Zarządzenie Nr 1038/2025

Prezydenta Miasta Rzeszowa

z dnia 19 grudnia 2025 r.

w sprawie ustalenia wewnętrznej procedury dokonywania zgłoszeń i obsługi incydentów bezpieczeństwa informacji w Urzędzie Miasta Rzeszowa

Na podstawie art. 33 ust. 1 i 2 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2025 r., poz. 1153) i § 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 r., poz. 773)

zarządza się, co następuje:

§ 1

Ustala się wewnętrzną procedurę dokonywania zgłoszeń i obsługi incydentów bezpieczeństwa informacji w Urzędzie Miasta Rzeszowa, w brzemieniu określonym w załączniku do niniejszego zarządzenia

§ 2

Wykonanie zarządzenia powierza się Sekretarzowi Miasta Rzeszowa.

§ 3

Zarządzenie wchodzi w życie z dniem podpisania.

Prezydent Miasta Rzeszowa

Konrad Fijołek

Załącznik
do zarządzenia Nr 1038/2025
Prezydenta Miasta Rzeszowa
z dnia 19 grudnia 2025 r.

Wewnętrzna procedura dokonywania zgłoszeń i obsługi incydentów bezpieczeństwa informacji w Urzędzie Miasta Rzeszowa

Słownik pojęć

§ 1

Przez użyte w niniejszej procedurze zgłaszania i obsługi incydentów bezpieczeństwa w Urzędzie Miasta Rzeszowa, zwaną dalej procedurą – określenia rozumie się:

1) Urząd – Urząd Miasta Rzeszowa;
2) Pracownik – osoba zatrudniona w Urzędzie na podstawie umowy o pracę, powołania, wyboru, a także stażysta, praktykant lub inna osoba wykonująca zadania na rzecz Urzędu na podstawie umowy cywilnoprawnej;
3) Incydent Bezpieczeństwa Informacji – każde zdarzenie, które doprowadziło lub mogło doprowadzić do naruszenia bezpieczeństwa informacji, w szczególności do naruszenia poufności, integralności lub dostępności informacji przetwarzanych w Urzędzie. Incydentem jest w szczególności:
    a) Incydent Cyberbezpieczeństwa – zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo, w rozumieniu ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;
    b) Naruszenie Ochrony Danych Osobowych – naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych, w rozumieniu art. 4 pkt 12 rozporządzenie 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) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm);
    c) Incydent Bezpieczeństwa Fizycznego – zdarzenie naruszające bezpieczeństwo fizyczne osób, mienia, pomieszczeń, budynków

lub infrastruktury technicznej Urzędu (np. kradzież, włamanie, zalanie, pożar).

4) System Qasystent – dedykowany system teleinformatyczny Urzędu, służący do ewidencji i obsługi zgłoszeń, w tym incydentów bezpieczeństwa informacji;
5) Koordynator Zgłoszeń – wyznaczony pracownik Wydziału Organizacyjno-Administracyjnego, odpowiedzialny za wstępną analizę, klasyfikację i przydział zgłoszeń incydentów;
6) Właściciel Incydentu – osoba odpowiedzialna za merytoryczną obsługę Incydentu Bezpieczeństwa Informacji po jego przydzieleniu przez Koordynatora Zgłoszeń. W zależności od kategorii Incydentu Bezpieczeństwa Informacji, Właścicielem Incydentu jest:
    a) Dyrektor Wydziału Zarządzania Infrastrukturą Urzędu – dla Incydentów Bezpieczeństwa Fizycznego;
    b) Zastępca Dyrektora Biura Obsługi Informatycznej i Telekomunikacyjnej (dalej: Zastępca Dyrektora OI) – dla Incydentów Cyberbezpieczeństwa;
    c) Dyrektor Wydziału Kontroli i Nadzoru (dalej: Dyrektor WKN) – dla Naruszeń Ochrony Danych Osobowych.
7) Zespół ds. Obsługi Incydentów (dalej: ZOI) – zespół składający się z Koordynatora Zgłoszeń oraz Właścicieli Incydentów, powoływany przez Sekretarza Miasta Rzeszowa doraźnie w celu koordynacji działań przy obsłudze Incydentów Bezpieczeństwa Informacji złożonych lub o wysokim priorytecie.

