Burmistrz Miasta i Gminy Osiek
ul. Rynek 1, 28-221 Osiek

Zarządzenie Nr 114/2025
Burmistrza Miasta i Gminy Osiek
z dnia 13 listopada 2025 r.

w sprawie wprowadzenia Procedury zarządzania incydentami cyberbezpieczeństwa w Urzędzie Miasta i Gminy Osiek

Na podstawie art. 22 ust. 1 pkt 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t. j. Dz. U. z 2024 r. poz. 1077, 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) zarządzam, co następuje:

§1

Wprowadzona zostaje Procedura zarządzania incydentami cyberbezpieczeństwa w Urzędzie Miasta i Gminy w Osieku, stanowiąca Załącznik Nr 1 do niniejszego Zarządzenia.

§2

Zobowiązuje się pracowników Urzędu Miasta i Gminy w Osieku do zapoznania się z niniejszą procedurą

§3

Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ
Miasta i Gminy
Magdalena Marynowska

RADCA PRAWNY
Agata Cholewa
KL-K-781

Załącznik nr 1 do Zarządzenia Nr 114/2025
Burmistrza Miasta i Gminy Osiek
z dnia 13 listopada 2025 r.

Procedura zarządzania incydentami cyberbezpieczeństwa w Urzędzie Miasta i Gminy w Osieku

§ 1
INFORMACJE WSTĘPNE

Procedura zarządzania incydentami cyberbezpieczeństwa, zwana dalej „Procedurą" jest dokumentem wewnętrznym **Urzędu Miasta i Gminy w Osieku**. Opisuje zasady zarządzania incydentem cyberbezpieczeństwa stosowane przez Urząd Miasta i Gminy, dalej „Urzędem" w celu spełnienia wymagań wynikających w szczególności z:

1. Dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.U.UE.L.2022.333.80);
2. art. 22 ust. 1 pkt 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U.2024 poz. 1077 z późn. zm.);
3. § 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.2024 poz. 773).

§ 2
TERMINOLOGIA

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.
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. **Koordynator KSC** – osoba odpowiedzialna za utrzymanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.
8. **Obsługa incydentu** – czynności umożliwiające wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytet i podejmowanie działań naprawczych i ograniczenie skutków incydentu.
9. **Podatność** – właściwość systemu informacyjnego, która może być wykorzystana przez zagrożenie cyberbezpieczeństwa.
10. **System informacyjny** – zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego
11. **Użytkownik** – osoba posiadająca dostęp do systemu informacyjnego Urzędu służącego do realizacji zadania publicznego.
12. **Zagrożenie cyberbezpieczeństwa** – potencjalna przyczyna wystąpienia incydentu.
13. **Zarządzanie incydentem** – obsługa incydentu, wyszukiwanie powiązań między incydentami, usuwanie przyczyn ich wystąpienia oraz opracowywanie wniosków wynikających z obsługi incydentu.

§ 3
OSOBY ODPOWIEDZIALNE ZA CYBERBEZPIECZEŃSTWO URZĘDU

1. Burmistrz Miasta i Gminy Osiek, ponosząc odpowiedzialność w szczególności za:
   1) wyznaczenie osoby odpowiedzialnej za utrzymanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa - Koordynatora KSC;
   2) przekazanie do CSIRT NASK w terminie 14 dni od dnia wyznaczenia, danych Koordynatora KSC, a także informacji o zmianie tych danych w terminie 14 dni od dnia ich zmiany.

      Przekazanie danych Koordynatora KSC odbywa się w sposób następujący:

      a) za pośrednictwem formularza elektronicznego pod 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. Koordynator KSC, który realizuje następujące zadania:
   1) przyjmuje od Użytkowników informacje o zdarzeniach mogących stanowić incydent cyberbezpieczeństwa lub podejrzenie ich wystąpienia w Urzędzie;
   2) koordynuje obsługę zgłaszanych incydentów cyberbezpieczeństwa;
   3) przygotowuje raport incydentu cyberbezpieczeństwa w podmiocie publicznym do CSIRT NASK, zgodnie ze wzorem stanowiącym do niniejszej Procedury;
   4) dokonuje zgłoszenia incydentu w podmiocie publicznym do CSIRT NASK. Zgłoszenie incydentu odbywa się za pomocą formularza dostępnego na stronie internetowej https://incydent.cert.pl;
   5) koordynuje wdrażanie działań naprawczych po wystąpieniu incydentu cyberbezpieczeństwa;
   6) szkoli i podnosi świadomość Użytkowników oraz pozostałych pracowników Urzędu w zakresie incydentów cyberbezpieczeństwa, ich zgłaszania, przeciwdziałania i prewencyjnych sposobach zabezpieczenia przed ich występowaniem;
   7) 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;
   8) w przypadku wystąpienia incydentu cyberbezpieczeństwa ściśle współpracuje z Użytkownikami, pracownikami Urzędu, innymi osobami lub podmiotami świadczącymi Urzędowi usługi dotyczące obsługi informatycznej, w celu wdrożenia działań naprawczych;
   9) wraz z 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 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 kradzież urządzeń wykorzystywanych do przetwarzania i przechowywania informacji;
12. zniszczenia lub kradzież nośników danych;
13. próby wyłudzeń informacji;
14. ataki socjotechniczne.

