# PROCEDURA ZARZĄDZANIA INCYDENTAMI ZWIĄZANYMI Z BEZPIECZEŃSTWEM INFORMACJI I CYBERBEZPIECZEŃSTWEM

## § 1
## Postanowienia ogólne

1. „Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji oraz cyberbezpieczeństwem" (zwana dalej „Procedurą") ma na celu zapewnienie ciągłości operacyjnej oraz ograniczenie wpływów przypadków naruszeń bezpieczeństwa zasobów informacyjnych na działalność jednostki.
2. Podstawą prawną do opracowania i wdrożenia procedury jest:
   1) art. 22 Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;
   2) § 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. Definicje użyte w niniejszej procedurze oznaczają:
   1) Inspektor Ochrony Danych - osoba wyznaczona przez Administratora Danych Osobowych zwana dalej "IOD";
   2) Administrator Systemów Informatycznych - osoba wyznaczona przez Administratora Danych Osobowych, odpowiedzialna za sprawność i konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych zwana dalej "ASI";
   3) Administrator Danych Osobowych "ADO" – jednostka organizacyjna reprezentowana przez Burmistrza.

## § 2
## 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 mogą 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) prób 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 (np. pozostawienie włączonego komputera i / lub nie wylogowanie się po zakończeniu pracy lub podczas przerwy w pracy, pozostawienie niezabezpieczonych dokumentów drukowanych zawierających dane osobowe itp.).

## § 3
## Przykładowe zdarzenia które mogą być zakwalifikowane jako podejrzenie naruszenia bezpieczeństwa informacji

1. Za przykładowe zdarzenia, które mogą być zakwalifikowane jako podejrzenie naruszenia bezpieczeństwa informacji można uznać np.:
   1) Awarię sprzętu lub oprogramowania, które wskazują na umyślne działanie w kierunku naruszenia ochrony danych, a także niewłaściwe działanie systemu, a w tym sam fakt pozostawienia serwisantów bez nadzoru;
   2) Nieprzewidziane oddziaływanie czynników zewnętrznych na infrastrukturę teleinformatyczną jak np.: pożar, zalanie pomieszczeń, zerwanie linii wysokiego napięcia, niepożądana ingerencja firmy remontowej, wybuch gazu, napad itp.;
   3) Nieodpowiednie warunki środowiskowe panujące w serwerowni takie jak zbyt wysoka temperatura lub nadmierna wilgotność;
   4) Wystąpienie nieautoryzowanej manipulacji danymi w systemie;
   5) praca w systemie lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.
   6) Ujawniono istnienie nie autoryzowanych kont dostępu do danych lub tzw. "bocznej furtki", itp.
   7) Ujawnianie nieupoważnionym osobom danych osobowych lub objętych tajemnicą elementów systemu zabezpieczeń;

8) Wystąpienie nieprawidłowości związanych z przechowywania danych, w tym osobowych np. pozostawienie otwartych biur, szaf, biurek, niewylogowanie się z systemu itp.

## § 4
## Zgłaszanie incydentów związanych z bezpieczeństwem informacji oraz cyberbezpieczeństwem

1. W przypadku ujawnienia incydentu pracownik niezwłocznie powiadamia o tym fakcie ADO, ASI oraz IOD.
2. Jednocześnie wskazuje się, że ASI został przez ADO wyznaczony jako osoba odpowiedzialna za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, w związku z realizacją zadań wynikających z art. 22-24 Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.
3. Zgłoszenia dokonuje się telefonicznie lub osobiście.
4. Zgłoszenie należy potwierdzić szczegółową notatką służbową, którą przekazuje do ADO oraz w kopii do IOD oraz ASI.
5. Notatka powinna zawierać następujące informacje:
   1) imię i nazwisko zgłaszającego;
   2) stanowisko;
   3) dokładne miejsce oraz datę wystąpienia incydentu;
   4) opis incydentów sposób adekwatny do posiadanej wiedzy i umiejętności zgłaszającego.
6. Wzór notatki stanowi załącznik nr 1 do niniejszej procedury.
7. Brak umiejętności poprawnego rozpoznania incydentu przez osobą zgłaszającą nie może być przyczyną zaniechania zgłoszenia.
8. W przypadku nieobecności IOD lub ASI incydent należy zgłosić do ADO lub osoby wskazanej przez ADO.

## § 5
## Postepowanie z incydentami związanymi z bezpieczeństwem informacji oraz cyberbezpieczeństwem

1. Zgłoszenie incydentu rejestrowane jest przez IOD oraz ASI i przechowywane w dokumentach IOD.
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 przypadki kiedy zgłoszenie zakwalifikowane zostało jako incydent bezpieczeństwa informacji lub cyberbezpieczeństwa, IOD oraz ASI dokonuje jego oceny istotności.
5. 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

4) koszty usunięcia skutków incydentu;
5) szacowany czas naprawy skutków wywołanych incydentem;
6) oszacowanie zasobów koniecznych do przywrócenia ciągłości działania systemów.

