Verte
Centrum szkoleń

Verte
Ul Mieszczańska 29/13 50-201 Wrocław

Czas trwania: 3-4h

Cyberbezpieczna szkoła 2026/2027 – jak wdrożyć nowe obowiązki, przygotować procedury i reagować na incydenty

CO ZYSKASZ?

- Certyfikat
- Materiały szkoleniowe
- Wzory dokumentów
- Sesja QA

PROGRAM SZKOLENIA

1. Cyberbezpieczeństwo szkoły w roku szkolnym 2026/2027

- aktualne podstawy prawne – KSC, NIS2, RODO i przepisy o ochronie danych,
- które obowiązki dotyczą szkół i placówek oświatowych,
- odpowiedzialność dyrektora, organu prowadzącego i pracowników,
- cyberbezpieczeństwo a ochrona danych osobowych.

2. Organizacja systemu cyberbezpieczeństwa w placówce

- podział zadań i odpowiedzialności,
- identyfikacja zasobów, systemów i danych wymagających ochrony,
- analiza ryzyka i ocena podatności,
- dostęp do SIO, dziennika elektronicznego, poczty i systemów kadrowo-płacowych,
- współpraca z informatykami i podmiotami zewnętrznymi.

3. Dokumentacja i procedury – co powinna posiadać szkoła

- polityka bezpieczeństwa informacji i SZBI,
- zarządzanie dostępami, hasłami i uprawnieniami,
- kopie zapasowe i odtwarzanie danych,
- korzystanie z poczty, urządzeń służbowych i nośników danych,
- praca zdalna i dostęp do systemów poza szkołą,
- aktualizacja i przegląd dokumentacji.

4. Incydent cyberbezpieczeństwa – procedura krok po kroku

- czym jest incydent i jak go rozpoznać,
- phishing, ransomware, przejęcie konta, wyciek danych i utrata urządzenia,
- pierwsze działania po wykryciu incydentu,
- zabezpieczenie informacji i ograniczenie skutków,
- dokumentowanie i eskalacja zdarzenia,
- incydent cyberbezpieczeństwa a naruszenie ochrony danych osobowych,
- kiedy konieczne jest zgłoszenie zdarzenia i kto odpowiada za zgłoszenie.

5. Pracownik jako element systemu bezpieczeństwa

- obowiązki nauczycieli i pracowników administracji,
- bezpieczne logowanie i uwierzytelnianie wieloskładnikowe,
- rozpoznawanie phishingu i socjotechniki,
- zasady korzystania z prywatnych urządzeń,
- szkolenia pracowników i dokumentowanie ich przeprowadzenia.

6. Cyberbezpieczeństwo uczniów

- bezpieczeństwo cyfrowe w środowisku szkolnym,
- ochrona kont i danych uczniów,
- cyberprzemoc, przejęcie konta i publikacja danych lub wizerunku,

- zgłaszanie zdarzeń przez ucznia i rodzica,
- współpraca szkoły z rodzicami i odpowiednimi służbami.

7. Kontrola gotowości szkoły – audyt krok po kroku

- przegląd dokumentacji,
- kontrola uprawnień i dostępów,
- weryfikacja zabezpieczeń i kopii zapasowych,
- test procedury reagowania na incydent,
- plan działań naprawczych i harmonogram wdrożenia.

WZORY DOKUMENTÓW

- Procedura reagowania na incydent cyberbezpieczeństwa
- Instrukcja postępowania pracownika po wykryciu incydentu
- Karta zgłoszenia i rejestr incydentów cyberbezpieczeństwa
- Checklista dyrektora- cyberbezpieczna szkoła 2026/2027
- Wzór rejestru uprawnień i dostępów do systemów
- Procedura nadawania, zmiany i odbierania uprawnień
- Procedura tworzenia i weryfikacji kopii zapasowych
- Zasady korzystania z poczty elektronicznej, haseł i urządzeń służbowych
- Procedura korzystania z urządzeń prywatnych do celów służbowych
- Formularz przeglądu cyberbezpieczeństwa placówki
- Wzór zarządzenia dyrektora wprowadzającego procedury

PROWADZĄCY

Justyna Świder - Radca prawny wpisany na listę Okręgowej Izby Radców Prawnych w Katowicach. Specjalista z zakresu prawa cywilnego, w tym oświatowego i samorządowego oraz administracyjnego. Biegle porusza się w prawie pracy. Absolwentka Wydziału Prawa i Administracji, a także Wydziału Filologicznego Uniwersytetu Jagiellońskiego w Krakowie. Wieloletni pracownik samorządowy w sektorze publicznym oraz autorka komentarzy eksperckich z zakresu prawa cywilnego, oświatowego, administracyjnego, samorządowego oraz prawa pracy.

Verte
Centrum szkoleń

Verte
Ul Mieszczańska 29/13 50-201 Wrocław

Tel. 71 321 56 41 Fax: 71 321 79 71 Mail: biuro@centrumverte.pl www.centrumverte.pl