

Zarządzenie nr 3/2026/2027
Dyrektora Szkoły Podstawowej nr 13
im. Huberta Wagnera w Będzinie
z dnia 11 września 2026 roku

w sprawie wprowadzenia
Procedury zarządzania incydentami bezpieczeństwa informacji i cyberbezpieczeństwa
w Szkole Podstawowej nr 13 im. Huberta Wagnera

W związku z realizacją wytycznych ustawy z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa

zarządza się, co następuje:

§ 1.

Z dniem 11 września 2026 r., wprowadza się w Szkole Podstawowej nr 13 im. Huberta Wagnera "Procedurę zarządzania incydentami bezpieczeństwa informacji i cyberbezpieczeństwa", stanowiącą załączniki do niniejszego zarządzenia.

§ 2.

Zobowiązuje się wszystkich pracowników Szkoły Podstawowej nr 13 im. Huberta Wagnera do stosowania i przestrzegania "Procedury zarządzania incydentami bezpieczeństwa informacji i cyberbezpieczeństwa", o której mowa w § 1.

§ 3.

Wyznacza się Pełnomocnika ds. bezpieczeństwa informacji i cyberbezpieczeństwa w Szkole Podstawowej nr 13 im. Huberta Wagnera w osobie dyrektora szkoły – Pauliny Piesiak do monitorowania przypadków mogących mieć negatywny wpływ na bezpieczeństwo informacji i cyberbezpieczeństwo.

§ 4.

Zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR SZKOŁY
Paulina Piesiak
mgr Paulina Piesiak
.....
podpis i pieczęć dyrektora

SZKOŁA PODSTAWOWA NR 13
im. Huberta Wagnera
42-500 Będzin, ul. Rewolucjonistów 18
REGON 271502680 NIP 625-21-97-672
tel./fax 32/267-50-35

PROCEDURA ZARZĄDZANIA INCYDENTAMI BEZPIECZEŃSTWA INFORMACJI I CYBERBEZPIECZEŃSTWA

W

Szkole Podstawowej nr 13 im. Huberta Wagnera

ul. Rewolucjonistów 18,

42-500 Będzin

Spis treści

<u>1. Cel, zakres i użytkownicy</u>	Błąd! Nie zdefiniowano zakładki.
<u>2. Kontrole bezpieczeństwa według normy PN-EN ISO/IEC 27001</u>	Błąd! Nie zdefiniowano zakładki.
<u>3. Zarządzanie incydentami</u>	Błąd! Nie zdefiniowano zakładki.
<u>4. Podstawa prawna</u>	Błąd! Nie zdefiniowano zakładki.
<u>5. Terminologia</u>	Błąd! Nie zdefiniowano zakładki.
<u>6. Osoby odpowiedzialne za cyberbezpieczeństwo</u>	Błąd! Nie zdefiniowano zakładki.
<u>7. Klasyfikacja incydentów</u>	Błąd! Nie zdefiniowano zakładki.
<u>8. Kategorie incydentów</u>	Błąd! Nie zdefiniowano zakładki.
<u>9. Zgłaszanie zdarzeń i obsługa incydentu cyberbezpieczeństwa</u> ...	Błąd! Nie zdefiniowano zakładki.
<u>10. Otwarta lista incydentów bezpieczeństwa informacji objętych obowiązkiem rejestracji</u> ...	Błąd! Nie zdefiniowano zakładki.
<u>11. Przeglądy procedury i obowiązki użytkowników</u>	Błąd! Nie zdefiniowano zakładki.
<u>Załącznik nr 1 - Zgłaszanie osób kontaktowych do CSIRT NASK</u>	Błąd! Nie zdefiniowano zakładki.
<u>Załącznik nr 2 - Rejestr incydentów bezpieczeństwa informacji i cyberbezpieczeństwa</u>	Błąd! Nie zdefiniowano zakładki.
<u>Załącznik nr 3 - Raport incydentu bezpieczeństwa informacji i cyberbezpieczeństwa</u>	Błąd! Nie zdefiniowano zakładki.
<u>Załącznik nr 4 - Wyciąg z Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa</u>	Błąd! Nie zdefiniowano zakładki.

