PROCEDURA ZARZĄDZANIA INCYDENTAMI CYBERBEZPIECZEŃSTWA

Egzemplarz zatwierdzony: x TAK ☐ NIE

Podpis osoby zatwierdzającej:

DYREKTOR
Gminnego Zespołu Obsługi Oświaty
mgr Alicja Babiarz-Synakiewicz

.....

SPIS TREŚCI

1 Informacje wstępne

Procedura zarządzania incydentami cyberbezpieczeństwa, zwana dalej „Procedurą" jest dokumentem wewnętrznym **Gminnego Zespołu Obsługi Oświaty w Mroczy** opisującym zasady zarządzania incydentem cyberbezpieczeństwa stosowane przez Jednostkę w celu spełnienia wymagań wynikających w szczególności z:

1) dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.U.UE.L.2016.194.1,
2) ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t. j. Dz. U. z 2018 r., poz. 1560 ze zm.),
3) przepisów szczególnych, regulujących funkcjonowanie Jednostki,
4) dobrych praktyk z zakresu bezpieczeństwa informacji, ochrony danych osobowych oraz cyberbezpieczeństwa.

2 Definicje

1) **CSIRT NASK** – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy;
2) **cyberbezpieczeństwo** – odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy;
3) **incydent** – zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo;
4) **incydent cyberbezpieczeństwa** – zbiorcza nazwa obejmująca terminy incydent, incydent w podmiocie publicznym, incydent krytyczny;
5) **incydent w podmiocie publicznym** – incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny, o którym mowa w art. 4 pkt 7–15 Ustawy;
6) **incydent krytyczny** – incydent skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi, klasyfikowany przez właściwy CSIRT;

7) **Jednostka – Gminny Zespół Obsługi Oświaty w Mroczy;**
8) **Kierownik Jednostki** – osoba reprezentująca i zarządzająca Jednostką;
9) **Koordynator KSC** – osoba odpowiedzialna za utrzymanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, o której mowa w art. 21 ust. 1 Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t. j. Dz. U. z 2018 r., poz. 1560 ze zm.);
10) **Przedstawiciel KJ** – osoba wyznaczona przez Kierownika Jednostki do ścisłej współpracy z Koordynatorem KSC;
11) **obsługa incydentu** – czynności umożliwiające wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację, podejmowanie działań naprawczych i ograniczenie skutków incydentu;
12) **podatność** – właściwość systemu informacyjnego, która może być wykorzystana przez zagrożenie cyberbezpieczeństwa;
13) **system informacyjny** – system teleinformatyczny, o którym mowa w art. 3 pkt 3 Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2017 r. poz. 570 oraz z 2018 r. poz. 1000 i 1544), wraz z przetwarzanymi w nim danymi w postaci elektronicznej;
14) **Użytkownik** – osoba posiadająca dostęp do systemu informacyjnego Jednostki służącego do realizacji zadania publicznego;
15) **Ustawa** – Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t. j. Dz. U. z 2018 r., poz. 1560 ze zm.);
16) **zagrożenie cyberbezpieczeństwa** – potencjalna przyczyna wystąpienia incydentu;
17) **zarządzanie incydentem** – obsługę incydentu, wyszukiwanie powiązań między incydentami, usuwanie przyczyn ich wystąpienia oraz opracowywanie wniosków wynikających z obsługi incydentu.

3 Osoby odpowiedzialne za cyberbezpieczeństwo Jednostki

3.1 Kierownik Jednostki

3.1.1 Kierownik Jednostki wyznacza osobę odpowiedzialną za utrzymanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa - Koordynatora KSC.

3.1.2 Kierownik Jednostki, w terminie 14 dni od dnia wyznaczenia, przekazuje do CSIRT NASK dane Koordynatora KSC, a także informacje o zmianie tych danych w terminie 14 dni od dnia ich zmiany.

1) Przekazanie danych Koordynatora KSC odbywa się w sposób następujący:
   a) za pośrednictwem formularza elektronicznego pod adres adres e-mail: ksc@cert.pl;
      lub
   b) w formie pisemnej pod adres do korespondencji CSIRT NASK:
      NASK - Państwowy Instytut Badawczy
      ul. Kolska 12
      01-045 Warszawa

2) Przekazanie danych Koordynatora KSC powinno zawierać:
   a) nazwę Jednostki,
   b) sektor, w którym działa Jednostka,
   c) imię i nazwisko, telefon kontaktowy oraz adres poczty elektronicznej e-mail.

