Zarządzenie nr 77/2023

Wójta Gminy Osieck

z dnia 1 sierpnia 2023r.

W sprawie wprowadzenia Procedury zarządzania incydentami cybernetycznymi w Urzędzie Gminy w Osiecku

Na podstawie art. 22 ust. 1. Ustawy z dnia 5 lipca 2018r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2023r. poz. 913) zarządzam co następuje:

§1

Wprowadzam w Urzędzie Gminy w Osiecku Procedurę zarządzania incydentami cybernetycznymi.

§2

Zobowiązuję wszystkich pracowników Urzędu Gminy W Osiecku do zapoznania się z niniejszą Procedurą.

§3

Pisemne poświadczenie o zapoznaniu się z procedurą należy złożyć u Sekretarza Gminy w wykazie stanowiącym zał. nr.3 do Procedury.

§4

Zarządzenie wchodzi z dniem podjęcia.

WÓJT
Zowczak
mgr inż. Karolina Zowczak

Urząd Gminy w Osiecku			
Procedura zarządzania incydentami cybernetycznymi			
Stron: 12	Data: 01.08.2023r.	Wersja: 01	Poziom poufności: Wewnętrzny

Załącznik nr. 1 do Zarządzenia nr 77/2023 Wójta Gminy Osieck z dnia 1 sierpnia 2023r.

Egzemplarz zatwierdzony ☐ TAK ☐ NIE

Podpis Administratora :

WÓJT

.....mgr inż. Karolina Zowczak.....

1. Postanowienia ogólne

1.1 Procedura zarządzania incydentami cybernetycznymi, zwana dalej „Procedurą" jest dokumentem stosowanym wewnętrznie w Urzędzie Gminy Osieck.

1.2 Procedura obejmuje swoim zakresem zasady zarządzania incydentami cybernetycznymi stosowane przez Jednostkę w celu zachowania możliwie wysokiego poziomu bezpieczeństwa oraz spełnienia wymagań wynikających w szczególności z :

1) ustawy z dnia 5 lipca 2018r o krajowym systemie cyberbezpieczeństwa(t. j. Dz. U. z 2018r., poz. 1560 ze zm.),
2) dobrych praktyk z zakresu cyberbezpieczeństwa, bezpieczeństwa informacji oraz ochrony danych osobowych.

1.3 Definicje

1) **ADO/Administrator Danych Osobowych**- Gmina Osieck reprezentowana przez Wójta.
2) **CSIRT NASK**- Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy.
3) **Cyberbezpieczeństwo**-odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.
4) **Incydent**- zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo.
5) **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 CSIRT NASK.
6) **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 7–1.
7) **IOD**- Inspektor Ochrony Danych Osobowych wyznaczony przez Gminę Osieck.
8) **Jednostka**- Urząd Gminy Osieck
9) **Koordynator ds. cyberbezpieczeństwa**- osoba odpowiedzialna za utrzymywanie kontaktu z podmiotami krajowego systemu cyberbezpieczeństwa, wyznaczona na podstawie art. 21. ust.1. Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t. j. Dz. U. z 2018 r., poz. 1560 ze zm.).
10) **Obsługa incydentu** – czynności umożliwiające wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację, podejmowanie działań naprawczych i ograniczenie skutków incydentu.
11) **Podatność**-właściwość systemu informacyjnego, która może być wykorzystana przez zagrożenie cyberbezpieczeństwa.

12) **Pracownik**- Osoba mająca dostęp do systemu informacyjnego jednostki i wykonująca zadania na jej rzecz.
13) **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 2017 r. poz. 570 oraz z 2018 r. poz. 1000 i 1544), wraz z przetwarzanymi w nim danymi w postaci elektronicznej.
14) **Ustawa**- Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t. j. Dz. U. z 2018 r., poz. 1560 ze zm.).
15) **Zagrożenie cyberbezpieczeństwa**- potencjalna przyczyna wystąpienia incydentu.
16) **Zarządzanie incydentem**- obsługa incydentu, wyszukiwanie powiązań między incydentami, usuwanie przyczyn ich wystąpienia oraz opracowywanie wniosków wynikających z obsługi incydentu.

2. Koordynator ds. cyberbezpieczeństwa

2.1 ADO wyznacza Koordynatora ds. cyberbezpieczeństwa tj. osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.

2.2 ADO bądź osoba przez niego upoważniona przekazuje, w terminie 14dni od wyznaczenia dane Koordynatora ds. cyberbezpieczeństwa do CSIRT NASK.

