ZARZĄDZENIE Nr 9/2022/2023

Dyrektora Ogólnokształcącej Szkoły Muzycznej I i II stopnia
 im. K. Lipińskiego w Lublinie

z dnia 11 października 2022 r.

**w sprawie wdrożenia „Procedury wewnętrznej – Zasady Zgłaszania Incydentów Cyberbezpieczeństwa przez Ogólnokształcącą Szkołę Muzyczną I i II stopnia im. Karola Lipińskiego w Lublinie”**

Na podstawie Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560) zarządzam, co następuje:

**§ 1**

Wprowadzam „Procedurę wewnętrzną – Zasady Zgłaszania Incydentów Cyberbezpieczeństwa do CSIRT NASK przez Ogólnokształcącą szkołę Muzyczną I i II stopnia im. Karola Lipińskiego w Lublinie” będącą Załącznikiem nr 1 do niniejszego Zarządzenia.

**§ 2**

Jednocześnie zobowiązuję każdego pracownika, który przetwarza dane w systemach

teleinformatycznych do zapoznania się z procedurą, poświadczenia tego zapoznania podpisem

oraz stosowania się do jej zapisów.

**§ 3**

Zarządzenie wchodzi w życie z dniem podpisania.

Załącznik nr 1 do Zarządzenia nr 9/2022/2023 Dyrektora Ogólnokształcącej Szkoły Muzycznej I i II st. im. K. Lipińskiego w Lublinie z dnia 11.10.2022 r.

**PROCEDURA WEWNĘTRZNA**

**ZASADY ZGŁASZANIA INCYDENTÓW CYBERBEZPIECZEŃSTWA DO CSIRT NASK PRZEZ OGÓLNOKSZTAŁCĄCĄ SZKOŁĘ MUZYCZNĄ I i II STOPNIA W LUBLINIE**

1. **Zakres obowiązywania**

Procedura postępowania obowiązuje w Ogólnokształcącej Szkoły Muzycznej I i II stopnia im. Karola Lipińskiego w Lublinie.

1. **Odpowiedzialność**

**Dyrektor odpowiedzialny jest za:**

* wprowadzenie Zarządzeniem procedury pt.: „Zasady zgłaszania incydentów cyberbezpieczeństwa”.
* zapoznanie pracowników z treścią procedury pt.: „Zasady zgłaszania incydentów cyberbezpieczeństwa”.

**Pracownik** – odpowiedzialny jest za wypełnienie Formularza Zgłaszania Incydentów Cyberbezpieczeństwa i dokonanie zgłoszenia do Informatyka.

**Informatyk zobowiązany jest do:** przyjęcia zgłoszenia od pracownika, pomoc przy uzupełnianiu Formularza Zgłoszeń Incydentów, prowadzenie Rejestru incydentów sieci informatycznej, odpowiednio szybkiej reakcji i przeprowadzenia postępowania wyjaśniającego oraz oceny zdarzenia pod kątem bezpieczeństwa dla systemu oraz baz danych. Poinformowanie IOD oraz ADO o klasyfikacji incydentu i jego skutkach dla ochrony i bezpieczeństwa danych.

**Inspektor Ochrony Danych (IOD) odpowiedzialny jest za:** współdziałanie z Informatykiem oraz zgłaszającym.

**Definicje**:

**Incydentem cyberbezpieczeństwa** jest wykryte zdarzenie w systemie informacyjnym placówki, które powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania realizowanego przez komórkę/dział placówki.

1. **Opis postepowania**
	1. Wszystkie wykryte w szkole zdarzenia są oceniane przez Informatyka pod kątem zakwalifikowania go jako incydent cyberbezpieczeństwa.
	2. Zgłoszeniu podlegają wszystkie informacje dotyczące incydentu znane w chwili dokonywania zgłoszenia.
	3. Pracownik dokonujący zgłoszenia odpowiada za wyczerpujące opisanie incydentu w „Formularzu zgłoszenia incydentu cyberbezpieczeństwa” adekwatnie do posiadanej wiedzy i umiejętności. Brak wiedzy i umiejętności poprawnego rozpoznania incydentu po stronie zgłaszającego nie może być przyczyną zaniechania zgłoszenia.
	4. Pracownik zgłasza incydent do Informatyka jak najszybciej jak to jest możliwe.
	5. Zgłoszenia dokonuje się na adres e-mail: incydenty@osmuzlublin.pl
	6. Po rozmowie z Informatykiem pracownik wypełnia Formularz zgłoszenia incydentu.
	7. Po wypełnieniu formularza pracownik dostarcza go w wersji papierowej do Informatyka.
	8. Informatyk uzupełnia pola w części A, B oraz C, pracownik pozostałe w miarę posiadanej wiedzy. Informatyk współuczestniczy w wypełnianiu jeżeli pracownik potrzebuje pomocy merytorycznej.
	9. Po ostatecznym zatwierdzeniu prawidłowości wypełnienia formularza Informatyk dokonuje dalszych czynności w porozumieniu z IOD i Dyrekcją jeżeli zachodzi taka konieczność.
	10. Incydent odnotowywany jest w ewidencji incydentów prowadzonej przez Informatyka.
	11. Formularz zgłoszenia przekazywany jest do Dyrektora. W jego posiadaniu znajduje się również Informatyk oraz Inspektor Ochrony Danych.
2. **Załączniki**
	1. Załącznik nr 1 Rejestr incydentów
	2. Załącznik nr 2 Formularz zgłaszania incydentów cyberbezpieczeństwa
	3. Załącznik nr 3 Oświadczenie pracownika o zapoznaniu z procedurą

….………………..…………………………..

Opracował Zatwierdził