Załącznik nr 1 do Zarządzenia nr 9/2025/2026 z dnia 10.03.2026 r.

PROCEDURA ZARZĄDZANIA INCYDENTAMI ZWIĄZANYMI Z BEZPIECZEŃSTWEM INFORMACJI I CYBERBEZPIECZEŃSTWIE W GDAŃSKIEJ SZKOLE SZERMIERKI

I. Postanowienia ogólne, definicje

1. Procedura zarządzenia incydentami związanymi z bezpieczeństwem informacji oraz cyberbezpieczeństwem ma na celu zapewnienie ciągłości operacyjnej oraz ograniczenie wpływu przypadków naruszeń bezpieczeństwa zasobów informacyjnych na działalność Gdańskiej Szkoły Szermierki .
2. Podstawą prawną do opracowania i wdrożenia dokumentu jest:
   a) art. 22 ust.1 pkt 1 Ustawy o krajowym systemie cyberbezpieczeństwa z dnia 5 lipca 2018 r.
   b) §20 ust. 2 pkt 13 Rozporządzenia Rady Ministrów z dnia 21 maja 2024 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 zadani 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, zwany dalej „IOD".
6. **Administrator Danych Osobowych** (zwany dalej „ADO") – Gdańska Szkoła Szrmierki
7. **Osoba kontaktowa** – osoba zgłoszona przez Dyrektora placówki do CSIRT NASK jak osoba kontaktowa (zg. z art. 22 ust 1 pkt 5 ustawy z dnia 5 lipca 2018r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560)

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:
   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 działanie 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 wykorzystania zasobów informatycznych lub niewłaściwe postępowanie z dokumentacją papierową;
   b) działania szkodliwego oprogramowania;
   c) próby omijania systemów zabezpieczeń;
   d) nieautomatyzowanego dostępu do systemów, aplikacji i dokumentów;
   e) zniszczenie 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 placówce 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 o w Gdańsku.

IV. Zgłaszanie incydentów związanych z bezpieczeństwem informacji oraz cyberbezpieczeństwem

1. W przypadku ujawnienia incydentu pracownik niezwłocznie powiadamia o tym fakcie Administratora Danych Osobowych/ Osobę Kontaktową oraz Inspektora Ochrony Danych (jeżeli incydent może dotyczyć danych osobowych). Zgłoszenie dokonuje się telefonicznie lub osobiście. Zgłoszenie należy następnie potwierdzić szczegółową notatką służbową, którą przekazuje się do Osoby Kontaktowej.
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. Wzór notatki stanowi załącznik nr 1 do niniejszej Procedury.
4. Brak umiejętności poprawnego rozpoznania incydentu przez osobę zgłaszającą nie może być przyczyną zaniechania zgłoszenia.
5. W przypadku nieobecności Osoby Kontaktowej incydent należy zgłosić do ADO lub osoby wyznaczonej przez ADO w sposób wskazany w pkt. 1.

V. Podejmowanie działań w związku ze zgłaszanymi incydentami związanymi z bezpieczeństwem informacji oraz cyberbezpieczeństwem

1. Zgłoszenie incydentu rejestrowane jest przez Osobę Kontaktową i przechowywane w teczce. Osoba zgłaszająca incydent powinna w miarę możliwości zabezpieczyć materiał dowodowy (np. zrzut ekranu monitora, zdjęcie niebezpiecznych 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 Osoba Kontaktowa w porozumieniu z ADO i IOD.

2. Przy ocenie istotności incydentu pod uwagę brane są następujące czynniki:
   a) powstałe szkody będące wynikiem incydentu;
   b) wpływ incydentu na działania systemów;
   c) wpływ incydentu na ciągłość działania placówki;
   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 Osoba Kontaktowa informuje zgłaszającego.
4. W przypadku zakwalifikowania zdarzenia jako incydentu związanego z bezpieczeństwem informacji lub cyberbezpieczeństwem, Osoba Kontaktowa podejmuje działania zabezpieczające i naprawcze zmierzające do zniwelowania szkód powstałych w wyniku incydentu.
5. W przypadku stwierdzenia incydentu w podmiocie publicznym lub incydentu krytycznego Osoba Kontaktowa 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).
6. 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 dostępnych innych dostępnych środków komunikacji (np. na numer telefonu +48223808274).
7. W zgłoszeniu 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.

VI. Reagowanie na awarię

1. Jeśli awaria dotyczy systemu krytycznego i może mieć wpływ na wydajność systemów teleinformatycznych, Osoba Kontaktowa informuje ADO.
2. W przypadku gdy awarię można usunąć samodzielnie, to Osoba Kontaktowa 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 Osoba Kontaktowa podejmuje decyzję, iż nie może samodzielnie usunąć awarii, decyzję tę oraz wszelkie dodatkowe informacje dotyczące awarii eskaluje do producenta sprzętu lub oprogramowania. Jeżeli naprawa dotyczy sprzętu, producent naprawy dokonuje w obecności Osoby Kontaktowej. Jeżeli naprawa dotyczy oprogramowania (np. wersji BIOS), wgrywana poprawka powinna zostać pozytywnie zweryfikowana w środowisku testowym

VII. Reagowanie na błędy w oprogramowaniu

1. Po otrzymaniu zgłoszenia dotyczącego wystąpienia błędu systemowego lub aplikacyjnego w oprogramowaniu, Osoba Kontaktowa 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,
   d) instalację nowej wersji oprogramowania.
2. Jeżeli Osoba Kontaktowa nie może sam naprawić błędu w oprogramowaniu przekazuje 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 Osoba Kontaktowa informuje ADO.

VIII. Zwiększanie świadomości pracowników na temat cyberbezpieczeństwa

1. Brak wiedzy i umiejętności poprawnego rozpoznania i klasyfikacji oraz oceny poziomu istotności incydentu po stronie zgłaszającego nie może być przyczyną zaniechania powiadomienia osób odpowiedzialnych w placówce o zaistniałym incydencie lub podejrzeniu jego wystąpienia. Dlatego w miarę posiadanych zasobów, co najmniej raz w roku należy przeprowadzić okresowe szkolenia/ przekazać materiały informacyjne pracownikom placówki w zakresie zarządzania incydentami cyberbezpieczeństwa.

Signed by / Podpisano przez:

Adam Władek

Date / Data: 2026-03-10 13:12