Warszawa, dnia 27 stycznia 2025 r.

Poz. 6

ZARZĄDZENIE NR 1
PREZESA GŁÓWNEGO URZĘDU MIAR

z dnia 27 stycznia 2025 r.

w sprawie polityki bezpieczeństwa informacji Głównego Urzędu Miar

Na podstawie art. 16 ust. 1 pkt 9 ustawy z dnia 11 maja 2001 r. – Prawo o miarach (Dz. U. z 2022 r. poz. 2063) w związku z art. 1 i art. 2 ust. 1 pkt 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2024 r. poz. 1557 i 1717), § 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:

Rozdział 1
Przepisy ogólne

§ 1. 1. Polityka bezpieczeństwa informacji Głównego Urzędu Miar, zwana dalej „polityką”, określa podstawowe zasady zarządzania systemem zarządzania bezpieczeństwem informacji, zwanym dalej „SZBI”, oraz podmioty odpowiedzialne za ochronę informacji w Głównym Urzędzie Miar, zwanym dalej „GUM”, w celu zapewnienia odpowiedniego poziomu bezpieczeństwa informacji w GUM.

2. Kierownictwo GUM w pełni wspiera podejmowane działania zmierzające do zapewnienia bezpieczeństwa informacji w GUM, a także zapewnia niezbędne środki na ich realizację.

3. Za prawidłową realizację polityki odpowiada Zespół do spraw 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, zwany dalej „Zespołem”.

4. Do przestrzegania polityki zobowiązani są wszyscy użytkownicy korzystający z aktywów GUM.

§ 2. Użyte w zarządzeniu określenia oznaczają:

1) aktywa – wszystko, co stanowi wartość dla GUM i w związku z tym wymaga ochrony, w szczególności:

   a) aktywa informacyjne – wiedza, dane oraz wszelkie informacje wpływające na wartość GUM, w tym informacje udokumentowane,
   b) zasoby ludzkie – pracownicy i ich wiedza, umiejętności, doświadczenie i kwalifikacje,
   c) usługi i licencje,
   d) wartości niematerialne, w tym: wizerunek, kultura organizacyjna i wartości etyczne,
   e) systemy teleinformatyczne i cyberprzestrzeń GUM,

f) urządzenia dostępowe i oprogramowanie,
g) zabezpieczenia fizyczne, środowiskowe, techniczne i organizacyjne,
h) siedziba i nieruchomości oraz poszczególne pomieszczenia użytkowane przez GUM;

2) bezpieczeństwo informacji – zabezpieczenie i zachowanie informacji w zakresie integralności, dostępności i poufności przed nieautoryzowanym dostępem lub zmianą, uwzględniając rozliczalność, autentyczność, niezaprzeczalność i niezawodność;

3) incydent – incydent bezpieczeństwa informacji będący zdarzeniem, które ma lub może mieć niekorzystny wpływ na bezpieczeństwo informacji w GUM;

4) podatność – właściwość aktywa lub grupy aktywów, która może być wykorzystana przez co najmniej jedno zagrożenie;

5) sytuacja awaryjna – zdarzenie, którego skutki powodują utratę ciągłości działania GUM; może dotyczyć jednej lub kilku komórek organizacyjnych GUM, których procesy zostały zakłócone;

6) sytuacja kryzysowa – niespodziewane i niepożądane zdarzenie lub serię takich zdarzeń związanych z bezpieczeństwem przetwarzania informacji, w szczególności w systemach teleinformatycznych, które mogą zakłócić lub zakłócają proces realizacji zadań GUM; sytuacja kryzysowa może dotyczyć w szczególności bezpieczeństwa ludzi, mienia w znacznych rozmiarach lub środowiska, wywołując znaczne ograniczenia w funkcjonowaniu GUM;

