ZARZĄDZENIE NR 491/2022
WÓJTA GMINY INOWROCŁAW

z dnia 8 czerwca 2022 r.

w sprawie zarządzania incydentami w zakresie zadań publicznych zależnych od systemu informacyjnego.

Na podstawie art. 22 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2020 r., poz. 1369 z późn. zm.), w związku z art. 33 ust. 1, 3 i 5 ustawy z dnia 8 marca 1990r. o samorządzie gminnym (Dz. U. z 2022r., poz. 559 z późn. zm.) zarządza się, co następuje:

§ 1. Ilekroć w zarządzeniu i załączniku do zarządzenia jest mowa o:

1) **Gmina** – należy przez to rozumieć gminę Inowrocław jako jednostkę samorządu terytorialnego;
2) **Urzędzie** – należy przez to rozumieć Urząd Gminy Inowrocław;
3) **Wydziale** – należy przez to rozumieć wydział w rozumieniu określonym w Regulaminie Organizacyjnym Urzędu Gminy Inowrocław;
4) **Wójcie** – należy przez to rozumieć Wójta Gminy Inowrocław;
5) **Jednostce organizacyjnej** – należy przez to rozumieć jednostkę organizacyjną w rozumieniu określonym w Regulaminie Organizacyjnym Urzędu Gminy Inowrocław;
6) **Kierowniku jednostki organizacyjnej** – należy przez to rozumieć kierownika jednostki organizacyjnej w rozumieniu określonym w Regulaminie Organizacyjnym Urzędu Gminy Inowrocław;
7) **Dyrektorze wydziału** – należy przez to rozumieć dyrektora w rozumieniu określonym w Regulaminie Organizacyjnym Urzędu Gminy Inowrocław;
8) **Użytkownik** – osoba posiadająca dostęp do systemu informacyjnego Jednostki służącego do realizacji zadania publicznego;
9) **Przewodniczący Zespołu ds. Bezpieczeństwa Informacji** – osoba odpowiedzialna za utrzymanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, o której mowa w art. 21 ust. 1 Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2020r., poz. 1369 ze zm.);
10) **Ustawie** – należy przez to rozumieć ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;
11) **CSIRT NASK** – należy przez to rozumieć Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy;
12) **Cyberbezpieczeństwie** – należy przez to rozumieć odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy;
13) **Poufności danych lub usług** – należy przez to rozumieć dane lub usługi, które są dostępne wyłącznie dla uprawnionych osób;
14) **Integralności danych lub usług** – należy przez to rozumieć dane lub usługi, które są prawdziwe i nie zostały w sposób nieuprawniony („złośliwie") zmienione;
15) **Dostępności danych lub usług** – należy przez to rozumieć dane lub usługi, do których uprawnione osoby mają dostęp w ustalonym z góry czasie (np. w czasie godzin pracy);
16) **Autentyczności danych lub usług** – należy przez to rozumieć dane lub usługi, co do których mamy pewność ich pochodzenia (treści i autorstwa);

17) **Incydencie** – należy przez to rozumieć zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo, które powoduje lub może powodować obniżenie jakości lub przerwanie realizacji zadania publicznego zależnego od systemu informacyjnego;

18) **Incydencie cyberbezpieczeństwa** – zbiorcza nazwa obejmująca terminy incydent, incydent w podmiocie publicznym, incydent krytyczny;

19) **Incydencie 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;

20) **Incydencie krytycznym** – 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;

21) **Podatności** – należy przez to rozumieć właściwość systemu informacyjnego, która może spowodować zagrożenie cyberbezpieczeństwa;

22) **Zagrożeniu cyberbezpieczeństwa** – należy przez to rozumieć potencjalną przyczynę wystąpienia incydentu;

23) **Systemie informacyjnym** – należy przez to rozumieć 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.

§ 2. 1.Za zapewnienie adekwatności, skuteczności i jednolitości zarządzania incydentami w Urzędzie Gminy Inowrocław oraz jednostkach organizacyjnych odpowiedzialny jest Przewodniczący Zespołu ds. Bezpieczeństwa Informacji lub osoba przez niego upoważniona.

