

## Procedura zarządzania incydentami bezpieczeństwa informacji i cyberbezpieczeństwem

### Rozdział 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 Starostwa Powiatowego w Kole.
2. Definicje użyte w niniejszej procedurze oznaczają:
  - 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
  - 3) **Administratorem Danych Osobowych** jest Starostwo Powiatowe w Kole reprezentowane przez Starostę, który ustala cele i sposoby przetwarzania danych osobowych. ADO mając na uwadze jak ważne jest bezpieczeństwo przetwarzanych danych osobowych ze względu na ochronę podstawowych praw i wolności osób fizycznych, a w szczególności ich prawo do ochrony danych osobowych oraz w celu zapewnienia zgodności z wymaganiami prawa, a w tym ochronę dobrego imienia jednostki, ustanawia system ochrony danych osobowych tj. zasady oraz zabezpieczenia stosowane podczas przetwarzania danych osobowych.
  - 4) **Inspektor Ochrony Danych** – osoba wyznaczony przez Administratora Danych Osobowych zwanej dalej „IOD”.
  - 5) **Administrator Systemów Informatycznych** - osoba wyznaczona przez Administratora Danych Osobowych, odpowiedzialna za sprawność i konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych zwana dalej "ASI".

### Rozdział 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 przyczyna mogą być:
  - 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;
  - 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;
  - świadome i celowe działania mające na celu naruszenie poufności zasobów, w tym poufności danych.
2. Incydentami bezpieczeństwa informacji w szczególności są:
  - naruszenie poufności, to jest ujawnienie informacji niepowołanym osobom;
  - naruszenie integralności, to jest zniszczenie, uszkodzenie lub przekłamanie informacji;
  - naruszenie dostępności, to jest braku dostępu do danych przez uprawnionych użytkowników.

3. Przyczyny incydentów bezpieczeństwa informacji oraz cyberbezpieczeństwa mogą dotyczyć:
- niewłaściwego wykorzystywania zasobów informatycznych lub niewłaściwe postępowanie z dokumentacją papierową;
  - działania szkodliwego oprogramowania;
  - próby omijania systemów zabezpieczeń;
  - nieautoryzowanego dostępu do systemów, aplikacji i dokumentów;
  - zniszczenia lub kradzieży urządzeń wykorzystywanych do przetwarzania i przechowywania informacji;
  - zniszczenia lub kradzieży nośników danych;
  - prób wyłudzeń informacji;
  - ataków socjotechnicznych, ataków z wykorzystaniem technik zagrażających poufności, integralności lub dostępności informacji;
  - nieprawidłowości w zakresie zabezpieczenia przechowywania danych, w tym danych osobowych;
  - naruszenia zasad obowiązujących w Urzędzie dotyczących bezpieczeństwa informacji, w tym danych osobowych.

### **Rozdział 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 Kole.

### **Rozdział IV**

#### **Zgłaszanie incydentów związanych z bezpieczeństwem informacji oraz cyberbezpieczeństwem**

1. W przypadku ujawnienia incydentu pracownik niezwłocznie powiadamia o tym fakcie Administratora Danych Osobowych i Administratora Systemów Informatycznych oraz Inspektora Ochrony Danych (jeżeli incydent może dotyczyć danych osobowych).
2. Zgłoszenia dokonuje się telefonicznie lub osobiście. Zgłoszenie należy potwierdzić szczegółową notatką służbową, którą przekazuje się do ASI.
3. Notatka musi zawierać następujące informacje:
  - Imię i Nazwisko zgłaszającego,
  - stanowisko oraz komórka organizacyjna,
  - dokładne miejsce oraz datę wystąpienia incydentu,
  - opis incydentów w sposób adekwatny do posiadanej wiedzy i umiejętności zgłaszającego.
4. Brak umiejętności poprawnego rozpoznania incydentu przez osobę zgłaszającą nie może być przyczyną zaniechania zgłoszenia.
5. W przypadku nieobecności ASI incydent należy zgłosić do ADO lub osoby wskazanej przez ADO.

### **Rozdział V**

#### **Podejmowanie działań w związku ze zgłaszanymi incydentami związanymi z bezpieczeństwem informacji oraz cyberbezpieczeństwem**

1. Zgłoszenie incydentu rejestrowane jest przez ASI i przechowywane w teczce.
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.
4. W przypadku, kiedy zgłoszenie zakwalifikowane zostało jako incydent bezpieczeństwa informacji lub cyberbezpieczeństwa, ASI dokonuje oceny jego istotności. Powyższe działania wykonuje ASI w porozumieniu z ADO i IOD.

