Raport z Audytu Systemu Zarządzania Bezpieczeństwem Informacji w Szkole Podstawowej nr 9 z Oddziałami Przedszkolnymi im. Marii Skłodowskiej-Curie w Inowrocławiu

1. Wprowadzenie

Niniejszy raport przedstawia wyniki audytu Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) przeprowadzonego w Szkole Podstawowej nr 9 z Oddziałami Przedszkolnymi im. Marii Skłodowskiej-Curie w Inowrocławiu.

Audyt miał na celu ocenę zgodności ustanowionego i wdrożonego SZBI z wymaganiami normy PN-EN ISO/IEC 27001:2023-08, która stanowi polską wersję międzynarodowego standardu ISO/IEC 27001:2022.

Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji zgodnego z postanowieniami tej normy jest strategiczną decyzją szkoły, mającą na celu zapewnienie poufności, integralności i dostępności informacji. Ponadto, audyt uwzględniał obowiązujące przepisy prawa, w tym w szczególności Ogólne Rozporządzenie o Ochronie Danych (RODO) oraz krajowe standardy cyberbezpieczeństwa (NSC).

Ocena dotyczyła zarówno zgodności formalnej z dokumentacją SZBI, jak i efektywności wdrożonych zabezpieczeń oraz procesów zarządzania ryzykiem.

Zakres audytu obejmował kluczowe obszary funkcjonowania szkoły, w których przetwarzane są informacje, w tym systemy informatyczne wykorzystywane do zarządzania danymi uczniów, pracowników, finansów oraz komunikacji. Badaniu podlegały również procesy administracyjne, procedury operacyjne, zabezpieczenia fizyczne budynków i pomieszczeń, a także świadomość personelu w zakresie bezpieczeństwa informacji. Audyt dotyczył okresu od 1 września 2024 do 1 czerwca 2025.

System Zarządzania Bezpieczeństwem Informacji (SZBI) w kontekście szkoły podstawowej definiowany jest jako zbiór procedur, regulaminów, instrukcji, zasad i innych dokumentów obowiązujących w szkole, których celem jest zapewnienie bezpieczeństwa informacjom znajdującym się w jej posiadaniu.

Metodologia audytu opierała się na przeglądzie dokumentacji SZBI (polityk, procedur, instrukcji), wywiadach z kluczowymi pracownikami odpowiedzialnymi za różne aspekty bezpieczeństwa informacji i obserwacjach praktyk stosowanych w szkole. Kryteria audytu stanowiły wymagania normy PN-EN ISO/IEC 27001:2023-08, przepisy RODO oraz wytyczne zawarte w krajowych standardach cyberbezpieczeństwa. Podczas audytu zastosowano podejście procesowe, zgodne z modelem Deminga PDCA (Planuj → Wykonaj → Sprawdź → Działaj), który stanowi fundament ciągłego doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji.

Audyt został przeprowadzony przez Michała Matyjasika, nauczyciela informatyki w Szkole Podstawowej nr 9im. Marii Skłodowskiej-Curie w Inowrocławiu

2. Podsumowanie wykonawcze

Audyt Systemu Zarządzania Bezpieczeństwem Informacji w Szkole Podstawowej nr 9 z Oddziałami Przedszkolnymi im. Marii Skłodowskiej-Curie wykazał, że system jest efektywny w realizacji celów bezpieczeństwa informacji ale wymaga dalszego doskonalenia, aby w pełni realizować założone cele.

Najważniejsze obszary wymagające poprawy obejmują:

- **poprawę świadomości pracowników w zakresie cyberbezpieczeństwa,**
- **aktualizację procedur postępowania.**

Mocnymi stronami SZBI szkoły są:

- zaangażowanie kierownictwa w kwestie bezpieczeństwa informacji,
- wdrożenie podstawowych zabezpieczeń fizycznych,
- posiadanie udokumentowanej polityki bezpieczeństwa.

Wdrożenie normy ISO 27001 przynosi szkole wiele korzyści, w tym minimalizację ryzyka wycieku lub utraty cennych danych, wzrost poziomu bezpieczeństwa informacji oraz zapewnienie ciągłości funkcjonowania placówki.

