**Zarządzenie Nr. 0050.49.2023**
**Wójta Gminy Święciechowa**
**z dnia 13 marca 2023 roku**

**w sprawie wprowadzenia procedury zarządzania incydentami związanymi z bezpieczeństwem informacji i cyberbezpieczeństwem w Urzędzie Gminny w Święciechowie.**

Na podstawie art. 22 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa ( Dz. U. z 2022 roku poz. 1863 – ze zmianami ) oraz art. 30 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym ( Dz. U. z 2023 r. poz. 40), zarządzam co następuje:

**§ 1.**

Wprowadza się w Urzędzie Gminy w Święciechowie Procedurę zarządzania incydentami cyberbezpieczeństwa, stanowiącą załącznik do niniejszego zarządzenia.

**§ 2.**

Zobowiązuje wszystkich pracowników Urzędu Gminy w Święciechowie do zapoznania się z niniejszą Procedurą.

**§ 3.**

Zarządzenie wchodzi z dniem podpisania.

Załącznik do Zarządzenia Nr 0050.49.2023
Wójta Gminy Święciechowa
z dnia 13 marca 2023 roku.

# PROCEDURA ZARZĄDZANIA INCYDENTAMI CYBERBEZPIECZEŃSTWA W URZĘDZIE GMINY W ŚWIĘCIECHOWIE

## ROZDZIAŁ I
## WSTĘP

1. Procedura zarządzania incydentami cyberbezpieczeństwa, zwana dalej ,, Procedurą'' jest dokumentem wewnętrznym Urzędu Gminy w Święciechowie opisującym zasady zarządzania incydentami cyberbezpieczeństwa stosowane przez Jednostkę w celu spełnienia wymagań wynikających w szczególności z:

1) dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.U.UE.L.2016.194.1),

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) ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa ( Dz. U. z 2022 roku poz. 1863 – ze zmianami ),

4) przepisów szczególnych, regulujących funkcjonowanie Jednostki,

5) dobrych praktyk z zakresu bezpieczeństwa informacji, ochrony danych osobowych oraz cyberbezpieczeństwa.

2. Podstawą prawną do opracowania i wdrożenia niniejszej Procedury jest art. 22 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa ( Dz. U. z 2022 roku poz. 1863 – ze zmianami ).

## ROZDZIAŁ II
## DEFINICJE

1) **CSIRT NASK** – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy,

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

3) **incydent** – zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo,

4) **incydent cyberbezpieczeństwa** – zbiorcza nazwa obejmująca terminy incydent, incydent w podmiocie publicznym, incydent krytyczny,

5) **incydent w podmiocie publicznym** – incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny, o którym mowa w art. 4 pkt 7–15 Ustawy,

6) **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,

7) **Jednostka** – Urząd Gminy w Święciechowie,

8) **Kierownik Jednostki** – osoba reprezentująca i zarządzająca Jednostką,

9)**Administrator Danych Osobowych „ADO”** – Wójta Gminy Święciechowa

11) **Inspektor Ochrony Danych** – osoba wyznaczona przez Administratora Danych Osobowych zwana dalej ,, IOD’’

12) **Osoba pełniąca funkcję odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa** – osoba wyznaczona przez Administratora Danych Osobowych.

13) **podatność** – właściwość systemu informacyjnego, która może być wykorzystana przez zagrożenie cyberbezpieczeństwa,

14) **Użytkownik** – osoba posiadająca dostęp do systemu informacyjnego Jednostki służącego do realizacji zadania publicznego,

15) **obsługa incydentu** – czynności umożliwiające wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację, podejmowanie działań naprawczych i ograniczenie skutków incydentu,

16) **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 (Dz. U. z 2023 r. poz. 57), wraz z przetwarzanymi w nim danymi w postaci elektronicznej,

17) **zarządzanie incydentem** – obsługę incydentu, wyszukiwanie powiązań między incydentami, usuwanie przyczyn ich wystąpienia oraz opracowywanie wniosków wynikających z obsługi incydentu.

## ROZDZIAŁ 3
## KATEGORIE INCYDENTÓW

1. Incydent bezpieczeństwa informacji oraz cyberbezpieczeństwa to zdarzenie, którego skutkiem jest lub może być naruszenie bezpieczeństwa aktywów informacyjnych, powoduje lub może spowodować obniżenie jakości lub zatrzymanie 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 powodować 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) zdarzenie zamierzone, świadome i celowe (np. włamania do systemu, wirusowe zainfekowanie systemu, kradzież sprzętu) mające na celu naruszenie poufności zasobów informacyjnych, w tym poufności danych osobowych.

