

Warszawa, dnia 12 czerwca 2023 r.

Poz. 12

**ZARZĄDZENIE NR 3  
PREZESA GŁÓWNEGO URZĘDU MIAR**

z dnia 12 czerwca 2023 r.

**w sprawie postępowania z incydentami bezpieczeństwa informacji  
w Głównym Urzędzie Miar**

Na podstawie § 20 ust. 2 pkt 13 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 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 2017 r. poz. 2247) oraz art. 22 i art. 23 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913) zarządza się, co następuje:

§ 1. Zarządzenie reguluje sposób postępowania z incydentami bezpieczeństwa informacji w Głównym Urzędzie Miar, zwanym dalej „GUM”.

§ 2. Użyte w zarządzeniu pojęcia oznaczają:

- 1) incydent bezpieczeństwa informacji – zdarzenie, które ma lub może mieć niekorzystny wpływ na bezpieczeństwo informacji w GUM;
- 2) incydent cyberbezpieczeństwa – incydent bezpieczeństwa informacji w rozumieniu art. 2 pkt 5 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913);
- 3) incydent krytyczny – incydent bezpieczeństwa informacji w rozumieniu art. 2 pkt 6 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;
- 4) obsługa incydentu bezpieczeństwa informacji – obsługę incydentu bezpieczeństwa informacji w rozumieniu art. 2 pkt 10 ustawy z dnia 5 lipca 2023 r. o krajowym systemie cyberbezpieczeństwa;
- 5) system HelpDesk – system pomocy technicznej GUM;
- 6) Zespół – zespół ds. bezpieczeństwa informacji, o którym mowa w decyzji Prezesa Głównego Urzędu Miar dotyczącej ustanowienia oraz określenia zadań pełnomocnika Prezesa Głównego Urzędu Miar do spraw Zintegrowanego Systemu Zarządzania.

§ 3. 1. Pracownik, w przypadku wykrycia wystąpienia incydentu bezpieczeństwa informacji, zwanego dalej incydemtem”, niezwłocznie dokonuje jego zgłoszenia w systemie HelpDesk.

2. Zgłoszenie incydentu powinno zawierać:

- 1) opis symptomów wystąpienia incydentu;
- 2) wskazanie okoliczności i czasu, w jakich zgłaszający zetknął się z incydemtem;

3) informacje, które mogą wskazywać na przyczynę wystąpienia incydentu, o ile zgłaszający incydent posiada te informacje.

3. W przypadku braku dostępności systemu HelpDesk lub sytuacji wymagającej natychmiastowego działania, pracownik dokonuje zgłoszenia drogą elektroniczną na adres [incydenty@gum.gov.pl](mailto:incydenty@gum.gov.pl) lub telefonicznie albo osobiście kierownikowi komórki organizacyjnej GUM właściwej do spraw bezpieczeństwa, który przekazuje informacje o zgłoszeniu przewodniczącemu Zespołu w celu obsługi incydentu.

§ 4. Pracownik, który dokonał zgłoszenia, zobowiązany jest do:

- 1) podjęcia czynności niezbędnych dla powstrzymania niepożądanych skutków zaistniałego naruszenia;
- 2) niepodejmowania działań, które wiążą się z zaistniałym naruszeniem i mogą utrudnić jego udokumentowanie i analizę;
- 3) powstrzymanie się od pracy w systemie teleinformatycznym, a w przypadku podejrzenia cyberataku, wyłączenia urządzenia;
- 4) zabezpieczenia dostępu do pomieszczenia, nośników informacji i urządzeń służących do przetwarzania informacji, a także zabezpieczenia dowodów incydentu;
- 5) współpracy z pracownikami uczestniczącymi w obsłudze incydentu, w szczególności stosowania się do wskazówek Przewodniczącego Zespołu oraz koordynatora obsługi incydentu, o którym mowa w § 5 ust. 2.

§ 5. 1. Przewodniczący Zespołu zapoznaje się z zaistniałą sytuacją, weryfikuje, czy zgłoszenie dotyczy bezpieczeństwa informacji oraz czy wskazuje na wystąpienie incydentu.