3.1.3 Kierownik Jednostki dokonuje zgłoszenia incydentu w podmiocie publicznym do CSIRT NASK. Zgłoszenie incydentu odbywa się za pomocą formularza dostępnego na stronie internetowej https://incydent.cert.pl/

3.2 Koordynator KSC

3.2.1 Koordynator KSC realizuje następujące zadania:
   a) przyjmuje od Przedstawiciela KJ informacje o zdarzeniach mogącym stanowić incydent cyberbezpieczeństwa lub podejrzeniu ich wystąpienia w Jednostce,
   b) koordynuje obsługę zgłaszanych incydentów cyberbezpieczeństwa,
   c) wspiera Jednostkę w przygotowaniu zgłoszenia incydentu w podmiocie publicznym do CSIRT NASK, zgodnie ze wzorem stanowiącym załącznik nr 1 do niniejszej Procedury i przekazuje go do Przedstawiciela KJ,
   d) koordynuje wdrażanie działań naprawczych po wystąpieniu incydentu cyberbezpieczeństwa,
   e) szkoli i podnosi świadomość Użytkowników i pracowników Jednostki w zakresie incydentów cyberbezpieczeństwa, ich zgłaszania, przeciwdziałania i prewencyjnych sposobach zabezpieczenia Zleceniodawcy przed ich występowaniem,

f) koordynuje prace związane z informowaniem osób, na rzecz których zadanie publiczne jest realizowane w zakresie dostępu do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowania skutecznych sposobów zabezpieczania się przed tymi zagrożeniami,

g) w przypadku wystąpienia incydentu cyberbezpieczeństwa ściśle współpracuje z Użytkownikami i pracownikami Jednostki, innymi osobami lub podmiotami świadczącymi Jednostce usługi dotyczące obsługi informatycznej, w celu wdrożenia działań naprawczych,

h) wraz z Przedstawicielem KJ oraz innymi osobami zaangażowanymi przy wystąpieniu zdarzenia, dokonuje oceny danego zdarzenia pod względem możliwości zakwalifikowania go jako incydentu w odniesieniu do przepisów Ustawy, w tym ewentualnej konieczności dokonania zgłoszenia wystąpienia incydentu w podmiocie publicznym do właściwego CSIRT,

i) doradza i wspiera Przedstawiciela KJ w prawidłowym prowadzeniu rejestru incydentów cyberbezpieczeństwa.

3.3 Przedstawiciel KJ

3.3.1 Przedstawiciel KJ realizuje następujące zadania:

a) przyjmuje od Użytkowników i pracowników Jednostki zgłoszenia o zdarzeniach mogącym stanowić incydent cyberbezpieczeństwa lub podejrzeniu ich wystąpienia w Jednostce,

b) we współpracy z Koordynatorem KSC wstępnie weryfikuje otrzymane od Użytkowników i pracowników Jednostki informacje o zdarzeniu pod względem przesłanek identyfikujących zaistnienie incydentu cyberbezpieczeństwa,

c) gromadzi wszelkie informacje o zdarzeniu mogącym stanowić incydent cyberbezpieczeństwa oraz niezwłocznie informuje i przekazuje Koordynatorowi KSC uzyskane od pozostałych Użytkowników i pracowników Jednostki ustalenia ze zdarzeniem związane,

d) wraz z Koordynatorem KSC oraz innymi osobami zaangażowanymi przy wystąpieniu zdarzenia, dokonuje oceny danego zdarzenia pod względem możliwości zakwalifikowania go jako incydentu w odniesieniu do przepisów Ustawy, w tym ewentualnej konieczności dokonania zgłoszenia wystąpienia incydentu w podmiocie publicznym do właściwego CSIRT.

e) utrzymuje kontakt oraz pozostaje w ścisłej współpracy z Koordynatorem KSC lub wszelkimi innymi osobami w celu wzajemnej wymiany informacji w zakresie zarządzania i obsługi incydentu cyberbezpieczeństwa,

f) przekazuje Koordynatorowi KSC dane kontaktowe osoby zastępującej go w przypadku nieobecności w pracy.

g) prowadzi rejestr incydentów cyberbezpieczeństwa.

