ZARZĄDZENIE NR 72/2022
WÓJTA GMINY KOBYLANKA
z dnia 24 czerwca 2022 r.

w sprawie wprowadzenia w Urzędzie Gminy Kobylanka oraz gminnych jednostkach organizacyjnych procedury zarządzania incydentami związanymi z bezpieczeństwem informacji i cyberbezpieczeństwem

Na podstawie art. 22 ust. 1 pkt 1 Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369), zarządza się co następuje:

§ 1. Wprowadza się w Urzędzie Gminy Kobylanka oraz w gminnych jednostkach organizacyjnych Procedurę zarządzania incydentami cyberbezpieczeństwa.

§ 2.1. Zobowiązuje się wszystkich pracowników Urzędu Gminy oraz pracowników jednostek organizacyjnych Urzędu Gminy Kobylanka do zapoznania się z niniejszą Procedurą do stosowania jej i przestrzegania.

2. Pisemne oświadczenia o zapoznaniu i przestrzeganiu postanowień Procedury należy złożyć do Sekretarza Gminy.

§ 3. Zarządzenie wchodzi z dniem podpisania

WÓJT
Julita Pilecka

PROCEDURA ZARZĄDZANIA INCYDENTAMI CYBERBEZPIECZEŃSTWA W URZĘDZIE GMINY W KOBYLANCE ORAZ GMINNYCH JEDNOSTKACH ORGANIZACYJNYCH

GMINA KOBYLANKA

Urząd Gminy w Kobylance
Adres: ul. Szkolna 12
73-108 Kobylanka
Powiat: stargardzki
Telefon: 91 57 88 540; 91 56 10 31
Fax: 91 5788 520
E-mail: ugk@kobylanka.pl; poi@kobylanka.pl

ROZDZIAŁ 1

WSTĘP

Procedura zarządzania incydentami związanymi z cyberbezpieczeństwem ma na celu zapewnienie ciągłości działania w realizacji zadań publicznych realizowanych przez podmiot publiczny oraz ograniczenie wpływu przypadków naruszeń bezpieczeństwa zasobów informacyjnych na działalność Urzędu oraz gminne jednostki organizacyjne. Podstawą prawną do opracowania i wdrożenia niniejszej procedury jest art. 22 ust.1 pkt. 1 ustawy o krajowym systemie cyberbezpieczeństwa z dnia 5 lipca 2018r. (Dz. U. z 2020r. poz. 1369).

ROZDZIAŁ 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 CSIRT NASK.
3. CSIRT NASK – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy.
4. Osoba pełniącą funkcję odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa - osoba wyznaczona przez Administratora Danych Osobowych.
5. Inspektor Ochrony Danych - osoba wyznaczona przez Administratora Danych Osobowych zwana dalej „IOD".
6. Administrator Systemów Informatycznych - osoba wyznaczona przez Administratora Danych Osobowych, odpowiedzialna za sprawność i konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych zwana dalej „ASI", w Urzędzie taką funkcję pełni Informatyk.
7. Administrator Danych Osobowych — Gmina Kobylanka reprezentowana przez Wójta Gminy Kobylanka - zwany dalej ADO.
8. Urząd - Urząd Gminy w Kobylance.

9. Gminne Jednostki Organizacyjne – Szkoła Podstawowa w Kobylance, Szkoła Podstawowa w Reptowie, Szkoła Podstawowa w Kunowie, Gminny Ośrodek Pomocy Społecznej w Kobylance, Gminna Biblioteka Publiczna w Kobylance, Centrum Kultury i Rekreacji w Kobylance.

ROZDZIAŁ 3

KATEGORIE INCYDENTÓW

1. Incydent 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.
2. Przyczyną powstania incydentu cyberbezpieczeństwa 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 (naruszenia integralności, dostępności danych);

c) świadome i celowe działania mające na celu:

- ujawnienie informacji niepowołanym do tego podmiotom, wywołując w ten sposób naruszenie poufności zasobów informacyjnych, w tym poufności danych;
- zniszczenie, usunięcie zasobów informacyjnych, wywołując w ten sposób naruszenie integralności lub/i dostępności zasobów informacyjnych w tym danych.

