ORG.120.9.2023

ZARZĄDZENIE
WÓJTA GMINY KAŹMIERZ

z dnia 15 maja 2023 r.

w sprawie zarządzania incydentami cyberbezpieczeństwa

Na podstawie art. 22 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2023 poz. 913) zarządzam, co następuje:

§ 1. Wprowadza się w Urzędzie Gminy Kaźmierz Procedurę zarządzania incydentami cyberbezpieczeństwa, stanowiącą załącznik do niniejszego Zarządzenia.

§ 2. Zarządzenie wchodzi w życie z dniem podpisania.

Wójt Gminy Kaźmierz

Zenon Gałka

Załącznik Nr 1 do zarządzenia Nr ORG.120.9.2023
Wójta Gminy Kaźmierz
z dnia 15 maja 2023 r.

PROCEDURA
ZARZĄDZANIA INCYDENTAMI CYBERBEZPIECZEŃSTWA

§ 1. Procedura zarządzania incydentami cyberbezpieczeństwa, zwana dalej „Procedurą" jest dokumentem wewnętrznym Urzędu Gminy Kaźmierz 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 (Dz.U.2023r. poz 913),
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 – Urząd Gminy Kaźmierz,
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 (Dz. U. z 2023 r. poz. 913),
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 2023 r. poz. 57), 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 (Dz. U. z 2023 r. poz. 913),
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. 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/

§ 4. Koordynator KSC realizuje następujące zadania:

1) przyjmuje od Przedstawiciela KJ informacje o zdarzeniach mogącym stanowić incydent cyberbezpieczeństwa lub podejrzeniu ich wystąpienia w Jednostce,
2) koordynuje obsługę zgłaszanych incydentów cyberbezpieczeństwa,
3) 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,
4) koordynuje wdrażanie działań naprawczych po wystąpieniu incydentu cyberbezpieczeństwa,
5) szkoli i podnosi świadomość Użytkowników i pracowników Jednostki w zakresie incydentów cyberbezpieczeństwa, ich zgłaszania, przeciwdziałania i prewencyjnych sposobach zabezpieczenia Zleceniodawcy przed ich występowaniem,
6) 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,
7) 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,
8) 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,
9) doradza i wspiera Przedstawiciela KJ w prawidłowym prowadzeniu rejestru incydentów cyberbezpieczeństwa.
10) prowadzi rejestr incydentów cyberbezpieczeństwa.

§ 5. Przedstawiciel KJ realizuje następujące zadania:

1) przyjmuje od Użytkowników i pracowników Jednostki zgłoszenia o zdarzeniach mogącym stanowić incydent cyberbezpieczeństwa lub podejrzeniu ich wystąpienia w Jednostce,
2) we współpracy z Koordynatorem KSC wstępnie weryfikuje otrzymane od Użytkowników i pracowników Jednostki informacje o zdarzeniu pod względem przesłanek identyfikujących zaistnienie incydentu cyberbezpieczeństwa,
3) 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,
4) 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.
5) 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,
6) przekazuje Koordynatorowi KSC dane kontaktowe osoby zastępującej go w przypadku nieobecności w pracy.

§ 6. 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.

§ 7. 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 i Koordynatora KCS.

2. 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.

3. Przy ocenie istoty zdarzenia, o którym mowa w pkt 1, uwzględnia się następujące czynniki:

1) wpływ zdarzenia na działanie systemów informacyjnych;
2) wpływ zdarzenia na ciągłość realizacji zadań publicznych z wykorzystaniem systemów informacyjnych;
3) wpływ zdarzenia na dostępność, integralność, poufności oraz autentyczności danych wykorzystywanych do realizacji zadań publicznych.

4. Koordynator KSC wspólnie z Przedstawicielem KJ oraz innymi osobami zaangażowanymi w zarządzania i obsługę incydentu cyberbezpieczeństwa weryfikują zgromadzone o zdarzeniu informacje na ich podstawie dokonując ostatecznej oceny incydentu cyberbezpieczeństwa pod względem przesłanek stanowiących o zaistnieniu incydentu w podmiocie publicznym podlegającemu zgłoszeniu do CSIRT NASK.

5. 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.

6. Po sporządzeniu Raportu incydentu cyberbezpieczeństwa – w przypadku gdy zdarzenie zakwalifikowano jako incydent w podmiocie publicznym – Jednostka zobowiązana jest do dokonania zgłoszenia do właściwego CSIRT.

7. 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.

8. Koordynator KSC wspiera i doradza Jednostce w przygotowaniu zgłoszenia incydentu w podmiocie publicznym, stosownie do ust. 11.

9. Dokonując zgłoszenia incydentu w podmiocie publicznym zgodnie z ust. 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.

10. Po dokonaniu zgłoszenia o incydencie, o którym stanowi ust. 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).

11. W przypadku powzięcia nowych informacji dotyczących obsługiwanego incydentu cyberbezpieczeństwa, Kierownik Jednostki przy współpracy z Koordynatorem KSC, zgodnie z ust. 11, informują o tych okolicznościach CSIRT NASK, uzupełniając wcześniejsze zgłoszenie.

