ZPO3.021.4.2025

# Zarządzenie nr 4/2025
# Dyrektora Zespołu Placówek Oświatowych nr 3
# w Mławie
# z dnia 28 stycznia 2025 r.

w sprawie wprowadzenia Procedury zarządzania incydentami i naruszeniami bezpieczeństwa informacji.

Na podstawie:
§ 19 ust. 2 pkt 13 Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U.2024 r., poz. 773),
art. 22 ust. pkt 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077),
§ 6 ust. 2 pkt 9 Statutu Zespołu Placówek Oświatowych nr 3 w Mławie,

Dyrektor Zespołu Placówek Oświatowych nr 3 w Mławie zarządza, co następuje:

**§ 1**

W Zespole Placówek Oświatowych nr 3 w Mławie wprowadza się Procedurę zarzadzania incydentami i naruszeniami bezpieczeństwa informacji.

**§ 2**

Na osobę odpowiedzialną za zarządzanie incydentami Cyberbezpeiczeństwa wyznacza się p. **Mariusz Sobotkę.**

**§ 3**

Zarządzenie wchodzi w życie z dniem 28 stycznia 2025 r.

***Dyrektor Zespołu Placówek***
***Oświatowych nr 3 w Mławie***
***Mariusz Lempek***

# PROCEDURA ZARZĄDZANIA INCYDENTAMI I NARUSZENIAMI BEZPIECZEŃSTWA INFORMACJI

## 1. Cel i zakres procedury

Dokument ma na celu ustanowienie jednolitych zasad zarządzania incydentami i naruszeniami bezpieczeństwa informacji w **Zespole Placówek Oświatowych nr 3 w Mławie**.

Niniejsza procedura ustanowiona jest w celu realizacji wymagań § 19 ust 2 Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U z 2024r. poz. 773); art. 21 ust. 1 ustawy z dnia 5 lipca 2018r. o Krajowym Systemie Cyberbezpieczeństwa (Dz. U. z 2024r. poz. 1077 ze zm.) oraz zarządzeniem nr 10/2025 Burmistrza Miasta Mława z dnia 16 stycznia 2025r. w sprawie wyznaczenia osoby odpowiedzialnej za utrzymanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa dla Urzędu Miasta Mława oraz jednostek organizacyjnych.

## 2. Terminy i skróty

| | |
|---|---|
| **Jednostka** | Zespół Placówek Oświatowych nr 3 w Mławie |
| **Dyrektor** | Dyrektor Zespołu Placówek Oświatowych nr 3 w Mławie |
| **Cyberbezpieczeństwo** | odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy, |
| **Incydent** | zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo, |
| **Podatność** | właściwość systemu informacyjnego, która może być wykorzystana przez zagrożenie cyberbezpieczeństwa, |
| **Ryzyko** | wpływ niepewności na cele |
| **Zarządzanie Ryzykiem** | system metod i działań zmierzających do obniżenia ryzyka do poziomu akceptowalnego, przy uwzględnieniu kosztów działania oraz zabezpieczenia się w racjonalny sposób przed jego skutkami, obejmuje identyfikowanie i ocenę ryzyka oraz reagowanie na nie; proces zarządzania ryzykiem obejmuje ryzyko występujące we wszystkich procesach decyzyjnych i na każdym szczeblu zarządzania, |
| **Identyfikacja Ryzyka** | proces wyszukiwania, rozpoznawania i opisywania ryzyka, |
| **Analiza Ryzyka** | proces dążący do poznania charakteru ryzyka oraz określenia poziomu ryzyka, |
| **Kryteria Ryzyka** | poziomy odniesienia, względem których określa się sposób postępowania z ryzykiem, |
| **Ewaluacja Ryzyka** | proces porównywania wyników analizy ryzyka z kryteriami ryzyka, w celu stwierdzenia czy ryzyko i/lub jego wartość są akceptowalne i tolerowane, |
| **Ocena Ryzyka** | całościowy proces identyfikacji, analizy oraz ewaluacji ryzyka, |
| **Zdarzenie** | wystąpienie lub zmiana konkretnego zestawu okoliczności, |
| **Prawdopodobieństwo Ryzyka** | możliwość, szansa wystąpienia zdarzenia, |
| **Następstwo Ryzyka** | skutek, rezultat zdarzenia, mający wpływ na cele, |
| **Ryzyko Akceptowalne** | wielkość, poziom ryzyka, jakie organizacja jest gotowa w dowolnym czasie zaakceptować, tolerując jego istnienie oraz skutki, |
| **Środek Kontroli** | wszystko to, co modyfikuje ryzyko, |
| **Proces** | uporządkowany logicznie ciąg czynności, działań, decyzji i uzgodnień, |
| **Właściciel Ryzyka** | osoba odpowiedzialna za zarządzanie ryzykiem, mająca kompetencje do podjęcia działań zaradczych w stosunku do obszaru, którym zarządza, właściciel systemu lub aplikacji |
| **Dostępność informacji** | właściwość polegającą na tym, że informacja jest możliwa do wykorzystania przez uprawniony podmiot na jego żądanie, w założonym czasie, |
| **Integralność informacji** | właściwość polegającą na tym, że informacja nie została zmodyfikowana w sposób nieuprawniony, |