Przedmiot i zakres stosowania

§ 2

1. Niniejsza procedura określa zasady i tryb postępowania w przypadku wystąpienia lub podejrzenia wystąpienia Incydentu Bezpieczeństwa Informacji w Urzędzie.
2. Procedurę stosują wszyscy Pracownicy Urzędu.
3. Każdy Pracownik, który stwierdził lub powziął uzasadnione podejrzenie wystąpienia Incydentu Bezpieczeństwa Informacji, jest zobowiązany do jego niezwłocznego zgłoszenia, zgodnie z zasadami określonymi w § 3 niniejszej procedury.

Kanały zgłoszeń

§ 3

Zgłoszenia Incydentów Bezpieczeństwa Informacji dokonuje się w trybie priorytetowym, za pośrednictwem jednego z poniższych kanałów:

1) System Qasystent (kanał podstawowy):
    a) zgłaszający dokonuje zgłoszenia poprzez dedykowany formularz „Incydent Bezpieczeństwa Informacji";
    b) w formularzu zgłoszenia należy podać możliwie najdokładniejsze informacje, w tym co najmniej;
        - datę i godzinę stwierdzenia zdarzenia;
        - przybliżoną datę i godzinę wystąpienia zdarzenia (jeśli jest znana);
        - dokładny opis zdarzenia, w tym zaobserwowane skutki;
        - miejsce zdarzenia (np. adres lokalu, numer pokoju, nazwa systemu teleinformatycznego);
        - zaangażowane zasoby (np. komputer, serwer, dokument papierowy);
        - dane kontaktowe osoby zgłaszającej (imię, nazwisko, numer telefonu).
    c) do zgłoszenia należy dołączyć wszelkie materiały mogące pomóc w analizie, np. zrzuty ekranu, zdjęcia.
2) Telefonicznie (kanał pomocniczy):
    a) dopuszcza się zgłoszenie telefoniczne wyłącznie w sytuacji, gdy dokonanie zgłoszenia przez System Qasystent jest niemożliwe (np. awaria systemu, brak dostępu do komputera);
    b) zgłoszenia telefoniczne przyjmuje Koordynator Zgłoszeń;
    c) koordynator Zgłoszeń, przyjmując zgłoszenie, sporządza notatkę służbową zawierającą informacje wskazane w pkt 1 lit. b niniejszego paragrafu i niezwłocznie rejestruje zgłoszenie w Systemie Qasystent, załączając do niego sporządzoną notatkę.

Rejestracja, klasyfikacja i przydział Incydentu Bezpieczeństwa Informacji

§ 4

1. Po dokonaniu klasyfikacji, Koordynator Zgłoszeń bez zbędnej zwłoki przydziela zgłoszenie w Systemie Qasystent do właściwego Właściciela Incydentu w celu podjęcia dalszych działań.
2. W przypadku, gdy Incydent Bezpieczeństwa Informacji ma charakter mieszany (np. kradzież laptopa z danymi osobowymi), Koordynator Zgłoszeń przydziela zgłoszenie do wszystkich właściwych Właścicieli Incydentów, wyznaczając jednego z nich jako Wiodącego Właściciela Incydentu, odpowiedzialnego za koordynację

całości działań i finalne raportowanie.

3. W przypadku wątpliwości co do klasyfikacji, Koordynator Zgłoszeń konsultuje się z potencjalnymi Właścicielami Incydentów.

Obsługa i analiza Incydentu Bezpieczeństwa Informacji

§ 5

Właściciel Incydentu po otrzymaniu zgłoszenia jest zobowiązany do:

1) oceny zasadności zgłoszenia i oceny priorytetu Incydentu Bezpieczeństwa Informacji;
2) niezwłocznego podjęcia działań powstrzymujących i ograniczających skutki Incydentu Bezpieczeństwa Informacji (np. odizolowanie systemu z sieci, zablokowanie konta użytkownika, zabezpieczenie pomieszczenia, wezwanie odpowiednich służb);
3) przeprowadzenia szczegółowej analizy mającej na celu ustalenie przyczyn, przebiegu i skutków Incydentu Bezpieczeństwa Informacji;
4) zabezpieczenia materiału dowodowego (np. logów systemowych, kopii dysków, nagrań z monitoringu) w sposób gwarantujący jego integralność i autentyczność;
5) bieżącego i rzetelnego dokumentowania wszystkich podjętych czynności i ustaleń w Systemie Qasystent.