2. Przewodniczący Zespołu ds. Bezpieczeństwa Informacji lub osoba przez niego upoważniona wykonują swoje czynności przy pomocy członków Zespołu ds. Bezpieczeństwa Informacji.

3. Zarządzanie incydentami dotyczy w szczególności koordynacji zgłaszania i obsługi incydentów.

4. Wójt wyznacza Przewodniczącego Zespołu ds. Bezpieczeństwa Informacji do utrzymywania kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.

5. Wójt, w terminie 14 dni od dnia wyznaczenia, przekazuje do CSIRT NASK dane Przewodniczącego Zespołu ds. Bezpieczeństwa Informacji, a także informacje o zmianie tych danych w terminie 14 dni od dnia ich zmiany.

6. Przekazanie danych Przewodniczącego Zespołu ds. Bezpieczeństwa Informacji odbywa się w sposób następujący:
   a) za pośrednictwem formularza elektronicznego pod adres e-mail: ksc@cert.pl;
      lub
   b) w formie pisemnej pod adres do korespondencji CSIRT NASK:
      NASK - Państwowy Instytut Badawczy
      ul. Kolska 12
      01-045 Warszawa

   Przekazanie danych Przewodniczącego Zespołu ds. Bezpieczeństwa Informacji powinno zawierać:
   a) nazwę Jednostki,
   b) sektor, w którym działa Jednostka,
   c) imię i nazwisko, telefon kontaktowy oraz adres poczty elektronicznej e-mail.

7. Przewodniczący Zespołu ds. Bezpieczeństwa Informacji oraz zespół ds. bezpieczeństwa informacji powoływany jest pismem okólnym Wójta.

8. Do zadań Zespołu ds. Bezpieczeństwa Informacji w zakresie koordynacji zarządzania incydentami należy w szczególności:

1) przyjmowanie od Użytkowników i pracowników Jednostki zgłoszenia o zdarzeniach mogącym stanowić incydent cyberbezpieczeństwa lub podejrzeniu ich wystąpienia w Jednostce,

2) wstępne weryfikowanie we współpracy z Przewodniczącym Zespołu ds. Bezpieczeństwa Informacji otrzymane od Użytkowników i pracowników Jednostki informacji o zdarzeniu pod względem przesłanek identyfikujących zaistnienie incydentu cyberbezpieczeństwa,

3) gromadzenie wszelkich informacji o zdarzeniu mogącym stanowić incydent cyberbezpieczeństwa oraz niezwłocznie informuje i przekazuje Koordynatorowi KSC uzyskane od pozostałych Użytkowników i pracowników Jednostki ustalenia ze zdarzeniem związane,

4) wraz z Przewodniczącym Zespołu ds. Bezpieczeństwa Informacji oraz 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.

5) zapewnienie obsługi incydentu poprzez:

   a) przeprowadzenie postępowań wyjaśniających okoliczności wystąpienia incydentu,

   b) przygotowanie projektu szczegółowych wyjaśnień przekazywanych do CSIRT NASK, w tym informacji uzupełniających do pierwotnego zgłoszenia,

   c) przygotowanie projektu rekomendacji dla dyrektorów wydziałów oraz kierowników j.o. w celu minimalizacji bądź usunięcia skutków wystąpienia incydentu oraz zapobiegania ich wystąpieniu w przyszłości;

6) wsparcie Jednostki w przygotowaniu zgłoszenia incydentu w podmiocie publicznym do CSIRT NASK, zgodnie ze wzorem stanowiącym załącznik nr 2 do załącznika nr 1 do niniejszej Procedury,

7) prowadzenie rejestru incydentów dla Gminy Inowrocław;

8) podejmowanie czynności zmierzających do zapewnienia dostępu do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa.