§ 5

ZGŁASZANIE ZDARZEŃ PRZEZ UŻYTKOWNIKÓW ORAZ OBSŁUGA INCYDENTU CYBERBEZPIECZEŃSTWA

1. Każdy Użytkownik i/lub pracownik Urzędu, który zaobserwuje zdarzenie mogące stanowić incydent cyberbezpieczeństwa lub podejrzewa, iż wystąpił incydent cyberbezpieczeństwa w Urzędzie - w tym, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez Urząd – zobowiązany jest poinformować o w/w okolicznościach Koordynatora KSC.
2. Poinformowanie Koordynatora KSC, o którym mowa w ust. 1, winno nastąpić niezwłocznie, jednak nie później niż w terminie 2 godzin od wystąpienia zdarzenia lub podejrzenia jego wystąpienia oraz winno być potwierdzone w formie pisemnej za pośrednictwem poczty elektronicznej e-mail.
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, poufność oraz autentyczność danych wykorzystywanych do realizacji zadań publicznych.

4. Koordynator KSC wspólnie z osobami zaangażowanymi w zarządzanie i obsługę incydentu cyberbezpieczeństwa weryfikują zgromadzone o zdarzeniu informacje, w tym w szczególności informacje:
   1) opisujące wpływ incydentu w podmiocie publicznym na realizowane zadanie publiczne, w tym:
      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;
   2) informacje o przyczynie i źródle incydentu;
   3) informacje o podjętych działaniach zapobiegawczych.
5. Na podstawie informacji, o których mowa w ust. 4 dokonywana jest ostateczna ocena incydentu cyberbezpieczeństwa pod względem przesłanek stanowiących o zaistnieniu incydentu w podmiocie publicznym podlegającemu zgłoszeniu do CSIRT NASK.
6. Ustalenia dotyczące incydentu cyberbezpieczeństwa winny zostać odnotowane w dokumencie „Raport incydentu cyberbezpieczeństwa",
7. Po sporządzeniu Raportu incydentu cyberbezpieczeństwa – w przypadku, gdy zdarzenie zakwalifikowano jako incydent w podmiocie publicznym – Urząd zobowiązany jest do dokonania zgłoszenia do właściwego CSIRT.
8. Incydent cyberbezpieczeństwa, każdorazowo należy odnotować w „Rejestrze incydentów cyberbezpieczeństwa".
9. Koordynator KSC 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.
10. Dokonując zgłoszenia incydentu w podmiocie publicznym zgodnie z ust. 11, dla wiadomości CSIRT NASK należy uwzględnić oznaczenie wszystkich informacji prawnie chronionych, w tym stanowiących tajemnicę Urzędu, jeśli takie informacje są zostaną zawarte w zgłoszeniu.
11. Po dokonaniu zgłoszenia o incydencie do CSIRT NASK, Koordynator KSC gromadzi 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).

12. W przypadku powzięcia nowych informacji dotyczących obsługiwanego incydentu cyberbezpieczeństwa, Koordynator KSC informuje o tych okolicznościach CSIRT NASK, uzupełniając wcześniejsze zgłoszenie. Sposób informowana na zasadach określonych w ust. 11.
13. Koordynator KSC wdraża działania naprawcze i zabezpieczające mające na celu ograniczenie skutków incydentu cyberbezpieczeństwa, w szczególności incydentu w podmiocie publicznym, 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 antywirusowych 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;
    6) analizie incydentów cyberbezpieczeństwa, które wystąpiły w Urzędzie;
    7) po zakończeniu obsługi incydentu cyberbezpieczeństwa, w terminie nieprzekraczającym 21 dni od zakończenia obsługi incydentu, 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.
14. W celu potwierdzenia skuteczności przeprowadzonych w Urzędzie 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.)

§ 7
SZKOLENIA

1. Każdy Użytkownik i pracownik Urzędu winien zapoznać się z Ustawą oraz informacji o zagrożeniach cyberbezpieczeństwa.
2. Koordynator KSC z własnej inicjatywy lub na wniosek Burmistrza przeprowadza wewnętrzne szkolenia, o których mowa w ust. 1.
3. 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 Urzędu, mające na celu przekazanie informacji o zaistniałym incydencie cyberbezpieczeństwa i prewencyjnych sposobach zabezpieczenia Urzędu przed podobnymi incydentami.
4. 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.
2. W zależności od potrzeb mogą zostać przeprowadzone także dodatkowe przeglądy po stwierdzeniu istotnego naruszenia bezpieczeństwa, pojawieniu się zasadniczych zmian w Urzędzie, jego strukturze lub jego 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. Burmistrz Miasta i Gminy w Osieku zapewnia dostęp do niniejszej Procedury każdemu Użytkownikowi i pracownikowi Urzędu.
5. Każdy Użytkownik oraz pracownik Urzędu zobowiązany jest zapoznać się z niniejszą Procedurą potwierdzając tę okoliczność własnoręcznym podpisem na oświadczeniu stanowiącym niniejszej Procedury.

RAPORT INCYDENTU CYBERBEZPIECZEŃSTWA

I. 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 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. Sposób przebiegu incydentu

.....

7. Skutki oddziaływania incydentu na systemy informacyjne podmiotu publicznego

.....

8. Przyczyna i źródło incydentu

.....

9. Informacja o podjętych działaniach zapobiegawczych

.....

10. Informacja o podjętych lub planowanych działaniach naprawczych

.....

11. Czy doszło do naruszenia danych osobowych

☐ TAK ☐ NIE

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.

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.						
9.						
10.						

Kategorie incydentu:

A – Podejrzana wiadomość e-mail
B – Próba oszustwa
C – Podatności
D – Złośliwe oprogramowanie
E – Nielegalne treści
F - Inny incydent