1. Przestrzegania Polityki Bezpieczeństwa Informacji i zasad bezpieczeństwa informacji ustanowionych w pozostałych dokumentach powiązanych,
2. Przestrzegania Polityki Ochrony Danych Osobowych i związanych z nią przepisów,
3. Zgłaszania incydentów związanych z bezpieczeństwem informacji,
4. Udział w programie szkoleń z obszaru bezpieczeństwa informacji.

- **Uczeń**

Wszyscy uczniowie, mający dostęp do zasobów informacyjnych szkoły w zakresie wynikającym z ich zajęć.
Obowiązkiem uczniów jest:

1. Przestrzeganie Polityki Bezpieczeństwa Informacji i zasad bezpieczeństwa informacji ustanowionych w pozostałych dokumentach powiązanych,
2. Przestrzeganie Polityki Ochrony Danych Osobowych i związanych z nią przepisów,
3. Zgłaszanie incydentów związanych z bezpieczeństwem informacji,
4. Udział w programie szkoleń z obszaru bezpieczeństwa informacji.
5. Słuchanie poleceń Nauczycieli i pozostałej kadry dydaktycznej w zakresie korzystania z urządzeń elektronicznych i Internetu na obszarze Szkoły.

3. Zasady bezpieczeństwa Informacji

Właściwości dokumentu

Nazwa	**Zasady bezpieczeństwa informacji**
Zatwierdzanie i nadzór	Dyrektor Szkoły
Recenzja	Oficer Bezpieczeństwa Informacji w Szkole
Częstotliwość przeglądu	Raz w roku lub po każdej znaczącej zmianie w procesie
Lokalizacja przechowywania	Intranet / dedykowany folder na dysku sieciowym

Historia wersji

Wersja	Data	Autor	Opis zmian
0.1	01.10.2024	Coventry University	Przygotowanie projektu szablonu

Spis treści

Proszę pamiętać, że dokument musi być dostosowany do kontekstu Szkoły. Jeżeli jakieś zapisy uznacie za niemożliwie do realizacji, to oczywiście warto przemyśleć dlaczego tak jest a następnie usunąć/zmodyfikować/zastąpić innym zabezpieczeniem kompensującym ryzyko.

Ogólne wytyczne

1. Użytkownik, oznacza, każdą osobę (Pracownika Szkoły oraz Ucznia) korzystającą z zasobów informatycznych, w tym Internetu, Szkoły.
2. Szkoła dostarcza Pracownikowi sprzęt informatyczny jako narzędzie umożliwiające wykonywanie pracy (zadań) na rzecz Szkoły.
3. Użytkownik ponosi odpowiedzialność za powierzony mu sprzęt i oprogramowanie oraz sposób ich działania.
4. Użytkownik ponosi konsekwencje finansowe i prawne posiadania nielegalnego oprogramowania na sprzęcie teleinformatycznym powierzonym mu przez Szkołę.
5. Surowo zabrania się testowania i/lub łamania zabezpieczeń urządzeń i systemu teleinformatycznego udostępnianego przez Spółkę.
6. Sprzęt powierzony przez Szkołę nie może być udostępniany osobom nieupoważnionym.
7. Zabronione jest samodzielne dokonywanie jakichkolwiek zmian w konfiguracji dostarczonych urządzeń lub oprogramowania, chyba że zmiana została zaakceptowana przez Oficera Bezpieczeństwa Informacji Szkoły. Dotyczy to w szczególności zmian w ustawieniach związanych z zabezpieczeniami.
8. Każdy użytkownik zobowiązany jest do zapoznania się ze wszystkimi regulacjami, instrukcjami i procedurami wewnętrznymi, które są wdrażane przez Dyrekcje Szkoły.