5. Przy ocenie istotności incydentu pod uwagę brane są następujące czynniki:
  - powstałe szkody będące wynikiem incydentu;
  - wpływ incydentu na działanie systemów;
  - wpływ incydentu na ciągłość działania Urzędu;
  - koszty usunięcia skutków incydentu;
  - szacowany czas naprawy skutków wywołanych incydentem;
  - oszacowanie zasobów koniecznych do przywrócenia ciągłości działania systemów.
6. Zakwalifikowanie zgłoszenia incydentu jako „fałszywy alarm” kończy postępowanie, o czym ASI informuje zgłaszającego.
7. W przypadku zakwalifikowania zdarzenia jako incydentu związanego z bezpieczeństwem informacji lub cyberbezpieczeństwem, ASI podejmuje działania zabezpieczające i naprawcze zmierzające do zniwelowania szkód powstałych w wyniku incydentu.
8. W przypadku stwierdzenia incydentu w podmiocie publicznym lub incydentu krytycznego, ASI lub ADO (w porozumieniu z 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).
9. 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 lub fax).
10. W zgłoszeniu przekazuje się informacje zgodnie z formularzem oraz zgodnie z wymogami art. 23 ust. 1 ustawy z dnia 05 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.
11. 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.

## **Rozdział VI**

### **Reagowanie na awarię**

1. Jeśli awaria dotyczy systemu krytycznego i może mieć wpływ na wydajność systemów teleinformatycznych, ASI informuje ADO.
2. W przypadku, gdy awarię można usunąć samodzielnie, to ASI dokonuje naprawy. Do podstawowych działań w takim wypadku zaliczyć możemy:
  - a) wymianę stacji roboczej,
  - b) wymianę podzespołów w stacji roboczej,
  - c) wymianę urządzenia sieciowego,
  - d) odtworzenie danych z kopii zapasowej.
3. Jeżeli ASI podejmie decyzję, iż nie może samodzielnie usunąć awarii, decyzję tę oraz wszelkie dodatkowe informacje dotyczące awarii kieruje do producenta sprzętu lub oprogramowania. Jeżeli naprawa dotyczy sprzętu, producent naprawy dokonuje w obecności ASI. Jeżeli naprawa dotyczy oprogramowania (np. wersji BIOS), wgrzywana poprawka powinna zostać pozytywnie zweryfikowana w środowisku testowym.

## **Rozdział VII**

### **Reagowanie na błędy w oprogramowaniu**

1. Po otrzymaniu zgłoszenia dotyczącego wystąpienia błędu systemowego lub aplikacyjnego w oprogramowaniu, ASI diagnozuje przyczyny błędu oraz podejmuje działania zmierzające do rozwiązania problemu. Do podstawowych działań w tym zakresie możemy zaliczyć:
  - a) wykorzystanie bazy wiedzy o błędach w oprogramowaniu,
  - b) zmianę konfiguracji oprogramowania,
  - c) ponowną instalację oprogramowania,
  - d) instalację nowej wersji oprogramowania.

2. Jeżeli ASI nie może sam naprawić błędu w oprogramowaniu przekazuje tę informację do producenta oprogramowania (pracownik powinien w tym przypadku postępować zgodnie z umowami serwisowymi lub licencjami).
3. Jeżeli istnieje powód wskazujący na to, że przyczyną błędu w oprogramowaniu było naruszenie bezpieczeństwa, to ASI o tym fakcie informuje ADO.

## **Rozdział VIII**

### **Reagowanie na wykrycie złośliwego kodu mobilnego**

1. Po otrzymaniu zgłoszenia dotyczącego pojawienia się złośliwego kodu mobilnego na stacji roboczej, serwerze, lub samodzielelnemu wejściu w posiadanie wiedzy o takim zdarzeniu, ASI w pierwszej kolejności powinien:
  - a) odłączyć komputer od sieci komputerowej,
  - b) sprawdzić aktualność baz danych wirusów (jeśli są nieaktualne należy dokonać aktualizacji),
  - c) sprawdzić poprawność działania oprogramowania antywirusowego (jeśli oprogramowanie nie działa poprawnie należy je odinstalować i zainstalować ponownie),
  - d) uruchomić pełne skanowanie komputera i nośników informacji, z jakimi mógł mieć styczność.
2. Jeżeli atak złośliwego kodu mobilnego nie został zneutralizowany przez oprogramowanie antywirusowe, ASI nakazuje użytkownikowi przerwanie pracy. Następnie dokonuje ponownej instalacji systemu operacyjnego i oprogramowania oraz odzyskania danych z kopii zapasowych. Kopie zapasowe należy sprawdzić programem antywirusowym przed wgraniem do komputera.
3. Jeżeli istnieje powód wskazujący na to, że przyczyną ataku złośliwego kodu mobilnego było naruszenie bezpieczeństwa, to ASI informuje o tym fakcie ADO.