BURMISTRZ DRAWNA
73-220 DRAWNO
ul. Kościelna 3
woj. zachodniopomorskie
tel. (95) 768-20-31

ZARZĄDZENIE NR 22/2021
BURMISTRZA DRAWNA
z dnia 1 marca 2021r.

w sprawie wprowadzenia Procedury zarządzania incydentami związanymi z bezpieczeństwem informacji i cyberbezpieczeństwem w Urzędzie Miejskim w Drawnie i gminnych jednostkach organizacyjnych

Na podstawie art. 22 ust. 1 pkt. 1 ustawy z dnia 5 lipca 2018r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369 z późn. zm.) **zarządzam, co następuje:**

§1. Wprowadza się Procedurę zarządzania incydentami związanymi z bezpieczeństwem informacji i cyberbezpieczeństwem w Urzędzie Miejskim w Drawnie i gminnych jednostkach organizacyjnych, stanowiącą załącznik do niniejszego Zarządzenia.

§ 2. Wykonanie Zarządzenia powierza się Inspektorowi Ochrony Danych, Administratorowi Systemów Informatycznych, kierownikom referatów i kierownikom gminnych jednostek organizacyjnych.

§ 3. 1. Zobowiązuje się wszystkich pracowników Urzędu Miejskiego w Drawnie do zapoznania się z niniejszą Procedurą

2. Pisemne oświadczenie o zapoznaniu się i przestrzeganiu postanowień Procedury należy złożyć do Inspektora Ochrony Danych.

§ 4. Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ DRAWNA
mgr inż. Andrzej Chmielewski

Załącznik
do Zarządzenia nr 22/2021
Burmistrza Drawna
z dnia 1 marca 2021r.

PROCEDURA ZARZĄDZANIA INCYDENTAMI ZWIĄZANYMI Z BEZPIECZEŃSTWEM INFORMACJI I CYBERBEZPIECZEŃSTWEM W URZĘDZIE MIEJSKIM W DRAWNIE I GMINNYCH JEDNOSTKACH ORGANIZACYJNYCH

Zatwierdził(a): Dnia 01.03.2021	BURMISTRZ DRAWNA mgr inż. Andrzej Chmielewski ..... Podpis administratora danych

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 Miejskiego w Drawnie oraz gminnych jednostek organizacyjnych.

2. Podstawą prawną do opracowania i wdrożenia dokumentu jest:

1) art. 22 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;
2) § 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 (Naukowa i Akademicka Sieć Komputerowa - Państwowego Instytutu Badawczego ul. Kolska 12, 01-045 Warszawa).

5. Inspektor Ochrony Danych – osoba wyznaczona przez Administratora Danych Osobowych, odpowiedzialna za zapewnienie prawidłowości przetwarzania danych osobowych zwany dalej „IOD".

6. Administrator Systemów Informatycznych – osoba wyznaczona przez Administratora Danych Osobowych, odpowiedzialna za sprawność i konserwację oraz wdrożenie technicznych zabezpieczeń systemów informatycznych zwany dalej „ASI".

7. Administrator Danych Osobowych – Urząd Miejski w Drawnie reprezentowany przez Burmistrza Drawna zwany dalej „ADO".

8. Jednostki organizacyjne Gminy Drawno – Drawieński Ośrodek Kultury, Biblioteka Publiczna, Środowiskowy Dom Samopomocy, Miejsko-Gminny Ośrodek Pomocy Społecznej, Przedszkole Miejskie, Szkoła Podstawowa, zwane dalej „gminnymi jednostkami organizacyjnymi".

II. Kategorie incydentów.

1. Incydent bezpieczeństwa informacji oraz cyberbezpieczeństwa to zdarzenie, którego skutkiem jest lub może być naruszenie bezpieczeństwa aktywów informacyjnych oraz który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny. Jego przyczyną może być:

1) zdarzenie losowe zewnętrzne (np. klęski żywiołowe, pożary, zakłócenia w dostawie energii elektrycznej, itp.), którego wystąpienie może spowodować zniszczenie lub

uszkodzenie infrastruktury informatycznej albo dokumentacji papierowej oraz zakłócenie ciągłości pracy systemów nie powodując naruszenia poufności danych;
2) 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;
3) świadome i celowe działania mające na celu naruszenie poufności zasobów informacyjnych, w tym poufności danych.

