ZARZĄDZENIE NR ORG.120.44.2022
Wójta Gminy Baboszewo
z dnia 01 września 2022 r.

w sprawie wprowadzenia Procedury zarządzania incydentami cyberbezpieczeństwa w Urzędzie Gminy w Baboszewie

Na podstawie art. 33 ust. 1 ustawy o samorządzie gminnym (Dz.U. 2022 r. poz. 559 z późn. zm.) w związku z art. 22 ust. 1 pkt 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2022 r. poz. 1863 z późn. zm.) zarządzam, co następuje:

§1

Wprowadzam Procedurę zarządzania incydentami cyberbezpieczeństwa w Urzędzie Gminy w Baboszewie, która stanowi załącznik do niniejszego zarządzenia.

§2

Zobowiązuję wszystkich pracowników do zapoznania się niniejszą Procedurą.

§3

Wykonanie niniejszego zarządzenia powierza się Sekretarzowi Gminy Baboszewo oraz Kierownikowi Referatu Organizacyjnego.

§4

Zarządzenie wchodzi w życie z dniem podjęcia.

WÓJT

mgr inż. Bogdan Janusz Pietruszewski

Załącznik do
Zarządzenia Nr ORG.120.44.2022
Wójta Gminy Baboszewo
z dnia 01 września 2022 r.

PROCEDURA ZARZĄDZANIA INCYDENTAMI CYBERBEZPIECZEŃSTWA W URZĘDZIE GMINY W BABOSZEWIE

§1
Postanowienia ogólne

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. Procedura została opracowana i wdrożona na podstawie art. 22 ust.1 pkt 1 Ustawy o krajowym systemie cyberbezpieczeństwa z dnia 05 lipca 2018 r.

§2
Definicje

1. Incydent w podmiocie publicznym - incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny.
2. 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.
3. Osoby odpowiedzialne za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa – osoby wyznaczone przez Administratora Danych Osobowych.
4. Inspektor Ochrony Danych – osoba wyznaczona przez Administratora Danych Osobowych zwanego dalej „IOD".
5. Administrator Systemów Informatycznych – osoba wyznaczona przez Administratora Danych Osobowych, odpowiedzialna za sprawność i konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych zwanego dalej „ASI".
6. Administrator Danych Osobowych – Wójt Gminy Baboszewo oraz Kierownik jednostki organizacyjnej Gminy Baboszewo.
7. Urząd – Urząd Gminy w Baboszewie.
8. Jednostki organizacyjne Gminy Baboszewo zwane dalej jednostkami – Zakład Wodociągów i Kanalizacji w Baboszewie, Gminny Ośrodek Pomocy Społecznej, Gminna Biblioteka Publiczna.

§3
Kategorie incydentów i ich przyczyny

1. Incydent cyberbezpieczeństwa zwany dalej incydentem to zdarzenie, którego skutkiem jest lub może być naruszenie bezpieczeństwa aktywów informacyjnych oraz powodujące lub mogące 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 cyberbezpieczeństwo 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 cyberbezpieczeństwa mogą dotyczyć:
   1) niewłaściwego wykorzystywania 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 wyłudzeń 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 dotyczących bezpieczeństwa informacji, w tym danych osobowych.

§4
Zakres obowiązywania procedury

Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji oraz cyberbezpieczeństwem obowiązuje w Urzędzie Gminy w Baboszewie oraz dotyczy również jednostek organizacyjnych Gminy Baboszewo, o których mowa w §2 ust. 8.

§5
Zgłaszanie incydentów cyberbezpieczeństwa

1. W przypadku ujawnienia incydentu pracownik niezwłocznie powiadamia o tym fakcie przynajmniej jedną z osób wyznaczonych do utrzymywania kontaktów z podmiotami krajowego systemy cyberbezpieczeństwa, które powiadamiają Administratora Systemów Informatycznych (kiedy incydent dotyczy systemów komputerowych) oraz Inspektora Ochrony Danych.
2. Zgłoszenie następuje telefonicznie.
3. Telefoniczne zgłoszenie należy następnie potwierdzić szczegółową notatką służbową, którą przekazuje się do osób odpowiedzialnych za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa poprzez swojego bezpośredniego przełożonego lub bezpośrednio w przypadku pracowników zatrudnionych na samodzielnych stanowiskach.
4. 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.
5. Brak umiejętności poprawnego rozpoznania incydentu przez osobę zgłaszającą nie może być przyczyną zaniechania zgłoszenia.
6. W przypadku dłuższej nieobecności osób odpowiedzialnych za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa incydent należy zgłosić do ASI lub IOD w sposób określony w niniejszym paragrafie.

§6
Podejmowanie działań w związku ze zgłaszanymi incydentami związanymi z bezpieczeństwem informacji oraz cyberbezpieczeństwem

1. Zgłoszenie incydentu rejestrowane jest przez osoby odpowiedzialne za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa i przechowywane w teczce „Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji oraz cyberbezpieczeństwem dla Urzędu Gminy w Baboszewie".
2. Osoba zgłaszająca incydent powinna w miarę możliwości zabezpieczyć materiał dowodowy (np. zrzut ekranu monitora, zdjęcie niezabezpieczonych materiałów zawierających dane osobowe itp.).
3. 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.
4. Powyższe działania wykonuje osoba odpowiedzialna za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa w porozumieniu z ASI oraz IOD.
5. 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;
   4) koszty usunięcia skutków incydentu;

5) szacowany czas naprawy skutków wywołanych incydentem;
6) oszacowanie zasobów koniecznych do przywrócenia ciągłości działania systemów.

6. Zakwalifikowanie zgłoszenia incydentu jako „fałszywy alarm" kończy postępowanie, o czym osoba odpowiedzialna za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa informuje zgłaszającego.
7. W przypadku zakwalifikowania zdarzenia jako incydentu związanego z bezpieczeństwem informacji lub cyberbezpieczeństwem, osoby odpowiedzialne za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa oraz IOD wspólnie z ASI podejmuje działania zabezpieczające i naprawcze zmierzające do zniwelowania szkód powstałych w wyniku incydentu.
8. Poinformowany o wynikach analizy incydentu oraz podjętych działaniach naprawczych IOD informuje ADO. W przypadku nieobecności IOD, Administratora powiadamia ASI.
9. W przypadku stwierdzenia incydentu w podmiocie publicznym lub incydentu krytycznego osoba wskazana do kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, nie później niż w ciągu 24 godzin od momentu wykrycia zgłasza incydent do właściwego CSIRT NASK.
10. 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).
11. 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.
12. 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.

WÓJT

mgr inż. Bogdan Janusz Pietruszewski