Kolejnym krokiem, jakim należy podjąć, jest doskonalenie SZBI w celu podniesienia poziomu bezpieczeństwa informacji w szkole.

3. Szczegółowe ustalenia audytu

Szczegółowe ustalenia audytu przedstawiono w odniesieniu do poszczególnych klauzul normy PN-EN ISO/IEC 27001:2023-08.

3.1. Kontekst organizacji (Klauzula 4)

Audyt wykazał, że szkoła posiada udokumentowane informacje dotyczące jej kontekstu wewnętrznego i zewnętrznego w odniesieniu do bezpieczeństwa informacji. Zidentyfikowano zainteresowane strony (uczniowie, rodzice, pracownicy, organy nadzorujące) oraz ich wymagania dotyczące bezpieczeństwa informacji, w tym oczekiwania dotyczące ochrony danych osobowych zgodnie z RODO.
Zakres SZBI został określony i udokumentowany, obejmując systemy informatyczne, dane oraz procesy związane z działalnością szkoły. Nie stwierdzono wyłączeń z zakresu SZBI. Szkoła ustanowiła, wdrożyła, utrzymuje i dąży do ciągłego doskonalenia SZBI poprzez identyfikację i reagowanie na potencjalne zagrożenia i słabości. Należy jednak zweryfikować, czy udokumentowany proces uwzględnia **specyficzne zagrożenia** i podatności charakterystyczne dla sektora edukacyjnego w Polsce, takie jak cyberataki na szkoły i kwestie związane z ochroną danych uczniów.

3.2. Przywództwo (Klauzula 5)

Kierownictwo szkoły aktywnie uczestniczy w SZBI, demonstrując swoje zaangażowanie poprzez inicjowanie działań mających na celu poprawę bezpieczeństwa. Ustanowiona Polityka Bezpieczeństwa Informacji jest zgodna ze strategicznym kierunkiem szkoły i została zakomunikowana wszystkim pracownikom. W szkole przydzielono role, odpowiedzialności i uprawnienia w zakresie bezpieczeństwa informacji, w tym wyznaczono Pełnomocnika SZBI, który odpowiada za nadzorowanie i wdrażanie systemu. Potwierdza to, że kierownictwo szkoły traktuje bezpieczeństwo informacji jako priorytet na wszystkich poziomach organizacji.

3.3. Planowanie (Klauzula 6)

Szkoła wdrożyła proces określania ryzyka i szans w odniesieniu do bezpieczeństwa informacji, identyfikując potencjalne zagrożenia i podatności, a także możliwości doskonalenia kadry nauczycielskiej. Zaplanowano działania mające na celu osiągnięcie tych celów. Szkoła posiada również procedury planowania zmian w SZBI, zapewniając, że zmiany są kontrolowane i nie wpływają negatywnie na bezpieczeństwo informacji.

Tabela 1: Podsumowanie zidentyfikowanych ryzyka bezpieczeństwa informacji i planów postępowania z nimi

Opis Ryzyka	**Potencjalny Wpływ**	**Prawdopodobieństwo**	**Plan Postępowania z Ryzykiem**
Phishing na pracowników skutkujący wyciekiem danych logowania	Nieautoryzowany dostęp do systemów, wyciek danych osobowych uczniów i pracowników	Średnie	Przeprowadzenie szkoleń z zakresu świadomości cyberbezpieczeństwa, wdrożenie uwierzytelniania wieloskładnikowego
Brak aktualizacji oprogramowania systemowego i aplikacji	Podatność na ataki z wykorzystaniem znanych luk bezpieczeństwa, możliwość infekcji złośliwym oprogramowaniem	Średnie	Wdrożenie automatycznych aktualizacji, regularne skanowanie podatności

Niewystarczające zabezpieczenia fizyczne	Nieautoryzowany dostęp do infrastruktury IT, możliwość uszkodzenia lub kradzieży sprzętu	Niskie	Monitoring wizyjny