2.3 Każda zmiana Koordynatora ds. cyberbezpieczeństwa bądź jego danych jest zgłaszana do CSIRT NASK w terminie do 14 dni od dnia ich zmiany.

2.4 Koordynatorem ds. cyberbezpieczeństwa powinna być osoba:
1) Dyspozycyjna- tak aby w przypadku incydentu lub zagrożenia można było z nią sprawnie i szybko nawiązać kontakt. Zwłaszcza po godzinach pracy jednostki.
2) Decyzyjna- tak aby w razie potrzeby mogła podjąć decyzję o przekazaniu/udostępnieniu informacji niezbędnych do obsługi incydentu oraz podjąć działania rekomendowane przez CSIRT lub wydać konkretne polecenia w jednostce.
3) Technicznym zrozumieniu tematu- tak aby mieć łatwość komunikacji z CSIRT. Nie oznacza to jednak, że musi być osobą techniczną.
4) O silnie rozwiniętej sieci kontaktów wewnętrznych w jednostce.

2.5 Przekazanie danych Koordynatora ds. cyberbezpieczeństwa odbywa się za pośrednictwem formularza elektronicznego na stronie internetowej https://incydent.cert.pl/osoba-kontaktowa#!/lang=pl

2.6 Przekazanie danych Koordynatora ds. cyberbezpieczeństwa powinno zawierać:
1) Nazwę jednostki i jej dane adresowe
2) Imię i nazwisko, numer telefonu oraz adres e-mail Koordynatora ds. cyberbezpieczeństwa.
3) Umiejscowienie Koordynatora ds. cyberbezpieczeństwa:
   - Wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo.
   - Zewnętrzny podmiot świadczący usługi z zakresu cyberbezpieczeństwa.
4) Skan decyzji/zarządzenia o wyznaczeniu osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.

2.7 Zakres zadań Koordynatora ds. cyberbezpieczeństwa obejmuje:

1) Przyjmowanie zgłoszeń od ADO lub osoby przez niego upoważnionej oraz IOD informacji o incydencie cybernetycznym bądź podejrzeniu jego wystąpienia w jednostce.
2) Niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia zdarzenia dokonywanie zgłoszenia incydentu w podmiocie publicznym do CSIRT NASK za pomocą formularza elektronicznego na stronie internetowej https://incydent.cert.pl/. W razie nieobecności Koordynatora ds. cyberbezpieczeństwa zgłoszenia dokonuje ADO lub osoba przez niego upoważniona.
3) W przypadku wystąpienia incydentu w podmiocie publicznym utrzymuje kontakt z CSIRT NASK i na bieżąco uzupełnia informacje wymagane przez podmioty krajowego systemu cyberbezpieczeństwa.
4) Sporządzanie raportu incydentu cybernetycznego zgodnie ze wzorem stanowiącym załącznik nr. 1 do niniejszej procedury i przekazanie go ADO bądź osobie przez niego upoważnionej.
5) Umieszczanie incydentu lub jego podejrzenia w rejestrze incydentów cybernetycznych zgodnie ze wzorem stanowiącym załącznik nr. 2 do niniejszej procedury.
6) Koordynowanie obsługi zgłaszanych incydentów cybernetycznych oraz wdrażanie działań naprawczych po wystąpieniu incydentu.
7) Regularnie, nie rzadziej niż 1 raz na miesiąc, przygotowanie materiałów merytorycznych do udostępniania na stronie internetowej jednostki, które pozwolą zapewnić osobom, na rzecz których jednostka realizuje zadanie publiczne, dostęp do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami.
8) Szkolenie i przeprowadzanie akcji edukacyjnych pracowników jednostki w zakresie zgłaszania i identyfikacji incydentów cybernetycznych oraz metod i sposobów przeciwdziałania oraz zapobiegania ich wystąpienia.
9) Niezwłocznie, najpóźniej w ciągu 2 godzin od zidentyfikowania informowanie IOD o wystąpieniu incydentu lub podejrzeniu wystąpienia incydentu, który narusza dane osobowe.

3. Zgłaszanie incydentów cybernetycznych

3.1 Pracownik, który zidentyfikuje bądź podejrzewa wystąpienie incydentu cybernetycznego, jest zobowiązany niezwłocznie zgłosić zdarzenie swojemu bezpośredniemu przełożonemu. Przełożony zgłasza fakt Administratorowi i Inspektorowi ochrony danych.