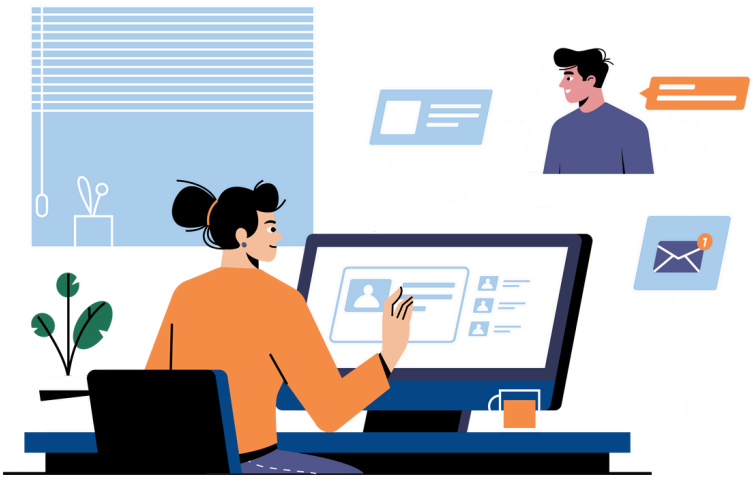
Praca zdalna

Uwaga, to dotyczy sprzętu zakupionego przez Szkołę a nie np. prywatnego laptopa nauczyciela wykorzystywanego do pracy. Do tej sytuacji będzie obnosił się punkt mówiący o pracy na prywatnych urządzeniach albo BYOD od angielskiego Bring Your Own Device.

1. Wynoszenie powierzonego sprzętu mobilnego poza siedzibę Szkoły musi być uzasadnione obowiązkami wykonywanymi przez użytkownika.
2. Użytkownik sprzętu mobilnego ma obowiązek go chronić. Należy unikać ryzykownych zachowań, które mogą obejmować m.in.:

- pozostawienie sprzętu bez nadzoru (w samochodzie, pokojach hotelowych itp.),
- pozostawienie torby z laptopem bez nadzoru,
- nie wylogowywanie się użytkownika w przypadku czasowej nieobecności lub braku aktywności,
- ustawienie monitorów umożliwiające podgląd zawartości ekranu osobom nieupoważnionym.

3. W przypadku zagubienia powierzonego sprzętu mobilnego używanego poza Spółką, użytkownik powinien zwłocznie zgłosić powyższy fakt do Oficera Bezpieczeństwa Informacji Szkoły, a w przypadku kradzieży dodatkowo, zgłosić ten fakt Policji.



Bezpieczne logowanie i zarządzanie hasłami

Informacja o identyfikatorach oczywiście do usunięcia dla szkół, które nie posługują się nimi. Polityka haseł powinna być zgodna z bieżącymi wytycznymi w tym obszarze: Kompleksowo o hasłach | CERT Polska. Popularna w wielu organizacjach polityka częstej zmiany, np. co 30 dni haseł oraz często stosowanie krótkich, zaledwie 8 znakowych haseł nie jest dobrym pomysłem.

1. Użytkownik ponosi odpowiedzialność za wszelkie czynności wykonywane przy użyciu jego identyfikatora i hasła.
2. Hasła użytkowników lub inne poświadczenia podlegają specjalnej ochronie.
3. Każdy użytkownik mający dostęp do systemu informatycznego Szkoły zobowiązany jest do:

- zachowania w tajemnicy wszystkich swoich haseł lub innych danych uwierzytelniających wykorzystywanych do pracy w systemie informatycznym Szkoły,
- niezwłocznej zmiany hasła w przypadku podejrzenia lub faktycznego ujawnienia hasła,
- używać haseł o minimalnej długości 12 znaków, hasło musi zawierać wielkie i małe litery oraz cyfry i/lub znaki specjalne,
- zaleca się stosowanie uwierzytelniania dwuskładnikowego wszędzie gdzie to możliwe.

4. Hasła nie mogą być zapisywane w żaden jednoznaczny sposób (np. pliki tekstowe, notatnik itp.).
5. Dozwolone jest korzystanie z zatwierdzonego systemu dedykowanego do bezpiecznego przechowywania haseł (menedżer haseł)
6. Zabronione jest logowanie się do systemu przy użyciu danych uwierzytelniających innego użytkownika.
7. Użytkownik zobowiązany jest do blokowania komputera, który nie jest obecnie używany, przed nieautoryzowanym dostępem, wymuszając chronioną hasłem blokadę ekranu (zasada czystego ekranu).