9) wdrażanie działań naprawczych po wystąpieniu incydentu cyberbezpieczeństwa,

10) szkolenie i podnoszenie świadomości Użytkowników i pracowników Jednostki w zakresie incydentów cyberbezpieczeństwa, ich zgłaszania, przeciwdziałania i prewencyjnych sposobach zabezpieczenia Zleceniodawcy przed ich występowaniem,

9. Do zadań Przewodniczącego Zespołu ds. Bezpieczeństwa Informacji należy w szczególności:

1) koordynowanie obsługi zgłaszanych incydentów cyberbezpieczeństwa,

2) prawo do kwalifikacji zdarzenia jako incydent niezależnie od przeprowadzonego ustalenia przez wydział lub jednostkę;

3) zatwierdzanie wyjaśnień przekazywanych do CSIRT NASK, w tym informacji uzupełniających do pierwotnego zgłoszenia;

4) zatwierdzanie rekomendacji dla dyrektorów wydziałów oraz kierowników j.o. w celu minimalizacji bądź usunięcia skutków wystąpienia incydentu oraz zapobiegania ich wystąpieniu w przyszłości;

5) decydowanie o przekazaniu do CSIRT NASK w niezbędnym zakresie (gdy jest to konieczne do realizacji zadań CSIRT NASK) informacji stanowiących tajemnice prawnie chronione, w tym stanowiących tajemnicę przedsiębiorstwa, oraz oznaczanie ich w przekazywanej treści informacji.

6) koordynowanie wdrażaniem działań naprawczych po wystąpieniu incydentu cyberbezpieczeństwa,

d) nadzorowanie nad prawidłowym prowadzeniem rejestru incydentów cyberbezpieczeństwa;

10. Wszyscy pracownicy wydziałów i j.o. zobowiązani są w trybie pilnym do zgłaszania incydentów zgodnie z Procedurą stanowiącą załącznik nr 1 do niniejszego zarządzenia.
11. Zobowiązuje się dyrektorów wydziałów oraz kierowników j.o. do przyjęcia i wdrożenia rekomendacji, o których mowa w ust. 7 pkt 3, lub w przypadku niemożności ich realizacji – do przekazania do Przewodniczącego Zespołu ds. Bezpieczeństwa Informacji pisemnych informacji wraz z uzasadnieniem o konieczności odstąpienia od nich.

§ 3. 1. Zespół ds. Bezpieczeństwa Informacji jest odpowiedzialny za prowadzenie oraz aktualizowanie rejestru incydentów występujących w wydziałach i j.o.

2. Za prowadzenie nadzoru nad danymi, o których mowa w ust. 1, odpowiada Przewodniczący Zespołu ds. Bezpieczeństwa Informacji.
3. Zespół, o którym mowa w § 2 ust. 8, jest odpowiedzialny za przedstawienie Przewodniczącemu Zespołu ds. Bezpieczeństwa Informacji szczegółowych danych wymaganych w rejestrze incydentów.
4. Zespół, o którym mowa w § 2 ust. 8, ma także obowiązek zgłoszenia ryzyka z obszaru bezpieczeństwa informacji w przypadku braku możliwości zastosowania działań doskonalących, eliminujących przyczyny i skutki incydentu. Zasady zarządzania ryzykiem z obszaru bezpieczeństwa informacji zostały określone odrębnym zarządzeniem.

§ 4. Zespół ds. Bezpieczeństwa Informacji jest odpowiedzialny także za prowadzenie szkoleń wewnętrznych dla pracowników, które organizuje z własnej inicjatywy lub na wniosek Kierownika Jednostki.

§ 4. Zgodnie z art. 37 ust. 1 ustawy, do informacji o podatnościach, incydentach i zagrożeniach cyberbezpieczeństwa oraz o ryzyku wystąpienia incydentu nie stosuje się ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej.

§ 5. Wykonanie zarządzenia powierza się Zastępcy, Sekretarzowi, Skarbnikowi oraz dyrektorom wydziałów i kierownikom jednostek organizacyjnych.