Szczególne obowiązki

§ 6

1. W przypadku podejrzenia lub stwierdzenia Naruszenia Ochrony Danych Osobowych, Dyrektor WKN lub osoba przez niego wyznaczona, jako Właściciel Incydentu, dokonuje we współpracy z Inspektorem Ochrony Danych Urzędu Miasta Rzeszowa (dalej: IOD) oceny ryzyka naruszenia praw lub wolności osób fizycznych.
2. W przypadku stwierdzenia wysokiego ryzyka naruszenia praw lub wolności, o którym mowa w ust. 1, IOD przygotowuje rekomendację oraz projekt zawiadomienia osób, których dane dotyczą. Czynności te realizowane są w porozumieniu z komórka organizacyjną Urzędu, w której stwierdzono naruszenie.
3. Za skuteczne przekazanie (wysyłkę) zawiadomienia do osób, których dane dotyczą, odpowiada kierownik komórki organizacyjnej, w której doszło do naruszenia.
4. Dyrektor WKN lub osoba przez niego wyznaczona jest odpowiedzialna za przygotowanie projektu zgłoszenia naruszenia do Prezesa Urzędu Ochrony

Danych Osobowych i przedłożenie go do akceptacji Administratora (Prezydenta Miasta), z zachowaniem terminu 72 godzin od stwierdzenia naruszenia.

5. W przypadku wystąpienia Incydentu Cyberbezpieczeństwa podlegającego obowiązkowi zgłoszenia zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa, właściwy Właściciel Incydentu przygotowuje projekt zgłoszenia do właściwego CSIRT (Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego) i przedkłada go do akceptacji Prezydenta Miasta lub osoby przez niego upoważnionej.
6. W przypadkach uzasadnionych przepisami prawa lub skalą incydentu (np. podejrzenie popełnienia przestępstwa), właściwy Właściciel Incydentu, po uzyskaniu akceptacji Prezydenta Miasta lub Sekretarza Miasta, dokonuje zgłoszenia do organów ścigania.

Zamykanie Incydentu Bezpieczeństwa Informacji i działania poincydentalne

§ 7

1. Po zakończeniu analizy i działań naprawczych, Właściciel Incydentu sporządza raport z obsługi Incydentu Bezpieczeństwa Informacji, który załącza do zgłoszenia w Systemie Qasystent.
2. Raport, o którym mowa w ust. 1, musi zawierać co najmniej:
   1) unikalny numer zgłoszenia;
   2) chronologiczny opis zdarzenia i podjętych działań;
   3) ustalenia dotyczące przyczyn i skutków Incydentu Bezpieczeństwa Informacji;
   4) ocenę wpływu Incydentu Bezpieczeństwa Informacji na działanie Urzędu oraz bezpieczeństwo informacji, w tym danych osobowych;
   5) rekomendacje działań korygujących i zapobiegawczych mających na celu uniknięcie podobnych Incydentów Bezpieczeństwa Informacji w przyszłości;
   6) informację o dokonanych zgłoszeniach do organów zewnętrznych (UODO, CSIRT, Policja).
3. Po załączeniu kompletnego raportu, o którym mowa w ust. 1 Właściciel Incydentu dokonuje formalnego zamknięcia obsługi incydentu w Systemie Qasystent.
4. Koordynator Zgłoszeń dokonuje weryfikacji kompletności dokumentacji zamkniętego Incydentu Bezpieczeństwa Informacji.
5. Po analizie, ZOI (w przypadku powołania) przedstawia Sekretarzowi Miasta Rzeszowa propozycje wdrożenia działań naprawczych, które po akceptacji są przekazywane do realizacji właściwym komórkom organizacyjnym Urzędu.

6. Realizacja wdrożonych rekomendacji podlega monitorowaniu.

Postanowienia końcowe

§ 8

1. Wszyscy pracownicy Urzędu są zobowiązani do pełnej i niezwłocznej współpracy z Koordynatorem Zgłoszeń i Właścicielami Incydentów w procesie obsługi incydentu.
2. Wszelkie informacje dotyczące zgłoszonych i obsługiwanych incydentów stanowią tajemnicę służbową i nie mogą być ujawniane osobom nieupoważnionym.