Zespół Szkół nr 2
w Nowym Tomyślu
64-300 Nowy Tomyśl, os. Północ 37
tel. 61 44 21 102, 61 44 22 288
NIP 788-173-66-95

**Załącznik do ZARZĄDZENIE Nr 6 /2023**

**Dyrektora Zespołu Szkół nr 2 w Nowym Tomyślu**

z dnia 02.11.2023r.

# Procedura postępowania z incydentami bezpieczeństwa informacji i cyberbezpieczeństwa

1. Definicje

Ceberbezpieczeństwo – odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy,

Incydent w podmiocie publicznym – incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny,

Incydent bezpieczeństwa – pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem danych osobowych, które stwarzają znaczne prawdopodobieństwo wystąpienia naruszenia ochrony danych osobowych,

Incydent ceberbezpieczeństwa – to zdarzenie, którego skutkiem jest lub może być naruszenie bezpieczeństwa aktywów informacyjnych oraz który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez Starostwo Powiatowe w Nowym Tomyślu,

Incydent krytyczny- incydent skutkujący znaczną szkodą dla bezpieczeństwa lub porządku prawnego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw lub wolności obywatelskich lub życia i zdrowia ludzi, klasyfikowany przez właściwy CSIRT NASK,

Administrator Danych Osobowych – Dyrektor Zespołu Szkół nr 2 w Nowym Tomyślu,

Inspektor Ochrony Danych (IOD) – osoba wyznaczona przez Administratora Danych Osobowych,

Administrator Systemów Informatycznych (ASI) – osoba wyznaczona przez Administratora Danych Osobowych,

Naruszenie ochrony danych osobowych ( zgodnie z art. 4 ust. 1pkt 12 RODO) oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia.

2. Kategorię incydentów
1) Przyczyną incydentu bezpieczeństwa lub ceberbezpieczeństwa może być:
a) zdarzenie losowe zewnętrzne ( np. klęski żywiołowe, pożary, zakłócenia w dostawie energii elektrycznej itp.) którego wystąpienie może spowodować zniszczenie lub uszkodzenie infrastruktury informatycznej albo dokumentacji papierowej oraz zakłócenie ciągłości pracy systemów nie powodując naruszenia poufności danych;
b) zdarzenie losowe wewnętrzne ( np. błędy w oprogramowaniu, awarię sprzętu itp.), które mogą powodować zakłócenia ciągłości pracy systemów, a także prowadzić do zniszczenia lub utraty danych;
c) świadome i celowe działania mające na celu naruszenie poufności zasobów informacyjnych, w tym poufności danych.

3. Incydentami bezpieczeństwa informacji w szczególności są:
   1) naruszenia poufności, to jest ujawnienie informacji niepowołanym osobom;
   2) naruszenie integralności, to jest zniszczenie, uszkodzenie lub przekłamanie informacji;
   3) naruszenie dostępności, to jest brak dostępu do danych przez uprawnionych użytkowników.
4. Przyczyny incydentów bezpieczeństwa informacji oraz ceberbezpieczeństwa mogą dotyczyć:
   a) niewłaściwego wykorzystania zasobów informatycznych lub niewłaściwe postępowanie z dokumentacja papierową;
   b) działania szkodliwego oprogramowania;
   c) próby omijania systemów zabezpieczeń;
   d) nieautoryzowanego dostępu do systemów, aplikacji i dokumentów;
   e) zniszczenia lub kradzieży urządzeń wykorzystywanych do przetwarzania i przechowywania informacji;
   f) zniszczenie lub kradzieży nośników danych;
   g) próby wyłudzeń informacji;
   h) ataków socjotechnicznych, ataków z wykorzystywaniem technik zagrażających poufności, integralności lub dostępności informacji,
   i) nieprawidłowości w zakresie zabezpieczenia przechowywania danych, w tym danych osobowych,
   j) naruszenie zasad obowiązujących w Szkole dotyczących bezpieczeństwa informacji, w tym danych osobowych.