7) użytkownik – osobę fizyczną korzystającą z systemów teleinformatycznych oraz innych aktywów GUM, w szczególności pracownika, osobę świadczącą usługi, realizującą dostawy oraz wykonującą roboty budowlane na rzecz GUM na podstawie umowy cywilnoprawnej, w tym umowy zlecenia lub umowy o dzieło, osobę odbywającą praktykę, staż lub wolontariat, eksperta oraz pracownika podmiotu zewnętrznego realizującego zadania na rzecz GUM, który uzyskał uprawnienie albo upoważnienie do przetwarzania danych osobowych w danym zakresie, w tym do przetwarzania informacji w systemach teleinformatycznych;

8) zabezpieczenie – działanie lub rozwiązanie, które ogranicza prawdopodobieństwo wystąpienia zagrożenia lub minimalizuje jego negatywne skutki oraz wpływa na osiągnięcie celów, w szczególności:

a) organizacyjne, w tym struktury organizacyjne, polityki, procedury, instrukcje, zarządzenia, regulaminy, klauzule w umowach, szkolenia, audyty, kontrole,
b) techniczne, w tym systemy bezpieczeństwa teleinformatycznego, systemy kontroli dostępu, urządzenia alarmowe, monitoring wizyjny, oprogramowanie antywirusowe,
c) fizyczne, w tym ogrodzenie, drzwi, pomieszczenia plombowane, zamykane szafy, sejfy, strefy ochronne i środowiskowe, w tym bezpieczeństwo okablowania, klimatyzacja;

9) zagrożenie – potencjalną przyczynę niepożądanego zdarzenia, która może wywołać szkodę w systemie bezpieczeństwa informacji w GUM.

§ 3. W GUM informacje przetwarzane są zgodnie z obowiązującymi przepisami prawa, które zapewniają ich integralność, dostępność i poufność, oraz z wdrożonymi w GUM normami ISO.

§ 4. 1. SZBI obejmuje swoim zakresem wszystkie informacje i dane przetwarzane przez GUM, niezależnie od formy i nośnika przetwarzania lub dystrybucji, utrwalone na nośnikach elektronicznych, systemach komputerowych oraz wytworzone w dokumentach, będące własnością GUM oraz powierzone w ramach umów lub porozumień, z wyłączeniem informacji niejawnych chronionych ustawowo.

2. Szczegółowe zasady dotyczące ochrony informacji niejawnych i ochrony danych osobowych określają odrębne regulacje wewnętrzne.

§ 5. Polityka obejmuje swoim zakresem siedzibę GUM oraz miejsca i sytuacje, w których informacje związane z działalnością GUM są przetwarzane poza jego siedzibą, w szczególności sytuacje zdalnego korzystania z sieci komputerowej GUM, w tym podczas pracy zdalnej.

Rozdział 2
Zasady zapewnienia bezpieczeństwa informacji

§ 6. W GUM obowiązują w szczególności następujące zasady stosowania zabezpieczeń:

1) adekwatności zabezpieczeń – używane mechanizmy zabezpieczeń powinny być adekwatne do zagrożeń, podatności, wartości aktywów i innych istotnych okoliczności, a ich dobór powinien uwzględniać wymogi prawne oraz wyniki audytów i analiz ryzyka bezpieczeństwa informacji przetwarzanych w GUM;

2) kompleksowości ochrony (asekuracji zabezpieczeń) – ochrona aktywów systemu przetwarzania informacji powinna opierać się na stosowaniu różnych, wzajemnie się uzupełniających, mechanizmów ochrony, w tym ochrony: prawnej, fizycznej, osobowej, technicznej oraz organizacyjnej;

3) unikania niepotrzebnego dublowania zabezpieczeń, przy uwzględnieniu racjonalnego gospodarowania środkami publicznymi, optymalizacji potrzeb oraz ograniczeń i uwarunkowań prawno-organizacyjnych GUM;

4) stałej gotowości – niedopuszczalne jest tymczasowe wyłączanie mechanizmów zabezpieczających system funkcjonujący w GUM bez zastosowania alternatywnych mechanizmów; system powinien być sprawny i przygotowany na zidentyfikowane zagrożenia;

5) ochrony niezbędnej – minimalny wymagany poziom bezpieczeństwa informacji przetwarzanych w GUM wynika z obowiązujących przepisów prawa, natomiast zastosowanie wyższych poziomów bezpieczeństwa informacji uzasadniają szczególne potrzeby GUM i wyniki szacowania ryzyka;

6) podwyższonego poziomu ochrony zbiorów informacji – w szczególnie uzasadnionych przypadkach zbiór informacji powinien być bardziej chroniony niż poszczególne informacje, które się na niego składają.

