ZARZĄDZENIE NR 636/2023
BURMISTRZA MIASTA I GMINY CHMIELNIK

z dnia 16 lutego 2023 r.

w sprawie wprowadzenia procedury zarządzania incydentami związanymi z bezpieczeństwem informacji i cyberbezpieczeństwem w Urzędzie Miasta i Gminy w Chmielniku

Na podstawie art. 30 ust. 1 i art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz. U. z 2023 r. poz. 40) § 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 (t.j. Dz. U. z 2017 r. poz. 2247 z późn. zm.), a także w oparciu o art. 22 Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2022 r. poz. 1863, 2666) zarządza się, co następuje:

§ 1. Wprowadza się Procedurę zarządzania incydentami związanymi z bezpieczeństwem informacji i cyberbezpieczeństwem w Urzędzie Miasta i Gminy w Chmielniku stanowiącą załącznik do niniejszego zarządzenia.

§ 2. Zarządzenie wchodzi w życie z dniem wydania.

Burmistrz Miasta i Gminy
Chmielnik

Paweł Wójcik

Załącznik do zarządzenia Nr 636/2023

Burmistrza Miasta i Gminy Chmielnik

z dnia 16 lutego 2023 r.

PROCEDURA ZARZĄDZANIA INCYDENTAMI ZWIĄZANYMI Z

BEZPIECZEŃSTWEM INFORMACJI I CYBERBEZPIECZEŃSTWEM W URZĘDZIE MIASTA I GMINY W CHMIELNIKU

I. Postanowienia ogólne, definicje

1. Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji oraz cyberbezpieczeństwem ma na celu zapewnienie ciągłości operacyjnej oraz ograniczenie wpływu przypadków naruszeń bezpieczeństwa zasobów informacyjnych na działalność Urzędu Miasta i Gminy w Chmielniku.

2. Podstawą prawną do opracowania i wdrożenia dokumentu jest:

a) art. 22 ust. 1 pkt 1 Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;

b) § 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. Incydent w podmiocie publicznym - incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny.

4. 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.

5. Inspektor Ochrony Danych - osoba wyznaczona przez Administratora Danych Osobowych, zwany dalej „IOD".

6. Administrator Danych Osobowych „ADO" – Gmina Chmielnik reprezentowana przez Burmistrza Miasta i Gminy Chmielnik.

II. 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.).

III. Zakres obowiązywania procedury zarządzania incydentami związanymi z bezpieczeństwem informacji oraz cyberbezpieczeństwem

1. Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji oraz cyberbezpieczeństwem obowiązuje w Urzędzie Miasta i Gminy w Chmielniku.

IV. Zgłaszanie incydentów

1. W przypadku ujawnienia incydentu pracownik niezwłocznie powiadamia o tym fakcie IOD, ADO oraz informatyka zatrudnione w urzędzie. 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;

b) jednostka organizacyjna lub nazwa podmiotu zewnętrznego;

c) miejsce i datę wystąpienia incydentu;

d) opis incydentu w sposób adekwatny do posiadanej wiedzy i umiejętności zgłaszającego.

3. Brak umiejętności poprawnego rozpoznania incydentu przez osobę zgłaszającą nie może być przyczyną zaniechania zgłoszenia.

V. Podejmowanie działań w związku ze zgłaszanymi incydentami związanymi z bezpieczeństwem informacji oraz cyberbezpieczeństwem.

1. Zgłoszenie incydentu rejestrowane jest przez informatyka urzędu w rejestrze incydentów związanych z bezpieczeństwem informacji i cyberbezpieczeństwem. 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.

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, informatycy urzędu podejmują 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 incydencje zawiadamiany jest właściwy CSIRT NASK (Naukowa i Akademicka Sieć Komputerowa - Państwowego Instytutu Badawczego ul. Kolska 12, 01-045 Warszawa)

6. Zgłoszenia do CSIRT NASK przekazywane są w sposób elektroniczny. Procedura zgłoszeń opisana jest pod adresem internetowym https://incydent.cert.pl https://incydent.cert.pl/#!/lang=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 z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

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.