| | |
|---|---|
| **Poufność informacji** | właściwość polegająca na tym, że informacja nie jest udostępniana ani ujawniana nieautoryzowanym osobom, podmiotom lub procesom, |
| **Zgodność prawna** | właściwość polegająca na tym, że dane działanie związane z informacją jest zgodne z przepisami powszechnie obowiązującego prawa, któremu podlega działalność Urzędu. |

## 3. Kwalifikowanie incydentów bezpieczeństwa informacji

1. Incydent lub zdarzenie związane z bezpieczeństwem informacji może zgłosić każdy pracownik, petent, przedstawiciel instytucji, na każdym etapie procesów lub świadczonej usługi.
2. Pracownicy są zobowiązani do reagowania na zdarzenia związane z bezpieczeństwem informacji, incydenty związane z bezpieczeństwem informacji, w tym incydenty stanowiące naruszenie ochrony danych osobowych.
3. W zakresie obsługi incydentów pracownicy podlegają szkoleniu w ramach szkolenia wstępnego oraz obowiązkowo podczas szkoleń okresowych.
4. Za kontakty z osobami z zewnątrz jednostki w tym mediami odpowiedzialny jest **Dyrektor**.
5. Za incydent przyjmuje się praktycznie każde zdarzenie, które nie należy do standardowych operacji i które powoduje lub może powodować:
   1) zakłócenia lub przerwy w funkcjonowaniu Zespołu Placówek Oświatowych nr 3 w Mławie, np. cyklicznie powtarzające się takie zdarzenia związane z określoną niedostępnością systemów mających wpływ na normalny tok pracy, lub możliwości świadczenia usług w okresie przekraczającym **15 min**,
   2) zmiany w zakresie informacji świadczące o braku integralności danych,
   3) ujawnienie lub dostęp do informacji przez osoby nieupoważnione,
   4) utrata danych.

## 4. Postępowanie z incydentami bezpieczeństwa informacji

### 4.1. Zgłaszanie incydentów bezpieczeństwa informacji.

1. Zgłaszanie zdarzeń i incydentów bezpieczeństwa informacji realizowane jest w następujący sposób:
   1) Zgłaszanie i rejestrowanie incydentów **musi być przeprowadzone mailowo na adres incydent@mlawa.pl oraz do obsługi informatycznej**.
   2) Osoba odpowiedzialna za zarzadzanie incydentami Cyberbezpieczeństwa rejestruje i zgłasza zdarzenie.
   3) Każdy pracownik podczas obserwacji zdarzenia, incydentu związanego z bezpieczeństwem informacji powinien sprawdzić schemat postępowania. Jeżeli dla danego zdarzenia nie określono inaczej, pracownik ma obowiązek zgłosić zdarzenie lub incydent osobie odpowiedzialnej za zarzadzanie incydentami Cyberbezpieczeństwa.