3.2 Do typowych przyczyn wystąpienia incydentów cybernetycznych należą:

1) klęski żywiołowe,
2) pożar,
3) zakłócenia w dostawie energii elektrycznej,
4) awaria sprzętu, w tym niestandardowe zachowanie komputerów,

5) błędy użytkowników np. udostępnienie danych osobom nieupoważnionym w formie elektronicznej czy wyjawienie haseł do systemów,
6) niewłaściwe wykorzystywanie zasobów informatycznych,
7) szkodliwe oprogramowanie,
8) próby omijania systemów zabezpieczeń,
9) nieautoryzowany dostęp,
10) zniszczenie lub kradzież urządzeń,
11) próby wyłudzania informacji,
12) ataki socjotechniczne.

3.3 Pracownik, który stwierdzi wystąpienie incydentu cybernetycznego bądź podejrzewa jego wystąpienie ma obowiązek zabezpieczyć dowody umożliwiające ustalenie przyczyn i skutków. Zaniechuje wszelkich działań i prób samodzielnego naprawiania skutków zdarzenia. Nie opuszcza miejsca zdarzenia do czasu otrzymania instrukcji postępowania od ADO, IOD lub Koordynatora ds. cyberbezpieczeństwa.

4. Analiza zgłoszonych incydentów cybernetycznych

4.1 Koordynator ds. cyberbezpieczeństwa we współpracy z ADO lub osobą przez niego upoważnioną analizuje otrzymane informacje pod względem przesłanek identyfikujących zaistnienie incydentu cybernetycznego oraz weryfikuje czy stanowi on incydent w podmiocie publicznym, który należy zgłosić do CSIRT NASK.

4.2 Czynniki brane pod uwagę przy analizie incydentu cybernetycznego:
1) Wpływ na ciągłość działania jednostki, w tym ciągłość realizacji zadań publicznych z wykorzystaniem systemów informatycznych.
2) Wpływ na dostępność, integralność i poufność danych.
3) Wpływ na działanie systemów informatycznych.

4.3 Analiza musi zawierać informacje:
1) Liczbę osób, na które miał wpływ incydent.
2) Zadania publiczne, na które incydent miał wpływ.
3) Zasięg geograficzny obszaru, którego dotyczy incydent.
4) Przyczynę zaistnienia incydentu, sposób jego przebiegu oraz skutki jego oddziaływania na systemy informacyjne podmiotu publicznego.

4.4 Komunikacja związana z analizą wystąpienia incydentu lub podejrzenia jego wystąpienia następuje poprzez:
1) Bezpośrednie spotkanie.
2) Kontakt telefoniczny.
3) Pocztą e-mail z wykorzystaniem zaszyfrowanych wiadomości. Hasło do zaszyfrowanego pliku przekazywane jest innym kanałem komunikacji.

4.5 Wszystkie ustalenia związane z analizą incydentu cybernetycznego należy odnotować w raporcie incydentu cybernetycznego stanowiącym załącznik nr. 1 do niniejszej Procedury.

4.6 Wszelkie zgromadzone dodatkowe ustalenia wynikające z analizy obsługiwanego incydentu cybernetycznego Koordynator ds. cyberbezpieczeństwa przekazuje do CSIRT NASK, uzupełniając wcześniejsze zgłoszenie.

5. Działania naprawcze i zabezpieczające po incydencie cybernetycznym

5.1 ADO lub osoba przez niego upoważniona wdraża ustalone wspólnie z Koordynatorem ds. cyberbezpieczeństwa działania naprawcze i zabezpieczające mające na celu ograniczenie skutków incydentu cybernetycznego.

Działania polegają w szczególności na:

1) Przywróceniu systemów informatycznych do pełnej funkcjonalności.
2) Dokonaniu niezbędnych zmian w systemach i urządzeniach np. zmiana haseł, ustawień na urządzeniach np. firewall, UTM.
3) Przeglądu i aktualizacji analizy ryzyka jednostki.
4) Przeglądu i aktualizacji planów ciągłości działania jednostki.
5) Przeglądu i aktualizacji procedur i polityk związanych z bezpieczeństwem informacji obowiązujących w jednostce.
6) Analizie incydentów cybernetycznych, które wystąpiły w jednostce o podobnym charakterze.
7) W przypadku incydentu cybernetycznego wynikającego z podatności systemu wykonanie skanowania podatności i/lub testów penetracyjnych.
8) W ciągu 14 dni od zakończenia obsługi incydentu cybernetycznego przeprowadzeniu szkolenia pracownikom uczestniczących w incydencie oraz w ciągu 30 dni przeprowadzeniu szkolenia/akcji edukacyjnej dla wszystkich pracowników.
9) W przypadku, gdy do incydentu cybernetycznego doszło z umyślnej woli pracownika, ADO może wszcząć w stosunku do niego postępowanie dyscyplinarne.

