INSTRUKCJA ZGŁASZANIA I OBSŁUGI INCYDENTÓW

Celem niniejszej instrukcji jest określenie obowiązujących w Szkole Podstawowej im. Marii Skłodowskiej-Curie, procedur postępowania w sytuacji wystąpienia lub uzasadnionego podejrzenia wystąpienia incydentu bezpieczeństwa teleinformatycznego w tym również naruszenia ochrony danych osobowych. Dla uproszczenia w dalszej części instrukcji oba rodzaje zdarzeń nazywane będą **incydentem**.

Incydent bezpieczeństwa teleinformatycznego – takie pojedyncze zdarzenie lub seria zdarzeń, związanych z bezpieczeństwem informacji niejawnych (chronionych), które zagrażają ich poufności, dostępności lub integralności (Rozporządzenie Prezesa Rady Ministrów z dnia 20.07.2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego).

Naruszenie ochrony danych osobowych - naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych (art. 4 pkt 12 RODO).

Incydent w podmiocie publicznym – incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny (Ustawa o Krajowym Systemie Cyberbezpieczeństwa z dnia 5.07.2018 r.).

§ 1

Za wystąpienie lub uzasadnione podejrzenie wystąpienia incydentu uznaje się w szczególności:

1) odnośnie zdarzeń zachodzących w systemie informatycznym

- ujawnienie informacji chronionych, w tym zawierających dane osobowe osobie nieupoważnionej bez względu na to, czy miało charakter działania świadomego, czy nieświadomego.
- brak lub niedostępność spodziewanych informacji z poziomu obsługi użytkownika systemu informatycznego uprawnionego do przetwarzania danych;
- niezgodność danych w systemie informatycznym z danymi w postaci papierowej lub innymi kopiami utrwalonymi uprzednio na nośnikach elektronicznych;
- widoczne ślady włamania do systemu – np. zmiany w konfiguracji;
- zmiany sum kontrolnych plików;
- zapisy w logach systemowych świadczące o naruszeniu bezpieczeństwa, wykonywaniu niedozwolonych operacji itp.;

- samodzielne akcje podejmowane przez system (nawiązywanie połączeń, wysyłanie wiadomości e-mail itp.);
- intensywna praca dysku w czasie, gdy z komputera nikt nie korzysta;
- powtarzające się zawieszenia systemu;
- spowolnienie pracy systemu lub sieci;
- inne niż zwykle lub dodatkowe okna powitalne, w tym z prośbą o podanie hasła;
- odmowa przyjęcia hasła użytkownika;
- pojawianie się niestandardowych okien, napisów i innych elementów ekranu;
- znaczące zmiany w zajętości dysku;
- nienaturalne rozmiary zapisywanych na dysku plików;
- pojawienie się niespodziewanych nazw plików lub katalogów;
- powtarzające się nagłe zrywanie połączeń sieciowych;
- ujawnienie indywidualnych haseł dostępu do informacji chronionych;
- otrzymanie niespodziewanego e-maila z załącznikami (np. typu .doc, .exe, .com).

2) odnośnie zdarzeń dotyczących elektronicznych i papierowych nośników informacji:

- nieuprawnione wykonanie kopii nośników zawierających informacje chronione;
- zmiana lub usunięcie informacji zapisanych na kopiach bezpieczeństwa lub kopiach archiwalnych;
- zgubienie nośnika zawierającego informacje chronione;
- wykrycie braku nośnika zawierającego informacje chronione w miejscu jego przechowywania;
- odkrycie niezniszczonych nośników z informacjami chronionymi w koszu na śmieci;
- znalezienie nośnika z informacjami chronionymi;
- przekazanie nośnika z informacjami chronionymi osobie nieuprawnionej do ich otrzymania;

3) odnośnie stanu zabezpieczenia pomieszczeń, w których są przetwarzane informacje chronione:

- nieuprawniony dostęp (próba dostępu) do obszaru przetwarzania danych;
- pozostawienie bez nadzoru osoby nieupoważnionej w pomieszczeniu, gdzie znajdują się dane osobowe;
- niewłaściwe działanie fizycznych zabezpieczeń pomieszczeń gdzie przetwarza się informacje chronione;

- niewłaściwe parametry środowiska takie jak temperatura, wilgotność, dla pomieszczeń, w których są przetwarzane informacje chronione w systemie informatycznym oraz na nośnikach papierowych i elektronicznych.