1. Cel, zakres i użytkownicy

Celem tego dokumentu jest zapewnienie szybkiego wykrywania zagrożeń bezpieczeństwa, słabych punktów i zdarzeń oraz szybkiego reagowania na incydenty związane z bezpieczeństwem.

Niniejszy dokument ma zastosowanie do całego zakresu Systemu Zarządzania Bezpieczeństwem Informacji, tj. do wszystkich pracowników i innych zasobów wykorzystywanych w ramach zakresu SZBI, a także do dostawców i innych osób spoza Szkoły Podstawowej nr 13 im. Huberta Wagnera, które mają kontakt z systemami i informacjami.

Użytkownikami niniejszego dokumentu są wszyscy pracownicy Szkoły Podstawowej nr 13 im. Huberta Wagnera, a także wszystkie wyżej wymienione osoby.

2. Kontrole bezpieczeństwa według normy PN-EN ISO/IEC 27001

- Norma ISO/IEC 27001, punkt normy 7.4, Aneks A: A.5.7, A.5.24, A.5.25, A.5.26, A.5.27, A.5.28, A.6.4, A.6.8.

3. Zarządzanie incydentami

Incydent związany z bezpieczeństwem informacji to pojedyncze zdarzenie bądź seria niepożądanych lub nieoczekiwanych zdarzeń związanych z bezpieczeństwem informacji, które z dużym prawdopodobieństwem mogą zagrozić operacjom biznesowym i bezpieczeństwu informacji.

4. Podstawa prawna

- a) art. 22 ust.1 Ustawy o krajowym systemie cyberbezpieczeństwa z dnia 5 lipca 2018 r.
- b) §19 ust. 2 pkt. 13 Rozporządzenie 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.

5. Terminologia

- 1) **Incydent w podmiocie publicznym** - incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny.
- 2) **CSIRT NASK** – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego

działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy.

- 3) **CSIRT GOV** – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego.
- 4) **CSIRT MON** – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Ministra Obrony Narodowej.
- 5) **Cyberbezpieczeństwo** – odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.
- 6) **Incydent** – zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo.
- 7) **Incydent w podmiocie publicznym** - incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny.
- 8) **Incydent krytyczny** – incydent skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi, klasyfikowany przez właściwy CSIRT.
- 9) **Obsługa incydentu** – czynności umożliwiające wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację, podejmowanie działań naprawczych i ograniczenie skutków incydentu.
- 10) **Podatność** – właściwość systemu informacyjnego, która może być wykorzystana przez zagrożenie cyberbezpieczeństwa.
- 11) **System informacyjny** – system teleinformatyczny, o którym mowa w art. 3 pkt 3 Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, wraz z przetwarzanymi w nim danymi w postaci elektronicznej.
- 12) **Użytkownik** – osoba posiadająca dostęp do systemu informacyjnego Szkoły Podstawowej nr 13 im. Huberta Wagnera służącego do realizacji zadania publicznego.
- 13) **Ustawa** – Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.
- 14) **Zagrożenie cyberbezpieczeństwa** – potencjalna przyczyna wystąpienia incydentu.
- 15) **Zarządzanie incydentem** – obsługa incydentu, wyszukiwanie powiązań między incydentami, usuwanie przyczyn ich wystąpienia oraz opracowywanie wniosków wynikających z obsługi incydentu.

- 16) **Zarządzanie ryzykiem** – skoordynowane działania w zakresie zarządzania cyberbezpieczeństwem w odniesieniu do oszacowanego ryzyka.