4 Przyczyny wystąpienia incydentu

Przyczynę wystąpienia incydentu cyberbezpieczeństwa mogą stanowić:

1) klęski żywiołowe,
2) pożary,
3) zakłócenia w dostawie energii elektrycznej,
4) błędy w oprogramowaniu,
5) awaria sprzętu,
6) błędy użytkowników, których wystąpienie może spowodować zniszczenie lub uszkodzenie infrastruktury informatycznej oraz zakłócenie ciągłości pracy systemów informacyjnych,
7) niewłaściwe wykorzystywanie zasobów informatycznych,
8) działanie szkodliwego oprogramowania,
9) próby omijania systemów zabezpieczeń,
10) nieautoryzowany dostęp do systemów informacyjnych i aplikacji,
11) zniszczenia lub kradzieży urządzeń wykorzystywanych do przetwarzania i przechowywania informacji,
12) zniszczenia lub kradzieży nośników danych,
13) próby wyłudzeń informacji,
14) ataki socjotechniczne.

5 Zgłaszanie zdarzeń przez Użytkowników oraz wstępna obsługa incydentu cyberbezpieczeństwa

1) Każdy Użytkownik lub pracownik Jednostki, który zaobserwuje zdarzenie mogące stanowić incydent cyberbezpieczeństwa lub podejrzewa, iż wystąpił incydent cyberbezpieczeństwa w Jednostce - w tym który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego

przez Jednostkę – zobowiązany jest poinformować o w/w okolicznościach Przedstawiciela KJ.

2) Przedstawiciel KJ na podstawie informacji otrzymanych od Użytkownika lub pracownika Jednostki o zdarzeniu mogącym stanowić incydent cyberbezpieczeństwa, niezwłocznie informuje o powyższym Koordynatora KSC.
3) Poinformowanie Koordynatora KSC, o którym mowa w pkt 2, winno nastąpić w formie telefonicznej pod numer komórkowy Koordynatora i potwierdzone w formie pisemnej za pośrednictwem poczty elektronicznej e-mail, najpóźniej do 2 godzin od wystąpienia zdarzenia lub podejrzeniu jego wystąpienia.
4) Przedstawiciel KJ we współpracy z Koordynatorem KSC dokonuje wstępnej weryfikacji otrzymanych informacji pod względem przesłanek identyfikujących zaistnienie incydentu cyberbezpieczeństwa, w tym czy stanowi on incydent w podmiocie publicznym podlegający zgłoszeniu do CSIRT NASK.
5) Przy ocenie istoty zdarzenia, o którym mowa w pkt 1, uwzględnia się następujące czynniki:
    a) wpływ zdarzenia na działanie systemów informacyjnych;
    b) wpływ zdarzenia na ciągłość realizacji zadań publicznych z wykorzystaniem systemów informacyjnych;
    c) wpływ zdarzenia na dostępność, integralność, poufności oraz autentyczności danych wykorzystywanych do realizacji zadań publicznych.
6) O wystąpieniu zdarzenia mającego charakter incydentu cyberbezpieczeństwa, Przedstawiciel KJ informuje Koordynatora KSC przekazując mu następujące informacje:
    a) wskazanie zadania publicznego, na które incydent cyberbezpieczeństwa miał wpływ,
    b) liczbę osób, na które incydent miał wpływ,
    c) moment wystąpienia i wykrycia incydentu cyberbezpieczeństwa oraz czas jego trwania,
    d) zasięg geograficzny obszaru, którego dotyczy incydent,
    e) przyczynę zaistnienia incydentu i sposób jego przebiegu oraz skutki jego oddziaływania na systemy informacyjne podmiotu publicznego;
    f) informacje o przyczynie i źródle incydentu;
    g) informacje o podjętych działaniach zapobiegawczych;