4) **odnośnie nierespektowania obowiązujących zasad przetwarzania danych osobowych:**
   - dopuszczenie do przetwarzania danych osób bez nadania im odpowiednich upoważnień;
   - udostępnianie danych osobowych osobom / podmiotom nieupoważnionym;
   - powierzanie przetwarzania danych osobowych podmiotom zewnętrznym bez zawarcia umowy powierzenia zgodnej z wymaganiami art. 28 ust. 3 RODO;
   - zbieranie danych osobowych bez wykonywania obowiązków informacyjnych, o których mowa w art. 13 i 14 RODO;
   - pozyskiwanie danych osobowych z nielegalnych źródeł;
   - przetwarzanie danych osobowych niezgodne z deklarowanym (lub określonym przepisami prawa) celem i zakresem;
   - przetwarzanie z naruszeniem zasady ograniczenia przechowywania danych;
   - tworzenie nowych zasobów danych osobowych lub modyfikacja istniejących bez zgody dyrektora;
   - przetwarzanie danych osobowych w obszarze niezabezpieczonym;
   - wykonanie nieuprawnionych kopii danych osobowych;
   - brak aktualnych kopii zapasowych danych osobowych;
   - niszczenie nośników z danymi osobowymi w sposób pozwalający na ich odczyt;
   - brak przeszkolenia osób dopuszczonych do przetwarzania danych w zakresie zasad ich przetwarzania i ochrony.

§ 2

Osoba, która podejrzewa lub stwierdzi incydent ma obowiązek niezwłocznie:

1) powiadomić o zaistniałym zdarzeniu bezpośredniego przełożonego lub/i IOD, a w przypadku incydentu związanego z przetwarzaniem danych w systemie informatycznym również Administratora Systemu Informatycznego (ASI);
2) określić (opisać) symptomy, świadczące o wystąpieniu lub możliwości wystąpienia incydentu;
3) określić sytuację i czas, w jakim zauważono zdarzenie;
4) podać wszelkie istotne informacje, mogące pomóc w ustaleniu przyczyny wystąpienia incydentu;

5) przekazać IOD i ASI informacje niezbędne do opracowania „Raportu dotyczącego incydentu naruszenia bezpieczeństwa informacji" oraz zgłoszeń incydentu do CSIRT NASK i Urzędu Ochrony Danych Osobowych, jeżeli wystąpi konieczność wysłania zgłoszenia.
Ramowy wzór „Raportu" znajduje się w **Załączniku nr 1** do niniejszej Instrukcji.

§ 3

IOD, ASI i ewentualnie powołany zespół po otrzymaniu zgłoszenia oceniają sytuację i podejmują odpowiednie do potrzeb działania, a w szczególności:

- dokonują rozpoznania zdarzenia;
- oceniają wagę problemu;
- lokalizują źródło problemu;
- zarządzają incydentem, przez co rozumie się obsługę incydentu, usuwanie przyczyn wystąpienia incydentu oraz opracowanie wniosków wynikających z obsługi incydentu.

§ 4

1. W sytuacji gdy incydent dotyczy cyberbezpieczeństwa, w tym systemu informatycznego ASI we współdziałaniu z IOD podejmują działania zmierzające do określenia i zakwalifikowania rodzaju zdarzenia, jako błąd użytkownika systemu, awarię systemu lub naruszenie bezpieczeństwa systemu. ASI podejmuje odpowiednie do potrzeb działania, a w szczególności:

- ocenia wagę problemu;
- ocenia możliwość wystąpienia strat w zasobach informacyjnych i systemowych w przypadku dalszego działania systemu;
- lokalizuje źródło problemu (przeprowadza analizę posiadanych danych);
- podejmuje decyzję o wstrzymaniu lub dalszej pracy systemu;
- przygotowuje informację dla dyrektora, który podejmuje decyzję o zgłoszeniu incydentu do CSIRT NASK;
- przygotowuje we współpracy z IOD projekt zgłoszenia do CSIRT NASK.