6. Osoby odpowiedzialne za cyberbezpieczeństwo

- 1) Dyrektor Szkoły Podstawowej nr 13 im. Huberta Wagnera ponosi odpowiedzialność w szczególności za:
 - a) wyznaczenie osoby odpowiedzialnej za utrzymanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. - **Pełnomocnika ds. bezpieczeństwa informacji i cyberbezpieczeństwa**;
 - b) przekazanie do CSIRT NASK w terminie 14 dni od dnia wyznaczenia, danych **Pełnomocnika ds. bezpieczeństwa informacji i cyberbezpieczeństwa**, a także informacji o zmianie tych danych w terminie 14 dni od dnia ich zmiany. Przekazanie danych **Pełnomocnika ds. bezpieczeństwa informacji i cyberbezpieczeństwa** odbywa się w sposób następujący: Poprzez stronę internetową: **<https://incydent.cert.pl/osoba-kontaktowa#!/lang=pl,entityType=publicInstitution>** (załącznik nr 1 do niniejszej Procedury) lub w formie pisemnej pod adres do korespondencji CSIRT NASK: NASK -Państwowy Instytut Badawczy, ul. Kolska 12, 01-045 Warszawa.
- 2) **Pełnomocnik ds. bezpieczeństwa informacji i cyberbezpieczeństwa**, który realizuje następujące zadania:
 - a) przyjmuje od Użytkowników informacje o zdarzeniach mogących stanowić incydent cyberbezpieczeństwa lub podejrzenie ich wystąpienia w Szkole Podstawowej nr 13 im. Huberta Wagnera;
 - b) koordynuje obsługę zgłaszanych incydentów cyberbezpieczeństwa;
 - c) przygotowuje zgłoszenie incydentu w podmiocie publicznym do CSIRT NASK, zgodnie ze wzorem stanowiącym **załącznik nr 1** do niniejszej Procedury;
 - d) dokonuje zgłoszenia incydentu w podmiocie publicznym do CSIRT NASK.
 - e) Koordynuje wdrażanie działań naprawczych po wystąpieniu incydentu cyberbezpieczeństwa;
 - f) odpowiada za organizację szkoleń i podnoszenia świadomości pracowników Szkoły Podstawowej nr 13 im. Huberta Wagnera w zakresie incydentów cyberbezpieczeństwa, ich zgłaszania, przeciwdziałania i prewencyjnych sposobach zabezpieczenia przed ich występowaniem;
 - g) koordynuje prace związane z informowaniem osób, na rzecz których zadanie

publiczne jest realizowane w zakresie dostępu do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowania skutecznych sposobów zabezpieczania się przed tymi zagrożeniami;

- h) w przypadku wystąpienia incydentu cyberbezpieczeństwo ściśle współpracuje z Użytkownikami, pracownikami Szkoły Podstawowej nr 13 im. Huberta Wagnera, innymi osobami lub podmiotami świadczącymi Szkole Podstawowej nr 13 im. Huberta Wagnera usługi dotyczące obsługi informatycznej, w celu wdrożenia działań naprawczych;
- i) wraz z innymi osobami zaangażowanymi przy wystąpieniu zdarzenia, dokonuje oceny danego zdarzenia pod względem możliwości zakwalifikowania go jako incydentu w odniesieniu do przepisów Ustawy, w tym ewentualnej konieczności dokonania zgłoszenia wystąpienia incydentu w podmiocie publicznym do właściwego CSIRT;
- j) prowadzi rejestr incydentów cyberbezpieczeństwa.

3) Użytkownicy systemów informatycznych zobowiązani są do:

- a) zgłaszania incydentów cyberbezpieczeństwa do **Pełnomocnika ds. bezpieczeństwa informacji i cyberbezpieczeństwa**.
- b) przestrzegania polityk i procedur bezpieczeństwa informacyjnego.
- c) współpracy przy działaniach naprawczych po incydencie.
- d) dokumentowania działań związanych z obsługą incydentów.
- e) stosowania środków ochrony, takich jak oprogramowanie antywirusowe.
- f) unikania działań osłabiających zabezpieczenia systemu.