7) Informacje, o których mowa w pkt 6 powyżej, Przedstawiciel KJ przekazuje Koordynatorowi KSC za pośrednictwem poczty elektronicznej e-mail, w postaci zaszyfrowanej wiadomości. Hasło do zaszyfrowanego pliku jest przekazywane za pośrednictwem wiadomości sms wysłanej pod numer telefonu komórkowego Koordynatora KSC, przekazywany w za pośrednictwem rozmowy telefonicznej lub bezpośredniego spotkania.
8) Koordynator KSC wspólnie z Przedstawicielem KJ oraz innymi osobami zaangażowanymi w zarządzania i obsługę incydentu cyberbezpieczeństwa weryfikują zgromadzone o zdarzeniu informacje – ze szczególnym uwzględnieniem informacji, o których mowa w pkt 5 i pkt 6 – na ich podstawie dokonując ostatecznej oceny incydentu cyberbezpieczeństwa pod względem przesłanek stanowiących o zaistnieniu incydentu w podmiocie publicznym podlegającemu zgłoszeniu do CSIRT NASK.
9) Ustalenia dotyczące incydentu cyberbezpieczeństwa winny zostać odnotowane w dokumencie „Raport incydentu cyberbezpieczeństwa" - stanowiącym **załącznik nr 1** do niniejszej Procedury – przygotowywanym wspólnie przez Przedstawiciela KJ oraz Koordynatora KSC.
10) Po sporządzeniu Raportu incydentu cyberbezpieczeństwa – w przypadku gdy zdarzenie zakwalifikowano jako incydent w podmiocie publicznym – Jednostka zobowiązana jest do dokonania do właściwego CSIRT.
11) Kierownik Jednostki niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia zdarzenia, dokonuje zgłoszenia incydentu w podmiocie publicznym do CSIRT NASK zgodnie z dyspozycją przepisu art. 23 Ustawy.
12) Koordynator KSC wspiera i doradza Jednostce w przygotowaniu zgłoszenia incydentu w podmiocie publicznym, stosownie do pkt 11 powyżej.
13) Dokonując zgłoszenia incydentu w podmiocie publicznym zgodnie z pkt 12, dla wiadomości CSIRT NASK należy uwzględnić oznaczenie wszystkich informacji prawnie chronionych, w tym stanowiących tajemnicę przedsiębiorstwa jeśli takie informacje są zostaną zawarte w zgłoszeniu.
14) Po dokonaniu zgłoszenia o incydencie, o którym stanowi pkt 12, Przedstawiciel KJ w ścisłej współpracy z Koordynatorem KSC gromadzą dodatkowe informacje o incydencie cyberbezpieczeństwa na podstawie analizy systemów monitorujących, systemów zabezpieczeń, urządzeń sieciowych, logów oraz baz wiedzy

(szczególnie z uwzględnieniem przesłanek i powiązań z wcześniejszymi analogicznymi zdarzeniami lub incydentami cyberbezpieczeństwa, o ile takie występowały).

15) W przypadku powzięcia nowych informacji dotyczących obsługiwanego incydentu cyberbezpieczeństwa, Kierownik Jednostki we współpracy z Koordynatorem KSC informują o tych okolicznościach CSIRT NASK, uzupełniając wcześniejsze zgłoszenie. Punkt 11 stosuje się odpowiednio.

16) Przedstawiciel KJ po zasięgnięciu opinii Koordynatora KSC wdraża działania naprawcze i zabezpieczające mające na celu ograniczenie skutków incydentu cyberbezpieczeństwa, w szczególności incydentu w podmiocie publicznym, polegające w szczególności na:
    a) przywróceniu pełnej funkcjonalności systemu informacyjnego,
    b) zapewnienie bezpieczeństwa dla systemu informacyjnego np. zmiana haseł, wzmacnianie bezpieczeństwa instalacji i ustawień systemów (hardening), włączanie innych, wymaganych zabezpieczeń (na przykład zabezpieczeń firewall, dodatkowej kontroli dostępu, zmiany reguł w systemach IPS itp.),
    c) usunięcie z systemów śladów incydentów cyberbezpieczeństwa (min. poprzez usunięcie szkodliwego oprogramowania, odblokowanie kont użytkowników zablokowanych wskutek wystąpienia incydentu itp.),
    d) przeglądu, aktualizacji lub wdrożenia planów ciągłości działania, wpływających na realizację zadania publicznego,
    e) przeglądu oraz aktualizacji procedur i/lub polityk związanych z bezpieczeństwem informacji oraz danych osobowych,
    f) analizie incydentów cyberbezpieczeństwa, które wystąpiły w Jednostce lub jednostkach o podobnym profilu działania.
    g) po zakończeniu obsługi incydentu cyberbezpieczeństwa, w terminie nieprzekraczającym 21 dni od jego wystąpienia, Koordynator KSC przeprowadza szkolenie dla wszystkich Użytkowników,
    h) w przypadku gdy do incydentu doszło z winy umyślnej Użytkownika, przechodzi on szkolenie indywidualne z zakresu cyberbezpieczeństwa zakończone testem wiedzy.