6. Zakwalifikowanie zgłoszenia jako „fałszywy alarm" kończy postępowanie.
7. W przypadku zakwalifikowania zdarzenia jako incydentu związanego z bezpieczeństwem informacji lub cyberbezpieczeństwem, ASI wespół z IOD podejmuje działania zabezpieczające i naprawcze zmierzające do zniwelowania szkód powstałych w wyniku incydentu.
8. W przypadku stwierdzenia incydentu w podmiocie publicznym lub incydentu krytycznego, ADO (w porozumieniu z IOD oraz ASI), nie później niż w ciągu 24 godzin od momentu wykrycia, zgłasza incydent do właściwego CSIRT NASK (Naukowa i Akademicka Sieć Komputerowa - Państwowy Instytut Badawczy ul. Kolska 12, 01-045 Warszawa).
9. Zgłoszenia do CSIRT NASK przekazywane są w sposób elektroniczny. W przypadku braku możliwości przekazania zgłoszenia w sposób elektroniczny należy dokonać go przy użyciu innych dostępnych środków komunikacji tj. telefon, fax.
10. W zgłoszeniu przekazuje się informacje zgodne z formularzem oraz zgodnie z wymogami art. 23 ust. 1 ustawy z dnia 5 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 może powiadomić organy ścigania.

## § 6
## Reagowanie na awarię

1. Jeśli awaria dotyczy systemu krytycznego i może mieć wpływ na wydajność systemów teleinformatycznych, ASI informuje ADO oraz IOD.
2. W przypadku gdy awarię można usunąć samodzielnie, ASI dokonuje naprawy. Do podstawowych działań w takim wypadku zaliczyć można:
   1) wymianę stacji roboczej;
   2) wymianę podzespołów w stacji roboczej;
   3) wymianę urządzenia sieciowego;
   4) odtworzenie danych z kopii zapasowej.
3. W przypadku gdy ASI uzna, iż nie jest w stanie samodzielnie usunąć awarii, informację dotyczącą awarii przekazuje do producenta sprzętu lub oprogramowania.
4. Jeżeli konieczność naprawy dotyczy sprzętu wówczas naprawa dokonywana jest przez producenta w obecności ASI.
5. Jeżeli konieczność naprawy dotyczy oprogramowania, wgrywana poprawka powinna zostać pozytywnie zweryfikowana w środowisku testowym.

## § 7
## 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 takim wypadku zaliczyć można:

1) wykorzystanie bazy wiedzy o błędach w oprogramowaniu;
2) zmianę konfiguracji oprogramowania;
3) ponowną instalację oprogramowania;
4) instalację nowej wersji oprogramowania.

2. W przypadku gdy ASI nie jest w stanie samodzielnie naprawić błędu w oprogramowaniu, przekazuje tę informację do producenta oprogramowania (pracownik powinien w tym przypadku postępować zgodnie z umowami serwisowymi lub licencjami).
3. W przypadku gdy zaistnieje powód wskazujący na to, że przyczyną błędu w oprogramowaniu było naruszenie bezpieczeństwa, ASI informuje o tym fakcie ADO oraz IOD.

## § 8
## Reagowanie na wykrycie złośliwego kodu mobilnego

1. Po otrzymaniu zgłoszenia dotyczącego pojawienia się złośliwego kodu mobilnego na stacji roboczej, serwerze, lub samodzielnemu wejściu w posiadanie wiedzy o takim zdarzeniu, ASI w pierwszej kolejności powinien:
   1) odłączyć komputer od sieci komputerowej;
   2) sprawdzić aktualność baz danych wirusów (jeśli są nieaktualne należy dokonać aktualizacji),
   3) sprawdzić poprawność działania oprogramowania antywirusowego (jeśli oprogramowanie nie działa poprawnie należy je odinstalować i zainstalować ponownie),
   4) uruchomić pełne skanowanie komputera i nośników informacji, z jakimi mógł mieć styczność,
2. Jeśli atak złośliwego kodu mobilnego nie został zneutralizowany przez oprogramowanie antywirusowe to 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. Jeśli istnieje powód wskazujący na to, że przyczyną ataku złośliwego kodu mobilnego było naruszenie bezpieczeństwa, to ASI informuje ADO.

## § 9
## Szkolenia

W celu zwiększenia wśród pracowników umiejętności poprawnego rozpoznania i klasyfikacji incydentów zaleca się, co najmniej raz do roku przeprowadzać okresowe szkolenie pracowników w zakresie zarządzania incydentami. Niezależnie od prowadzonych szkoleń wskazane jest przeprowadzanie szkolenia każdego nowo zatrudnionego pracownika celem zapewnienia znajomości zasad prawidłowego zgłaszania incydentów.

BURMISTRZ
inż. Paweł Macha

**Załącznik nr 1 do Procedury Zarządzania Incydentami** (wzór notatki służbowej ze zgłoszeniem)

## Zgłaszanie incydentów związanych z bezpieczeństwem informacji oraz cyberbezpieczeństwem

Imię i nazwisko osoby zgłaszającej:
.....

Stanowisko oraz komórka organizacyjna:
.....

Dokładne miejsce i data wystąpienia incydentu:.....

.....
.

.....
.

Opis incydentu w sposób adekwatny do posiadanej wiedzy i umiejętności zgłaszającego:
.....
.

.....
.

.....
.

.....
.