2. Incydentami bezpieczeństwa informacji w szczególności są:

1) naruszenie poufności, to jest ujawnienie informacji niepowołanym osobom;
2) naruszenie integralności, to jest zniszczenie, uszkodzenie lub przekłamanie informacji;
3) naruszenie dostępności, to jest braku dostępu do danych przez uprawnionych użytkowników.

3. Przyczyny incydentów bezpieczeństwa informacji oraz cyberbezpieczeństwa mogą dotyczyć:

1) niewłaściwego wykorzystania zasobów informatycznych lub niewłaściwe postępowanie z dokumentacją papierową;
2) działania szkodliwego oprogramowania;
3) próby omijania systemów zabezpieczeń;
4) nieautoryzowanego dostępu do systemów, aplikacji i dokumentów;
5) zniszczenia lub kradzieży urządzeń wykorzystywanych do przetwarzania i przechowywania informacji;
6) zniszczenia lub kradzieży nośników danych;
7) próby wyłudzenia informacji;
8) ataków socjotechnicznych, ataków z wykorzystaniem technik zagrażających poufności, integralności lub dostępności informacji;
9) nieprawidłowości w zakresie zabezpieczenia przechowywania danych, w tym danych osobowych;
10) naruszenia zasad obowiązujących w Urzędzie Miejskim w Drawnie oraz gminnych jednostkach organizacyjnych dotyczących bezpieczeństwa informacji, w tym danych osobowych.

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

Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji oraz cyberbezpieczeństwem obowiązuje w Urzędzie Miejskim w Drawnie oraz gminnych jednostkach organizacyjnych wymienionych w rozdziale I pkt 8.

IV. Zgłaszanie incydentów związanych z bezpieczeństwem informacji oraz cyberbezpieczeństwem w Urzędzie Miejskim w Drawnie.

1. W przypadku ujawnienia incydentu pracownik Urzędu niezwłocznie powiadamia o tym fakcie Inspektora Ochrony Danych, który jednocześnie pełni funkcję osoby odpowiedzialnej za utrzymywanie kontaktów z właściwym zespołem CSIRT NASK oraz powiadamia Administratora Systemów Informatycznych (kiedy incydent dotyczy systemów

komputerowych.) Zgłoszenie następuje telefonicznie, mailowo lub osobiście. Dane kontaktowe IOD oraz ASI znajdują się na stronie podmiotowej Biuletynu Informacji Publicznej Urzędu Miejskiego w zakładce „Ochrona danych osobowych (RODO)". Zgłoszenie należy następnie potwierdzić szczegółową notatką służbową, którą pracownik przekazuje do IOD poprzez swojego bezpośredniego przełożonego lub bezpośrednio do IOD w przypadku pracowników zatrudnionych na samodzielnych stanowiskach.

2. Notatka musi zawierać następujące informacje:

1) imię i nazwisko osoby zgłaszającej;
2) stanowisko oraz komórka organizacyjna Urzędu;
3) dokładne miejsce oraz datę wystąpienia incydentu;
4) 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.

4. W przypadku dłuższej nieobecności IOD incydent należy zgłosić do ASI w sposób określony w pkt. 1.

V. Zgłaszanie incydentów związanych z cyberbezpieczeństwem przez gminne jednostki organizacyjne.

1. W przypadku stwierdzenia incydentu krytycznego lub incydentu w podmiocie publicznym przez pracowników gminnych jednostek organizacyjnych wyszczególnionych w rozdziale I pkt 8 należy niezwłocznie telefonicznie, mailowo lub osobiście powiadomić o tym fakcie Administratora Danych Osobowych jednostki a następnie Inspektora Ochrony Danych, który jednocześnie pełni funkcję osoby odpowiedzialnej za utrzymywanie kontaktów z właściwym zespołem CSIRT NASK. Fakt ten należy zgłosić do IOD mailowo i potwierdzić oficjalnym pismem opatrzonym podpisem kierownika/dyrektora jednostki.