5. Zgłaszanie incydentów bezpieczeństwa:

1). Każdy pracownik ma obowiązek zgłosić podejrzenie wystąpienia incydentu bezpieczeństwa lub ceberbezpieczeństwa.

2). Zgłoszenie incydentu bezpieczeństwa można zgłosić:

- drogą elektroniczną na adres: sekretariat@hzs2nt.pl
- pisemnie przekazując zgłoszenie do Sekretariatu Szkoły,
- w formie notatki bezpośredniemu przełożonemu lub osobie wyznaczonej do kontaktów w sprawie ceberbezpieczeństwa.

3). Zgłoszenie powinno zawierać następujące informacje:

- imię i nazwisko osoby zgłaszającej,
- dokładne miejsce oraz datę wystąpienia incydentu,
- opis incydentu, konsekwencja zdarzenia ( o ile zaistniały), uczestników zdarzenia oraz podjęte działania w celu minimalizacji skutków zdarzenia ( o ile zostały podjęte).

4). Brak umiejętności poprawnego rozpoznania incydentu przez osobę zgłaszającą nie może być przyczyną zaniechania zgłoszenia.

5) Za obsługę incydentów bezpieczeństwa odpowiada osoba wyznaczona do kontaktów w sprawie ceberbezpieczeństwa.

6). W przypadku nieobecności osoby wyznaczonej do kontaktów w sprawie ceberbezpieczeństwa obsługę incydentu należy zgłosić do ASI.

7). Osoba odpowiedzialna za obsługę incydentu bezpieczeństwa dokonuje analizy biorąc pod uwagę następujące czynniki:

- powstałe szkody będące wynikiem incydentu,
- wpływ incydentu na działanie systemów,
- wpływ incydentu na ciągłość działania Szkoły,
- koszty usunięcia skutków incydentu,
- szacowany czas naprawy skutków wywołanych incydentem,
- oszacowanie zasobów koniecznych do przywrócenia działania.

8). W przypadku gdy incydent bezpieczeństwa ma charakter naruszenia ochrony danych osobowych, to osoba obsługująca incydent zobowiązana jest do niezwłocznego przekazania informacji Inspektorowi Ochrony Danych.

9). W przypadku stwierdzenia incydentu ceberbezpieczeństwa osoba wyznaczona do kontaktów w sprawie ceberbezpieczeństwa w ciągu 24 godzin od momentu wykrycia zgłasza incydent do właściwego CSIRT NASK (Naukowa i Akademicka Sieć Komputerowa-Państwowego Instytutu Badawczego).

10). Zgłoszenia do CSRIT NASK przekazywane są w sposób elektroniczny. Procedura zgłoszeń opisana jest pod adresem internetowym https://incydent.cert.pl.

11). Zgłoszenie incydentu musi zostać zarejestrowane w rejestrze, którego wzór stanowi załącznik nr 1.

6. Podejmowanie działań wynikających ze zgłaszanych incydentów związanymi z bezpieczeństwem informacji oraz cyberbezpieczeństwem.

1) Osoba obsługująca incydent bezpieczeństwa zobowiązana jest do monitorowania wdrożenia działań naprawczych, tj. takich które mają zapobiegać ponownemu zdarzeniu,
2) Raz w roku zarejestrowane incydenty bezpieczeństw są analizowane przez ASI, IOD oraz Dyrektora Szkoły.

Załącznik nr 1 – Wzór rejestru incydentów bezpieczeństwa

| Lp. | Data zgłoszenia | Kategoria zgłoszenia(*incydent bezpieczeństwa,/ceberbezpieczeństwa lub naruszenia ochrony danych osobowych | Opis incydentu (zdarzenia) | Osoba zgłaszająca | Kategoria incydentu | Przyczyna lub potencjalna przyczyna wystąpienia incydentu | Opis działań podjętych w związku z incydentem | Data zamknięcia incydentu |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

DYREKTOR
M. Ginter
mgr Marzena Ginter