3.4. Wsparcie (Klauzula 7)

Szkoła zapewnia zasoby niezbędne do ustanowienia, wdrożenia, utrzymywania i ciągłego doskonalenia SZBI. Należy dążyć do stanu, gdzie kompetencje pracowników w zakresie bezpieczeństwa informacji są rozwijane poprzez regularne szkolenia i programy podnoszenia świadomości. Programy te powinny obejmować zagadnienia związane z cyberbezpieczeństwem. **Świadomość pracowników na temat Polityki Bezpieczeństwa Informacji oraz ich indywidualnych obowiązków w zakresie ochrony zasobów informacyjnych jest na poziomie wymagającym poprawy**. Procesy komunikacji wewnętrznej i zewnętrznej dotyczące SZBI są ustanowione i funkcjonują. Zarządzanie udokumentowanymi informacjami, w tym ich tworzenie, aktualizowanie i kontrola dostępu, odbywa się w sposób zgodny z procedurami. Błędy ludzkie stanowią istotną podatność, a dobrze przeszkolony personel jest ważną linią obrony.

3.5. Działania operacyjne (Klauzula 8)

Planowanie i kontrola operacyjna procesów związanych z bezpieczeństwem informacji są realizowane zgodnie z ustalonymi procedurami. **Oceny ryzyka bezpieczeństwa informacji są przeprowadzane sporadycznie i bez udokumentowanej metodyki.** Kontrola dostępu (fizycznego i logicznego) do informacji i systemów informatycznych jest realizowana poprzez system haseł oraz rejestry wejść/wyjść]. Zabezpieczenia przed złośliwym oprogramowaniem są wdrożone w postaci oprogramowania antywirusowego na stacjach roboczych. Zarządzanie podatnościami obejmuje instalowanie poprawek bezpieczeństwa. Szkoła posiada procedury postępowania z incydentami bezpieczeństwa informacji. Aspekty bezpieczeństwa informacji w relacjach z dostawcami są uwzględniane poprzez stosowne umowy.

3.6. Ocena wyników (Klauzula 9)

Monitorowanie, pomiary, analiza i ocena wyników związanych z bezpieczeństwem informacji są przeprowadzane sporadycznie, bez ustalonych metryk. Audyty wewnętrzne SZBI są planowane i przeprowadzane nieregularnie, bez udokumentowanego programu.

3.7. Doskonalenie (Klauzula 10)

Szkoła posiada procedury postępowania z niezgodnościami i podejmowania działań korygujących i zapobiegawczych.

- Polityka bezpieczeństwa informacji i ochrony danych osobowych (maj 2018)

- Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych (maj 2018)
- Instrukcja korzystania z monitoringu wizyjnego (maj 2018)
- Procedura zgłaszania przypadków naruszenia ochrony danych osobowych organowi prowadzącemu (maj 2018)
- Polityka bezpieczeństwa przetwarzania danych osobowych (2012)

Ustanowione procesy zapewniają, że niezgodności są identyfikowane, analizowane i eliminowane, a także podejmowane są działania w celu zapobiegania ich ponownemu wystąpieniu.

4. Niezgodności i zalecenia

Podczas audytu zidentyfikowano następujące niezgodności z wymaganiami normy PN-EN ISO/IEC 27001:2023-08, RODO oraz innymi obowiązującymi przepisami i standardami:

Tabela 2: Lista niezgodności i zaleceń

PN-EN ISO/IEC 27001:2023-08, kl. 7.2; RODO, art. 25	Nie wszyscy nowi pracownicy przechodzą szkolenie z bezpieczeństwa przed dostępem do systemów	Aktualizacja procedury zatrudnienia i prowadzenie rejestru szkoleń

5. Wnioski

Podsumowując, audyt Systemu Zarządzania Bezpieczeństwem Informacji w wykazał, że ogólna efektywność SZBI w szkole jest na zadowalającym poziomie, zapewnia podstawową ochronę informacji.

Audyt potwierdził zgodność z normą PN-EN ISO/IEC 27001:2023-08 oraz innymi kryteriami audytu, z uwagi na zidentyfikowane niezgodności opisane w sekcji 4 niniejszego raportu. Mocnymi stronami SZBI szkoły jest zaangażowanie kierownictwa, posiadanie udokumentowanej polityki bezpieczeństwa, wdrożenie podstawowych zabezpieczeń. Należy kontynuować wysiłki w celu utrzymania i dalszego rozwijania tych mocnych stron.

DYREKTOR SZKOŁY
mgr Maria Lipińska-Ankiel