2. W przypadku zaklasyfikowania zgłoszenia jako incydent Przewodniczący Zespołu zwołuje posiedzenie Zespołu oraz wyznacza koordynatora obsługi incydentu spośród członków Zespołu.

3. Jeżeli charakter incydentu tego wymaga, Przewodniczący Zespołu niezwłocznie:

- 1) zawiadamia odpowiednie służby porządkowe;
- 2) udziela wskazówek osobie dokonującej zgłoszenia w zakresie dalszego postępowania.

4. W przypadku zakwalifikowania zgłoszenia jako niedotyczącego bezpieczeństwa informacji, zgłoszenie jest zamykane, o czym informowany jest pracownik dokonujący zgłoszenia.

§ 6. W ramach obsługi incydentu Zespół:

- 1) podejmuje niezbędne działania, mające zminimalizować skutki incydentu;
- 2) przeprowadza postępowanie wyjaśniające;
- 3) zabezpiecza dostępne dowody;
- 4) wdraża plan przywrócenia właściwych warunków działania;
- 5) dokonuje analizy pod kątem, wystąpienia incydentu krytycznego lub incydentu cyberbezpieczeństwa;
- 6) podejmuje działania naprawcze i rekomenduje działania zapobiegawcze;
- 7) dokumentuje incydent w postaci raportu z incydentu, którego wzór określa załącznik nr 1 do zarządzenia;
- 8) nadaje mu priorytet, wynikający z istotności jego wpływu na funkcjonowanie GUM, konieczności natychmiastowej reakcji i podjęcia właściwych działań, uwzględniając wytyczne określone w załączniku nr 2 do zarządzenia;
- 9) przekazuje pracownikowi, który dokonał zgłoszenia, informacje o działaniach, jakie podjęto w następstwie zgłoszenia.

§ 7. Przewodniczący Zespołu:

- 1) prowadzi rejestr zgłoszonych incydentów, zgodnie ze wzorem rejestru określonym w załączniku nr 3 do zarządzenia;

- 2) niezwłocznie informuje Kierownictwo GUM o wystąpieniu incydentu krytycznego lub incydentu cyberbezpieczeństwa oraz we współpracy z koordynatorem zapewnia obsługę incydentu krytycznego lub incydentu cyberbezpieczeństwa zgodnie z ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;
- 3) koordynuje przygotowanie i aktualizowanie przez Zespół planów ciągłości działania;
- 4) dokonuje przeglądu incydentów, jak również danych z obsługi incydentów;
- 5) sporządza Kierownictwu GUM, nie rzadziej niż raz na 6 miesięcy, raport o obsłużonych incydentach, zawierający rekomendacje w zakresie działań doskonalących, którego wzór określa załącznik nr 4 do zarządzenia.

§ 8. Upoważnieni pracownicy GUM, zawierając umowę z podmiotem zewnętrznym, zobowiązani są do zamieszczenia w umowie klauzul zobowiązujących podmiot zewnętrzny do zgłaszania zdarzeń, incydentów oraz podatności związanych z bezpieczeństwem informacji pozyskanych w ramach ich realizacji za pośrednictwem osób do kontaktu wskazanych w umowie.

§ 9. Przewodniczący Zespołu po raz pierwszy sporządzi raport, o którym mowa w § 7 pkt 5, w terminie 6 miesięcy od dnia wejścia w życie zarządzenia.

§ 10. Informacje dotyczące incydentów są uwzględniane w ramach monitorowania i oceny ryzyka zgodnie z odrębnymi regulacjami obowiązującymi w GUM.

§ 11. Do incydentów w sprawach wszczętych i niezakończonych przed dniem wejścia w życie niniejszego zarządzenia stosuje się przepisy dotychczasowe.

§ 12. Traci moc zarządzenie nr 4 Prezesa Głównego Urzędu Miar z dnia 24 lutego 2021 r. w sprawie postępowania z incydentami naruszenia bezpieczeństwa informacji w Głównym Urzędzie Miar.

§ 13. Zarządzenie wchodzi w życie z dniem następującym po dniu podpisania.

