PROCEDURA ZARZĄDZANIA INCYDENTAMI CYBERBEZPIECZEŃSTWA

w Szkole Podstawowej nr 1 im. Stanisławy Łakomik w Czeladzi

W związku z realizacją wytycznych ustawy z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa w **Szkole Podstawowej nr 1 im. Stanisławy Łakomik w Czeladzi, ul. Reymonta 80, 41-250 Czeladź** wprowadzona zostaje procedura mająca na celu prawidłowe wywiązanie się z nałożonych obowiązków w zakresie cyberbezpieczeństwa w **Szkole Podstawowej nr 1 im. Stanisławy Łakomik w Czeladzi**, określająca zasady postępowania w chwili wystąpienia zagrożenia lub ataku, która przedstawia się następująco:

1. Do monitorowania przypadków mogących mieć negatywny wpływ na cyberbezpieczeństwo, wyznacza się w **Szkole Podstawowej nr 1 im. Stanisławy Łakomik w Czeladzi Pełnomocnika ds. bezpieczeństwa cyberprzestrzeni** w osobie: **Marek Woźniak**, przy czym każdy pracownik, który zauważy wystąpienie zdarzeń (zachowań w obsługiwanych systemach) mogących wskazywać na ingerencję w system osób trzecich, zobowiązany jest zawiadomić **Dyrektora Szkoły Podstawowej nr 1 im. Stanisławy Łakomik w Czeladzi**.
2. **Szkoła Podstawowa nr 1 im. Stanisławy Łakomik w Czeladzi** zobowiązana jest do zgłoszenia osoby kontaktowej do CSIRT NASK. Zgłoszenie może być zrealizowane listownie lub poprzez stronę internetową:

   https://incydent.cert.pl/osoba-kontaktowa#!/lang=pl,entityType=publicInstitution
   (załącznik nr 1 do niniejszej Procedury**)**
3. **Pełnomocnik ds. bezpieczeństwa cyberprzestrzeni** monitoruje w szczególności wystąpienie z poziomu Internetu i/lub domeny przypadków:
   a) skanowania,
   b) spamu przesyłanego za pośrednictwem polskich serwerów,
   c) ataków typu DoS (Denial of Service) i DDoS (Distributed Denial of Service),
   d) włamań i prób włamania.
4. **Pełnomocnik ds. bezpieczeństwa cyberprzestrzeni** reaguje na każde zgłoszenie dokonane przez pracownika **Szkoły Podstawowej nr 1 im. Stanisławy Łakomik w Czeladzi** dotyczące zdarzeń mogących wskazywać na cyberatak lub inną formę ingerencji w systemy eksploatowane w **Szkole Podstawowej nr 1 im. Stanisławy Łakomik w Czeladzi**, która wskazuje na niekontrolowane działanie osób trzecich oraz weryfikuje zgłoszenie i podejmuje stosowne działania, o których mowa w pkt. 6.