3. Incydentami cyberbezpieczeństwa w szczególności są takie działania jak:
   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.
4. Przyczyny incydentów 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;
i) integralności lub dostępności informacji;
j) nieprawidłowości w zakresie zabezpieczenia przechowywania danych, w tym danych osobowych;
k) naruszenia zasad obowiązujących w Urzędzie dotyczących bezpieczeństwa informacji, w tym danych osobowych.

5. O możliwości zaistnienia przypadku naruszenia cyberbezpieczeństwa mogą świadczyć:
a) nadmierne, w stosunku do wykonywanych zadań (zakresu upoważnienia), uprawnienia użytkownika do zasobów systemu;
b) niestabilna praca systemu teleinformatycznego;
c) korzystanie z zasobów systemu poza godzinami pracy (bez zgody przełożonego);
d) nowe „podejrzane" (nieznane) konta użytkowników;
e) wysoka aktywność kont, które długo pozostawały niewykorzystane;
f) zanotowanie w krótkim czasie dużej liczby nieudanych prób logowania;
g) anomalie w pracy systemu lub programu (świadczące np. o obecności wirusa komputerowego);
h) naruszenie lub wadliwe funkcjonowanie zabezpieczeń fizycznych w pomieszczeniach, w których następuje przetwarzanie informacji w Urzędzie lub Gminnych Jednostkach Organizacyjnych (uszkodzone zamki, okna, drzwi, naruszone plomby, itp.).

ROZDZIAŁ 4
ZAKRES OBOWIĄZYWANIA PROCEDURY ZARZĄDZANIA INCYDENTAMI ZWIĄZANYMI Z BEZPIECZEŃSTWEM INFORMACJI ORAZ CYBERBEZPIECZEŃSTWEM

Procedura zarządzania incydentami związanymi z cyberbezpieczeństwem obowiązuje w Urzędzie Gminy w Kobylance oraz w Gminnych Jednostkach Organizacyjnych.

ROZDZIAŁ 5
ZGŁASZANIE INCYDENTÓW ZWIĄZANYCH Z BEZPIECZEŃSTWEM INFORMACJI ORAZ CYBERBEZPIECZEŃSTWEM

W przypadku ujawnienia incydentu pracownik postępuje zgodnie z procedurami zarządzania incydentami związanymi z bezpieczeństwem informacji i cyberbezpieczeństwem opisanymi w „Polityce Bezpieczeństwa Informacji w Urzędzie Gminy w Kobylance. Procedury eksploatacyjne."

ROZDZIAŁ 6
ZGŁASZANIE INCYDENTÓW ZWIĄZANYCH Z CYBERBEZPIECZEŃSTWEM PRZEZ GMINNE JEDNOSTKI ORGANIZACYJNE

1. W przypadku stwierdzenia incydentu w Gminnych Jednostkach Organizacyjnych należy postępować zgodnie z przyjętymi procedurami w tychże jednostkach organizacyjnych.
2. W przypadku stwierdzenia incydentu przez Gminne Jednostki Organizacyjne polegającego na tym, że incydent powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez Gminną Jednostkę Organizacyjną (incydent w podmiocie publicznym[1]) należy niezwłocznie telefonicznie, lub mailowo w przypadku bezskutecznej próby kontaktu telefonicznego, powiadomić o tym fakcie osobę pełniącą funkcję odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa oraz postępować zgodnie z wdrożonymi w swojej jednostce organizacyjnej procedurami. Dane kontaktowe do osoby pełniącej funkcję odpowiedzialnej za utrzymywanie kontaktu z podmiotami krajowego systemu cyberbezpieczeństwa, oraz ASI Urzędu znajdują się na stronie internetowej: www.kobylanka.pl w zakładce Kontakt.
3. Zgłoszenia incydentów, o których mowa w pkt. 2, do osoby pełniącej funkcję odpowiedzialnej za utrzymanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa można dokonywać przez 24 godziny na dobę przez 7 dni w tygodniu oraz do ASI Urzędu w godzinach pracy Urzędu.

   W dalszej kolejności fakt ten należy zgłosić mailowo oficjalnym pismem opatrzonym podpisem kierownika jednostki do osób wymienionych w pkt.2.
4. W zgłoszeniu należ podać wszystkie informacje zgodnie z treścią art. 23 ust.1 Ustawy o krajowym systemie cyberbezpieczeństwa

[1] Art. 2 pkt 9 Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa