ZARZĄDZENIE Nr 16/2022

Wójta Gminy Tarnowiec

z dnia 17 listopada 2022 roku

w sprawie wprowadzenia Systemu Zarządzania Bezpieczeństwem Informacji

Na podstawie art.13 ust. 1 ustawy z dnia 17 lutego 2005r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz. U. z 2021 r. poz. 2070 z późn. zm.) w związku z § 20 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t.j. Dz. U. z 2017r. poz. 2247), art. 24 ust. 1 i 2, art. 32 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) (Dz. U. UE. L. z 2016 r. Nr 119 str. 1 z późn.zm.), art. 22 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369 z późn. zm.) oraz art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U. z 2022 r. poz. 559 z późn.zm.)

zarządza się, co następuje:

§ 1

1. W Urzędzie Gminy Tarnowiec, ustanawia się, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali System Zarządzania Bezpieczeństwem Informacji, zwany dalej: SZBI, zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.
2. SZBI odnosi się do ochrony informacji we wszystkich procesach, w których informacje są przetwarzane.
3. SZBI stanowi załącznik do niniejszego zarządzenia.

§ 2

Zarządzenie wchodzi w życie z dniem podpisania.

Zbigniew Kijowski
RADCA PRAWNY
WZ-K-172

p.o. Wójta Gminy Tarnowiec
Miłosz Leszkiewicz

Załącznik do Zarządzenia Wójta
Gminy Tarnowiec z dnia 17
listopada 2022 r. Nr 16/2022

System Zarządzania Bezpieczeństwem Informacji

Oprac.: Inspektor ochrony danych,
Pełnomocnik ds. ochrony informacji niejawnych w Urzędzie Gminy
w Tarnowcu Patrycja Kaczmarczyk-Hap

Spis treści

1. Definicje

Bezpieczeństwo Informacji - Zapewnienie podstawowych usług ochrony informacji (tj. poufności, integralności i dostępności) informacjom przetwarzanym przez Urząd,

Poufność - Zapewnienie stosowania zatwierdzonych ograniczeń w zakresie ujawniania i dostępu do informacji, w tym środków ochrony prywatności i informacji osobistych. Utrata poufności oznacza nieuprawnione ujawnienie informacji,

Integralność - Ochrona przed niewłaściwą modyfikacją lub zniszczeniem informacji, w tym zapewnienie niezaprzeczalności i autentyczności informacji. Utrata integralności oznacza nieuprawnioną modyfikację lub zniszczenie informacji,

Dostępność - Zapewnienie terminowego i niezawodnego dostępu i możliwości wykorzystania informacji. Utrata dostępności oznacza zaburzenie dostępu lub możliwości wykorzystania informacji lub systemu informatycznego,

PBI - Polityka Bezpieczeństwa Informacji,

IOD – Inspektor Ochrony Danych,

ASI – osoba zajmująca się informatyzacją w Urzędzie, informatyk,

SZBI – System Zarządzania Bezpieczeństwem Informacji,

Aktywa – Aktywa Informacyjne, zdefiniowane jako mające wartość dla organizacji i podlegające ochronie,

Urząd – Urząd Gminy w Tarnowcu,

Gmina - w odróżnieniu od Urzędu rozumiane jest poniżej jako wspólnota samorządowa mieszkańców na odpowiednim terytorium.

2. Deklaracja stosowania

1. Z punktu widzenia działalności Urzędu informacja jest cennym aktywem mającym wpływ na utrzymanie zgodności z obowiązującym prawem, możliwości wykonywania powierzonych zadań.
2. Wójt Gminy jest świadomy istniejących zagrożeń i ryzyka związanego z tworzeniem, przechowywaniem, przetwarzaniem i przesyłaniem informacji w tym danych osobowych.
3. W celu ochrony informacji, minimalizacji ryzyka i przeciwdziałaniu zagrożeniom ustanawia się niniejszy System Zarządzania Bezpieczeństwem Informacji. Definiuje on organizację bezpieczeństwa informacji, zarządzanie aktywami, stosowanie zabezpieczeń, sposób oceny zagrożeń, zarządzanie systemami i siecią teleinformatyczną, zarządzanie ciągłością działania.
4. Wójt opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali System Zarządzania Bezpieczeństwem Informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.
5. Wójt dba o bezpieczeństwo informacji chronionej niezależnie od jej formy (elektroniczna, papierowa, słowna).
6. System zarządzania bezpieczeństwem informacji obejmuje ochroną dane i informacje powierzone przez klientów, zarówno indywidualnych jak i instytucjonalnych, a także własne zasoby informacyjne, których przetwarzanie odbywa się w ramach procesów zgodnie z obowiązującymi przepisami prawa, zapewniając:
    a) dostęp wyłącznie osobom uprawnionym (poufność informacji),
    b) dokładność i kompletność informacji oraz metod jej przetwarzania (integralność

informacji),

c) dostęp do informacji i związanych z nią aktywów wówczas, gdy istnieje taka konieczność (dostępność informacji).