5. Na podstawie opublikowanego raportu CERT Polska z 2018 roku (https://www.cert.pl/news/single/zgloszenia-i-incydenty-w-2018-roku/), wykaz incydentów, w tym incydentów występujących najczęściej ze szczegółowym podziałem na poszczególne kategorie według klasyfikacji eCSIRT.net[1] przedstawia **tabela 1**.
6. Incydent w podmiocie publicznym – w **Szkole Podstawowej nr 1 im. Stanisławy Łakomik w Czeladzi**, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego **Pełnomocnik ds. bezpieczeństwa cyberprzestrzeni** zgłasza niezwłocznie:
   a) **Dyrektorowi Szkoły Podstawowej nr 1 im. Stanisławy Łakomik w Czeladzi**, w celu umożliwienia realizacji obowiązku wynikającego z art. 22 ust. 1 pkt 2 Ustawy o krajowym systemie cyberbezpieczeństwa tj. zgłoszenia incydentu niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia, do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV zawierającego informacje, o których mowa w **załączniku nr 2** do niniejszej Procedury.
   b) Inspektorowi ochrony danych (**IOD**) w **Szkole Podstawowej nr 1 im. Stanisławy Łakomik w Czeladzi**, na adres poczty elektronicznej: **iodo@marwikpoland.pl** oraz telefonicznie na numer kom: **694 167 023**.
7. **IOD** dokonuje ustalenia czy zidentyfikowany incydent nie stanowi jednocześnie naruszenia ochrony danych osobowych, a w konsekwencji czy nie wymaga podjęcia stosownych działań w tym zakresie tj. oceny wagi ryzyka naruszenia praw i wolności osób fizycznych, oceny zasadności odnotowania incydentu w rejestrze incydentów i naruszeń, zgłoszenia naruszenia do PUODO, i/lub zawiadomienia osób fizycznych których dane dotyczą.
8. W przypadku uzasadnionych podejrzeń, iż doszło do incydentu cyberbezpieczeństwa **Pełnomocnik ds. bezpieczeństwa cyberprzestrzeni** przygotowuje „Raport incydentu cyberbezpieczeństwa" stanowiący **załącznik nr 2** do niniejszej Procedury oraz odnotowuje zdarzenie w „Rejestrze incydentów cyberbezpieczeństwa" stanowiący **załącznik nr 3** do niniejszej Procedury.
9. Obowiązki podmiotów publicznych wynikające z Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa przedstawia **załącznik nr 4** do niniejszej Procedury.

[1] Projekt współpracy zespołów CSIRT

Tabela 1. Wykaz incydentów w podziale na kategorie wg klasyfikacji eCSIRT.net

Obraźliwe i nielegalne treści	**Spam**
	Dyskredytacja, obrażanie
	Pornografia dziecięca, przemoc
	Niesklasyfikowane
Złośliwe oprogramowanie	**Wirus**
	Robak sieciowy
	Koń trojański
	Oprogramowanie szpiegowskie
	Dialer
	Rootkit
	Niesklasyfikowane
Gromadzenie informacji	Skanowanie
	Podsłuch
	Inżynieria społeczna
	Niesklasyfikowane
Próby włamań	Wykorzystanie znanych luk systemowych
	Próby nieuprawnionego logowania
	Wykorzystanie nieznanych luk systemowych
	Niesklasyfikowane
Włamania	Włamanie na konto uprzywilejowane
	Włamanie na konto zwykłe
	Włamanie do aplikacji
	Bot
	Niesklasyfikowane
Dostępność zasobów	Atak blokujący serwis (DoS)
	Rozproszony atak blokujący serwis (DDoS)
	Sabotaż komputerowy
	Przerwa w działaniu usług (niezłośliwe)
	Niesklasyfikowane
Atak na bezpieczeństwo informacji	Nieuprawniony dostęp do informacji
	Nieuprawniona zmiana informacji
	Niesklasyfikowane
Oszustwa komputerowe	Nieuprawnione wykorzystanie zasobów
	Naruszenie praw autorskich
	Kradzież tożsamości, podszycie się
	Phishing
	Niesklasyfikowane
Podatne usługi	Otwarte serwisy podatne na nadużycia
	Niesklasyfikowane
inne	**…**

Załącznik nr 1

Zgłaszanie osób kontaktowych do CSIRT NASK

Obowiązkowi zgłoszenia osób kontaktowych właściwemu CSIRT podlegają wg ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560) **operatorzy usług kluczowych** (art 9 ust 1) oraz **podmioty publiczne** (art 22 ust 1 pkt 5).

Jeżeli chcą Państwo zgłosić incydent proszę użyć poniższego odnośnika:
Zgłaszanie incydentu do CSIRT NASK.