§ 7. W GUM obowiązują w szczególności następujące zasady dotyczące bezpieczeństwa fizycznego:

1) zamykania pomieszczeń – niedopuszczalne jest pozostawienie pod nieobecność pracownika niezabezpieczonego pomieszczenia służbowego, zarówno w godzinach pracy, jak i po jej zakończeniu; na zakończenie dnia pracy ostatnia wychodząca z pomieszczenia osoba powinna zamknąć wszystkie okna i drzwi oraz zabezpieczyć klucze do pomieszczenia;

2) nadzorowania dokumentów – po godzinach pracy wszystkie dokumenty zawierające informacje podlegające ochronie powinny być przechowywane w miejscach zabezpieczonych przed dostępem osób nieuprawnionych;

3) czystego biurka – podczas dłuższej nieobecności pracownika na stanowisku pracy dokumenty i informatyczne nośniki danych, w miarę możliwości organizacyjno-technicznych, należy przechowywać w miejscach zabezpieczonych przed dostępem osób nieuprawnionych;

4) czystej tablicy – po zakończonym spotkaniu należy uprzątnąć wszystkie materiały oraz wyczyścić tablice;

5) czystego kosza – dokumenty papierowe, z wyjątkiem materiałów promocyjnych, marketingowych i innych publicznie dostępnych, powinny być niszczone w sposób uniemożliwiający ich odczytanie.

§ 8. W GUM obowiązują w szczególności następujące zasady dotyczące bezpieczeństwa teleinformatycznego:

1) ograniczonego dostępu – na czas nieobecności pracownika dostęp do komputera jest blokowany, a po zakończeniu pracy komputer jest wyłączany, chyba że dany komputer musi pracować w trybie ciągłym;

2) ograniczonego wglądu – w czasie obecności pracownika monitor powinien być tak ustawiony, aby nie pozwalał na zapoznawanie się z wyświetlanymi treściami przez osoby nieuprawnione;

3) prywatności kont w systemach – każdy pracownik zobowiązany jest do pracy w systemach teleinformatycznych na przypisanych lub udostępnionych mu kontach; zabronione jest udostępnianie własnych kont osobom trzecim;

4) poufności haseł – każdy pracownik zobowiązany jest do zachowania poufności udostępnionych mu haseł i kodów dostępu, w szczególności do systemów teleinformatycznych;

5) legalnego oprogramowania – na stacjach roboczych zainstalowane jest wyłącznie legalne oprogramowanie umożliwiające automatyczne aktualizacje;

6) automatyzacji backupu – procesy tworzenia kopii zapasowych powinny być zautomatyzowane oraz niemożliwe do przerwania przez pracownika;

7) ochrony nośników danych – dane kopiowane na nośniki i wynoszone poza GUM powinny być odpowiednio zabezpieczone w czasie transportu i przechowywania, co najmniej poprzez szyfrowanie.

§ 9. W GUM obowiązują w szczególności następujące zasady dotyczące uprawnień i odpowiedzialności użytkowników:

1) wiedzy koniecznej (ograniczonego dostępu do informacji) – pracownicy posiadają dostęp tylko do tych informacji, które są konieczne do realizacji powierzonych im zadań; zasada ta dotyczy głównie informacji chronionych wewnętrznie, o których mowa w § 26 ust. 2 pkt 3;

2) indywidualnej odpowiedzialności – za utrzymanie odpowiedniego poziomu bezpieczeństwa poszczególnych aktywów lub ich elementów odpowiadają konkretne osoby, w zakresie nałożonych obowiązków i nadanych uprawnień;

3) separacji obowiązków – pojedyncze osoby nie mogą wykonywać krytycznych zadań w całości;

4) dyskrecji (ograniczonego zaufania i odpowiedzialnej konwersacji) – wszelkie informacje służbowe mogą być przekazywane wyłącznie w celu wykonywania zadań w zakresie do tego niezbędnym oraz osobom uprawnionym do pozyskania tych informacji; zasada ta ma ograniczone znaczenie dla pewnych grup informacji, w szczególności informacji dostępnych publicznie;

5) obecności koniecznej – prawo przebywania w określonych miejscach, istotnych dla bezpieczeństwa informacji przetwarzanych w GUM, mają tylko osoby uprawnione.