7. Decyzja o przyjęciu do stosowania Systemu Zarządzania Bezpieczeństwem Informacji ma na celu stałe podnoszenie bezpieczeństwa informacji poprzez stosowanie poziomu zabezpieczeń właściwego do ryzyka oraz przyjęcie modelu ciągłego udoskonalania.
8. Niniejsza Polityka Bezpieczeństwa Informacji jest adresowana do wszystkich pracowników Urzędu.

3. Cel

1. Niniejszy dokument określa ogólne zasady bezpiecznego korzystania z informacji jak i systemów informacyjnych oraz informatycznych. Zawiera on zbiór zasad, dzięki którym minimalizowane jest ryzyko związane z naruszeniem bezpieczeństwa informacji.
2. SZBI opiera się na poniższych przepisach:
    a. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz. U. z 2021 r. poz. 2070 z późn. zm.),
    b. Rozporządzenie 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) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.).
    c. Rozporządzenie 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 (t.j. Dz. U. z 2017 r. poz. 2247).
    d. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2022 r. poz. 1863).
    e. Narodowych Standardach Cyberbezpieczeństwa (NSC).
3. Głównym celem SZBI jest:
    a. Ustanowienie, wdrożenie, utrzymanie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), na który składają się procesy i procedury istotne dla zarządzania ryzykiem oraz doskonalenia bezpieczeństwa informacji,
    b. Ustanawianie organizacji bezpieczeństwa, czyli przekazanie zadań, kompetencji i obowiązków związanych z zapewnieniem bezpieczeństwa do odpowiednich stanowisk,
    c. Ustanowienie metody oceny zagrożeń i analizy ryzyka,
    d. Ustanowienie metody oceny poufności, integralności i dostępności informacji,
    e. Ustanowienie procedur bezpieczeństwa,
    f. Zapewnienie aktywom należytej ochrony w celu minimalizowania strat i ograniczenia ryzyka,
    g. Ustanowienie wymagań wobec stosowania ochrony fizycznej, środowiskowej i logicznej aktywów i informacji,
    h. Określenie zasad współpracy ze stronami trzecimi,
    i. Spełnienie wymagań standardów w zakresie bezpieczeństwa,
    j. Spełnienie wymagań przepisów prawa,
    k. Udoskonalanie SZBI poprzez wdrożenie mechanizmów nadzoru i wdrażania zmian.
4. Cel jest osiągany poprzez zapewnienie kompleksowego i elastycznego katalogu środków bezpieczeństwa i ochrony prywatności w celu zaspokojenia obecnych i przyszłych potrzeb ochrony w oparciu o zmieniające się zagrożenia, słabe punkty, wymagania i technologie.
5. System Zarządzania Bezpieczeństwem Informacji obejmuje swym zakresem Urząd Gminy, w tym systemy informacyjne, informatyczne i infrastrukturę teleinformatyczną Urzędu, przetwarzanie dokumentów papierowych oraz archiwizację informacji na dowolnych nośnikach.
6. Do przestrzegania zapisów SZBI zobowiązani są wszyscy pracownicy Urzędu, zgodnie z przyjętymi zasadami ochrony.

7. W celu zapewnienia jak najwyższego poziomu bezpieczeństwa informacji, będącej w posiadaniu lub przetwarzaniu przez Urząd, do zasad wynikających z SZBI powinni również stosować się dostawcy, audytorzy i konsultanci, którzy mają dostęp do informacji, dokumentów papierowych oraz zasobów i systemów informacyjnych oraz informatycznych.

4. Kategoryzacja informacji

Rodzaj informacji	Stopień poufności
1. informacje jawne	informacje uznawane za powszechnie dostępne
2. informacja udostępniana publicznie	informacje mogą być przekazywane na zewnątrz zgodnie z obowiązującymi przepisami prawa w szczególności ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej
3. informacja chroniona	informacje przekazywane na zewnątrz jedynie na podstawie podstawy prawnej z art. 6 i 9 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
4. informacje niejawne	informacje mogą być udostępniane tylko w konkretnych przypadkach ustawowych zgodnie z ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych

5. Procedura reakcji na incydenty

Celem procedury jest zapewnienie odpowiedniej reakcji na zaistniałe incydenty, zapewniając przy tym dostępności usług, realizację procesów, dostępność systemów/programów, sieci oraz podjęcie odpowiedniej reakcji na ataki związane z cyberprzestępczością. Procedura ma charakter ogólny i ma zastosowanie do wszystkich systemów informatycznych. Wójt Gminy wyznaczył osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami Krajowego Systemu Cyberbezpieczeństwa (KSC). Procedura została oparta na podstawie wymogów ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa oraz Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