VI. 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.:

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 IOD i informatyka urzędu (jeżeli naruszenie ma związek z systemami informatycznymi).

Każdy pracownik, bez względu na to, czy zostało mu wydane upoważnienie do przetwarzania danyc osobowych, czy tylko i wyłącznie zgoda na przebywanie w obszarze przetwarzania, jest zobowiązany do zgłoszenia swojego podejrzenia Inspektorowi Ochrony Danych oraz najwyższemu kierownictwu

Względem pracownika, który nie podejmuje ww. czynności, i bagatelizuje zdarzenie, co do którego można mieć podejrzenie, iż wystąpił incydent naruszenia danych osobowych, może zostać zastosowane postępowanie dyscyplinarne w trybie art. 52 Kodeksu Pracy.

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 IOD oraz ADO.

4. Notatka jest rejestrowana przez IOD i przechowywana w teczce „Rejestr naruszeń ochrony danych osobowych" prowadzonym zgodnie z art. 33 ust. 5 RODO. i sporządzany jest przez Inspektora Ochrony Danych „Protokół uchybienia/naruszenia" –stanowiący załącznik nr 1 do niniejszej Procedury.

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.

6. Zakwalifikowanie zgłoszenia incydentu jako „fałszywy alarm" kończy postepowanie o czym IOD informuje zgłaszającego.

7. W przypadku zakwalifikowania zdarzenia jako naruszenie ochrony danych osobowych, które skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych, ADO bez zbędnej zwłoki, nie później niż w terminie 72 godzin od stwierdzenia naruszenia powiadamia Urząd Ochrony Danych Osobowych.

8. Zgłoszenia do UODO przekazywane są w sposób elektroniczny. Procedura zgłoszeń opisana jest pod adresem internetowym

https://uodo.gov.pl/pl/525/2582

https://www.biznes.gov.pl/pl/opisy-procedur/-/proc/889

9. W przypadku incydentów dotyczących danych osobowych w zakresie wymiaru sprawiedliwości, Administrator ma jednocześnie na uwadze procedurę zgłoszenia naruszenia zgodną Zgodnie z art. 30 Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. Zgodnie z art. 44 Ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

10. IOD podejmuje również działania zabezpieczające i naprawcze zmierzające do niwelowania skutków powstałych w wyniku incydentu, jak również działania zaradcze dla uniknięcia wystąpienia podobnych incydentów w przyszłości.

11. Jeżeli zgłoszony incydent naruszenia ochrony danych osobowych może spowodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, a stosowane w Urzędzie techniczne i organizacyjne środki ochrony danych nie eliminują tego ryzyka, IOD bez zbędnej zwłoki informuje ADO o konieczności zawiadomienia osób , których dane dotyczą o takim naruszeniu i przygotowuje stosowne dokumenty do podpisu.

12. Jeżeli dojdzie do naruszenia ochrony danych osobowych i zdarzenie to może spowodować wysokie ryzyko naruszenia praw lub wolności osób, których dane dotyczą, Administrator powiadamia o tym fakcie te osoby.

1) Administrator informuje osoby fizyczne, których naruszenie dotyczy mając jednocześnie na uwadze zasadę przejrzystości – komunikat powinien być jasny, prosty, zrozumiały dla jego odbiorców.

2) Komunikat, zawiera:

   a) oznaczenie Administratora uwzględniając dane kontaktowe,

   b) opis konsekwencji, jakie naruszenie mogło spowodować,

   c) działania zaradcze, jakie Administrator podejmie w związku z incydentem.

3) W celu zawiadomienia osób fizycznych, których naruszenie dotyczy, Administrator korzysta ze wzoru „Zgłoszenie naruszenia osobie, której dane dotyczą" –stanowiący załącznik nr 2 do niniejszej Procedury.