Korzystanie z Internetu, poczty elektronicznej, komunikatorów internetowych w Szkole

1. **Jeśli korzystasz z Internetu w Szkole, musisz bezwzględnie unikać ryzykownych zachowań, w tym:**

- przeglądania stron internetowych zawierających treści niepożądane, w szczególności stron pornograficznych, rasistowskich, nawołujących do nienawiści, promujących sekty, hazardowych lub w jakikolwiek sposób obrażających uczucia innych osób lub naruszających szeroko rozumiane zasady współżycia społecznego,
- przeglądanie stron internetowych zawierających wszelkiego rodzaju złośliwe oprogramowanie (np. malware, exploity itp.),
- przeglądanie stron internetowych zawierających kody umożliwiające złamanie lub ominięcie ochrony praw autorskich,
- pobieranie z Internetu, instalowanie, przechowywanie lub rozpowszechnianie oprogramowania, które nie jest autoryzowane przez Spółkę.

2. Zabronione jest uzyskiwanie dostępu do stron internetowych, które są wykorzystywane do nielegalnej dystrybucji treści (utworów) z naruszeniem przepisów o ochronie praw autorskich.
3. Skrzynki pocztowe z podanym przez Szkołę adresem e-mail mogą być wykorzystywane wyłącznie do korespondencji związanej z działaniem Szkoły.
4. Zabrania się przekazywania poczty do skrzynek niezwiązanych ze Szkołą, w szczególności prywatnych.

Ten zapis oznacza, że np. Nauczyciel nie może wysyłać sobie materiałów na prywatną skrzynką – Szkoła musi rozważyć czy może sobie pozwolić na zabronienie tego w praktyce.

5. W przypadku wysyłania załączników stanowiących tajemnicę Szkoły lub chronionych odpowiednimi przepisami prawa (np. zawierających dane osobowe), załącznik taki musi być zaszyfrowany hasłem spełniającym wymagania określone w punkcie trzecim zasad. Hasło nie może zostać wysłane tym samym kanałem komunikacyjnym co wiadomość.

Wymagania dotyczące korzystania do pracy lub nauki w Szkole z urządzeń prywatnych użytkowników (BYOD)

1.Można stosować wyłącznie urządzenia i systemy wspierane przez producenta (dla których dostarczane są poprawki bezpieczeństwa).
2.W przypadku:

- utraty prywatnego sprzętu (np. w wyniku utraty lub kradzieży) służącego do przetwarzania poufnych danych Szkoły,
- podejrzenie ujawnienia poufnych danych Spółki,

użytkownik niezwłocznie informuje o wystąpieniu takiego zdarzenia Oficera Bezpieczeństwa Informacji Szkoły.

3. W przypadku zagubienia prywatnego urządzenia użytkownika, jego sprzedaży lub zakończenia współpracy ze Szkołą, użytkownik wyraża zgodę na usunięcie przez Szkołę wybranych lub wszystkich (w zależności od możliwości technicznych) danych należących do Szkoły.

4.W przypadku zakończenia współpracy ze Szkołą, zaprzestania korzystania z urządzenia na potrzeby BYOD lub utylizacji prywatnego urządzenia służącego do przetwarzania danych na rzecz Szkoły, użytkownik zobowiązuje się do skontaktowania się z Oficerem Bezpieczeństwa Informacji Szkoły w celu trwałego usunięcia z niego danych będących własnością Szkoły.

Zabezpieczanie informacji

1. Obowiązkiem użytkownika jest podjęcie kroków w celu zabezpieczenia informacji, które opracowuje lub tworzy. Użytkownik ma następujące opcje zabezpieczania informacji (plików):

- zaleca się umieszczanie danych w katalogu wskazanym przez Oficera Bezpieczeństwa Informacji Szkoły,
- korzystanie z zaakceptowanego przez Szkołę rozwiązania do przechowywania danych.

2. Inne rozwiązania do przechowywania danych Szkoły są zabronione.

3. Zabronione jest przetwarzanie informacji na zewnętrznych nośnikach danych (np. pendrive, dysk przenośny), które nie są własnością Szkoły i nie zostały zabezpieczone kryptograficznie.