Aby zgłosić osoby kontaktowe do CSIRT NASK lub zaktualizować ich dane należy:

- wypełnić poniższy formularz,
- wygenerowane pismo opatrzyć podpisem, elektronicznym lub tradycyjnym kierownika instytucji,
- przesłać pismo na skrzynkę ePUAP (Naukowa i Akademicka Sieć Komputerowa PIB; adres skrzynki: /NASK-Instytut/SkrytkaESP, w tytule proszę wpisać "Zgłoszenie osoby kontaktowej do CSIRT NASK") lub na adres NASK-PIB wskazany w dokumencie (w przypadku operatora usługi kluczowej załączając skan decyzji administracyjnej uznającej podmiot za operatora usługi kluczowej).

Przed wypełnieniem poniższego formularza polecamy zapoznać się ze wspólnymi **rekomendacjami CSIRT NASK oraz CSIRT GOV** w zakresie wyznaczania osób kontaktowych.

Zgłoszenie osoby kontaktowej – Jaki podmiot Państwo reprezentują?

Prosimy o wypełnienie poniższego formularza

Dane podmiotu zgłaszającego

Pełna nazwa instytucji

Nazwa skrócona

☐ Czy reprezentowany przez Państwa podmiot publiczny jest jednocześnie operatorem usługi kluczowej?

NIP

Numer REGON

Numer KRS

Ogólny adres e-mail

Adres siedziby (ulica, numer budynku, numer lokalu)

Kod pocztowy siedziby

Miasto siedziby

Informacje o zakresie sieciowym

Adres e-mail, na który mają być wysyłane informacje o nowych zdarzeniach wykrytych w Państwa sieci

Numery systemu autonomicznego lub adresy sieci w notacji CIDR (po jednym w linii)

Nazwy domen należących do Państwa instytucji (po jednej w linii)

Osoby kontaktowe

Przynajmniej jedna osoba musi być uplasowana w wewnętrznych strukturach odpowiedzialnych za cyberbezpieczeństwo.

Umiejscowienie osoby kontaktowej

○ Wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo

○ Zewnętrzny podmiot świadczący usługi z zakresu cyberbezpieczeństwa

Imię i nazwisko

Stanowisko lub funkcja

Adres e-mail

Numer telefonu

Dostępność

8-16

8-22

24h

Jednostki organizacyjne

Zgodnie z art 21 pkt 3 ustawy o KSC, "jednostka samorządu terytorialnego może wyznaczyć jedną osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa w zakresie zadań publicznych zależnych od systemów informacyjnych, realizowanych przez jej jednostki organizacyjne".

Nazwa jednostki organizacyjnej

Pełny adres jednostki organizacyjnej

Informacje dodatkowe

Informacje dodatkowe

Załączniki i wysyłanie zgłoszenia

Dołączenie plików lub wysłanie formularza jest możliwe po kliknięciu "Nie jestem robotem" poniżej.

Załącznik nr 2

RAPORT INCYDENTU CYBERBEZPIECZEŃSTWA

I. WSTĘPNY OPIS INCYDENTU

1. Data ..... Godzina .....
2. Osoba powiadamiająca o incydencie oraz inne osoby zaangażowane lub odpytane w związku z incydentem (imię, nazwisko, stanowisko służbowe, dane kontaktowe):

….....

3. Lokalizacja zdarzenia *(nr. pokoju, nazwa pomieszczenia, określenie komputerowego stanowiska roboczego, nazwa programu lub aplikacji itp.):*

.....

II. WSTĘPNA ANALIZA INCYDENTU

4. Zadanie publiczne, którego dotyczy zgłoszenie:

…….…….

5. Liczba osób, na które incydent miał wpływ

.....

6. Moment wystąpienia i wykrycia incydentu oraz czas jego trwania

.....

7. Zasięg geograficzny obszaru, którego incydent dotyczy

….....

8. Przyczyna zaistnienia incydentu:

☐ Podejrzana wiadomość e-mail ☐ Podatności

☐ Próba oszustwa ☐ Złośliwe oprogramowanie

☐ Nielegalne treści ☐ Inny …….

9. Źródło incydentu

…….

10. Sposób jego przebiegu

……..

11. Skutki jego oddziaływania na systemy informacyjne podmiotu publicznego

……..

12. Informacja o podjętych działaniach zapobiegawczych

…….

