„ ZATWIERDZAM”

Załącznik do Zarządzenia
Nr 6/2019 Starosty
Kędzierzyńsko-Kozielskiego
z dnia 24 stycznia 2019 r

PROCEDURA ZARZĄDZANIA INCYDENTAMI ZWIĄZANYMI Z BEZPIECZEŃSTWEM INFORMACJI I CYBERBEZPIECZEŃSTWEM W STAROSTWIE POWIATOWYM W KĘDZIERZYNIE-KOŹLU

SPORZĄDZIŁ: Krzysztof Księski

I. 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 05 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 – Starosta Kędzierzyńsko-Kozielski oraz Przewodniczący Zespołu ds. Orzekania o Niepełnosprawności w Kędzierzynie-Koźlu.

II. Kategorie incydentów

1. Incydent bezpieczeństwa informacji oraz cyberbezpieczenstwa 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. 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, 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.

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

1. Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji oraz cyberbezpieczeństwem obowiązuje w Starostwie Powiatowym w Kędzierzynie-Koźlu oraz Powiatowym Zespole ds. Orzekania o Niepełnosprawności w Kędzierzynie-Koźlu.

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 (kiedy incydent dotyczy systemów komputerowych). Zgłoszenie następuje telefonicznie. Dane kontaktowe IOD oraz ASI znajdują się na stronie internetowej www.powiat.kedzierzyn-kozle.pl . Telefoniczne zgłoszenie należy następnie potwierdzić szczegółową notatką służbową, którą

przekazuje się IOD poprzez swojego bezpośredniego przełożonego lub bezpośrednio do IOD w przypadku pracowników zatrudnionych na samodzielnych stanowiskach.

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.
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 Powiatu Kędzierzyńsko-Kozielskiego

1. W przypadku stwierdzenia incydentu krytycznego lub incydentu w podmiocie publicznym przez jednostki organizacyjne Powiatu Kędzierzyńsko-Kozielskiego wyszczególnione w punktach od 1 do 17, w załączniku nr 9 do Statutu Powiatu Kędzierzyńsko-Kozielskiego należy niezwłocznie telefonicznie powiadomić o tym fakcie IOD Starostwa Powiatowego w Kędzierzynie-Koźlu. 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.powiat.kedzierzyn-kozle.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 Inspektora Ochrony Danych zgłoszenia należy dokonywać do Administratora Systemów Informatycznych Starostwa Powiatowego w Kędzierzynie-Koźlu w sposób opisany w pkt.1. Dane kontaktowe ASI znajdują się na stronie internetowej www.powiat.kedzierzyn-kozle.pl.

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 Starostwa Powiatowego w Kędzierzynie-Koźlu”. 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 oraz informatykami zatrudnionymi w jednostkach organizacyjnych Powiatu Kędzierzyńsko-Kozielskiego (jeżeli zgłoszenie dotyczy naruszenia cyberbezpieczeństwa w tych jednostkach).

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 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. Jednostki organizacyjne Powiatu Kędzierzyńsko-Kozielskiego o których mowa w pkt V. 1 we własnym zakresie podejmują działania naprawcze zmierzające do zniwelowania szkód powstałych w wyniku incydentu.
6. Poinformowany o wynikach analizy incydentu oraz podjętych działaniach naprawczych IOD informuje ADO. W przypadku nieobecności IOD, Administratora powiadamia ASI.
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 właściwego CSIRT NASK (Naukowa i Akademicka Sieć Komputerowa - 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.

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 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) (Dz. Urz. UE L 119 z dnia 05 kwietnia 2016 r).