12. Przedstawiciel KJ po zasięgnięciu opinii Koordynatora KSC wdraża działania naprawcze i zabezpieczające mające na celu ograniczenie skutków incydentu cyberbezpieczeństwa, polegające w szczególności na:

1) przywróceniu pełnej funkcjonalności systemu informacyjnego,
2) 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.),

3) usunięcie z systemów śladów incydentów cyberbezpieczeństwa (min. poprzez usunięcie szkodliwego oprogramowania, odblokowanie kont użytkowników zablokowanych wskutek wystąpienia incydentu itp.),
4) przeglądu, aktualizacji lub wdrożenia planów ciągłości działania, wpływających na realizację zadania publicznego,
5) przeglądu oraz aktualizacji procedur i/lub polityk związanych z bezpieczeństwem informacji oraz danych osobowych,
6) analizie incydentów cyberbezpieczeństwa, które wystąpiły w Jednostce lub jednostkach o podobnym profilu działania,
7) po zakończeniu obsługi incydentu cyberbezpieczeństwa, w terminie nieprzekraczającym 21 dni od jego wystąpienia, Koordynator KSC przeprowadza szkolenie dla wszystkich Użytkowników,
8) w przypadku gdy do incydentu doszło z winy umyślnej Użytkownika, przechodzi on szkolenie indywidualne z zakresu cyberbezpieczeństwa zakończone testem wiedzy,
9) 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,
10) wzór Rejestru incydentów cyberbezpieczeństwa stanowi załącznik nr 2 do niniejszej procedury.

§ 8. 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, określoną przez Kierownika Jednostki w Polityce Ochrony Danych odrębnym zarzadzeniem.

§ 9. 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 szkolenia pracowników, o których mowa w ust.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 ust. 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 szkoleń.

§ 10. 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.

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.

Załącznik Nr 1.1 do zarządzenia Nr ORG.120.9.2023
Wójta Gminy Kaźmierz
z dnia 15 maja 2023 r.

WZÓR RAPORTU INCYDENTU CYBERBEZPIECZEŃSTWA

I. WSTĘPNY OPIS INCYDENTU

1. Data ..... Godzina .....
2. Osoba powiadamiająca o incydencie oraz inne osoby zaangażowane lub odpytane w związku z incydentem (imię, nazwisko, stanowisko służbowe, dane kontaktowe):
.....
3. Lokalizacja zdarzenia (nr. pokoju, nazwa pomieszczenia, określenie komputerowego stanowiska roboczego, nazwa programu lub aplikacji itp.):
.....

II. WSTĘPNA ANALIZA INCYDENTU

1. Zadanie publiczne, którego dotyczy zgłoszenie:
   .....
2. Liczba osób na które incydent miał wpływ
   .....
3. Moment wystąpienia i wykrycia incydentu oraz czas jego trwania
   .....
4. Zasięg geograficzny obszaru którego incydent dotyczy
   .....
5. Przyczyna zaistnienia incydentu:
   - ☐ Podejrzana wiadomość e-mail
   - ☐ Podatności
   - ☐ Próba oszustwa
   - ☐ Złośliwe oprogramowanie
   - ☐ Nielegalne treści
   - ☐ Inny ……..
6. Źródło incydentu
   .....
7. Sposób jego przebiegu
   .....
8. Skutki jego oddziaływania na systemy informacyjne podmiotu publicznego
   .....

9. Informacja o podjętych działaniach zapobiegawczych
   ……..
10. Informacja o podjętych działaniach naprawczych - jeśli charakter incydentu pozwala podjąć je od razu.
    ……
11. Czy doszło do naruszenia danych osobowych

☐ TAK ☐ NIE

W przypadku naruszenia danych osobowych należy dodatkowo uruchomić procedurę zgłaszania naruszeń związanych z ochroną danych osobowych.

W przypadku naruszenia danych osobowych podać nr zgłoszenia z rejestru naruszeń - ……..

W przypadku informacji dotyczącej nielegalnych treści zgłoszenie należy przesłać do zespołu Dyżurnet.pl

.....
(podpisy osób obsługujących incydent)

** Do Raportu należy dołączyć kopię zgłoszenia do CSIRT NASK.*

Załącznik Nr 1.2 do zarządzenia Nr ORG.120.9.2023
Wójta Gminy Kaźmierz
z dnia 15 maja 2023 r.

REJESTR INCYDENTÓW CYBERBEZPIECZEŃSTWA

Lp.	Data zgłoszenia	Zadanie publiczne, którego dotyczy zgłoszenie	Opis zdarzenia	Kategoria incydentu	Podjęte działania zapobiegawcze	Podjęte działania naprawcze
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						

Kategoria incydentu:
A - Podejrzana wiadomość email
B - Próba oszustwa
C - Podatności
D - Złośliwe oprogramowanie
E - Nielegalne treści
F - Inny incydent

Załącznik Nr 1.3 do zarządzenia Nr ORG.120.9.2023
Wójta Gminy Kaźmierz
z dnia 15 maja 2023 r.

Wykaz osób zapoznanych

z Procedurą Zarządzania Incydentami Cyberbezpieczeństwa

Lp.	Imię i nazwisko pracownika	Podpis
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
16.		
17.		