

PROCEDURA ZARZĄDZANIA INCYDENTAMI CYBERBEZPIECZEŃSTWA i Bezpieczeństwa Informacji

w Zespole Szkół Ogólnokształcących im. Armii Krajowej w Bielsku-Białej

§ 1. Postanowienia ogólne

1. Niniejsza procedura określa zasady postępowania w przypadku ujawnienia incydentów związanych z naruszeniem cyberbezpieczeństwa oraz bezpieczeństwa informacji na terenie Zespole Szkół Ogólnokształcącym w Bielsku-Białej, w skład którego wchodzi Szkoła Podstawowa nr 36 z Oddziałami Integracyjnymi oraz VI Liceum Ogólnokształcące z Oddziałami Integracyjnymi.
2. Ilekroć w dokumencie jest mowa o Incydencie, rozumie się przez to zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo systemów informatycznych Szkoły, ciągłość jej działania lub poufność, integralność i dostępność danych osobowych (w tym incydenty o charakterze cyberprzemocy).
3. Osobą odpowiedzialną za koordynację działań, zabezpieczenie techniczne i kontakt z instytucjami zewnętrznymi (w tym CERT Polska) jest Szkolny Koordynator ds. Cyberbezpieczeństwa, którym ustanawia się panią Agnieszkę Podobę.
4. W sprawach związanych z ochroną danych osobowych Szkolny Koordynator ściśle współpracuje z Inspektorem Ochrony Danych (IOD), którym jest pani Lucyna Nikiel

§ 2. Kategorie incydentów

Wszyscy pracownicy oraz uczniowie Szkoły zobowiązani są do natychmiastowego zgłaszania zdarzeń zakwalifikowanych do poniższych kategorii:

- **Incydent Techniczny / Systemowy:** zainfekowanie stacji roboczej złośliwym oprogramowaniem (np. ransomware), awaria i niedostępność dziennika elektronicznego, zablokowanie szkolnej sieci Wi-Fi/LAN, podejrzenie wycieku haseł dostępowych lub ataki typu phishing kierowane do pracowników.
- **Incydent Naruszenia Ochrony Danych Osobowych (RODO):** zagubienie lub kradzież przenośnego nośnika danych (pendrive, laptop) zawierającego dane uczniów lub pracowników, przesłanie wiadomości e-mail z danymi osobowymi do nieuprawnionego adresata, nieautoryzowany dostęp osób trzecich do systemów PESEL lub SIO.
- **Cyberprzemoc i Zagrożenia Cyfrowe Młodzieży:** nękanie, znieważanie, kradzież tożsamości w mediach społecznościowych, publikowanie wizerunku uczniów lub nauczycieli bez ich zgody, włamanie na prywatne lub szkolne konta uczniów.

§ 3. Algorytm postępowania i reakcji

1. Krok 1: Zabezpieczenie śladów (Działanie natychmiastowe)

- W przypadku incydentów technicznych nie należy wyłączać komputera z zasilania (aby nie utracić danych w pamięci RAM). Należy odłączyć kabel sieciowy (LAN) lub wyłączyć kartę Wi-Fi.
- W przypadku cyberprzemocy należy niezwłocznie wykonać zrzuty ekranu, zapisać wiadomości oraz zabezpieczyć adresy URL stron.

2. Krok 2: Zgłoszenie wewnętrzne

Świadek lub ofiara zdarzenia niezwłocznie zgłasza fakt do Szkolnego Koordynatora (Agnieszka Podoba) lub bezpośrednio do Dyrektora Szkoły za pomocą Karty Zgłoszenia Incydentu (Załącznik nr 1).

3. Krok 3: Analiza i minimalizacja skutków

Szkolny Koordynator podejmuje kroki techniczne w celu odizolowania zagrożenia. W przypadku podejrzenia naruszenia danych osobowych powiadamiany jest Inspektor Ochrony Danych Lucyna Nikiel w celu przeprowadzenia analizy ryzyka.

§ 4. Zgłoszenia zewnętrzne i terminy

Jeżeli incydent zostanie zakwalifikowany jako poważny, Dyrektor Szkoły we współpracy z właściwą osobą dokonuje formalnych zgłoszeń:

- **CERT Polska:** Zgłoszenia incydentów technicznych i zagrożeń sieciowych dokonuje Szkolny Koordynator poprzez platformę incydent.cert.pl.
- **Urząd Ochrony Danych Osobowych (UODO):** W przypadku stwierdzenia naruszenia ochrony danych skutkującego ryzykiem naruszenia praw lub wolności osób, Dyrektor Szkoły po konsultacji z IOD Lucyną Nikiel zgłasza naruszenie do PUODO w terminie do 72 godzin od stwierdzenia naruszenia.
- **Policja / Sąd Rodzinny:** W przypadku przestępstw popełnionych w sieci lub rażących aktów cyberprzemocy równieśniczej wyczerpujących znamiona czynów karalnych małoletnich.

§ 5. Konsekwencje i sankcje

1. Wobec uczniów naruszających zasady cyberbezpieczeństwa Szkoły lub dopuszczających się cyberprzemocy stosuje się kary statutowe zgodnie ze Statutem Szkoły Podstawowej nr 36 z Oddziałami Integracyjnymi oraz VI Liceum Ogólnokształcącym z Oddziałami Integracyjnymi w Zespole Szkół Ogólnokształcących im. Armii Krajowej w Bielsku - Białej tym: upomnienie lub nagana wychowawcy/Dyrektora, przesunięcie do innej równoległej klasy, a w skrajnych przypadkach skierowanie sprawy do Sądu Rodzinnego.

2. Wobec pracowników, których zaniechanie lub umyślne działanie doprowadziło do incydentu (np. rażące niedopełnienie obowiązków ochrony danych), stosuje się sankcje przewidziane w Kodeksie Pracy oraz Karcie Nauczyciela (w tym kary porządkowe lub dyscyplinarne).

§ 6. Rejestr incydentów

Każdy zgłoszony incydent podlega obowiązkowej rejestracji w ewidencji prowadzonej przez Szkolnego Koordynatora (wzór w Załączniku nr 2). Rejestr służy do celów dowodowych oraz analizy bezpieczeństwa placówki.

Załącznik nr 1 do Procedury

KARTA ZGŁOSZENIA INCYDENTU (WZÓR)

1. Osoba zgłaszająca (imię, nazwisko, funkcja/klasa):

.....

2. Data i godzina stwierdzenia incydentu:

.....

3. Typ incydentu (zaznacz właściwe):

☐ Atak techniczny / złośliwe oprogramowanie

☐ Wyciek lub zagrożenie naruszenia danych osobowych (RODO)

☐ Cyberprzemoc / nękanie w sieci

☐ Inne:

4. Opis zdarzenia oraz podjęte działania natychmiastowe:

.....

.....

5. Wykaz zabezpieczonych dowodów (np. logi, zrzuty ekranu, e-maile):

.....

.....

Podpis przyjmującego zgłoszenie

.....

Podpis zgłaszającego

Załącznik nr 2 do Procedury

REJESTR INCYDENTÓW CYBERBEZPIECZEŃSTWA (WZÓR)

Lp.	Data i godz.	Opis / Typ incydentu	Skutki i ryzyko (RODO/techniczne)	Podjęte działania i wnioski	Status / Podpis Koord.
1.	25.10.2026 godz. 09:30	Przykładowy opis: Phishing na e-mail sekretariatu.	Niskie. Hasła zmienione, brak wycieku danych.	Zablokowanie nadawcy, wymuszenie resetu haseł, szkolenie personelu.	Zamknięty A. Podoba