Warszawa, dnia 27 stycznia 2025 r.

Poz. 7

ZARZĄDZENIE NR 2
PREZESA GŁÓWNEGO URZĘDU MIAR

z dnia 27 stycznia 2025 r.

w sprawie postępowania z incydentami bezpieczeństwa informacji w Głównym Urzędzie Miar

Na podstawie art. 22 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222), § 19 ust. 1 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. poz. 773) oraz § 3 ust. 1 regulaminu organizacyjnego Głównego Urzędu Miar stanowiącego załącznik do zarządzenia nr 1 Prezesa Głównego Urzędu Miar z dnia 22 lutego 2024 r. w sprawie nadania regulaminu organizacyjnego Głównemu Urzędowi Miar (Dz. Urz. GUM poz. 8, 20 i 31) 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 – incydent bezpieczeństwa informacji będący zdarzeniem, które ma lub może mieć niekorzystny wpływ na bezpieczeństwo informacji w GUM;

2) incydent cyberbezpieczeństwa – incydent w rozumieniu art. 2 pkt 5 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222);

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 cyberbezpieczeństwa – obsługę incydentu w rozumieniu art. 2 pkt 10 ustawy z dnia 5 lipca 2018 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, 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 incydentem;

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 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, jest zobowiązany 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) powstrzymania 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 w trybie stacjonarnym lub zdalnym 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 jest informowany 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, którego wzór określa załącznik 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, są zobowiązani do sprawdzenia czy w umowie zostały zamieszczone klauzule zobowiązujące podmiot zewnętrzny do zgłaszania zdarzeń, incydentów oraz podatności związanych z bezpieczeństwem informacji pozyskanych w ramach realizacji umowy, za pośrednictwem osób do kontaktu wskazanych w umowie.

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

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

§ 11. Traci moc zarządzenie nr 3 Prezesa Głównego Urzędu Miar z dnia 12 czerwca 2023 r. w sprawie postępowania z incydentami bezpieczeństwa informacji w Głównym Urzędzie Miar.

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

Prezes Głównego Urzędu Miar: *Jacek Semaniak*

(podpisano elektronicznie)

Załączniki do zarządzenia nr 2
Prezesa Głównego Urzędu Miar
z dnia 27 stycznia 2025 r.
(Dz. Urz. GUM poz. 7)

Załącznik nr 1

WZÓR RAPORTU Z INCYDENTU

Raport ze zdarzenia/ incydentu/podatności związanego z bezpieczeństwem informacji		
Dane osoby/osób odpowiedzialnego/-ych za obsługę zdarzenia/incydentu/podatności		
Imię i nazwisko, stanowisko		
Komórka organizacyjna		
Telefon		
Informacje o incydencie		
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	☐	*Bezpieczeństwo danych osobowych*
	☐	*Bezpieczeństwo systemu teleinformatycznego*
	☐	*Bezpieczeństwo fizyczne*
	☐	*Inne:…..*
KO, których dotyczą skutki incydentu		
Zakres aktywów, których dotyczy incydent		
Priorytet incydentu	*Wybierz element.*	
Naruszone atrybuty bezpieczeństwa	☐	*Poufność*
	☐	*Integralność*
	☐	*Dostępność*
	☐	*Inne atrybuty:……*
Rodzaj ujawnionej informacji (jeżeli dotyczy)		
Postępowanie z incydentem		
Opis podjętych działań		
Przyczyny wystąpienia incydentu		
Skutki zdarzenia lub incydentu (zewnętrzne/wewnętrzne)		
Prognozowany czas likwidacji skutków		
Szacunkowe koszty		

Załącznik nr 2

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**
NISKI	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
ŚREDNI	Incydent może naruszać regulacje wewnętrzne GUM; skutkuje pośrednio lub bezpośrednio co najmniej kilkugodzinnymi utrudnieniami w realizacji zadań przez kilka komórek organizacyjnych GUM; 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
WYSOKI	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

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)

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 incyde--nt miał wpływ	Zasięg geogra--ficzny obszaru, którego dotyczy incydent	Skutki oddziaływa--nia incydentu na systemy informa--cyjne 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

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

Załącznik nr 4

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: ☐ Bezpieczeństwo danych osobowych ☐ Bezpieczeństwo systemu teleinformatycznego ☐ Bezpieczeństwo fizyczne ☐ Inne:…..			
1.4. Czy procedury zarządzania incydentami w GUM były skuteczne? *(należy uzasadnić)*			
1.5. Czy o incydentach powiadomiono podmioty zewnętrzne? ☐ TAK ☐ NIE Jeśli tak – jakie?.....			
2. Informacja o działaniach zapobiegawczych			
2.1. Jakie działania zapobiegawcze zostały wdrożone?			
2.2. Propozycja dalszych działań zapobiegawczych.			
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/	