Zarządzenie Nr 91/2023
Burmistrza Miasta i Gminy Prabuty
z dnia 4 lipca 2023 r.

w sprawie powołania osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa oraz wprowadzenia procedury reagowania na incydenty bezpieczeństwa komputerowego.

Na podstawie art. 33 ust. 3 i 5 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2023 r. poz. 40 z późn. zm.) art. 21 ust. 1 i 3 i art. 22 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913 z późn. zm.) zarządzam, co następuje:

§ 1.

Wyznaczam Pana Dariusza Pietkiewicza – Inspektora ds. obsługi informatycznej urzędu do utrzymywania kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa w zakresie zadań publicznych zależnych od systemów informacyjnych, realizowanych przez Urząd Miasta i Gminy w Prabutach.

§ 2.

Wyznaczona osoba jest odpowiedzialna za:
a) niezwłoczne zgłaszanie incydentów w Urzędzie Miasta i Gminy w Prabutach do CSIRT NASK, nie później jednak, niż w ciągu 24 godzin od momentu ich wykrycia,
b) zarządzanie incydentem w Urzędzie Miasta i Gminy w Prabutach,
c) współpracę w obsłudze incydentu w Urzędzie Miasta i Gminy w Prabutach z CSIRT NASK z uwzględnieniem przekazywania niezbędnych danych, w tym danych osobowych,
d) zapewnienie osobom, na rzecz których zadanie publiczne jest realizowane, dostępu do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami.

§ 3.

Zgłoszenie, zawierające imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby wyznaczonej, zostanie przesłane do właściwego CSIRT NASK.

§ 4.

Wprowadza się procedurę zarządzania incydentami związanymi z bezpieczeństwem informacji i cyberbezpieczeństwem w Urzędzie Miasta i Gminy Prabuty w brzmieniu stanowiącym załącznik Nr 1 do zarządzenia.

§ 5.

Nadzór nad realizacją zarządzenia powierzam Sekretarzowi Miasta i Gminy Prabuty.

§ 6.

Zarządzenie wchodzi w życie z dniem podpisania.

§ 7.

Traci moc zarządzenie Nr 79/2023 Burmistrza Miasta i Gminy Prabuty z dnia 9 czerwca 2023 r. w sprawie powołania osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa oraz wprowadzenia procedury reagowania na incydenty bezpieczeństwa komputerowego.

Załącznik nr 1 do Zarządzenia Nr 91/2023
Burmistrza Miasta i Gminy Prabuty
z dnia 4 lipca 2023 roku

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

§ 1

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.

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 zwanego dalej „IOD”

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

7. Administrator Danych Osobowych – Burmistrz Miasta i Gminy Prabuty.

§2

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:

a) 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;

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) świadome i celowe działania mające na celu naruszenie poufności zasobów informacyjnych, w tym poufności danych.

2. Incydentami bezpieczeństwa informacji w szczególności są:

a) naruszenie poufności, to jest ujawnienie informacji niepowołanym osobom;

b) naruszenie integralności, to jest zniszczenie, uszkodzenie lub przekłamanie informacji;

c) naruszenie dostępności, to jest braku 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.) 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 Urzędzie dotyczących bezpieczeństwa informacji, w tym danych osobowych.

§ 3

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 Prabuty.

§ 4

Zgłaszanie incydentów związanych z bezpieczeństwem informacji oraz cyberbezpieczeństwem

1. W przypadku ujawnienia incydentu pracownik niezwłocznie powiadamia o tym fakcie Administratora Systemów Informatycznych. Zgłoszenie następuje telefonicznie. Telefoniczne zgłoszenie należy następnie potwierdzić szczegółową notatką służbową.

2. Notatka musi zawierać następujące informacje:

a) Imię i nazwisko osoby zgłaszającej;

b) stanowisko oraz komórka organizacyjna Urzędu;

c) dokładne miejsce oraz 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.

§ 5

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 dla Urzędu Miasta i Gminy Prabuty”. 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 ASI.

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 ASI informuje zgłaszającego.

4. W przypadku zakwalifikowania zdarzenia jako incydentu związanego z bezpieczeństwem informacji lub cyberbezpieczeństwem, ASI podejmuje działania zabezpieczające i naprawcze zmierzające do zniwelowania szkód powstałych w wyniku incydentu.

5. Poinformowany o wynikach analizy incydentu oraz podjętych działaniach naprawczych ASI informuje ADO.

6. W przypadku stwierdzenia incydentu w podmiocie publicznym lub incydentu krytycznego ASI nie później niż w ciągu 24 godzin od momentu wykrycia zgłasza incydent do właściwego CSIRT NASK (Naukowa i Akademicka Sieć Komputerowa - Państwowego Instytutu Badawczego ul. Kolska 12, 01-045 Warszawa).

7. 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).

8. W zgłoszeniu przekazuje się informacje zgodnie z formularzem oraz zgodnie z treścią art. 23 ust. 1 Ustawy o krajowym systemie cyberbezpieczeństwa z dnia 5 lipca 2018 r.

9. 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.

Załącznik Nr 1 do Procedury

RAPORT O INCYDENCIE BEZPIECZEŃSTWA INFORMACJI

Dane osoby sporządzającej raport:

Imię i nazwisko: …… Stanowisko służbowe: …….

Sposób postępowania osób wyznaczonych do reagowania na incydenty bezpieczeństwa w sieci komputerowej:

Komu zgłoszono incydent: ……Data i godzina zgłoszenia: ……

Podpis osoby zgłaszającej: ……

Informacje o incydencie:

Data i czas zajścia incydentu: …… Data i czas wykrycia incydentu: ……
Data i czas zgłoszenia incydentu: ……

Dokładny opis przebiegu incydentu/ wpływu incydentu na realizację zadań publicznych/ podjęte działania/ zabezpieczenie materiału dowodowego:

……

……

……

……

Opis rozwiązania problemu/ koszty odtworzenia:

……

……

……

……..
podpis osoby sporządzającej raport