6. Szkolenia i akcje edukacyjne z zakresu cyberbezpieczeństwa

1) Wszyscy pracownicy jednostki powinni zostać przeszkoleni z niniejszej procedury i potwierdzić zaznajomienie się z nią na wykazie stanowiącym załączników nr. 3 do niniejszej procedury.
2) Wszyscy pracownicy powinni być przeszkoleni z zagrożeń cybernetycznych oraz metod przeciwdziałania i zapobiegania wystąpienia incydentów.
3) Po każdej zmianie procedury, powinno być przeprowadzone szkolenie w tym zakresie.
4) Koordynator ds. cyberbezpieczeństwa z własnej inicjatywy lub na wniosek ADO lub osoby przez niego upoważnionej przeprowadza wewnętrzne szkolenia i akcje edukacyjne o których mowa w pkt. 1 i 5.
5) Każde szkolenie wewnętrzne z zakresu cyberbezpieczeństwa oraz niniejszej procedury powinno być potwierdzone listą obecności bądź zaświadczeniem/certyfikatem imiennym dla uczestnika szkolenia.

7. Wykaz załączników

1) Załącznik nr. 1- Raport incydentu cybernetycznego.
2) Załącznik nr. 2- Rejestr incydentów cybernetycznych.
3) Załącznik nr. 3- Wykaz osób zapoznanych z Procedurą Zarządzania Incydentami Cybernetycznymi.

Załącznik nr. 1 do procedury

RAPORT INCYDENTU CYBERNETYCZNEGO

I. Informacje podstawowe	
Data	
Godzina	
Osoba zgłaszająca incydent	
Osoby zaangażowane lub odpytane w związku z incydentem	
Lokalizacja wykrycia incydentu (np. nr/nazwa pomieszczenia, stanowisko komputerowe, nazwa programu)	
II. Analiza incydentu cybernetycznego	
Zadania publiczne, na które miał wpływ incydent	
Liczba osób, na które miał wpływ incydent	
Zasięg geograficzny obszaru, którego dotyczy incydent	
Moment wystąpienia i wykrycia incydentu	
Przyczyna wystąpienia incydentu	☐ Podejrzana wiadomość e-mail ☐ Podatności ☐ Złośliwe oprogramowanie ☐ Próba oszustwa (Phishing, Vishing, Spoofing itd.) ☐ Nielegalne treści ☐ Kradzież, zgubienie nośnika informacji ☐ Błąd pracownika ☐ Inna ..... ** W przypadku wystąpienia incydentu w charakterze nielegalnych treści, zgłoszenie należy przesłać do zespołu NASK przez stronę internetową* https://dyzurnet.pl/
Źródło incydentu	
Przebieg zdarzenia	
Skutki oddziaływania incydentu na systemy informacyjne podmiotu publicznego	

Podjęte działania zapobiegawcze	

Podjęte działania naprawcze	
Czy doszło do naruszenia danych osobowych	☐ Tak ☐ Nie **W przypadku naruszenia danych osobowych podać nr. zgłoszenia z rejestru naruszeń .....*
W przypadku zgłaszania incydentu do CSIRT NASK należy dołączyć do raportu kopię zgłoszenia.	

....

Podpis Koordynatora ds. cyberbezpieczeństwa Podpis ADO

Załącznik nr.2 do procedury

REJESTR INCYDENTÓW CYBERNETYCZNYCH

Lp.	Data zgłoszenia	Zadanie publiczne na które miał wpływ incydent	Opis	Przyczyna wystąpienia incydentu	Podjęte działania naprawcze	Podjęte działania zapobiegawcze
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						
10.						

Załącznik nr. 3 do procedury

WYKAZ OSÓB ZAPOZNANYCH Z PROCEDURĄ ZARZĄDZANIA INCYDENTAMI CYBERNETYCZNYMI

Lp.	Imię i nazwisko	Podpis
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		