4) W przypadku nieobecności osoby, o której mowa powyżej, incydent zgłaszany jest bezpośredniemu przełożonemu, który rejestruje i zgłasza incydent.
5) W przypadku nieobecności bezpośredniego przełożonego, incydent rejestruje i zgłasza bezpośrednio pracownik, który zaobserwował incydent związany z bezpieczeństwem informacji.

2. W przypadku, gdy incydent zgłasza strona zewnętrzna (np. dostawca, petent, gość), każdy pracownik zobowiązany jest do przyjęcia zgłoszenia i postępowania zgodnie z punktem powyżej.
3. Odbiorcą zgłoszenia przesłanego drogą mailową na adres **incydent@mlawa.pl** jest Osoba odpowiedzialna za utrzymywanie kontaktów w zakresie Cyberbezpieczeństwa (zgodnie z zarządzeniem Burmistrza UM Mława) w Urzędzie Miasta Mława.
4. W przypadku zgłoszeń związanych z naruszeniem ochrony danych osobowych Osoba odpowiedzialna za utrzymywanie kontaktów w zakresie Cyberbezpieczeństwa, na podstawie otrzymanego zgłoszenia przekazuje je na adres **mk@open-audit.eu** lub telefonicznie do Inspektora Ochrony Danych Osobowych.
5. Przekazując informację o zdarzeniu należy w szczególności wskazać (wzór zawiera Załącznik nr 1):
   a) Dane zgłaszającego: Imię i Nazwisko, email, telefon oraz stanowisko i komórkę organizacyjną,
   b) Datę i godzinę oraz miejsce obserwacji incydentu,
   c) Opis zdarzenia (zasięg incydentu, liczba osób których dotyczy zgłoszenie),
   d) Inne informacje mogące mieć wpływ na ocenę zdarzenia.
6. Jeżeli istnieje taka możliwość – pracownik zobowiązany jest do dostarczenia materiału dowodowego potwierdzającego incydent (np. zdjęcia, zapisy z systemów itd.) wraz ze zgłoszeniem incydentu.
7. Zebrany materiał dowodowy dla zgłoszenia incydentu podlega archiwizacji przez okres **co najmniej dwóch lat**.

## 4.2. Analiza zgłoszonych incydentów bezpieczeństwa informacji

1. Po dokonaniu zgłoszenia incydentu do właściwej osoby następuje weryfikacja zgłoszenia, pod kątem poprawności wypełnienia, w szczególności:
   1) kompletny opis zdarzenia / incydentu (wskazanie osób, sytuacji, zasobów uczestniczących w incydencie),
   2) wpływ incydentu na ryzyko naruszenia praw i wolności osób (w przypadku naruszenia ochrony danych osobowych) i zawiadomienia osób, których dane dotyczą oraz Urzędu Ochrony Danych Osobowych,
   3) wpływ incydentu na ryzyko zagadnienia cyberbezpieczeństwa,
   4) podjęte i zaplanowanie działania naprawcze w następstwie incydentu,nar

5) skuteczność podjętych natychmiastowych działań naprawczych,
6) ewentualne koszty podjętych działań naprawczych do strat spowodowanych przez naruszenie.