Prezes Głównego Urzędu Miar: *Jacek Semaniak*

Załącznik nr 1 do zarządzenia  
Prezesa Głównego Urzędu Miar  
z dnia 12 czerwca 2023 r. (poz. 12)

WZÓR RAPORTU Z INCYDENTU	
Raport z incydentu bezpieczeństwa informacji	
<b>Dane koordynatora obsługi incydentu</b>	
Imię i nazwisko, stanowisko	
Komórka organizacyjna	
Telefon	
<b>Informacje o incydencie</b>	
Data i godzina wystąpienia	
Data i godzina przyjęcia zgłoszenia	
Miejsce wystąpienia incydentu	
Opis naruszenia bezpieczeństwa informacji (w tym przyczyna zaistnienia incydentu i sposób jego przebiegu)	
Obszar oddziaływania w GUM	<input type="checkbox"/> <i>Bezpieczeństwo danych osobowych</i>
	<input type="checkbox"/> <i>Bezpieczeństwo systemu teleinformatycznego</i>
	<input type="checkbox"/> <i>Bezpieczeństwo fizyczne</i>
	<input type="checkbox"/> <i>Inne: .....</i>
KO, których dotyczą skutki incydentu	
Zakres aktywów, których dotyczy incydent	
Priorytet incydentu	<i>Wybierz element.</i>
Naruszone atrybuty bezpieczeństwa	<input type="checkbox"/> <i>Poufność</i>
	<input type="checkbox"/> <i>Integralność</i>
	<input type="checkbox"/> <i>Dostępność</i>
	<input type="checkbox"/> <i>Inne atrybuty: .....</i>
Rodzaj ujawnionej informacji (jeżeli dotyczy)	
<b>Postępowanie z incydem</b>	
Opis podjętych działań	
Przyczyny wystąpienia incydentu	
Skutki zdarzenia lub incydentu (zewnętrzne/wewnętrzne)	
Prognozowany czas likwidacji skutków	
Szacunkowe koszty	

Dalsze działania naprawcze i zapobiegawcze (w przypadku braku możliwości natychmiastowej likwidacji skutków)	
Wykaz poinformowanych osób lub KO	
Wykaz poinformowanych podmiotów zewnętrznych	
Data zakończenia postępowania wyjaśniającego	
Zalecenia/rekomendacje	
Załączniki (materiał dowodowy)	

.....

Koordinator obsługi incydentu  
/akceptacja w EZD/

.....

Przewodniczący Zespołu do spraw bezpieczeństwa informacji  
/akceptacja w EZD/

Załącznik nr 2 do zarządzenia  
Prezesa Głównego Urzędu Miar  
z dnia 12 czerwca 2023 r. (poz. 12)

**WYTYCZNE DO NADAWANIA PRIORYTETÓW  
INCYDENTOM BEZPIECZEŃSTWA INFORMACJI**

**Tabela priorytetyzacji incydentów bezpieczeństwa informacji**

Priorytet	Opis potencjalnych skutków incydentu		Max. czas na podjęcie działań po otrzymaniu zgłoszenia	Max. czas obsługi incydentu
<b>NISKI</b>	Incydent nie generuje skutków prawnych, strat finansowych i wizerunkowych dla GUM; może skutkować pośrednio lub bezpośrednio krótkotrwałymi utrudnieniami w funkcjonowaniu pojedynczej komórki organizacyjnej GUM.		do 48 h	do 21 dni
<b>ŚREDNI</b>	Incydent może naruszać regulacje wewnętrzne GUM; skutkuje pośrednio lub bezpośrednio co najmniej kilkugodzinnymi utrudnieniami w realizacji zadań przez kilka komórek organizacyjnych; może negatywnie wpływać na wizerunek GUM lub generować straty finansowe.	krótkotrwała (2 h - 8 h) niedostępność usług/systemów, zakłócenia w funkcjonowaniu	do 24 h	do 7 dni
<b>WYSOKI</b>	Incydent może skutkować naruszeniem prawa powszechnie obowiązującego, skutkuje pośrednio lub bezpośrednio długotrwałymi utrudnieniami w funkcjonowaniu większości komórek organizacyjnych; może wpływać na podejmowanie decyzji przez kierownictwo GUM; generuje straty finansowe powyżej 100.000 zł oraz negatywnie wpływa na wizerunek GUM.	długotrwała (pow. 8 h) niedostępność usług/systemów/ zakłócenia w funkcjonowaniu	do 4 h	do 2 dni