§ 6. Zarządzenie wchodzi w życie z dniem podpisania.

Wójt Gminy Inowrocław

Tadeusz Kacprzak

Załącznik do zarządzenia Nr 491/2022

Wójta Gminy Inowrocław

z dnia 8 czerwca 2022 r.

PROCEDURA ZGŁASZANIA PRZEZ PRACOWNIKA WYDZIAŁU URZĘDU GMINY INOWROCŁAW / J.O. INCYDENTU W PODMIOCIE PUBLICZNYM REALIZUJĄCYM ZADANIE PUBLICZNE ZALEŻNE OD SYSTEMU INFORMACYJNEGO

PRZEDMIOT I ZAKRES STOSOWANIA: Realizacja przepisów ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa w zakresie związanym ze zgłoszeniem incydentu w podmiocie publicznym realizującym zadanie publiczne zależne od systemu informacyjnego przez pracowników Urzędu Gminy Inowrocław i jednostek organizacyjnych.

CEL: Sprawne zgłaszanie incydentów w podmiocie publicznym realizującym zadanie publiczne zależne od systemu informacyjnego.

TERMINOLOGIA: Definicje stosowane w niniejszej Procedurze zostały wskazane w § 1 zarządzenia.

OPIS POSTĘPOWANIA:

§ 1. Zasady ogólne

1. Procedura dotyczy wyłącznie zgłaszania incydentu, który spełnia jednocześnie następujące trzy przesłanki:
   1) dotyczy zadania publicznego, tj. zadania wynikającego z przepisów powszechnie obowiązującego prawa,
   2) dotyczy zadania publicznego, które jest zależne od systemu informacyjnego,
   3) dotyczy zdarzenia, które powoduje albo może spowodować obniżenie jakości realizowanego zadania publicznego, lub dotyczy zdarzenia, które powoduje albo może spowodować przerwanie realizacji zadania publicznego.
2. Nie jest incydentem w podmiocie publicznym realizującym zadanie publiczne zależne od systemu informacyjnego zdarzenie:
   1) które nie obejmuje zakłóceń lub przerwy w wykonywaniu zadania publicznego,
   2) dotyczące zadania, w którym system informacyjny nie jest niezbędny lub nie jest przyczyną wystąpienia incydentu. W tej sytuacji (gdy nie stwierdzi się równoczesnego zaistnienia wszystkich trzech wskazanych w ust. 1 przesłanek) **nie zgłaszamy do CSIRT NASK**. Jest to wtedy tzw. zwykły incydent bezpieczeństwa i należy postępować w Urzędzie Gminy Inowrocław zgodnie z *Procedurą postępowania w sytuacji wystąpienia incydentu w obszarze ochrony danych osobowych i bezpieczeństwa informacji*, a w j.o. zgodnie z przyjętą wewnętrznie procedurą z zakresu Systemu Zarządzania Bezpieczeństwem Informacji.
3. Przyczyny wystąpienia incydentu

   Przyczynę wystąpienia incydentu cyberbezpieczeństwa mogą stanowić:
   1) klęski żywiołowe,
   2) pożary,
   3) zakłócenia w dostawie energii elektrycznej,
   4) błędy w oprogramowaniu,
   5) awaria sprzętu,
   6) błędy użytkowników, których wystąpienie może spowodować zniszczenie lub uszkodzenie infrastruktury informatycznej oraz zakłócenie ciągłości pracy systemów informacyjnych,

7) niewłaściwe wykorzystywanie zasobów informatycznych,
8) działanie szkodliwego oprogramowania,
9) próby omijania systemów zabezpieczeń,
10) nieautoryzowany dostęp do systemów informacyjnych i aplikacji,
11) zniszczenia lub kradzieży urządzeń wykorzystywanych do przetwarzania i przechowywania informacji,
12) zniszczenia lub kradzieży nośników danych,
13) próby wyłudzeń informacji,
14) ataki socjotechniczne.