4) Komunikat, o którym mowa powyżej nie będzie konieczny jeśli:

   a) Administrator wdrożył i zastosował takie środki techniczne i organizacyjne względem danych osobowych, których dotyczy naruszenie, że dostęp osób nieuprawnionych jest niemożliwy np.: szyfrowanie,

   b) Administrator zastosował również środki eliminujące prawdopodobieństwo wystąpienia wysokiego ryzyka naruszenia praw lub wolności osób, których dane dotyczą,

   c) Wymaga niewspółmiernie dużego wysiłku po stronie Administratora – wtedy Administrator wydaje komunikat publiczny lub stosuje inny równie skuteczny środek, za pomocą którego osoby zostaną w sposób skuteczny poinformowane o fakcie zaistnienia incydentu.

W przypadku incydentów dotyczących danych osobowych w zakresie wymiaru sprawiedliwości, Administrator ma jednocześnie na uwadze procedurę zgłoszenia naruszenia zgodną z Zgodnie z art. 31 Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r i Zgodnie z art. 45 Ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości

13. W przypadku stwierdzenia działań zamierzonych, przy jednoczesnym zidentyfikowaniu sprawcy incydentu dotyczącego naruszenia bezpieczeństwa przetwarzania danych osobowych ADO podejmuje decyzję dotyczącą wyciągnięcia ewentualnych konsekwencji dyscyplinarnych wobec sprawcy incydentu. Jednocześnie, w zależności od wagi incydentu, mogą być powiadomione organa ścigania.

Załącznik Nr 1 do Załącznika Nr 1

PROTOKÓŁ
UCHYBIENIA / NARUSZENIA [1]

DATA PROTOKOŁU:	
NAZWA ORGANIZACJI:	
IMIĘ I NAZWISKO OSOBY STWIERDZAJĄCEJ INCYDENT:	

OPIS INCYDENTU:

ZAGADNIENIE	OPIS
Opis, na czym polegał incydent	
Data i godzina przyjęcia zgłoszenia o incydencie	
Osoba zgłaszająca incydent	
Charakter incydentu	
Czas trwania incydentu	
Przyczyny wystąpienia incydentu	
Kategorie osób, których incydent dotyczy	
Ilość osób, których incydent dotyczy	
Kategorie danych osobowych, których incydent dotyczy	
Możliwe konsekwencje wystąpienia incydentu	
Ryzyko naruszenia praw i wolności	
Czy osoby, których dane dotyczą zostały powiadomione o incydencie?	
Czy organ nadzorczy będzie powiadomiony o naruszeniu?	
Jeśli organ nadzorczy nie będzie powiadomiony o naruszeniu, podać przyczynę, dla której administrator uznaje ryzyko naruszenia praw i wolności osób fizycznych, których naruszenie dotyczy za mało prawdopodobne	
Środki naprawcze zaproponowane przez osobę odpowiedzialną za rejestrowanie incydentów	

podpis osoby stwierdzającej naruszenie	Jako Administrator przyjmuję protokół przedstawiony przez osobę stwierdzającą naruszenie: podpis Administratora

1) niepotrzebne skreślić

[1] **niepotrzebne skreślić**

Załącznik Nr 2 do Załącznika Nr 1

ZGŁOSZENIE NARUSZENIA

OSOBIE, KTÓREJ DANE DOTYCZĄ

DATA PROTOKOŁU:	
NAZWA ORGANIZACJI:	
IMIĘ I NAZWISKO OSOBY STWIERDZAJĄCEJ INCYDENT:	

STWIERDZENIE NARUSZENIA:

ZAGADNIENIE	OPIS
Punkt kontaktowy, w ramach którego można uzyskać więcej informacji	
Opis możliwych konsekwencji wynikających z naruszenia ochrony danych osobowych	
Opis środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków	
Charakter naruszenia	

Podpis i pieczęć Administratora