Załącznik nr 3 do zarządzenia  
Prezesa Głównego Urzędu Miar  
z dnia 12 czerwca 2023 r. (poz. 12)

**WZÓR REJESTRU INCYDENTÓW BEZPIECZEŃSTWA INFORMACJI**

Lp.	Rok	Nr incydentu (rok/nr)	Obszar incydentu	Data zgłoszenia incydentu (rrrr-mm-dd 00:00)	Miejsce incydentu	Dane osoby zgłaszającej	Priorytet wykonania	Opis incydentu (w tym przyczyny jego zaistnienia, sposób przebiegu i skutki)
1	2	3	4	5	6	7	8	9

Wpływ incydentu w podmiocie publicznym na realizowane zadanie publiczne* * należy wypełnić w przypadku incydentów w obszarze cyberbezpieczeństwa									
Zadanie publiczne, na które incydent miał wpływ i opis wpływu incydentu na to zadanie	Liczba osób, na które incydent miał wpływ	Zasięg geograficzny obszaru, którego dotyczy incydent	Skutki oddziaływania incydentu na systemy informacyjne podmiotu publicznego	Data i godzina wystąpienia incydentu (rrrr-mm-dd 00:00)	Data i godzina wykrycia incydentu (rrrr-mm-dd 00:00)	Czas trwania incydentu	Czy incydent wymaga zgłoszenia do CSIRT? (TAK/NIE)	Data i godzina zgłoszenia incydentu do CSIRT (rrrr-mm-dd 00:00)	Osoby uprawnione do złożenia wyjaśnień ws. incydentu
10	11	12	13	14	15	16	17	18	19

Podjęte działania zapobiegawcze	Podjęte działania naprawcze i ocena ich skuteczności	Dane osoby/osób odpowiedzialnej/-ych za obsługę incydentu	Sporządzono Raport dot. incydentu TAK/NIE	Status	Data zakończenia obsługi incydentu
20	21	22	23	24	25

Załącznik nr 4 do zarządzenia  
Prezesa Głównego Urzędu Miar  
z dnia 12 czerwca 2023 r. (poz. 12)

## WZÓR RAPORTU O OBSŁUŻONYCH INCYDENTACH BEZPIECZEŃSTWA INFORMACJI

Raport o obsłużonych incydentach bezpieczeństwa informacji w Głównym Urzędzie Miar			
NR RAPORTU			
DATA SPORZĄDZENIA RAPORTU			
RAPORT ZA OKRES od .....do .....			
1. Analiza incydentów związanych z bezpieczeństwem informacji			
1.1. Liczba obsłużonych incydentów:			
1.2. Liczba incydentów o priorytecie: wysokim: ... średnim: ... niskim: ...			
1.3. Obszar oddziaływania w GUM: <input type="checkbox"/> Bezpieczeństwo danych osobowych <input type="checkbox"/> Bezpieczeństwo systemu teleinformatycznego <input type="checkbox"/> Bezpieczeństwo fizyczne <input type="checkbox"/> Inne:.....			
1.4. Czy procedury zarządzania incydentami w GUM były skuteczne? <i>(należy uzasadnić)</i>			
1.5. Czy o incydentach powiadomiono podmioty zewnętrzne? <input type="checkbox"/> TAK <input type="checkbox"/> NIE  Jeśli tak – jakie?.....			
2. Informacja o działaniach zapobiegawczych			
2.1. Jakie działania zapobiegawcze zostały wdrożone?			
2.2. Propozycja dalszych działań zapobiegawcze.			
Działanie 1:			
Odpowiedzialny:		Termin realizacji:	
Działanie 2:			
Odpowiedzialny:		Termin realizacji:	
3. Załączniki do raportu			



Sporządził	Akceptacja członków Zespołu ds. bezpieczeństwa informacji
..... Przewodniczący Zespołu do spraw bezpieczeństwa informacji /akceptacja w EZD/	..... /imię, nazwisko i akceptacja w EZD/