4. Zabronione jest ujawnianie informacji (danych, plików) należących do Szkoły osobom nieupoważnionym.

Bezpieczne miejsce pracy

1. W celu ograniczenia ryzyka nieuprawnionego dostępu, utraty lub uszkodzenia informacji w godzinach pracy i poza ich godzinami, użytkownik zobowiązany jest:

- przestrzegać zasady nie pozostawiania otwartych i niezabezpieczonych drzwi umożliwiających dostęp do pomieszczenia,
- zabezpieczyć kartę dostępu lub, a w przypadku zgubienia niezwłocznie poinformować o tym fakcie ochronę obiektu i Oficera Bezpieczeństwa Informacji Szkoły,
- przechowywać dokumenty papierowe i wymienne nośniki informacji w odpowiednio zabezpieczonych meblach biurowych,
- po zakończeniu pracy zorganizować swoje miejsce pracy, zapobiegając nieautoryzowanemu dostępowi do dokumentów zawierających chronione informacje (zasada „czystego biurka").

Zgłaszanie incydentów i zdarzeń

1. **W przypadku zauważenia zdarzenia, które może być świadectwem lub dowodem naruszenia bezpieczeństwa, nieprawidłowego działania oprogramowania, błędów lub awarii systemu, użytkownik powinien:**

- zaprzestać pracy na komputerze,
- niezwłocznie poinformować Oficera Bezpieczeństwa Informacji Szkoły/Informatyka i/lub bezpośredniego przełożonego/Dyrekcję o zajściu, który podejmuje analizę w zakresie konieczności odłączenia komputera od sieci.

2. Zgłoszenie można wykonywać:

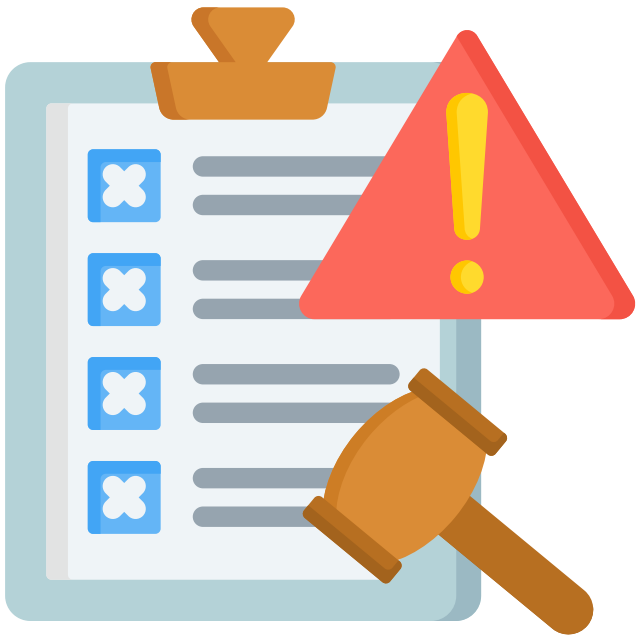
- Pocztą elektroniczną na adres zgloszenia-it@szkola.pl
- Osobiście do Oficera Bezpieczeństwa Informacji Szkoły/Informatyka i/lub bezpośredniego przełożonego/Dyrekcję

3. Wniosek powinien zawierać:

- wskazanie użytkownika lub obszaru, który był świadkiem/uczestnikiem zdarzenia,
- wskazanie lub identyfikacja systemu, którego dotyczy incydent,
- przybliżony czas wystąpienia incydentu,
- opis okoliczności i miejsc, w których doszło do zdarzenia oraz symptom /opis zdarzenia.