2. Incydentami bezpieczeństwa informacji w szczególności są:

a) naruszenie poufności, tzn. ujawnienie informacji niepowołanym osobom;
b) naruszenie integralności, tzn. zniszczenie, uszkodzenie lub przekłamanie informacji;
c) naruszenie dostępności, tzn. brak 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 jednostce dotyczących bezpieczeństwa informacji, w tym danych osobowych (np. pozostawienie włączonego komputera i / lub nie wylogowanie się po zakończeniu pracy lub podczas przerwy w pracy, pozostawienie niezabezpieczonych dokumentów drukowanych zawierających dane osobowe itp.).

4. O możliwości zaistnienia przypadku naruszenia cyberbezpieczeństwa mogą świadczyć:
a) nadmierne, w stosunku do wykonywanych zadań ( zakres upoważnienia ), uprawnienia użytkownika do zasobów systemu,
b) niestabilna praca systemu teleinformatycznego,
c) korzystanie z zasobów systemu poza godzinami pracy ( bez zgody przełożonego),
d) nowe ,, podejrzane'' ( nieznane ) konta użytkowników,
e) wysoka aktywność kont, które długo pozostawały niewykorzystane,
f) zanotowanie w krótkim czasie dużej liczby nieudanych prób logowania,
g) anomalie w pracy systemu lub programu ( świadczące np. o obecności wirusa komputerowego ),
h) naruszenie lub wadliwe funkcjonowanie zabezpieczeń fizycznych w pomieszczeniach, w których następuje przetwarzanie informacji w Urzędzie ( uszkodzone zamki, okna itp. )

## ROZDZIAŁ 4
## ZAKRES OBOWIĄZYWANIA PROCEDURY ZARZĄDZANIA INCYDENTAMI ZWIĄZANYMI Z BEZPIECZEŃSTWEM INFORMACJI ORAZ CYBERBEZPIECZEŃSTWEM

Procedura zarządzania incydentami związanymi z cyberbezpieczeństwem obowiązuje w Urzędzie Gminy w Święciechowie.

## ROZDZIAŁ 5
## ZGŁASZANIE INCYDENTÓW ZWIĄZANYCH Z BEZPIECZEŃSTWEM INFORMACJI ORAZ CYBERBEZPIECZEŃSTWEM

1. W przypadku ujawnienia incydentu pracownik niezwłocznie powiadamia o tym fakcie Inspektora Ochrony Danych, Administratora Danych Osobowych, Sekretarza Gminy oraz Administratora Systemów Informatycznych Naruszenie bezpieczeństwa informacji oraz cyberbezpieczeństwa może być zgłaszane przez pracowników - użytkowników i administratorów systemów. Osoba zgłaszająca odpowiada za wyczerpujący opis incydentu odpowiednio do posiadanej wiedzy i umiejętności.

2. Zgłoszenie musi zawierać następujące informacje:
a) imię i nazwisko osoby zgłaszającej oraz stanowisko;
b) ID komputera,
c) miejsce i datę wystąpienia incydentu;
d) opis incydentu w sposób adekwatny do posiadanej wiedzy i umiejętności zgłaszającego.
e) Administrator Systemów Informatycznych po rozpoznaniu incydentu zobowiązany jest do opisania zdarzenia w sposób szczegółowy, do rozszerzenia opisu zgłaszającego.
3. Brak umiejętności poprawnego rozpoznania incydentu przez osobę zgłaszającą nie może być przyczyną zaniechania zgłoszenia.

## ROZDZIAŁ 6
## PODEJMOWANIE DZIAŁAŃ W ZWIĄZKU ZE ZGŁASZANYMI INCYDENTAMI ZWIĄZANYMI Z BEZPIECZEŃSTWEM INFORMACJI ORAZ CYBERBEZPIECZEŃSTWEM

1. Zgłoszenie incydentu rejestrowane jest przez IOD i ADO oraz jest przechowywane w teczce *,, Procedura prowadzenia ewidencji naruszeń ochrony danych osobowych u administratora".* Osoba zgłaszająca incydent powinna w miarę możliwości zabezpieczyć materiał dowodowy (np. zrzut ekranu monitora, zdjęcie niezabezpieczonych materiałów zawierających dane osobowe itp.). Działania związane z obsługą zdarzenia w pierwszej kolejności dotyczą rozpoznania i kwalifikacji zgłoszenia. W przypadku, kiedy zgłoszenie zakwalifikowane zostało jako incydent bezpieczeństwa informacji lub cyberbezpieczeństwa, dokonywana jest jego ocena istotności. Powyższe działania wykonuje informatyk urzędu w porozumieniu z ADO i IOD.