2. Informacja o incydentach powinna być okresowo przekazana do Inspektora Ochrony Danych w celu określenia potrzeby wykonania ponownej analizy ryzyka pod kątem bezpieczeństwa informacji.
3. Po przeprowadzeniu analizy, każdy incydent, który wymaga podjęcia dodatkowych środków naprawczych powinien zostać przedstawiony **Dyrektorowi** wraz z planem postępowania przez Osobę odpowiedzialną za utrzymywanie kontaktów w zakresie Cyberbezpieczeństwa.
4. Wszystkie zaistniałe incydenty należy rejestrować (wzór rejestru zawiera Załącznik nr 2) oraz postępowanie z nimi podlega rocznemu przeglądowi. Podczas przeglądu zarządzania może być przeprowadzana analiza i mogą być ustalane ewentualne strategiczne działania korygujące wynikające długookresowej analizy incydentów.
5. Jeżeli Incydent stanowi incydent w zakresie cyberbezpieczeństwa, zdarzenie takie zgłaszane jest do CSIRT NASK w terminie 24 godzin od momentu wykrycia zdarzenia.
6. W zgłoszeniu uwzględnia się w szczególności:
   1) dane podmiotu zgłaszającego, w tym nazwę podmiotu, numer we właściwym rejestrze, siedzibę i adres,
   2) imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby składającej zgłoszenie,
   3) imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby uprawnionej do składania wyjaśnień dotyczących zgłaszanych informacji,
   4) opis wpływu incydentu w podmiocie publicznym na realizowane zadanie publiczne, w tym:
      a) wskazanie zadania publicznego, na które incydent miał wpływ,
      b) liczbę osób, na które incydent miał wpływ,
      c) moment wystąpienia i wykrycia incydentu oraz czas jego trwania,
      d) zasięg geograficzny obszaru, którego dotyczy incydent,
      e) przyczynę zaistnienia incydentu i sposób jego przebiegu oraz skutki jego oddziaływania na systemy informacyjne,
      f) informacje o przyczynie i źródle incydentu,
      g) informacje o podjętych działaniach zapobiegawczych,
      h) informacje o podjętych działaniach naprawczych,
      i) inne istotne informacje.

| Załącznik nr 1. Zgłoszenie o zdarzeniu incydentu/naruszenia | | | |
|---|---|---|---|
| ***Procedura zarządzania incydentami i naruszeniami bezpieczeństwa informacji*** | Strona/ stron | 1/1 | Zarządzenie nr 4/2025 Dyrektora Zespołu Placówek Oświatowych nr 3 w Mławie z dnia 28 stycznia 2025 r. |
| **Cel dokumentu:** *Określenie zasad zarządzania incydentami i naruszeniami bezpieczeństwa informacji* | **Wersja nr:**<br>**Z dnia:** | **1**<br>**28-01-2025** | |

**Data i godzina:** ……

**Miejsce incydentu:** ……

**Dane zgłaszającego:**

| Imię i Nazwisko | Email | Telefon | Stanowisko | Komórka organizacyjna |
|---|---|---|---|---|
| | | | | |

**Opis zdarzenia (zasięg incydentu, liczba osób których dotyczy zgłoszenie itd.):**

……

**Inne informacje mogące mieć wpływ na ocenę zdarzenia:**

……

**Załączony materiału dowodowego potwierdzającego incydent (np. zdjęcia, zapisy z systemów itd.):**

……

| Załącznik nr 2. Rejestr incydentów | | | |
|---|---|---|---|
| ***Procedura zarządzania incydentami i naruszeniami bezpieczeństwa informacji*** | Strona/ stron | 1/1 | Zarządzenie nr 4/2025 Dyrektora Zespołu Placówek Oświatowych nr 3 w Mławie z dnia 28 stycznia 2025 r. |
| **Cel dokumentu:** *Określenie zasad zarządzania incydentami i naruszeniami bezpieczeństwa informacji* | **Wersja nr:**<br>**Z dnia:** | **1**<br>**28-01-2025** | |

| Lp. | Data i godzina | Data i godzina | Zgłaszający | Opis incydentu | Klasyfikacja | Wpływ / Skutki | Przyczyna incydentu | Podjęte działania | Odpowiedzialny | Data zamknięcia | Status | Wnioski |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | | | | | | | | | | | | |
| 2 | | | | | | | | | | | | |
| 3 | | | | | | | | | | | | |
| … | | | | | | | | | | | | |