17) W celu potwierdzenia skuteczności przeprowadzonych w Jednostce działań naprawczych i zapobiegawczych incydentom cyberbezpieczeństwa, mogą zostać

przeprowadzone dodatkowe działania weryfikacyjne do których należą: przeprowadzenie testów podatności systemu IT, jeżeli incydent spowodowany został podatnością tego systemu lub inne czynności analityczne i sprawdzające.

6 Naruszenie danych osobowych w związku z incydentem

W przypadku gdy incydent w podmiocie publicznym spowoduje naruszenie ochrony danych osobowych wówczas należy postępować zgodnie z 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) oraz z wewnętrzną procedurą stanowiącą załącznik nr ... do Polityki ochrony danych

7 Szkolenia

1. Każdy Użytkownik i pracownik Jednostki winien zostać przeszkolony z zakresu Ustawy oraz informacji o zagrożeniach cyberbezpieczeństwa.
2. Koordynator KSC z własnej inicjatywy lub na wniosek Kierownika Jednostki przeprowadza wewnętrzne szkolenia, o których mowa w pkt 1.
3. Dodatkowo szkolenia winny zostać przeprowadzane w przypadku każdej istotnej zmiany zasad lub przepisów dotyczących Ustawy w zakresie odnoszącym się do podmiotu publicznego. Przepis pkt 2 stosuje się odpowiednio.
4. W przypadku zaistnienia incydentu cyberbezpieczeństwa - po zakończeniu obsługi tego incydentu - Koordynator KSC winien przeprowadzić w terminie 21 dni od zakończenia obsługi incydentu szkolenie dla pracowników Jednostki, mające na celu przekazanie informacji o zaistniałym incydencie cyberbezpieczeństwa i prewencyjnych sposobach zabezpieczenia Jednostki przed podobnymi incydentami.
5. Każde szkolenie wewnętrzne powinno być udokumentowane poprzez sporządzenie dokumentów potwierdzających uczestnictwo w takim szkoleniu przez jego uczestników (lista obecności lub zaświadczenie/certyfikat imienny dla osoby uczestniczącej w szkoleniu).

8 Dystrybucja oraz aktualizacja Procedury

1. Niniejsza Procedura podlega regularnym (nie rzadziej niż raz na rok) przeglądom dokonywanym przez Koordynatora KSC wraz z Przedstawicielem KJ.
2. W zależności od potrzeb mogą zostać przeprowadzone także dodatkowe przeglądy po stwierdzeniu istotnego naruszenia bezpieczeństwa, pojawieniu się zasadniczych zmian w Jednostce, jej strukturze lub jej otoczeniu (nowe zagrożenia, technologie).
3. Każdy Użytkownik, który wykorzystuje system informacyjny do realizacji zadań publicznych pozostających w jego zakresie obowiązków, jest zobowiązany do zapoznania się z obowiązkami związanymi z przepisami wynikającymi z Ustawy.
4. Kierownik Jednostki zapewnia dostęp do niniejszej Procedury każdemu Użytkownikowi i pracownikowi Jednostki.
5. Każdy Użytkownik i pracownik Jednostki zobowiązany jest zapoznać się z niniejszą Procedurą oraz potwierdzić tę okoliczność w dokumencie „Wykaz osób zapoznanych z Procedurą Zarządzania Incydentami Cyberbezpieczeństwa" - którego wzór stanowi **załącznik nr 3** do niniejszej Procedury.

9. Wykaz załączników

Załącznik nr 1 – Wzór raportu incydentu cyberbezpieczeństwa,
Załącznik nr 2 – Rejestr incydentów cyberbezpieczeństwa,
Załącznik nr 3 – Wykaz osób zapoznanych z Procedurą Zarządzania Incydentami Cyberbezpieczeństwa.