2. W sytuacji, gdy dyrektor podjął decyzję o zgłoszeniu incydentu osoba wyznaczona do współpracy z CSIRT NASK przy obsłudze incydentu (Sekretarz, ASI) wysyła zgłoszenie (nie później niż 24 godziny od momentu wykrycia) i współpracuje z CSIRT NASK przy obsłudze incydentu.
Ramowy wzór zgłoszenia do CSIRT NASK znajduje się w **załączniku nr 2** do niniejszej instrukcji.

§ 5

1. W przypadku gdy incydent dotyczy naruszeniu ochrony danych IOD powiadamia o tym dyrekcję szkoły, uprawnionego do podjęcia działań zmierzających do wyjaśnienia sprawy i poinformowania odpowiednich organów o zaistniałej sytuacji.
2. W sytuacji potwierdzenia wystąpienia incydentu należy przeprowadzić szacowania ryzyka naruszenia praw i wolności osób, których może dotyczyć zgłoszone zdarzenie, w tym oceny skutków zdarzenia na prywatność osób, których incydent dotyczy.
3. Szacowanie ryzyka dotyczące sytuacji naruszenia ochrony danych jest przeprowadzane w zależności od sytuacji przez IOD, ASI i kierownika komórki organizacyjnej, której dotyczył incydent.
4. IOD sporządza notatkę zawierającą opis zdarzenia i podjętych działań, którą przekazuje dyrekcji szkoły.

§ 6

1. W sytuacji, gdy incydent kwalifikuje się, zgodnie z art. 33 RODO, jako naruszenie ochrony danych osobowych, które powinno zostać zgłoszone do Prezesa Urzędu Ochrony Danych Osobowych IOD we współpracy z ASI przygotowuje projekt zgłoszenia na formularzu (wzór ramowy), który stanowi **załącznik nr 3.**
   Zgłoszenie przekazywane jest do PUODO przez Administratora (nie później niż 72 godziny po stwierdzeniu incydentu) w poprzez wypełnienie formularza elektronicznego, zgodnie z trybem określonym przez organ na stronie internetowej https://uodo.gov.pl.

§ 7

1. W sytuacji gdy stwierdzone naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, o naruszeniu należy zawiadomić wszystkie osoby, których dane dotyczą.
2. IOD we współpracy z radcą prawnym dokonują analizy czy będzie wymagane w odniesieniu do wymogów art. 34 ust. 3 RODO zawiadomienie o przedmiotowym naruszeniu osób, których dane dotyczą. W razie podjęcia decyzji o konieczności spełnienia obowiązku informacyjnego wobec tych osób, IOD opracowuje treść zawiadomienia, które podpisane zostanie przez dyrektora.

§ 8

Po zakończeniu obsługi incydentu IOD i ASI podejmują działania, celem wyeliminowania, bądź zminimalizowania wystąpienia podobnej sytuacji w przyszłości.

§ 9

IOD prowadzi ewidencję naruszeń ochrony danych osobowych zgodnie ze wzorem (wzór ramowy) zawartym w **Załączniku nr 4** do niniejszej Instrukcji.

§ 10

W sprawach nieuregulowanych w niniejszej instrukcji mają zastosowanie przepisy RODO, ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000) oraz ustawy z dnia 5.07.2018 r. o Krajowym Systemie Cyberbezpieczeństwa.

Osoby dopuszczone w do przetwarzania danych osobowych zobowiązane są do bezwzględnego stosowania zasad określonych w niniejszej instrukcji.

Załączniki:

1. Wzór „Protokołu z obsługi incydentu".
2. Wzór „Formularz zgłoszenia incydentów CSIRT NASK"
3. Wzór „Zgłoszenie naruszenia ochrony danych osobowych"
4. Wzór „Ewidencja naruszeń ochrony danych osobowych".