1. Opis postepowania

a. Dokonanie oceny incydentu rozpoczyna się na skutek zdarzenia, które ma wpływ na realizację procesów przetwarzania oraz bezpieczeństwo danych i/lub informacji, zgodnie z załącznikiem nr 1.

b. Źródłem informacji o problemie może być zgłoszenie, komunikat zewnętrzny.

c. Podstawą reakcji jest zapewnienie bezpieczeństwa w pierwszej kolejności ludziom, jeżeli ich życie, bezpieczeństwo lub zdrowie są zagrożone na skutek zdarzenia.

d. Zaistniałe incydenty odnotowuj się w rejestrze, stanowiącym załącznik nr 2.

e. Osoba zgłaszająca incydent/zdarzenie powinna w miarę możliwości zabezpieczyć materiał dowodowy (np. zrzut ekranu monitora, zdjęcie niezabezpieczonych materiałów zawierających dane osobowe itp.).

f. Działania związane z obsługą zgłoszenia w pierwszej kolejności dotyczą rozpoznania i kwalifikacji zgłoszenia. Ocenę zdarzenia dokonuje kierownik/pracownik danego obszaru, gdzie wystąpiło zdarzenie, w porozumieniu z informatykiem, IOD oraz innymi wyznaczonymi przez administratora pracownikami.

g. 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;
   d) koszty usunięcia skutków incydentu;
   e) szacowany czas naprawy skutków wywołanych incydentem;
   f) oszacowanie zasobów koniecznych do przywrócenia ciągłości działania systemów.

h. Zakwalifikowanie zgłoszenia incydentu jako „fałszywy alarm" kończy postępowanie.

i. Zakwalifikowanie zgłoszenia jako naruszenie zasad ochrony danych uruchamia procedurę naruszenia opisaną w Polityce ochrony danych osobowych.

j. W przypadku zakwalifikowania zdarzenia jako incydentu związanego z bezpieczeństwem informacji, podejmowane są działania zabezpieczające i naprawcze zmierzające do zniwelowania szkód powstałych w wyniku incydentu.

k. W przypadku incydentu dotyczącego systemów informatycznych działania te prowadzone są przy współpracy z informatykiem.

l. W przypadku, gdy waga incydentu dotyczy systemów informatycznych i zakwalifikowana jest jako wysoka, o incydencje zawiadamiany jest zespół reagowania na incydenty CERT Polska - zgodnie z informacją zamieszoną na stronie www.cert.pl.

m. W przypadku stwierdzenia działań zamierzonych, przy jednoczesnym zidentyfikowaniu sprawcy incydentu dotyczącego naruszenia bezpieczeństwa informacji, Administrator podejmuje decyzję dotyczącą wyciągnięcia ewentualnych konsekwencji dyscyplinarnych wobec sprawcy incydentu. Jednocześnie, w zależności od wagi incydentu, mogą być zawiadomione organy ścigania.

6. Okres obowiązywania

SZBI wchodzi w życie z dniem wskazanym w Zarządzeniu Wójta Gminy Tarnowiec wprowadzającym niniejszy System.

7. Struktura Systemu Zarządzania Bezpieczeństwem Informacji

1. W skład dokumentacji Systemy Zarządzania Bezpieczeństwem Informacji wchodzą następujące przyjęte w Urzędzie dokumenty:
   a. niniejszy dokument,
   b. Polityka Ochrony Danych Osobowych w Urzędzie Gminy Tarnowiec
   c. Instrukcja Analizy Ryzyka Bezpieczeństwa Danych Osobowych oraz Informacji w Urzędzie Gminy Tarnowiec,

2. Powyższe dokumenty zawierają m.in. opis następujących obszarów bezpieczeństwa:
   a. Organizację Bezpieczeństwa Informacji,
   b. Analizę i zarządzanie ryzykiem,
   c. Plan postępowania z ryzykiem,
   d. Zidentyfikowanie aktywów,
   e. Zabezpieczenia organizacyjne,
   f. Zabezpieczenia fizyczne,
   g. Zabezpieczenia informatyczne,
   h. Zasady dostępu do pomieszczeń,
   i. Zasady nadawania upoważnień,

j. Zasady nadawania uprawnień,
k. Obowiązki,
l. Procedurę naruszeń,
m. Zarządzanie incydentami związanymi z bezpieczeństwem informacji i cyberprzestępczością,

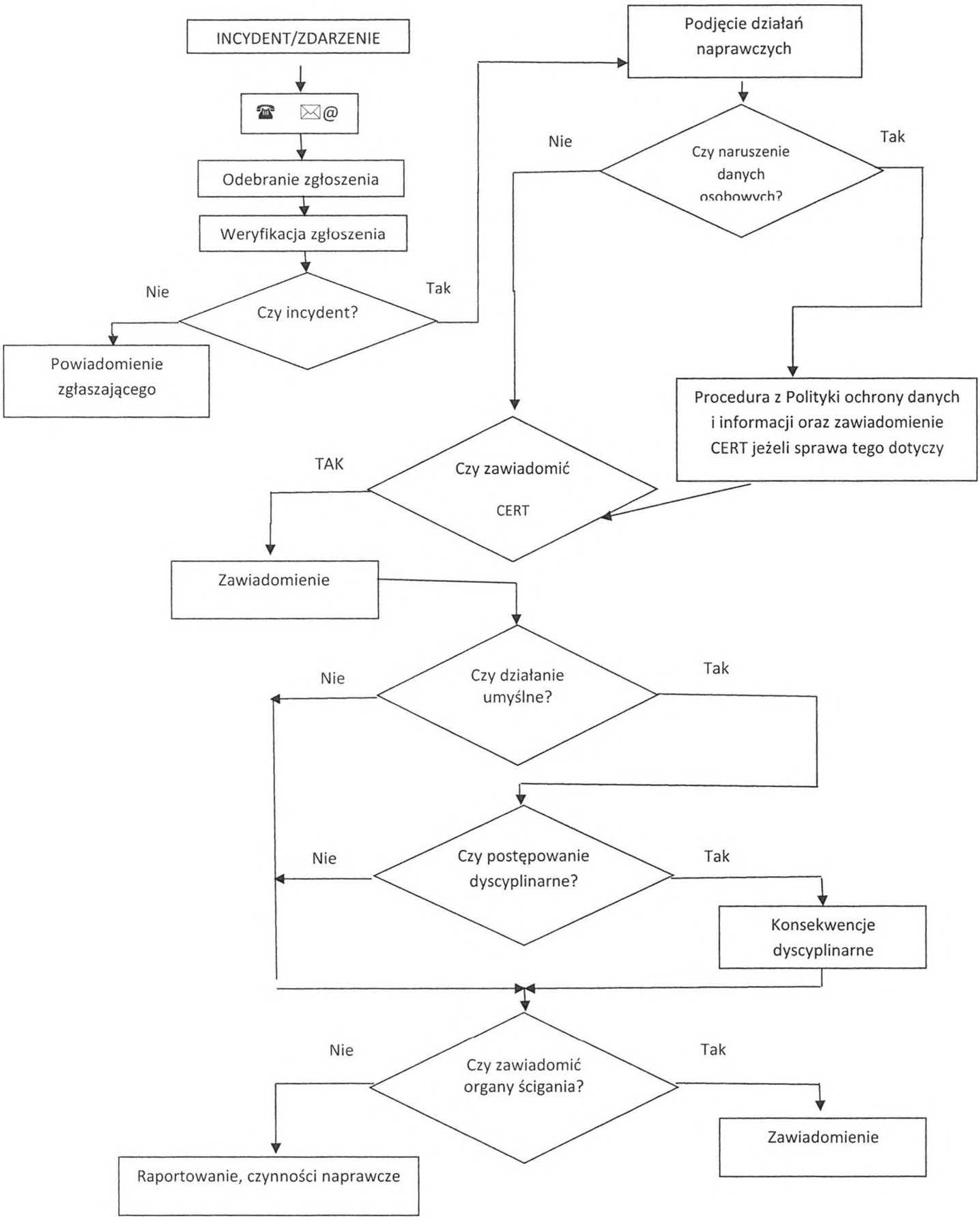
8. Dystrybucja SZBI

Każdy z pracowników Urzędu jest zobowiązany zapoznać się z dokumentacją stanowiącą System Zarządzania Bezpieczeństwem Informacji.

9. Organizacja Bezpieczeństwa Informacji

Zarządzanie i nadzór nad bezpieczeństwem informacji jest realizowane przez: Wójta Urzędu, , Sekretarza, Administratora Systemów Informatycznych (informatyka) oraz Inspektora Ochrony Danych. Powyższe osoby tworzą Zespół Bezpieczeństwa Informacji. Role i zadania ww. osób w ramach prac zespołu polega m.in na przeprowadzeniu analizy incydentu, podjęcia planów naprawczych, dokonanie właściwych zgłoszeń, opracowaniu zaleceń dla pracowników jednostki. Do głównych działań zarządzania i nadzoru należy rozwijanie, doskonalenie oraz monitorowanie SZBI. Za ustanowienie, wdrożenie i utrzymanie SZBI odpowiedzialny jest Wójt Gminy.

Załącznik nr 1



Załącznik nr 2

Lp.	Zdarzenie/incydent	Ocena	Zaplanowane i podjęte działania	Termin realizacji działań	Osoby odpowiedzialne za zrealizowanie planu oraz jego nadzór