13. Informacja o podjętych działaniach naprawczych - jeśli charakter incydentu pozwala podjąć je od razu.

14. Czy doszło do naruszenia danych osobowych

☐ TAK ☐ NIE

W przypadku naruszenia danych osobowych należy dodatkowo uruchomić procedurę zgłaszania naruszeń związanych z ochroną danych osobowych.

W przypadku naruszenia danych osobowych podać nr zgłoszenia z rejestru incydentów - ……

.....

(podpisy osób obsługujących incydent)

** Do Raportu należy dołączyć kopię zgłoszenia do CSIRT NASK.*

Załącznik nr 3

REJESTR INCYDENTÓW CYBERBEZPIECZEŃSTWA

w **Szkole Podstawowej nr 1 im. Stanisławy Łakomik w Czeladzi**

Lp.	Data zgłoszenia	Zadanie publiczne, którego dotyczy zgłoszenie	Opis zdarzenia	Kategoria incydentu	Podjęte działania zapobiegawcze	Podjęte działania naprawcze
1	2	3	4	5	6	7
1.						
2.						
3.						
4.						
5.						
6.						

Kategorie incydentu (kolumna nr 7):

A – Podejrzana wiadomość e-mail B – Próba oszustwa

C – Podatności

D – Złośliwe oprogramowanie E – Nielegalne treści

F - Inny incydent

Załącznik nr 4

Wyciąg z Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa

Rozdział 5

Obowiązki podmiotów publicznych

Art. 21.

1. Podmiot publiczny, o którym mowa w art. 4 pkt 7–15, realizujący zadanie publiczne zależne od systemu informacyjnego jest obowiązany do wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.

2. Organ administracji publicznej może wyznaczyć jedną osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa w zakresie zadań publicznych zależnych od systemów informacyjnych, realizowanych przez jednostki jemu podległe lub przez niego nadzorowane.

3. Jednostka samorządu terytorialnego może wyznaczyć jedną osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa w zakresie zadań publicznych zależnych od systemów informacyjnych, realizowanych przez jej jednostki organizacyjne.

Art. 22.

1. Podmiot publiczny, o którym mowa w art. 4 pkt 7–15, realizujący zadanie publiczne zależne od systemu informacyjnego:

1) zapewnia zarządzanie incydentem w podmiocie publicznym;

2) zgłasza incydent w podmiocie publicznym niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia, do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV;

3) zapewnia obsługę incydentu w podmiocie publicznym i incydentu krytycznego we współpracy z właściwym CSIRT MON, CSIRT NASK lub CSIRT GOV, przekazując niezbędne dane, w tym dane osobowe;

4) zapewnia osobom, na rzecz których zadanie publiczne jest realizowane, dostęp do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami, w szczególności przez publikowanie informacji w tym zakresie na swojej stronie internetowej;

5) przekazuje do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV dane osoby, o której mowa w art. 21, obejmujące imię i nazwisko, numer telefonu oraz adres poczty elektronicznej, w terminie 14 dni od dnia jej wyznaczenia, a także informacje o zmianie tych danych w terminie 14 dni od dnia ich zmiany.

2. Zgłoszenie, o którym mowa w ust. 1 pkt 2, przekazywane jest w postaci elektronicznej, a w przypadku braku możliwości przekazania go w postaci elektronicznej – przy użyciu innych dostępnych środków komunikacji.

Art. 23.

1. Zgłoszenie, o którym mowa w art. 22 ust. 1 pkt 2, zawiera:

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 podmiotu publicznego;

5) informacje o przyczynie i źródle incydentu;

6) informacje o podjętych działaniach zapobiegawczych;

7) informacje o podjętych działaniach naprawczych;

8) inne istotne informacje.

2. Podmiot publiczny, o którym mowa w art. 4 pkt 7–15, przekazuje informacje znane mu w chwili dokonywania zgłoszenia, które uzupełnia w trakcie obsługi incydentu w podmiocie publicznym.