4. Zgłoszenia może dokonać każdy pracownik (w miarę możliwości po konsultacji z bezpośrednim przełożonym) wydziału Urzędu Gminy Inowrocław oraz jednostki organizacyjnej (j.o. lub zgodnie z zasadami ustalonymi wewnętrznie w j.o. osoba do tego uprawniona – zawsze biorąc pod uwagę tryb pilny na poinformowanie o incydencie.
5. Tryb pilny oznacza niezwłoczne zgłoszenie, które nie może przekroczyć 24 godzin od wykrycia incydentu.

§ 2. Sposób postępowanie z incydentem w wydziale/j.o.

1. W sytuacji wystąpienia w wydziale/j.o. incydentu, który **spełnia przesłanki określone w § 1 ust. 1**, należy niezwłocznie – w trybie pilnym – wykonać 3 następujące kroki:
   1) pobrać elektroniczną wersję *Formularza zgłoszenia incydentu w podmiocie publicznym realizującym zadanie publiczne zależne od systemu informacyjnego* stanowiącego załącznik nr 1 do niniejszej procedury (dostępny w Biuletynie Informacji Publicznej) i uzupełnić obligatoryjnie całą część B i C formularza;
   2) wysłać elektroniczną wersję wypełnionego formularza na **adres mailowy: admin@gminainowroclaw.eu oraz dodatkowo do wiadomości na adres: sekretariat@gminainowroclaw.eu**;
   3) zawiadomić telefonicznie (nr 52 3555842) o wystąpieniu incydentu i przesłaniu zgłoszenia. Należy dodatkowo potwierdzić, że dotyczy wystąpienia incydentu w podmiocie publicznym zależnym od systemu informatycznego, a następnie odczytać treść pkt 1 i 3 z części B i pkt 4 z części C z ww. formularza.
2. Jeżeli incydent jednocześnie narusza przepisy innych ustaw, np. stanowi naruszenie przepisów o ochronie danych osobowych, należy zastosować się do wytycznych z danego obszaru, przyjętych do stosowania w Urzędzie Gminy Inowrocław.
3. W j.o., w których nie funkcjonuje sformalizowana procedura, o której mowa w ust. 3, zaleca się wdrożenie jej.
4. W sytuacjach wyjątkowych, np. awarii sieci internetowej i braku możliwości przekazania zgłoszenia elektronicznie , dopuszczalne jest dokonanie zgłoszenia przy użyciu alternatywnych środków komunikacji:
   1) przez wypełniony formularz za pomocą faxu na nr 52 354 04 90 lub
   2) przez zgłoszenie telefoniczne (nr 52 3555842) wraz z podaniem niezbędnych informacji zgodnie z treścią przeznaczonego do tego formularza.

§ 3. Doprecyzowanie zgłoszenia incydentu

1. Jeżeli pracownik wydziału lub j.o. będzie miał trudności w zakwalifikowaniu danego zdarzenia jako incydent, o którym mowa w § 1 ust. 1, może skonsultować je z Zespołem ds. Bezpieczeństwa Informacji (tel. 52 3555842).

2. Dopuszcza się możliwość tzw. doprecyzowania zgłoszenia danego zdarzenia wstępnie zakwalifikowanego jako incydent, o którym mowa w § 1 ust. 1, gdyż może zdarzyć się, że ze względu na zbyt krótki czas na dokonanie zgłoszenia nie zakończono szczegółowej analizy weryfikacyjnej zdarzenia bądź nie zebrano wszystkich dowodów w sprawie.
3. Po przeprowadzeniu postępowania wyjaśniającego, o którym mowa w ust. 2, i zebraniu wszystkich istotnych faktów i dowodów, które nie były znane w momencie zgłoszenia, należy w trybie pilnym uzupełnić wcześniejsze zgłoszenie.