2. W zgłoszeniu należy podać wszystkie informacje zgodnie z treścią art. 23 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

3. W przypadku dłuższej nieobecności Inspektora Ochrony Danych, który jednocześnie pełni funkcję osoby odpowiedzialnej za utrzymywanie kontaktów z właściwym zespołem CSIRT NASK zgłoszenia należy dokonywać do Administratora Systemów Informatycznych w sposób opisany w pkt. 1. Dane kontaktowe ASI znajdują się na stronie podmiotowej Biuletynu Informacji Publicznej Urzędu Miejskiego w zakładce „Ochrona danych osobowych (RODO)".

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

1. Zgłoszenie incydentu rejestrowane jest przez IOD i przechowywane w teczce „Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji oraz 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 IOD, który jednocześnie pełni funkcję osoby odpowiedzialnej za utrzymywanie kontaktów z właściwym zespołem CSIRT NASK w porozumieniu z ASI oraz informatykami zatrudnionymi w gminnych jednostkach organizacyjnych (jeżeli zgłoszenie dotyczy naruszenia cyberbezpieczeństwa w tych jednostkach).

2. Przy ocenie istotności incydentu pod uwagę brane są następujące czynniki:

1) powstałe szkody będące wynikiem incydentu;
2) wpływ incydentu na działanie systemów;
3) wpływ incydentu na ciągłość działania Urzędu Miejskiego w Drawnie lub gminnych jednostek organizacyjnych;
4) koszty usunięcia skutków incydentu;
5) szacowany czas naprawy skutków wywołanych incydentem;
6) oszacowanie zasobów koniecznych do przywrócenia ciągłości działania systemów.

3. Zakwalifikowanie zgłoszenia incydentu jako „fałszywy alarm" kończy postępowanie, o czym IOD informuje ADO oraz zgłaszającego.

4. W przypadku zakwalifikowania zdarzenia jako incydentu związanego z bezpieczeństwem informacji lub cyberbezpieczeństwem, IOD, który jednocześnie pełni funkcję osoby odpowiedzialnej za utrzymywanie kontaktów z właściwym zespołem CSIRT NASK wspólnie z ASI podejmuje działania zabezpieczające i naprawcze zmierzające do zniwelowania szkód powstałych w wyniku incydentu, jak również działania zaradcze dla uniknięcia wystąpienia podobnych incydentów w przyszłości.

5. Gminne jednostki organizacyjne o których mowa w rozdziale I pkt 8 we własnym zakresie podejmują działania naprawcze zmierzające do zniwelowania szkód powstałych w wyniku incydentu.

6. IOD zostaje poinformowany o wynikach analizy incydentu oraz podjętych działaniach naprawczych. W przypadku nieobecności IOD, powiadamia się ASI.

7. W przypadku stwierdzenia incydentu w podmiocie publicznym lub incydentu krytycznego IOD, który jednocześnie pełni funkcję osoby odpowiedzialnej za utrzymywanie kontaktów z właściwym zespołem CSIRT NASK lub ASI (w przypadku nieobecności IOD) nie później niż w ciągu 24 godzin od momentu wykrycia zgłasza incydent do właściwego CSIRT NASK.

8. 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).

9. 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.

10. W przypadku stwierdzenia działań zamierzonych, przy jednoczesnym zidentyfikowaniu sprawcy incydentu dotyczącego naruszenia bezpieczeństwa informacji oraz cyberbezpieczeństwa ADO podejmuje decyzję dotyczącą wyciągania ewentualnych

konsekwencji dyscyplinarnych wobec sprawcy incydentu. Jednocześnie, w zależności od wagi incydentu mogą być powiadamiane organy ścigania.

VII. 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).

2. Działania podejmowane w związku ze zgłaszanymi incydentami związanymi z naruszeniem bezpieczeństwa przetwarzania danych osobowych opisane są w „Regulaminie wewnętrznych procedur postępowania w sytuacji wystąpienia naruszenia ochrony danych osobowych" stanowiący element Polityki Bezpieczeństwa Informacji w Urzędzie Miejskim w Drawnie oraz w gminnych jednostkach organizacyjnych.