Sankcje dyscyplinarne

1. Nieprzestrzeganie zasad określonych w niniejszych Zasadach może prowadzić do odpowiednich sankcji dyscyplinarnych.
2. W przypadku, gdy naruszenie określonych zasad doprowadzi do podejrzenia naruszenia prawa, Dyrekcja przekaże wszelkie dowody organom ścigania do dalszego postępowania.
3. Każdy użytkownik zobowiązany jest do trzymania się na bieżąco wszelkich regulaminów, instrukcji i procedur wewnętrznych, które są wprowadzane przez Dyrekcje Szkoły. Wszystkie przepisy są przechowywane na Dysku Google/OneDrive/Sharepoint/Dysku sieciowym.
4. W przypadku wprowadzenia nowego dokumentu (regulamin, procedura, instrukcje itp.), Oficer Bezpieczeństwa Informacji i/lub Bezpośredni Przełożony jest odpowiedzialny za zapewnienie skutecznego sposobu komunikowania powyższych przepisów użytkownikom.
5. Brak znajomości aktualnych przepisów bezpieczeństwa nie będzie podstawą do jakiegokolwiek rozpatrzenia niewinności użytkownika i może prowadzić do postępowania dyscyplinarnego.



4. Program Budowania Świadomości w Obszarze Cyberbezpieczeństwa w Szkole

Właściwości dokumentu

Nazwa	**Program Budowania Świadomości w Obszarze Cyberbezpieczeństwa w Szkole**
Zatwierdzanie i nadzór	Dyrektor Szkoły
Recenzja	Oficer Bezpieczeństwa Informacji w Szkole
Częstotliwość przeglądu	Raz w roku lub po każdej znaczącej zmianie w procesie
Lokalizacja przechowywania	Intranet / dedykowany folder na dysku sieciowym

Historia wersji

Wersja	Data	Autor	Opis zmian
0.1	01.10.2024	Coventry University	Przygotowanie projektu szablonu

Spis treści

Cel dokumentu

Celem niniejszej polityki jest zapewnienie, że wszyscy pracownicy Szkoły oraz Uczniowie, otrzymują odpowiednie szkolenia oraz regularne aktualizacje zasad i procedur organizacyjnych dotyczących bezpieczeństwa informacji.
Dyrekcja Szkoły jest dąży do zapewnienia bezpieczeństwa Uczniom i Kadrze poprzez szkolenia i inne działania podnoszące świadomość w obszarze cyberzagrożeń.

Program budowania świadomości

Program budowania świadomości porusza następujące zagadnienia:

- Zasady bezpieczeństwa Informacji
- Odpowiedzialność za działania Uczniów i Kadry Szkoły oraz sankcje dyscyplinarne
- Informacje dotyczące zgłaszania incydentów
- Edukacja w obszarze szeroko pojętego bezpieczeństwa cyfrowego

Załącznik 04.1 Plan Komunikacji i Szkoleń z Obszarze Cyberbezpieczeństwa stanowi integralną część Programu. Załącznik jest aktualizowany co roku przed rozpoczęciem roku szkolnego.

Role i obowiązki

Oficer Bezpieczeństwa Informacji w Szkole na zlecenie Dyrekcji jest odpowiedzialny za całościowe funkcjonowanie Programu.
Kadra Dydaktyczna wspomaga realizację programu.
Uczniowie zobowiązani są do uczestnictwa w Programie w ramach zajęć w Szkole.

4.1 Plan Komunikacji i Szkoleń z Obszarze Cyberbezpieczeństwa

Właściwości dokumentu

Nazwa	**Plan Komunikacji i Szkoleń z Obszaru Cyberbezpieczeństwa**
Nazwa szkoły	Szkoła

Historia wersji

Wersja	Data	Autor	Opis zmian
0.1	01.10.2024	Coventry University	Przygotowanie projektu szablonu

