PROCEDURA ZARZĄDZANIA INCYDENTAMI ZWIĄZANYMI Z BEZPIECZEŃSTWEM INFORMACJI I CYBERBEZPIECZEŃSTWEM W POWIATOWYM INSPEKTORACIE WETERYNARII W GŁUBCZYCACH

Spis treści

I. Postanowienia ogólne

1. Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji i cyberbezpieczeństwem (dalej – „procedura") ma na celu zapewnienie ciągłości operacyjnej oraz ograniczenie wpływu przypadków naruszeń bezpieczeństwa zasobów informacyjnych, w tym bezpieczeństwa przetwarzania danych osobowych w Powiatowym Inspektoracie Weterynarii w Głubczycach.
2. Procedura została opracowana na podstawie:

a. art. 22 ust.1 pkt 1 Ustawy z dnia 05 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa,

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.

II. 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 Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego.
3. Administrator Danych Osobowych (dalej „ADO") – osoba fizyczna, prawna, organ publiczny, jednostka bądź inny podmiot ustalający cele i sposoby przetwarzania danych osobowych. W procedurze – Powiatowy Lekarz Weterynarii w Głubczycach.
4. Administrator Systemów Informatycznych (dalej „ASI") – osoba wyznaczona przez Administratora Danych Osobowych, odpowiedzialna za sprawność i konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych.
5. Inspektor Ochrony Danych (dalej „IOD") - osoba wyznaczona przez Administratora Danych Osobowych, odpowiedzialna za wspieranie ADO w realizacji obowiązków dotyczących ochrony danych osobowych.

III. Zakres obowiązywania procedury

Procedura obowiązuje w Powiatowym Inspektoracie Weterynarii w Głubczycach. Procedura obowiązuje również podmioty zewnętrzne, które dopuszczono do przetwarzania danych osobowych.

IV. Kategorie incydentów bezpieczeństwa informacji oraz cyberbezpieczeństwa

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.

V. Przyczyny incydentów bezpieczeństwa informacji oraz cyberbezpieczeństwa

1. Niewłaściwe wykorzystywanie zasobów informatycznych lub niewłaściwe postępowanie z dokumentacją papierową;
2. Działanie szkodliwego oprogramowania;
3. Próby omijania systemów zabezpieczeń;
4. Nieautoryzowany dostęp do systemów, aplikacji i dokumentów;
5. Zniszczenie lub kradzież urządzeń wykorzystywanych do przetwarzania i przechowywania informacji;
6. Zniszczenie lub kradzież nośników danych;
7. Próby wyłudzeń informacji;
8. Ataki z wykorzystaniem technik zagrażających poufności, integralności lub dostępności informacji;
9. Nieprawidłowości w zakresie zabezpieczenia przechowywania danych, w tym danych osobowych;
10. Naruszenia zasad postępowania dotyczących bezpieczeństwa informacji, w tym danych osobowych.

VI. Zgłaszanie incydentów związanych z bezpieczeństwem informacji oraz cyberbezpieczeństwem w Inspektoracie

1. W przypadku ujawnienia incydentu krytycznego lub incydentu w podmiocie publicznym pracownik niezwłocznie powiadamia o tym fakcie Powiatowego Lekarza Weterynarii oraz Administratora Systemów Informatycznych (kiedy incydent dotyczy systemów komputerowych). Powiatowy Lekarz Weterynarii powiadamia natomiast Inspektora Ochrony Danych. Zgłoszenie następuje telefonicznie. Dane kontaktowe IOD oraz ASI znajdują się na stronie internetowej www.bip.piw.namyslow.pl

Telefoniczne zgłoszenie należy następnie potwierdzić szczegółową notatką służbową, którą przekazuje się IOD poprzez swojego bezpośredniego przełożonego lub bezpośrednio do IOD.

2. Notatka musi zawierać następujące informacje:
   a. imię i nazwisko osoby zgłaszającej;
   b. stanowisko oraz komórka organizacyjna;
   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.

VII. Podejmowanie działań w związku ze zgłaszanymi incydentami związanymi z bezpieczeństwem Informacji

1. Zgłoszenie incydentu rejestrowane jest przez IOD i przechowywane w teczce „Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji oraz cyberbezpieczeństwem dla Powiatowego Inspektoratu Weterynarii w Głubczycach.
2. 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.
W przypadku, gdy zgłoszenie dotyczy naruszenia cyberbezpieczeństwa powyższe działania wykonuje IOD w porozumieniu z ASI w Inspektoracie.
3. 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 Inspektoratu;
   d. koszty usunięcia skutków incydentu;
   e. szacowany czas naprawy skutków wywołanych incydentem;
   f. oszacowanie zasobów koniecznych do przywrócenia ciągłości działania systemów.
4. Zakwalifikowanie zgłoszenia incydentu jako „fałszywy alarm" kończy postępowanie, o czym IOD informuje zgłaszającego.
5. 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.
6. IOD informuje ADO o wynikach analizy incydentu oraz podjętych działaniach naprawczych.
7. W przypadku stwierdzenia incydentu w podmiocie publicznym lub incydentu krytycznego IOD lub ASI (w przypadku nieobecności IOD) nie później niż w ciągu 24 godzin od momentu wykrycia zgłasza incydent do CSIRT NASK (Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego przy Naukowej i Akademickiej Sieci Komputerowej - Państwowego Instytutu Badawczego ul. Kolska 12, 01-045 Warszawa).
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 o krajowym systemie cyberbezpieczeństwa z dnia 05 lipca 2018 r.
10. 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.

VIII. Podejmowanie działań w związku ze zgłaszanymi incydentami związanymi z naruszeniem 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 – RODO).
2. Działania podejmowane w związku ze zgłaszanymi incydentami związanymi z naruszeniem bezpieczeństwa przetwarzania danych osobowych opisane są w „Instrukcji postępowania w przypadku zagrożenia lub naruszenia ochrony danych osobowych" stanowiącej element Polityki Bezpieczeństwa Informacji w Powiatowym Inspektoracie Weterynarii w Głubczycach.

Andrzej Pawłowicz
IOD – PIW Głubczyce
20.10.2020