§ 4. Anulowanie zgłoszenia incydentu

Jeżeli w przeprowadzonym postępowaniu wyjaśniającym zostanie wykazane, że dane zdarzenie wstępnie zakwalifikowane i zgłoszone jako incydent nie spełnia jednak wszystkich trzech przesłanek, o których mowa w § 1 ust. 1, to niezwłocznie należy poinformować Zespół ds. Bezpieczeństwa Informacji i anulować zgłoszenie.

§ 5. Dystrybucja oraz aktualizacja Procedury

1. 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.
2. Kierownik Jednostki zapewnia dostęp do niniejszej Procedury każdemu Użytkownikowi i pracownikowi Jednostki.
3. Każdy Użytkownik i pracownik Jednostki zobowiązany jest zapoznać się z niniejszą

Załącznik Nr 1 do Załącznika Nr 1

Formularz zgłoszenia incydentu w podmiocie publicznym realizującym zadanie publiczne zależne od systemu informacyjnego	
Dotyczy jedynie zdarzenia związanego z systemami teleinformatycznymi, które powoduje lub może spowodować przerwanie realizacji, obniżenie jakości realizowanego zadania publicznego (tj. zadania wynikającego z przepisów powszechnie obowiązującego prawa)	
CZĘŚĆ A: Dane uzupełniane przez Urząd Gminy Inowrocław	
1. Nazwa podmiotu zgłaszającego	
2. Siedziba i adres zgłaszającego	
3. NIP zgłaszającego	
4. Imię i nazwisko osoby zgłaszającej	
5. Stanowisko służbowe osoby zgłaszającej	
6. Numer telefonu służbowego	
7. Adres poczty elektronicznej zgłaszającego	
8. Imię i nazwisko osoby uprawnionej do składania wyjaśnień dotyczących zgłaszanych informacji	
9. Numer telefonu służbowego	
10. Adres poczty elektronicznej	
CZĘŚĆ B: DANE WYDZIAŁU / Urząd Gminy Inowrocław	
1. Pełna nazwa wydziału / j.o., w których wystąpił incydent	
2. Siedziba i adres wydziału / j.o.	
3. Imię i nazwisko osoby zgłaszającej z wydziału / j.o.	
4. Stanowisko służbowe osoby zgłaszającej z wydziału / j.o.	
5. Numer telefonu służbowego osoby zgłaszającej	

6. Adres służbowej poczty elektronicznej osoby zgłaszającej	
CZĘŚĆ C: OPIS WPŁYWU INCYDENTU NA REALIZOWANE ZADANIA PUBLICZNE ZALEŻNE OD SYSTEMU INFORMACYJNEGO (uzupełnia wydział / j.o.) Uwaga:	
1. Zadania publiczne, na które incydent miał wpływ (m.in. zadania w statucie, ustawie o samorządzie gminnym)	
2. Klasyfikacja incydentu (lista wyboru)	
3. Przybliżona liczba osób, na które incydent miał wpływ	
4. Moment wystąpienia incydentu (w miarę możliwości: data, godzina)	
5. Moment wykrycia incydentu	
6. Czas trwania incydentu (jeśli nie wygasł – proszę wpisać „w toku”)	
7. Zasięg geograficzny obszaru występowania incydentu	
8. Przyczyna / źródło wystąpienia incydentu	
9. Dokładny opis przebiegu incydentu	
10. Skutki oddziaływania incydentu na systemy informacyjne wydziału / j.o.	
11. Informacje o podjętych działaniach zapobiegawczych	
12. Informacje o podjętych działaniach naprawczych	
13. Inne istotne informacje	

Załącznik Nr 2 do Załącznika Nr 1 Wzór rejestru incydentów bezpieczeństwa i cyberbezpieczeństwa

lp.	Data zgłoszenia	Kategoria zgłoszenia ("Incydent bezpieczeństwa/ cyberbezpieczeństwa lub Naruszenie ochrony danych osobowych)	Opis incydentu (zdarzenia)	Osoba zgłaszająca	Kategoria incydentu	Przyczyna lub potencjalna przyczyna wystąpienia incydentu	Opis działań podjętych w związku z incydentem	Data zamknięcia incydentu