§ 10. W GUM obowiązują następujące zasady dotyczące doskonalenia SZBI i minimalizowania ryzyka podatności:.

1) każdy użytkownik ma obowiązek niezwłocznie zgłosić wystąpienie lub podejrzenie wystąpienia incydentu;

2) obsługa incydentów przebiega zgodnie z zasadami określonymi we właściwych regulacjach wewnętrznych;

3) bezpiecznej współpracy z podmiotami zewnętrznymi – dokumenty regulujące współpracę powinny zawierać stosowne klauzule bezpieczeństwa, w tym o zachowaniu poufności, zasadach postępowania z pozyskaną informacją, niszczenia lub zwrotu dokumentacji po ich wykorzystaniu;

4) ewolucji – SZBI jest stale monitorowany i dostosowywany do zmieniających się warunków wewnętrznych i zewnętrznych.

§ 11. Katalog zasad, o których mowa w § 6–10, jest otwarty i może być rozszerzony lub uszczegółowiony w innych dokumentach stanowiących dokumentację SZBI.

§ 12. Zarządzanie uprawnieniami dostępu do informacji wymagających zachowania poufności jest ograniczone wyłącznie dla osób, które przetwarzają tego rodzaju informacje i jest realizowane zgodnie z odrębnymi regulacjami wewnętrznymi oraz zawartymi przez GUM umowami.

Rozdział 3
Środki zapewnienia bezpieczeństwa informacji

§ 13. Polityka realizowana jest w GUM poprzez:

1) zapewnienie odpowiedniej jakości procesów przetwarzania informacji, w szczególności skuteczności i adekwatności działania zabezpieczeń lub ich grup i środków chroniących przed nieuprawnionym ujawnieniem, odpowiednich warunków do ich użytkowania, sprawności i efektywności ich wykorzystywania oraz zapewnienie ciągłości procesów przetwarzania informacji;

2) szkolenia pracowników w celu zapewnienia im wiedzy odpowiedniej do zapewnienia bezpieczeństwa informacji w ramach zadań realizowanych na zajmowanych przez nich stanowiskach pracy;

3) ochronę fizyczną, osobową, techniczną i organizacyjną aktywów przed ich uszkodzeniem lub zniszczeniem w wyniku pożaru, zalania, ataku terrorystycznego, zjawisk naturalnych lub innych zagrożeń oraz przed dostępem osób nieupoważnionych, w szczególności przed nieuprawnionym wykorzystaniem, kradzieżą, uszkodzeniem, nieuprawnioną modyfikacją lub zniszczeniem;

4) zapewnienie możliwości sprawnego odtworzenia aktywów w przypadku ich zniszczenia;

5) zapewnienie gotowości do reakcji na sytuację awaryjną lub kryzysową;

6) zapewnienie rozwiązań organizacyjnych i systemowych regulujących zasady i sposób zarządzania bezpieczeństwem informacji;

7) zapewnienie spójnej polityki informacyjnej GUM;

8) zapewnienie właściwych regulacji w zakresie bezpieczeństwa informacji, w szczególności stosowanie klauzul poufności w zawieranych umowach cywilnoprawnych;

9) zapewnienie działań kontrolnych w zakresie przestrzegania zasad określonych w polityce.

