SEROCKIE INWESTYCJE SAMORZĄDOWE Sp. z o.o.

Zarządzenie Nr 21/2025
Prezesa Zarządu spółki
Serockie Inwestycje Samorządowe Sp. z o.o.
z dnia 30 września 2025 roku

w sprawie wprowadzenia Procedury zarządzania incydentami cyberbezpieczeństwa w spółce Serockie Inwestycje Samorządowe Sp. z o.o.

Na podstawie § 10 aktu założycielskiego spółki Serockie Inwestycje Samorządowe spółka z ograniczoną odpowiedzialnością z dnia 27 sierpnia 2019 r. (t.j. Uchwała nr 14/2025 z dnia 4 sierpnia 2025 r.), art. 22 ust. 1 pkt 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913, z późn. zm.) oraz § 19 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 (Dz.U. z 2024 poz. 773) zarządza się, co następuje:

§ 1.

1. Serockie Inwestycje Samorządowe Spółka z ograniczoną odpowiedzialnością z siedzibą w Serocku wprowadza do stosowania w spółce *Procedurę zarządzania incydentami cyberbezpieczeństwa*.
2. Procedura, o której mowa w ust. 1 określa załącznik nr 1 do niniejszego zarządzenia.

§ 2.

Zarządzenie wchodzi w życie z dniem podpisania.

Prezes Zarządu
Kamila Mokrzycka

SEROCKIE INWESTYCJE SAMORZĄDOWE Sp. z o.o.

Załącznik nr 1
do Zarządzenia nr 21/2025
Prezesa Zarządu spółki
Serockie Inwestycje Samorządowe Sp. z o.o.
z dnia 30 września 2025 roku

Procedura obsługi incydentu cyberbezpieczeństwa w Serockich Inwestycjach Samorządowych Sp. z o.o.

I. Cel i zakres

Celem procedury jest określenie zasad reagowania na incydenty cyberbezpieczeństwa w Serockich Inwestycjach Samorządowych Sp. z o.o. (zwanych dalej spółką).
Procedura obejmuje wszystkich pracowników, a także podmioty współpracujące, które mają dostęp do systemów informacyjnych spółki.

II. Definicje

- Incydent – zdarzenie mające lub mogące mieć niekorzystny wpływ na cyberbezpieczeństwo.
- CSIRT – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT NASK, CSIRT GOV, CSIRT MON).
- Obsługa incydentu – wykrycie, rejestracja, analiza, klasyfikacja, działania naprawcze i ograniczenie skutków incydentu.

III. Role i odpowiedzialności

1. Koordynator ds. cyberbezpieczeństwa – osoba wyznaczona na podstawie art. 21 ust. 1 ustawy; odpowiada za kontakt z CSIRT i nadzór nad obsługą incydentów.

2. Pracownicy – obowiązani są do niezwłocznego zgłaszania wszelkich podejrzanych zdarzeń informatycznych Koordynatorowi.

3. Kierownictwo – zapewnia wsparcie organizacyjne i decyzyjne oraz akceptuje działania naprawcze.

IV. Procedura postępowania

1. Wykrycie i zgłoszenie – każdy pracownik zgłasza incydent niezwłocznie do Koordynatora ds. cyberbezpieczeństwa (telefon, e-mail, osobiście).
2. Rejestracja – Koordynator prowadzi rejestr incydentów (data, zgłaszający, opis, klasyfikacja, podjęte działania).
3. Wstępna analiza i klasyfikacja – ocena, czy incydent ma charakter incydentu w podmiocie publicznym lub potencjalnie krytycznego.
4. Zgłoszenie do *CSIRT* – incydent zgłaszany jest niezwłocznie, nie później niż w ciągu 24 godzin od wykrycia, do właściwego CSIRT (NASK/GOV/MON).

5. Obsługa incydentu – *Koordynator*, we współpracy z *CSIRT*, podejmuje działania ograniczające skutki incydentu i przywracające bezpieczeństwo systemów.
6. Działania następcze – raport końcowy, wdrożenie rekomendacji.

V. Dokumentowanie i przeglądy

1. Rejestr incydentów przechowuje się co najmniej 2 lata.
2. Procedura podlega przeglądowi nie rzadziej niż raz na 2 lata lub po każdym incydencie krytycznym.

SEROCKIE INWESTYCJE SAMORZĄDOWE Sp. z o.o.

Załącznik 1: Wzór rejestru incydentów

Data zgłoszenia	Osoba zgłaszająca	Opis incydentu	Klasyfikacja	Podjęte działania	Uwagi
.....	.....	.....	.....	.....	.....
.....	.....	.....	.....	.....	.....
.....	.....	.....	.....	.....	.....
.....	.....	.....	.....	.....	.....
.....	.....	.....	.....	.....	.....
.....	.....	.....	.....	.....	.....
.....	.....	.....	.....	.....	.....
.....	.....	.....	.....	.....	.....
.....	.....	.....	.....	.....	.....
.....	.....	.....	.....	.....	.....
.....	.....	.....	.....	.....	.....
.....	.....	.....	.....	.....	.....
.....	.....	.....	.....	.....	.....
.....	.....	.....	.....	.....	.....
.....	.....	.....	.....	.....	.....

SEROCKIE INWESTYCJE SAMORZĄDOWE Sp. z o.o.

Załącznik 2: Formularz zgłoszenia incydentu do CSIRT

1. Dane podmiotu zgłaszającego	.....
2. Dane osoby dokonującej zgłoszenia (imię, nazwisko, tel., e-mail)	.....
3. Dane osoby uprawnionej do składania wyjaśnień	.....
4. Opis incydentu i jego wpływu na realizację zadania publicznego	.....
5. Liczba osób dotkniętych incydentem	.....
6. Moment wystąpienia i wykrycia incydentu oraz czas trwania	.....
7. Zasięg geograficzny incydentu	.....
8. Przyczyna incydentu i jego przebieg	.....
9. Podjęte działania zapobiegawcze	.....
10. Podjęte działania naprawcze	.....
11. Inne istotne informacje	.....

SEROCKIE INWESTYCJE SAMORZĄDOWE Sp. z o.o.

Załącznik 3: Instrukcja wypełniania formularza zgłoszenia incydentu

1. Wpisz pełną nazwę podmiotu zgłaszającego.
2. Podaj dane osoby dokonującej zgłoszenia – imię, nazwisko, numer telefonu i adres e-mail.
3. Wpisz dane osoby uprawnionej do składania wyjaśnień (jeśli jest inna niż osoba zgłaszająca).
4. Opisz incydent – wskaż, czego dotyczy, jak wpłynął na realizację zadania publicznego (np. brak dostępu do systemu, utrata danych).
5. Podaj szacunkową liczbę osób, których dotyczy incydent (np. mieszkańcy, pracownicy).
6. Zapisz dokładny moment wystąpienia, moment wykrycia oraz czas trwania incydentu.
7. Określ obszar geograficzny, którego dotyczy incydent (np. tylko Jednostka, cała gmina).
8. Podaj przypuszczalną przyczynę incydentu (np. awaria sprzętu, atak hakerski) oraz jego przebieg.
9. Opisz działania zapobiegawcze podjęte bezpośrednio po incydencie (np. odłączenie serwera, zmiana haseł).
10. Wpisz działania naprawcze (np. przywrócenie systemu z kopii zapasowej, aktualizacja zabezpieczeń).
11. Dodaj inne informacje, które mogą być istotne dla CSIRT (np. czy zgłoszono sprawę Policji).