[Szkoła] : Plan Komunikacji i Szkoleń z Obszaru Cyberbezpieczeństwa

Co komunikujemy?	Kiedy komunikujemy?	W jaki sposób komunikujemy? (metoda szkoleniowa)	Kto jest odpowiedzialny /szkoli?	Dla kogo?	Czy przeprowadzono zgodnie z planem?	Dowody na realizacje zgodną z planem
Polityki Bezpieczeństwa Informacji Szkoły i Zasady Bezpieczeństwa Informacji	Wrzesień	Rada Pedagogiczna	Dyrekcja / Oficer Bezpieczeństwa Informacji Szkoły	Nauczyciele i pracownicy administracyjni	NIE	
Zasady Bezpieczeństwa Informacji	Wrzesień	Godzina Wychowawcza - prezentacja zasad w formie wykładu	Oficer Bezpieczeństwa Informacji Szkoły / Wychowawca	Uczniowie	NIE	
Lekcja: Phishing	Październik	Godzina Wychowawcza - prezentacja szkoleniowa i warsztat	Oficer Bezpieczeństwa Informacji Szkoły / Wychowawca	Uczniowie	NIE	
Lekcja: Hasła – jak tworzyć i zarządzać hasłami?	Listopad	Godzina Wychowawcza - prezentacja szkoleniowa i warsztat	Oficer Bezpieczeństwa Informacji Szkoły / Wychowawca	Uczniowie	NIE	
Incydenty – jak reagować na zagrożenia?	Grudzień	Godzina Wychowawcza - prezentacja szkoleniowa i warsztat	Oficer Bezpieczeństwa Informacji Szkoły / Wychowawca	Uczniowie	NIE	
Cyberprzemoc – jak jej zapobiegać i na nią reagować?	Styczeń	Godzina Wychowawcza - prezentacja szkoleniowa i warsztat	Oficer Bezpieczeństwa Informacji Szkoły / Wychowawca	Uczniowie	NIE	
Dezinformacja – jak rozpoznać fałszywe informacje?	Luty/Marzec (Ferie)	Godzina Wychowawcza - prezentacja szkoleniowa i warsztat	Oficer Bezpieczeństwa Informacji Szkoły / Wychowawca	Uczniowie	NIE	
Wizyta przedstawiciela straży miejskiej lub policji	Cały rok, np. kwiecień	Szkolenie dla całej szkoły	Zaproszony przedstawiciell	Uczniowie i nauczyciele	NIE	
Ad hoc – wiadomości dotyczące bieżących zagrożeń cybernetycznych	Cały rok szkolny	Newsletter oraz w trakcie zebrań, godzin wychowawczych	Oficer Bezpieczeństwa Informacji Szkoły / Wychowawca	Wszyscy (uczniowie, nauczyciele, rodzice)	NIE	
Sprawozdania z udziału szkoły w konferencjach/wydarzeniach dotyczących bezpieczeństwa cyfrowego	po wydarzeniu, np.. Maj	Zebranie, prezentacja raportu	Oficer Bezpieczeństwa Informacji Szkół	Dyrekcja, nauczyciele, rodzice	NIE	
Prezentacje uczniów biorących udział w projektach/konkursach dotyczących bezpieczeństwa cyfrowego	po wydarzeniu, np.. Czerwiec	Zebranie, specjalne wydarzenie poświęcone cyberbezpieczeństwu	Uczniowie z opiekunem	Uczniowie i nauczyciele	NIE	
Gościnny wykład przedstawiciela Rodziców pracującego w branży cyberbezpieczeństwa	np.. Raz na semestr	Wykład	Zaproszony rodzic	Uczniowie i nauczyciele	NIE	
					NIE	
					NIE	
					NIE	
					NIE	
					NIE	
					NIE	
					NIE	
					NIE	
					NIE	
					NIE	

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.

Dalsze informacje na temat projektu

CYBERSEC

EDUCHECK

https://www.coventry.ac.uk/wroclaw/

https://kreatywnidlabiznesu.pl/cyber-sec-edu-check/

https://eccedu.net/

Finansowane przez Unię Europejską. Wyrażone poglądy i opinie są jednak poglądami i opiniami wyłącznie autora(-ów) i niekoniecznie odzwierciedlają poglądy Unii Europejskiej lub Europejskiej Agencji Wykonawczej ds. Edukacji i Kultury (EACEA). Ani Unia Europejska, ani EACEA nie mogą być za nie pociągnięte do odpowiedzialności.

PROJEKT NR 2023-2-PL01-KA210-VET-000176822

Dofinansowane przez Unię Europejską

LIDER: Research Institute Europe | Coventry University

PARTNERZY: KREA Stowarzyszenie Kreatywni dla Biznesu; European Centre for Career Education