ZARZĄDZENIE Nr 33/2022
WÓJTA GMINY Bądkowo
z dnia 12 maja 2022 r.

w sprawie wprowadzenia procedury zarządzania incydentami związanymi z bezpieczeństwem informacji i cyberbezpieczeństwem w Urzędzie Gminy w Bądkowie.

Na podstawie art. 30 ust. 1 i art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2022 r. poz. 559 z późn. zm.), § 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 (Dz. U. z 2020 r. poz. 1369 z późn. zm.)

zarządza się, co następuje:

§ 1

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

§ 2

Wykonanie zarządzenia powierza się Sekretarzowi Gminy.

§ 3

Zarządzenie wchodzi w życie z dniem podpisania.

Signature Not Verified
Dokument podpisany przez Ryszard Stępkowski
Data: 2022.05.18 11:25:54 CEST

Załącznik do Zarządzenia nr 33/2022
Wójta Gminy Bądkowo
z dnia 12 maja 2022 r.

PROCEDURA ZARZĄDZANIA INCYDENTAMI ZWIĄZANYMI Z BEZPIECZEŃSTWEM INFORMACJI I CYBERBEZPIECZEŃSTWEM W URZĘDZIE GMINY BĄDKOWO

Spis treści

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 Gminy w Bądkowie.
2. Podstawą prawną do opracowania i wdrożenia dokumentu jest:
   a) art. 22 ust. 1 pkt 1 Ustawy o krajowym systemie cyberbezpieczeństwa z dnia 5 lipca 2018 r.;
   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 Bądkowo reprezentowana przez Wójta.

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 Gminy Bądkowo.

IV. Zgłaszanie incydentów

1. W przypadku ujawnienia incydentu pracownik niezwłocznie powiadamia o tym fakcie Inspektora Ochrony Danych, Administratora Danych Osobowych oraz informatyków zatrudnionych 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 informatyków 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 wykonują informatycy 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. 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.
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 Inspektora Ochrony Danych i informatyków 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.
4. Notatka jest rejestrowana przez IOD i przechowywana w teczce „Rejestr naruszeń ochrony danych osobowych”
5. Zgłoszenia są rejestrowane w „Rejestrze naruszeń ochrony danych osobowych” prowadzonym zgodnie z art. 33 ust. 5 RODO.
6. 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.
7. Zakwalifikowanie zgłoszenia incydentu jako „fałszywy alarm” kończy postepowanie o czym IOD informuje zgłaszającego.

8. 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.
9. Zgłoszenia do UODO przekazywane są w sposób elektroniczny. Procedura zgłoszeń opisana jest pod adresem internetowym https://uodo.gov.pl/pl/134/233
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 zawiadomienie osób, których dane dotyczą wymagałoby niewspółmiernie dużego wysiłku, IOD przygotowuje publiczny komunikat lub wybiera inny stosowny środek, za pomocą którego zawiadomienie zostanie tym osobom przekazane.
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.

Signature Not Verified
Dokument podpisany przez Ryszard Stępkowski
Data: 2022.05.18 11:26:22 CEST