Załącznik nr1
do Zarządzenia Nr 44/2021
Wójta Gminy Ostrowite
z dnia 22.09.2021

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

I. 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. Podstawą prawną do opracowania i wdrożenia dokumentu jest art. 22 ust.1 pkt 1 ustawy z dnia 5 lipca 2018r. o krajowym systemie cyberbezpieczeństwa (tekst jedn. Dz. U. z 2020r., poz. 1369 z późn. zm.) oraz § 20 ust. 2 pkt 13 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (tekst jedn. Dz. U. z 2017r., poz. 2247 z późn. zm.).
3. Ilekroć jest mowa o:
    1) *Incydencie w podmiocie publicznym* - należy przez to rozumieć incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny;
    2) *Incydencie krytycznym* - należy przez to rozumieć 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) *Inspektorze Ochrony Danych* - należy przez to rozumieć osobę wyznaczoną przez Administratora Danych Osobowych zwanego dalej „IOD";
    4) *Administratorze Systemów Informatycznych* - należy przez to rozumieć osobę wyznaczoną przez Administratora Danych Osobowych, odpowiedzialna za sprawność i konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych zwanego dalej „ASI"
    5) *Administratorze Danych Osobowych* - należy przez to rozumieć Wójta Gminy Ostrowite.

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 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.

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

Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji oraz cyberbezpieczeństwem obowiązuje w Urzędzie Gminy Ostrowite.

IV. Zgłaszanie incydentów związanych z bezpieczeństwem informacji oraz cyberbezpieczeństwem

1. W przypadku ujawnienia incydentu pracownik niezwłocznie powiadamia o tym fakcie Inspektora Ochrony Danych oraz Administratora Systemów Informatycznych (gdy incydent dotyczy systemów komputerowych). Zgłoszenie następuje telefonicznie. Telefoniczne zgłoszenie należy następnie potwierdzić szczegółową notatką służbową, którą przekazuje się IOD.
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 jednostki organizacyjne Gminy Ostrowite

1. W przypadku stwierdzenia incydentu krytycznego lub incydentu w podmiocie publicznym przez jednostki organizacyjne Gminy Ostrowite należy niezwłocznie telefonicznie powiadomić o tym fakcie IOD. W dalszej kolejności fakt ten należy zgłosić do IOD mailowo i potwierdzić oficjalnym pismem opatrzonym podpisem kierownika jednostki. Dane kontaktowe IOD znajdują się na stronie internetowej www.ostrowite.pl.
2. W zgłoszeniu należy podać wszystkie informacje zgodnie z treścią art. 23 ust. 1 Ustawy o krajowym systemie cyberbezpieczeństwa.
3. W przypadku dłuższej nieobecności IOD zgłoszenia należy dokonywać do ASI w sposób opisany w pkt 1.

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 dla Urzędu Gminy Ostrowite i jednostek organizacyjnych". 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 w porozumieniu z ASI.
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;
   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 zgłaszającego.
4. W przypadku zakwalifikowania zdarzenia jako incydentu związanego z bezpieczeństwem informacji lub cyberbezpieczeństwem, IOD wspólnie z ASI podejmuje działania zabezpieczające i naprawcze zmierzające do zniwelowania szkód powstałych w wyniku incydentu.
5. O wynikach analizy incydentu oraz podjętych działaniach naprawczych IOD informuje ADO.
6. W przypadku stwierdzenia incydentu w podmiocie publicznym lub incydentu krytycznego wyznaczona osoba odpowiedzialna za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa – IOD lub w zastępstwie ASI (w przypadku nieobecności IOD) 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 z dnia 5 lipca 2018r. o krajowym systemie cyberbezpieczeństwa.
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.

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 2016r. 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 5 kwietnia 2016r).
2. Zgłoszenie naruszenia bezpieczeństwa przetwarzania danych osobowych do Prezesa Urzędu Ochrony Danych określa „Instrukcja postępowania w przypadku naruszenia bezpieczeństwa ochrony danych w Urzędzie Gminy Ostrowite".

WÓJT
mgr Mateusz Wojciechowski