**ZARZĄDZENIE Nr 3/2023**
**Dyrektora Ośrodka Pomocy Społecznej w Pyrzycach**
**z dnia 01 czerwca 2023 r.**

**w sprawie wprowadzenia procedury zarządzania incydentami związanymi z bezpieczeństwem informacji i cyberbezpieczeństwem oraz wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa**

Na podstawie art. 21 ust. 1 i art. 22 oraz art. 23 ustawy z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa (t. j. Dz. U. z 2023 r. poz. 913), a także § 20 ust. 2 pkt. 13 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych. **zarządza się, co następuje**:

**§ 1**

Wprowadza się do użytku służbowego: „Procedurę zarządzania incydentami związanymi z bezpieczeństwem informacji i cyberbezpieczeństwem", stanowiącą **Załącznik Nr 1** do niniejszego Zarządzenia.

**§ 2**

1. Zobowiązuje się wszystkich pracowników do zapoznania się z Procedurą, o której mowa w § 1.
2. Pisemne oświadczenie o zapoznaniu się i przestrzeganiu postanowień Procedury, stanowiące **Załącznik Nr 2** do niniejszego zarządzenia, należy złożyć na stanowisku ds. kadr.

**§ 3**

1. Wyznacza się Pana Bartosza Biegusa – Inspektora Ochrony Danych jako osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.
2. Zakres zadań osoby, o której mowa w ust. 1 określają przepisy ustawy o krajowym systemie cyberbezpieczeństwa.
3. Zobowiązuję osobę, o której mowa w ust. 1 do przekazania niezbędnych danych osoby kontaktowej do CSIRT NASK w ciągu 14 dni od wejścia w życie niniejszego zarządzenia.

**§ 4**

Zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR
Ośrodka Pomocy Społecznej
w Pyrzycach
mgr Aneta Wojcieszek

**Załącznik Nr 1**
do Zarządzenia Nr 3/2023
Dyrektora Ośrodka Pomocy
Społecznej w Pyrzycach
z dnia 01 czerwca 2023 r.

# PROCEDURA ZARZĄDZANIA INCYDENTAMI ZWIĄZANYMI Z BEZPIECZEŃSTWEM INFORMACJI I CYBERBEZPIECZEŃSTWEM

## Rozdział I
## POSTANOWINIA OGÓLNE I DEFINICJE
## § 1

1. Niniejsza procedura ma na celu zapewnienie ciągłości operacyjnej oraz ograniczenie wpływu przypadków naruszeń bezpieczeństwa zasobów informacyjnych na działalność instytucji.
2. Podstawą prawną do opracowania i wdrożenia dokumentu jest:
   1) art. 22 ust.1 pkt 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa,
   2) § 20 ust. 2 pkt.13 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.
3. Definicje pojęć użyte w treści niniejszej Procedury:
   1) Incydent w podmiocie publicznym - incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny.
   2) 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.
   3) Inspektor Ochrony Danych - osoba wyznaczona przez Administratora Danych Osobowych, zwany dalej „IOD".
   4) Administrator Systemów Informatycznych – osoba wyznaczona przez Administratora Danych Osobowych, odpowiedzialna za sprawność i konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych, zwany dalej „ASI"
   5) Administrator Danych Osobowych – Ośrodek Pomocy Społecznej w Pyrzycach, plac Ratuszowy 1, 74-200 Pyrzyce, reprezentowany przez Dyrektora, zwany dalej „ADO".
   6) Urząd – Ośrodek Pomocy Społecznej w Pyrzycach, plac Ratuszowy 1, 74-200 Pyrzyce.
   7) CSIRT NASK – podmiot o nazwie: Naukowa i Akademicka Sieć Komputerowa - Państwowy Instytut Badawczy, ul. Kolska 12, 01-045 Warszawa, wchodzący w skład krajowego systemu cyberbezpieczeństwa.

## Rozdział II
## KATEGORIE INCYDENTÓW
### § 2

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:
   1) 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;
   2) 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;
   3) świadome i celowe działania mające na celu naruszenie poufności zasobów informacyjnych, w tym poufności danych.
2. Incydentami bezpieczeństwa informacji w szczególności są:
   1) naruszenie poufności, to jest ujawnienie informacji niepowołanym osobom;
   2) naruszenie integralności, to jest zniszczenie, uszkodzenie lub przekłamanie informacji;
   3) naruszenie dostępności, to jest braku dostępu do danych przez uprawnionych użytkowników.
3. Przyczyny incydentów bezpieczeństwa informacji oraz cyberbezpieczeństwa mogą dotyczyć:
   1) niewłaściwego wykorzystywania zasobów informatycznych lub niewłaściwego postępowania z dokumentacją papierową;
   2) działania szkodliwego oprogramowania;
   3) próby omijania systemów zabezpieczeń;
   4) nieautoryzowanego dostępu do systemów, aplikacji i dokumentów;
   5) zniszczenia lub kradzieży urządzeń wykorzystywanych do przetwarzania i przechowywania informacji;
   6) zniszczenia lub kradzieży nośników danych;
   7) próby wyłudzeń informacji;
   8) ataków socjotechnicznych, ataków z wykorzystaniem technik zagrażających poufności, integralności lub dostępności informacji;
   9) nieprawidłowości w zakresie zabezpieczenia przechowywania danych, w tym danych osobowych;
   10) naruszenia zasad obowiązujących w Urzędzie dotyczących bezpieczeństwa informacji, w tym danych osobowych.

## Rozdział III
## ZAKRES OBOWIĄZYWANIA PROCEDURY
### § 3

1. Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji oraz cyberbezpieczeństwem obowiązuje w Urzędzie.

## Rozdział IV
## ZGŁASZANIE INCYDENTÓW ZWIĄZANYCH Z BEZPIECZEŃSTWEM INFORMACJI ORAZ CYBERBEZPIECZEŃSTWEM
### § 4

1. W przypadku ujawnienia incydentu pracownik Urzędu niezwłocznie powiadamia o tym fakcie ADO i ASI oraz IOD - jeżeli incydent może dotyczyć danych osobowych. Zgłoszenia dokonuje się telefonicznie lub osobiście. Zgłoszenie należy następnie potwierdzić szczegółową notatką służbową, którą przekazuje się do ASI.
2. Notatka służbowa, o której mowa w ust. 1, zawiera następujące informacje:
   1) imię i nazwisko osoby zgłaszającej;
   2) określenie stanowisko oraz komórki organizacyjnej;
   3) dokładne miejsce oraz datę wystąpienia incydentu;
   4) opis incydentu w sposób adekwatny do posiadanej wiedzy i umiejętności zgłaszającego.
3. Wzór notatki służbowej określono w Załączniku do niniejszej Procedury.
4. Brak umiejętności poprawnego rozpoznania incydentu przez osobę zgłaszającą nie może być przyczyną zaniechania zgłoszenia.
5. W przypadku nieobecności ASI incydent należy zgłosić do ADO, w sposób wskazany w pkt.1.

## Rozdział V
## PODEJMOWANIE DZIAŁAŃ W ZWIĄZKU ZE ZGŁASZANYMI INCYDENTAMI ZWIĄZANYMI Z BEZPIECZEŃSTWEM INFORMACJI ORAZ CYBERBEZPIECZEŃSTWEM
### § 5

1. Zgłoszenie incydentu rejestrowane jest przez ASI i przechowywane w osobnej teczce, zgodnie z zasadami określonymi w instrukcji kancelaryjnej.
2. Osoba zgłaszająca incydent powinna w miarę możliwości zabezpieczyć materiał dowodowy (np. zrzut ekranu monitora, zdjęcie niezabezpieczonych materiałów zawierających dane osobowe itp.).
3. Działania związane z obsługą zdarzenia w pierwszej kolejności dotyczą rozpoznania i kwalifikacji zgłoszenia.
4. W przypadku, kiedy zgłoszenie zakwalifikowane zostało jako incydent bezpieczeństwa informacji lub cyberbezpieczeństwa, dokonywana jest ocena istotności tego incydentu. Powyższe działania wykonuje ASI w porozumieniu z ADO i IOD.
5. Przy ocenie istotności incydentu pod uwagę brane są następujące czynniki:
   1) powstałe szkody będące wynikiem incydentu;
   2) wpływ incydentu na działanie systemów;
   3) wpływ incydentu na ciągłość działania Urzędu;
   4) koszty usunięcia skutków incydentu;
   5) szacowany czas naprawy skutków wywołanych incydentem;
   6) oszacowanie zasobów koniecznych do przywrócenia ciągłości działania systemów.
6. Zakwalifikowanie zgłoszenia incydentu jako „fałszywy alarm" kończy postępowanie, o czym ASI informuje zgłaszającego.

7. W przypadku zakwalifikowania zdarzenia jako incydentu związanego z bezpieczeństwem informacji lub cyberbezpieczeństwem, ASI podejmuje działania zabezpieczające i naprawcze zmierzające do zniwelowania szkód powstałych w wyniku incydentu.
8. W przypadku stwierdzenia incydentu w podmiocie publicznym lub incydentu krytycznego ASI lub ADO (w porozumieniu z IOD) nie później niż w ciągu 24 godzin od momentu wykrycia zgłasza incydent do właściwego CSIRT NASK (Naukowa i Akademicka Sieć Komputerowa - Państwowego Instytutu Badawczego ul. Kolska 12, 01-045 Warszawa).
9. Zgłoszenia do CSIRT NASK przekazywane są w sposób elektroniczny. Procedura zgłoszeń opisana jest pod adresem internetowym https://incydent.cert.pl. W przypadku braku możliwości przekazania zgłoszenia w sposób elektroniczny, incydent można zgłaszać przy użyciu innych dostępnych środków komunikacji (np. telefonicznie na numer telefonu +48223808274, za pomocą poczty elektronicznej cert@cert.pl).
10. W zgłoszeniu przekazuje się informacje zgodnie z formularzem oraz zgodnie z treścią art. 23 ust. 1 ustawy o krajowym systemie cyberbezpieczeństwa z dnia 5 lipca 2018 r.
11. W przypadku stwierdzenia działań zamierzonych, przy jednoczesnym zidentyfikowaniu sprawcy incydentu dotyczącego naruszenia bezpieczeństwa informacji oraz cyberbezpieczeństwa, ADO podejmuje decyzję dotyczącą wyciągnięcia ewentualnych konsekwencji dyscyplinarnych wobec sprawcy incydentu. Jednocześnie, w zależności od wagi incydentu mogą być powiadomione organy ścigania.

## Rozdział VI
## REAGOWANIE NA AWARIĘ
## § 6

1. Jeśli awaria dotyczy systemu krytycznego i może mieć wpływ na wydajność systemów teleinformatycznych, ASI informuje ADO.
2. W przypadku, gdy awarię można usunąć samodzielnie, to ASI dokonuje naprawy. Do podstawowych działań w takim wypadku zaliczyć możemy:
    1) wymianę stacji roboczej,
    2) wymianę podzespołów w stacji roboczej,
    3) wymianę urządzenia sieciowego,
    4) odtworzenie danych z kopii zapasowej.
3. Jeżeli ASI podejmie decyzję o niemożności samodzielnego usunięcia awarii, decyzję tę oraz wszelkie dodatkowe informacje dotyczące awarii, przekazuje do producenta sprzętu lub oprogramowania. Jeżeli naprawa dotyczy sprzętu, producent dokonuje naprawy w obecności ASI. Jeżeli naprawa dotyczy oprogramowania (np. wersji BIOS), wgrywana poprawka powinna zostać pozytywnie zweryfikowana w środowisku testowym.

## Rozdział VII
## REAGOWANIE NA BŁĘDY W OPROGRAMOWANIU
### § 7

1. Po otrzymaniu zgłoszenia dotyczącego wystąpienia błędu systemowego lub aplikacyjnego w oprogramowaniu, ASI diagnozuje przyczyny błędu oraz podejmuje działania zmierzające do rozwiązania problemu. Do podstawowych działań w tym zakresie możemy zaliczyć:
   1) wykorzystanie bazy wiedzy o błędach w oprogramowaniu,
   2) zmianę konfiguracji oprogramowania,
   3) ponowną instalację,
   4) instalację nowej wersji oprogramowania.
2. Jeżeli ASI nie może sam naprawić błędu w oprogramowaniu, przekazuje zlecenie naprawy do producenta oprogramowania (ASI postępuje w tym przypadku zgodnie z umowami serwisowymi lub licencjami).
3. Jeśli istnieje powód wskazujący na to, że przyczyną błędu w oprogramowaniu było naruszenie bezpieczeństwa, wówczas ASI informuje ADO.

## Rozdział VIII
## REAGOWANIE NA WYKRYCIE ZŁOŚLIWEGO KODU MOBILNEGO
### § 8

1. Po otrzymaniu zgłoszenia dotyczącego pojawienia się złośliwego kodu mobilnego na stacji roboczej, serwerze lub samodzielnemu wejściu w posiadanie wiedzy o takim zdarzeniu, ASI w pierwszej kolejności powinien:
   1) odłączyć komputer od sieci komputerowej,
   2) sprawdzić aktualność baz danych wirusów (jeśli są nieaktualne należy dokonać aktualizacji),
   3) sprawdzić poprawność działania oprogramowania antywirusowego (jeśli oprogramowanie nie działa poprawnie należy je odinstalować i zainstalować ponownie),
   4) uruchomić pełne skanowanie komputera i nośników informacji, z jakimi mógł mieć styczność,
2. Jeśli atak złośliwego kodu mobilnego nie został zneutralizowany przez oprogramowanie antywirusowe to ASI nakazuje użytkownikowi przerwanie pracy. Następnie dokonuje ponownej instalacji systemu operacyjnego i oprogramowania oraz odzyskania danych z kopii zapasowych. Kopie zapasowe należy sprawdzić programem antywirusowym przed wgraniem do komputera.
3. Jeśli istnieje powód wskazujący na to, że przyczyną ataku złośliwego kodu mobilnego było naruszenie bezpieczeństwa, to ASI informuje ADO.

## Rozdział IX
## POSTANOWIENIA KOŃCOWE
### § 9

1. W przypadkach incydentów nieprzewidzianych w niniejszej Procedurze – decyzje podejmuje ADO w porozumieniu z IOD.

DYREKTOR
Ośrodka Pomocy Społecznej
w Pyrzycach
mgr Aneta Wojcieszek

**Załącznik Nr 1**
do Procedury zarządzania incydentami związanymi z bezpieczeństwem informacji i cyberbezpieczeństwem.

**Zgłoszenie incydentu związanego z bezpieczeństwem informacji lub cyberbezpieczeństwem**

**NOTATKA SŁUŻBOWA**

Imię i nazwisko osoby zgłaszającej

.....

Stanowisko oraz komórka organizacyjna

.....

Dokładne miejsce oraz data wystąpienia incydentu

.....

.....

Opis incydentu (w sposób adekwatny do posiadanej wiedzy i umiejętności zgłaszającego)

.....

.....

.....

.....

.....
Podpis osoby sporządzającej notatkę