§ 14. Bezpieczeństwo systemów teleinformatycznych jest zapewniane w następujący sposób:

1) dostęp do systemów teleinformatycznych możliwy jest po pozytywnym uwierzytelnieniu użytkownika poprzez zastosowanie metod uwierzytelniania określonych w odrębnych regulacjach wewnętrznych;

2) informacje przetwarzane z wykorzystaniem systemu teleinformatycznego są chronione poprzez zastosowanie zabezpieczeń logicznych, ograniczenia uprawnień administracyjnych i rozwiązań kryptograficznych, natomiast dla dokumentów w formie papierowej oraz zapisanych na informatycznych nośnikach danych zastosowanie mają zasady określone w odrębnych regulacjach wewnętrznych;

3) proces dostępu do informacji przetwarzanych w systemach teleinformatycznych GUM jest monitorowany, a osoby posiadające dane uwierzytelniające do tych systemów są zobligowanie do ich ochrony zgodnie z zasadami bezpieczeństwa informacji w GUM.

§ 15. 1 W GUM stosowane są rozwiązania organizacyjne oraz środki ochrony fizycznej i technicznej zapewniające bezpieczeństwo informacji, które szczegółowo zostały określone w zarządzeniach Dyrektora Generalnego GUM dotyczących:

1) wprowadzenia w GUM zasad wydawania i użytkowania elektronicznych kart dostępu oraz wstępu pracowników, gości, interesantów i innych osób na teren GUM;

2) wprowadzenia do stosowania instrukcji bezpieczeństwa pożarowego w GUM;

3) zasad postępowania z kluczami do pomieszczeń GUM;

4) wprowadzenia do użytku zasad wjazdu i parkowania pojazdów na terenie GUM.

2. Dostęp do pomieszczeń służbowych GUM jest podzielony na strefy i monitorowany poprzez ochronę fizyczną wspomaganą systemami ochrony technicznej.

§ 16. W przypadku wystąpienia sytuacji kryzysowej, w celu zapewniania ciągłości działania, stosowane są w GUM rozwiązania określone w decyzjach i zarządzeniu Prezesa GUM dotyczących:

1) organizacji systemu Stałych Dyżurów w GUM;

2) realizacji w GUM przedsięwzięć po wprowadzeniu, zmianie lub odwołaniu stopni alarmowych i stopni alarmowych CRP;

3) utworzenia Zespołu Zarządzania Kryzysowego w GUM.

§ 17. Bezpieczeństwo systemów teleinformatycznych użytkowanych przez GUM, w tym oprogramowania wytwarzanego na potrzeby własne, jest realizowane poprzez spełnienie wymagań i stosowanie zabezpieczeń zgodnie z właściwymi przepisami prawa oraz regulacjami wewnętrznymi, które dotyczą w szczególności:

1) zapewnienia korzystania z legalnego i aktualnego oprogramowania;

2) minimalizowania ryzyka utraty informacji w wyniku awarii poprzez stosowanie rozwiązań redundantnych takich jak zasilanie energetyczne, łącze internetowe lub inne zabezpieczenia, w szczególności zasilacze UPS, kopie zapasowe;

3) ochrony informacji i danych przed błędami, utratą, nieuprawnioną modyfikacją;

4) stosowania adekwatnych mechanizmów kryptograficznych;

5) zapewnienia ochrony plików systemowych;

6) utwardzania systemów oraz skanowania sieci i przeprowadzania testów bezpieczeństwa;

7) redukcji ryzyk wynikających ze znanych podatności technicznych systemów teleinformatycznych;

8) niezwłocznego podejmowania działań po dostrzeżeniu nieujawnionych podatności mających wpływ na bezpieczeństwo informacji;

9) zapewnienia bezpieczeństwa informacji znajdującej się na elektronicznych nośnikach podczas prac serwisowych oraz gdy sprzęt informatyczny przeznaczony jest do przekazania lub utylizacji.

§ 18. Zarządzanie incydentami realizowane jest zgodnie z odrębnymi regulacjami wewnętrznymi i obejmuje działania zmierzające do zastosowania właściwej reakcji na stwierdzony incydent i podjęcia działań naprawczych.

§ 19. W przypadku, gdy realizacja usług lub dostaw realizowanych przez podmioty trzecie jest związana z bezpieczeństwem informacji, komórka organizacyjna GUM wnioskująca o realizację danej usługi lub dostawy zapoznaje te podmioty z niniejszym zarządzeniem.