7. Klasyfikacja incydentów

- 1) Ze względu na wpływ incydentu na bezpieczeństwo informacji przyjęto poniższy podział incydentów:
 - a) **incydent krytyczny** - oznacza utratę poufności, integralności lub dostępności informacji interesariuszy lub własnej informacji chronionej, poważne naruszenie obowiązków pracowniczych, włamanie, napaść, kradzież, uszkodzenia infrastruktury SZBI wywołane sytuacjami wypadkowymi,
 - b) **incydent poważny** oznacza pojawienie się pojedynczych przypadków niewypełniania obowiązków, wymagań polityk i procedur bezpieczeństwa obowiązujących w Szkole Podstawowej nr 13 im. Huberta Wagnera lub zasad, które mogą w rezultacie doprowadzić do incydentu krytycznego;

- c) **incydent istotny** - oznacza pojawienie się przypadków mogących mieć wpływ na bezpieczeństwo informacji, co do których zgłaszający mają wątpliwość kwalifikacyjną, a nie znajdują się wśród incydentów o statusie „krytyczny” lub „poważny”.

2) Działania jakie należy podjąć w przypadku zaistnienia incydentu o określonym statusie:

- a) **incydent krytyczny** - w stosunku do osób, co do których stwierdzono sprawstwo umyślne lub zaniechanie obowiązków, bezpośredni przełożony lub przełożony wyższego rzędu winien:
- wyciągnąć adekwatne konsekwencje służbowe i/lub
 - wyciągnąć adekwatne konsekwencje prawne i/lub,
 - przeprowadzić postępowanie dyscyplinarne,
- b) **incydent poważny** - **Pełnomocnik ds. bezpieczeństwa informacji i cyberbezpieczeństwa** w stosunku do osób odpowiedzialnych dokonuje pouczenia lub organizuje spotkanie w celu wyjaśnienia zajścia incydentu, a w razie ponownego wystąpienia incydentu zaleca przełożonym osoby odpowiedzialnej adekwatne działania dyscyplinarne,
- c) **incydent istotny** - **Pełnomocnik ds. bezpieczeństwa informacji i cyberbezpieczeństwa** w stosunku do osób odpowiedzialnych dokonuje pouczenia lub organizuje spotkanie w celu wyjaśnienia zajścia incydentu.

8. Kategorie incydentów

- 1) Incydent bezpieczeństwa informacji oraz cyberbezpieczeństwa 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 podmiot publiczny. Jego przyczyną 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, awarie 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.
- 2) Incydentami bezpieczeństwa informacji w szczególności są:

- a) naruszenie poufności, to jest ujawnienie informacji niepowołanym osobom;
 - b) naruszenie integralności, to jest zniszczenie, uszkodzenie lub przekłamanie informacji;
 - c) naruszenie dostępności, to jest braku dostępu do danych przez uprawnionych użytkowników.
- 3) Przyczyny incydentów bezpieczeństwa informacji oraz cyberbezpieczeństwa mogą dotyczyć:
- a) niewłaściwego wykorzystywania zasobów informatycznych lub niewłaściwe postępowanie z dokumentacją 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) zniszczenia lub kradzieży nośników danych;
 - g) próby wyłudzeń informacji;
 - h) ataków socjotechnicznych, ataków z wykorzystaniem technik zagrażających poufności, integralności lub dostępności informacji;
 - i) nieprawidłowości w zakresie zabezpieczenia przechowywania danych, w tym danych osobowych;
 - j) naruszenia zasad obowiązujących w Szkole Podstawowej nr 13 im. Huberta Wagnera dotyczących bezpieczeństwa informacji, w tym danych osobowych.

9. Zgłaszanie zdarzeń i obsługa incydentu cyberbezpieczeństwa

1) Wyznaczenie odpowiedzialności za monitorowanie zagrożeń

- a) Do monitorowania przypadków mogących mieć negatywny wpływ na cyberbezpieczeństwo, wyznacza się w Szkole Podstawowej nr 13 im. Huberta Wagnera **Pełnomocnika ds. bezpieczeństwa informacji i cyberbezpieczeństwa**, przy czym każdy pracownik Szkoły Podstawowej nr 13 im. Huberta Wagnera, który zauważy zdarzenia mogące wskazywać na ingerencję w system osób trzecich, zobowiązany jest niezwłocznie zawiadomić Dyrektora Szkoły Podstawowej nr 13 im. Huberta Wagnera oraz **Pełnomocnika ds. bezpieczeństwa informacji i cyberbezpieczeństwa**.