2. Przy ocenie istotności incydentu pod uwagę brane są następujące czynniki:
a) powstałe szkody będące wynikiem incydentu;

b) wpływ incydentu na działanie systemów;
c) wpływ incydentu na ciągłość działania Urzędu;
d) koszty usunięcia skutków incydentu;
e) szacowany czas naprawy skutków wywołanych incydentem;
f) oszacowanie zasobów koniecznych do przywrócenia ciągłości działania systemów
g) wpływ incydentu na poufność, integralność lub dostępność danych osobowych oraz ewentualne skutki dla osób fizycznych, których one dotyczą.

3. Zakwalifikowanie zgłoszenia incydentu jako „fałszywy alarm" kończy postępowanie, o czym informatyk informuje zgłaszającego.

4. W przypadku zakwalifikowania zdarzenia jako incydentu związanego z bezpieczeństwem informacji lub cyberbezpieczeństwem, informatyk urzędu podejmuje działania zabezpieczające i naprawcze zmierzające do zniwelowania szkód powstałych w wyniku incydentu.

5. W przypadku, gdy waga incydentu dotyczy systemów informatycznych i zakwalifikowana jest jako wysoka, o incydencie zawiadamiany jest właściwy CSIRT NASK (Naukowa i Akademicka Sieć Komputerowa - Państwowego Instytutu Badawczego ul. Kolska 12, 01-045 Warszawa). Ocena wagi naruszenia pod kątem ochrony danych osobowych jest przeprowadzana zgodnie z przyjętą procedurą zgłaszania i oceny naruszeń ochrony danych osobowych, równolegle do działań podejmowanych na podstawie tej Procedury.

6. 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 go w sposób elektroniczny można zgłaszać przy użyciu innych dostępnych środków komunikacji (np. na numer telefonu +48223808274). W zgłoszeniu przekazuje się informacje zgodnie z formularzem oraz zgodnie z treścią art. 23 ust. 1 Ustawy o krajowym systemie cyberbezpieczeństwa z dnia 05 lipca 2018 r. Zgłoszenia dokonuje informatyk urzędu. Zgłoszenie do Prezesa Urzędu Ochrony Danych Osobowych odbywa się zgodnie z przyjętą procedurą zgłaszania i oceny naruszeń ochrony danych osobowych.

7. 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 7
## Podejmowanie działań w związku ze zgłaszanymi incydentami naruszenia bezpieczeństwa przetwarzania danych osobowych.

1. W przypadku naruszenia ochrony danych osobowych mają zastosowanie przepisy art. 33-34 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych - RODO) ( Dz. Urz. UE L 119 z dnia 05 kwietnia 2016 r.).

2. W przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego lub zaistnienia sytuacji, które mogą wskazywać na naruszenie ochrony danych osobowych tj. w szczególności:
a) przypadkowe lub niezgodne z prawem zniszczenie danych;
b) przypadkowa lub niezgodna z prawem utrata danych;
c) przypadkowa lub niezgodna z prawem modyfikacja danych;
d) nieuprawnione ujawnienie danych;
e) nieuprawniony dostęp do danych osobowych;

każdy pracownik zatrudniony przy przetwarzaniu danych osobowych (pracownik, stażysta, praktykant itp.) jest zobowiązany przerwać przetwarzania danych osobowych i niezwłocznie powiadomić o tym fakcie swojego bezpośredniego przełożonego oraz Inspektora Ochrony Danych i informatyka urzędu (jeżeli naruszenie ma związek z systemami informatycznymi).

3. Fakt naruszenia lub podejrzenia naruszenia ochrony danych osobowych należy potwierdzić pisemnie poprzez niezwłoczne sporządzenie zgłoszenia w którym umieszcza się informację o dacie, czasie, miejscu, okolicznościach zdarzenia. Notatkę przekazuje się Inspektorowi Ochrony Danych oraz Administratorowi Danych Osobowych zgodnie z załącznikiem do *,,Procedury prowadzenia ewidencji naruszeń ochrony danych osobowych u administratora".*

4. Zgłoszenie jest rejestrowane i przechowywane w teczce.

5. Przy ocenie istotności incydentu pod uwagę brane są następujące czynniki:
a) charakter naruszenia ochrony danych osobowych;
b) kategorię i przybliżoną liczbę osób, których dane dotyczą;
c) kategorię i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
d) możliwe konsekwencje naruszenia ochrony danych osobowych;

e) wpływ incydentu na ciągłość działania Urzędu;
f) koszty usunięcia skutków incydentu;
g) szacowany czas naprawy skutków wywołanych incydentem.