2. W przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego lub zaistnienia sytuacji, które mogą wskazywać na naruszenie ochrony danych osobowych tj.:
   a. przypadkowe lub niezgodne z prawem zniszczenie danych;
   b. przypadkowa lub niezgodna z prawem utrata danych;
   c. przypadkowa lub niezgodna z prawem modyfikacja danych;
   d. nieuprawnione ujawnienie danych;
   e. nieuprawniony dostęp do danych osobowych.

   każdy pracownik zatrudniony przy przetwarzaniu danych osobowych (pracownik, stażysta, praktykant itp.) jest zobowiązany przerwać przetwarzania danych osobowych i niezwłocznie powiadomić o tym fakcie swojego bezpośredniego przełożonego oraz Inspektora Ochrony Danych i Administratora Systemów Informatycznych (jeżeli naruszenie ma związek z systemami informatycznymi).
3. Fakt naruszenia lub podejrzenia naruszenia ochrony danych osobowych należy potwierdzić pisemnie poprzez niezwłoczne sporządzenie notatki służbowej w której umieszcza się informację o dacie, czasie, miejscu, okolicznościach zdarzenia. Notatkę przekazuje się Inspektorowi Ochrony Danych Starostwa Powiatowego w Kędzierzynie-Koźlu za pośrednictwem swojego przełożonego lub bezpośrednio w przypadku osób zatrudnionych na samodzielnych stanowiskach. O zdarzeniu IOD niezwłocznie powiadamia ADO.
4. W przypadku dłuższej nieobecności IOD notatkę należy przekazać Administratorowi Systemów Informatycznych Starostwa Powiatowego w Kędzierzynie-Koźlu.
5. Notatka jest rejestrowana przez IOD i przechowywana w teczce „Rejestr naruszeń ochrony danych osobowych”
6. Zgłoszenia są rejestrowane w „Rejestrze naruszeń ochrony danych osobowych” prowadzonym zgodnie z art.33 ust. 5 RODO.
7. Przy ocenie istotności incydentu pod uwagę brane są następujące czynniki:
   a. charakter naruszenia ochrony danych osobowych;
   b. kategorię i przybliżoną liczbę osób których dane dotyczą;
   c. kategorię i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
   d. możliwe konsekwencje naruszenia ochrony danych osobowych;
   e. wpływ incydentu na ciągłość działania Urzędu;
   f. koszty usunięcia skutków incydentu;
   g. szacowany czas naprawy skutków wywołanych incydentem.
8. Zakwalifikowanie zgłoszenia incydentu jako „fałszywy alarm” kończy postepowanie o czym IOD informuje zgłaszającego.
9. Sprawdzenie naruszenia lub podejrzenia naruszenia ochrony danych osobowych kończy się sprawozdaniem, które przekazywane jest ADO. Sprawozdanie wykonuje IOD wraz z ASI.
10. W przypadku zakwalifikowania zdarzenia jako naruszenie ochrony danych osobowych, które skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych, ADO bez zbędnej zwłoki , nie później niż w terminie 72 godzin od stwierdzenia naruszenia powiadamia Urząd Ochrony Danych Osobowych.
11. Zgłoszenia do UODO przekazywane są w sposób elektroniczny. Procedura zgłoszeń opisana jest pod adresem internetowym https://uodo.gov.pl/pl/134/233
12. IOD wraz z ASI podejmuje również działania zabezpieczające i naprawcze zmierzające do niwelowania skutków powstałych w wyniku incydentu, jak również działania zaradcze dla uniknięcia wystąpienia podobnych incydentów w przyszłości.
13. Jeżeli zgłoszony incydent naruszenia ochrony danych osobowych może spowodować **wysokie ryzyko** naruszenia praw lub wolności osób fizycznych, a stosowane w Urzędzie techniczne i organizacyjne środki ochrony danych nie eliminują tego ryzyka, IOD bez zbędnej zwłoki

informuje ADO o konieczności zawiadomienia osób , których dane dotyczą o takim naruszeniu i przygotowuje stosowne dokumenty do podpisu.

14. Jeżeli zawiadomienie osób, których dane dotyczą wymagałoby niewspółmiernie dużego wysiłku, IOD przygotowuje publiczny komunikat lub wybiera inny stosowny środek, za pomocą którego zawiadomienie zostanie tym osobom przekazane.
15. W przypadku stwierdzenia działań zamierzonych, przy jednoczesnym zidentyfikowaniu sprawcy incydentu dotyczącego naruszenia bezpieczeństwa przetwarzania danych osobowych ADO podejmuje decyzję dotyczącą wyciągnięcia ewentualnych konsekwencji dyscyplinarnych wobec sprawcy incydentu. Jednocześnie, w zależności od wagi incydentu, mogą być powiadomione organa ścigania.