2) Zgłaszanie incydentów przez pracowników

- a) Każdy pracownik Szkoły Podstawowej nr 13 im. Huberta Wagnera oraz osoby zewnętrzne (np. dostawcy), które mają kontakt z systemami informacyjnymi lub danymi objętymi systemem zarządzania bezpieczeństwem informacji (SZBI), zobowiązani są do zgłaszania incydentów. Zgłoszenia należy dokonać do **Pełnomocnika ds. bezpieczeństwa informacji i cyberbezpieczeństwa** jak najszybciej, jednak nie później niż w ciągu 2 godzin od zaistnienia incydentu lub podejrzenia jego wystąpienia.
- b) Zgłoszenia można dokonać osobiście, mailowo, telefonicznie lub przez bezpośredniego przełożonego.

3) Weryfikacja i ocena incydentu

- a) **Pełnomocnik ds. bezpieczeństwa informacji i cyberbezpieczeństwa**, w porozumieniu z IOD weryfikuje zgłoszone informacje i ustala, czy incydent wymaga zgłoszenia do CSIRT NASK. Oceniane są następujące czynniki:
 - wpływ incydentu na działanie systemów informacyjnych,
 - wpływ incydentu na ciągłość realizacji zadań publicznych,
 - dostępność, integralność, poufność oraz autentyczność danych.

4) Gromadzenie materiału dowodowego

- a) Zgłaszający incydent powinien w miarę możliwości zabezpieczyć dowody, takie jak zrzuty ekranu lub zdjęcia materiałów zawierających dane osobowe. **Pełnomocnik ds. bezpieczeństwa informacji i cyberbezpieczeństwa** gromadzi informacje o incydencie, takie jak:
 - wpływ incydentu na zadania publiczne,
 - liczba osób, na które incydent miał wpływ,
 - przyczyny i przebieg incydentu oraz jego skutki.
- b) Weryfikacja zgłoszenia obejmuje zabezpieczenie materiału dowodowego w formie papierowej i elektronicznej oraz zapisanie wszystkich działań związanych z incydentem.

5) Dokumentowanie incydentów i raportowanie

- a) Każdy zgłoszony incydent dotyczący bezpieczeństwa informacji i cyberbezpieczeństwa musi zostać wpisany do „Rejestru incydentów bezpieczeństwa informacji i cyberbezpieczeństwa”, stanowiący **załącznik nr 2** do niniejszej procedury.
- b) **Pełnomocnik ds. bezpieczeństwa informacji i cyberbezpieczeństwa** sporządza „Raport incydentu bezpieczeństwa informacji i cyberbezpieczeństwa”, który

stanowi **załącznik nr 3** do niniejszej procedury. Raport zawiera m.in. informacje o wpływie incydentu na realizowane zadania publiczne, czasie jego trwania oraz podjętych działaniach.

6) Zgłaszanie incydentu do CSIRT NASK

- a) W przypadku incydentu, który powoduje lub może spowodować przerwanie realizacji zadania publicznego, **Pełnomocnik ds. bezpieczeństwa informacji i cyberbezpieczeństwa** zgłasza incydent do CSIRT NASK, nie później niż w ciągu 24 godzin od momentu wykrycia zdarzenia. Incydent zgłasza się drogą elektroniczną zgodnie z procedurami CSIRT.
- b) Informacje przekazywane do CSIRT obejmują:
 - przyczyny incydentu,
 - skutki incydentu,
 - czas trwania i zasięg incydentu.

7) Ocena i wdrożenie działań naprawczych

- a) **Pełnomocnik ds. bezpieczeństwa informacji i cyberbezpieczeństwa** ocenia incydent we współpracy z IOD, aby ustalić, czy incydent stanowi naruszenie ochrony danych osobowych.
- b) **Pełnomocnik ds. bezpieczeństwa informacji i cyberbezpieczeństwa** wdraża działania naprawcze, takie jak:
 - przywrócenie pełnej funkcjonalności systemów,
 - zmiana haseł i wprowadzenie dodatkowych zabezpieczeń,
 - usunięcie szkodliwego oprogramowania,
 - aktualizacja planów ciągłości działania.

8) Dodatkowe szkolenia i prewencja

- a) Po zakończeniu incydentu **Pełnomocnik ds. bezpieczeństwa informacji i cyberbezpieczeństwa** organizuje szkolenia dla pracowników, aby zapobiec podobnym incydom w przyszłości. Pracownicy, którzy dopuścili się umyślnego naruszenia, zostają objęci indywidualnym szkoleniem zakończonym testem wiedzy.

9) Zakończenie obsługi incydentu

- a) Po zakończeniu obsługi incydentu **Pełnomocnik ds. bezpieczeństwa informacji i cyberbezpieczeństwa** przygotowuje ostateczny raport oraz wprowadza zmiany w procedurach, jeśli to konieczne. Zespół dokumentuje wszystkie działania na każdym etapie obsługi incydentu.

10) Obowiązki wynikające z Ustawy o krajowym systemie cyberbezpieczeństwa

- a) Obowiązki podmiotów publicznych wynikające z Ustawy o krajowym systemie cyberbezpieczeństwa są szczegółowo opisane w załączniku nr 4 do niniejszej procedury.

10. Otwarta lista incydentów bezpieczeństwa informacji objętych obowiązkiem rejestracji

- 1) Identyfikacja złośliwego oprogramowania.
- 2) Niezgoda ze specyfikacją praca systemu informatycznego, wpływająca na procesy pracy.
- 3) Niedostępność systemu informatycznego.
- 4) Niedostępność danych.
- 5) Utrata danych (zniszczenie).
- 6) Utrata kontroli nad danymi (naruszenie poufności bądź integralności).
- 7) Utrata sprzętu przetwarzającego informacje bądź jej nośnika.
- 8) Uszkodzenie sprzętu przetwarzającego informacje bądź jej nośnika.
- 9) Awaria sprzętu bądź oprogramowania przetwarzającego informacje, uniemożliwiająca pracę bądź prowadząca do niewłaściwych wyników.
- 10) Przebywanie osób nieuprawnionych w obszarze wyłączonym z dostępu z przyczyn bezpieczeństwa.
- 11) Penetracja sieci LAN.
- 12) Brak kopii bezpieczeństwa bądź jej nieskuteczne odtworzenie.
- 13) Upublicznienie danych chronionych przez Szkołę Podstawową nr 13 im. Huberta Wagnera.
- 14) Brak stosownych zabezpieczeń w umowach ze stronami trzecimi (klauzula poufności).
- 15) Pozostawienie strony trzeciej bez nadzoru w obszarze wyłączonym z dostępu z przyczyn bezpieczeństwa.
- 16) Brak oświadczenia o poufności i upoważnienia do przetwarzania danych przez pracownika do takiej pracy dopuszczonego.
- 17) Niewłaściwe fizyczne zabezpieczenie danych na stanowisku pracy.
- 18) Naruszenie polityki haseł.
- 19) Naruszenie zasad postępowania z kluczami do pomieszczeń.
- 20) Skierowanie wydruku do drukarki innej niż bezpośrednio nadzorowana przez drukującego lub osoby z nim współpracujące.

- 21) Zalanie, pożar bądź inna awaria o charakterze destrukcyjnym pomieszczenia, w którym znajdują się dane lub środki przetwarzania danych.
- 22) Nieautoryzowane wykonanie lub udostępnienie klucza do pomieszczenia biurowego lub innego, związanego z przetwarzaniem danych.
- 23) Użycie niezinventaryzowanego bądź niedopuszczonego do użytkowania nośnika danych.
- 24) Użycie niezinventaryzowanego bądź niedopuszczonego do użytkowania oprogramowania.
- 25) Instalacja niedopuszczonego do użycia oprogramowania.
- 26) Fizyczne bądź logiczne obejście / złamanie zabezpieczeń teleinformatycznych (także uzyskanie dostępu do zawartości sieci www objętej blokadą).
- 27) Wykorzystanie publicznych serwisów pocztowych w celach służbowych.
- 28) Wykorzystanie poczty służbowej do celów nie związanych z powierzonymi obowiązkami.
- 29) Przesłanie danych do niewłaściwego odbiorcy.

11. Przeglądy procedury i obowiązki użytkowników

- 1) Niniejsza Procedura podlega regularnym (nie rzadziej niż raz na rok) przeglądom dokonywanym przez **Pełnomocnika ds. bezpieczeństwa informacji i cyberbezpieczeństwa**.
- 2) W zależności od potrzeb mogą zostać przeprowadzone także dodatkowe przeglądy po stwierdzeniu istotnego naruszenia bezpieczeństwa, pojawieniu się zasadniczych zmian w Szkole Podstawowej nr 13 im. Huberta Wagnera, jego strukturze lub jego otoczeniu (nowe zagrożenia, technologie).
- 3) Każdy Użytkownik, który wykorzystuje system informacyjny do realizacji zadań publicznych pozostających w jego zakresie obowiązków, jest zobowiązany do zapoznania się z obowiązkami związanymi z przepisami wynikającymi z Ustawy.

DYREKTOR SZKOŁY
Paulina Piesiak
mgr Paulina Piesiak

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

Obrażliwe 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
	Podsluch
	Inżynieria społeczna
	Niesklasyfikowane
Próby włamań	Wykorzystanie znanych luk systemowych
	Próby nieuprawnionego logowania
	Wykorzystanie nieznanых 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-Institut/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?

 Operator usługi kluczowej Wypełnienie obowiązku wynikającego z art 9 ust 1 ustawy o KSC	 Podmiot publiczny Wypełnienie obowiązku wynikającego z art 22 ust 1 pkt 5 ustawy o KSC	 Inny podmiot Dobrowolne zgłoszenie niezobowiązanego podmiotu
---	--	--

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

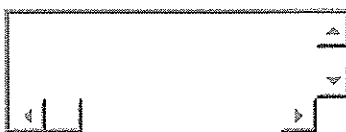
Jednostki organizacyjne

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".

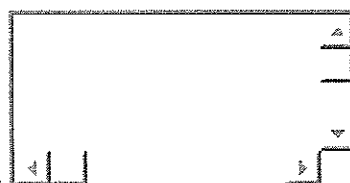
Nazwa jednostki organizacyjnej

A rectangular text input field with a small downward arrow icon on the right side.

Pełny adres jednostki organizacyjnej

A rectangular text input field with a small downward arrow icon on the right side.

Informacje dodatkowe

A rectangular text input field with a small downward arrow icon on the right side.

Informacje dodatkowe

Załączniki i wysyłanie zgłoszenia

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

REJESTR INCYDENTÓW BEZPIECZEŃSTWA INFORMACJI I CYBERBEZPIECZEŃSTWA

w Szkole Podstawowej nr 13 im. Huberta Wagnera

Lp.	Data zgłoszenia	Osoba zgłaszająca data i godzina	Zadanie publiczne, którego dotyczy zgłoszenie	Opis zdarzenia	Kategoria incydentu	Podjęte działania zapobiegawcze	Podjęte działania naprawcze
1	2	3	4	5	6	7	8
1.							
2.							
3.							
4.							

Kategorie incydentu (kolumna nr 8):

A – Podejrzana wiadomość e-mail B – Próba oszustwa

C – Podatności

D – Złośliwe oprogramowanie E – Nielegalne treści

F - Inny incydent

RAPORT INCYDENTU BEZPIECZEŃSTWA INFORMACJI I CYBERBEZPIECZEŃSTWA

I. WSTĘPNY OPIS INCYDENTU

1. Data Godzina
2. Osoba powiadamiająca o incydencie oraz inne osoby zaangażowane w związku z incydem (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.*

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 incydem 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 incydem w podmiocie publicznym i incydem 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 incydem 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 incydem oraz czas jego trwania,
 - d) zasięg geograficzny obszaru, którego dotyczy incydent,
 - e) przyczynę zaistnienia incydem i sposób jego przebiegu oraz skutki jego oddziaływania na systemy informacyjne podmiotu publicznego;
- 5) informacje o przyczynie i źródle incydem;
- 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 incydem w podmiocie publicznym.