Rozdział 4
Odpowiedzialność użytkowników

§ 20. 1. Właściwe zarządzanie SZBI w GUM zapewnia wewnętrzna struktura organizacyjna, w skład której wchodzą w szczególności:

1) Prezes GUM;

2) Wiceprezesi GUM;

3) Dyrektor Generalny GUM;

4) Zespół;

5) Inspektor Ochrony Danych, zwany dalej „IOD”;

6) pełnomocnik do spraw bezpieczeństwa cyberprzestrzeni;

7) pełnomocnik do spraw ochrony informacji niejawnych;

8) kierownicy komórek organizacyjnych GUM;

9) użytkownicy.

2. Odpowiedzialność za funkcjonowanie SZBI w GUM ponoszą wszystkie osoby, o których mowa w ust. 1, w zakresie odpowiednim do nałożonych na nich obowiązków, posiadanych uprawnień lub postanowień zamieszczonych w umowach, porozumieniach i innych pisemnych formach współpracy regulujących obszar bezpieczeństwa informacji.

3. Niezależnie od zakresu odpowiedzialności, o którym mowa w ust. 2, pracownicy są zobowiązani do przestrzegania obowiązku zachowania tajemnicy pracodawcy zgodnie z przepisami prawa pracy.

§ 21. 1. Prezes GUM:

1) decyduje o celach i środkach przetwarzania informacji, w tym danych osobowych, zgodnie z właściwością, jako ich administrator;

2) ustanawia SZBI oraz politykę;

3) akceptuje wyniki przeglądów zarządzania bezpieczeństwem informacji;

4) wyznacza albo powołuje:

   a) IOD – w przypadku danych osobowych, których cele i sposoby przetwarzania określa Prezes GUM jako administrator danych,
   b) pełnomocnika do spraw bezpieczeństwa cyberprzestrzeni,
   c) pełnomocnika do spraw ochrony informacji niejawnych.

2. Wiceprezesi GUM odpowiadają, w zakresie swojej właściwości, za nadzorowanie bezpieczeństwa informacji w GUM.

3. Dyrektor Generalny GUM:

1) decyduje o celach i środkach przetwarzania informacji, w tym danych osobowych, zgodnie z właściwością, jako ich administrator;

2) wyznacza IOD - w przypadku danych osobowych, których cele i sposoby przetwarzania określa GUM jako administrator danych;

3) akceptuje wyniki przeglądów zarządzania bezpieczeństwem informacji oraz raporty z incydentów;

4) wyznacza kierownikom komórek organizacyjnych GUM zadania mające na celu zapewnienie bezpieczeństwa informacji, w przypadku wystąpienia takiej potrzeby;

5) egzekwuje odpowiedzialność pracowników GUM za naruszenia związane z bezpieczeństwem informacji, w zakresie adekwatnym do nałożonych na nich obowiązków i posiadanych uprawnień.

4. Zespół odpowiada za:

1) zapewnienie integracji SZBI w systemie zarządzania GUM;

2) koordynację nadzoru nad dokumentacją zarządzania ryzykiem bezpieczeństwa informacji;

3) koordynację SZBI oraz stałe monitorowanie jego funkcjonowania;

4) rekomendowanie Prezesowi GUM oraz Dyrektorowi Generalnemu GUM niezbędnych działań i udoskonaleń dotyczących SZBI;

5) inicjowanie i nadzorowanie działań wdrożeniowych, korygujących i zapobiegawczych w zakresie bezpieczeństwa informacji;

6) organizowanie przeglądów SZBI oraz nadzorowanie realizacji ustaleń wynikających z przeglądów;

7) wydawanie zaleceń w zakresie związanym z funkcjonowaniem SZBI;

8) analizowanie, proponowanie i opiniowanie rozwiązań z zakresu bezpieczeństwa informacji;

9) inicjowanie działań zaradczych w przypadku wystąpienia incydentów i zagrożeń w zakresie funkcjonowania SZBI;

10) podejmowanie działań w kwestiach bezpieczeństwa informacji, w zakresie niezastrzeżonym do kompetencji innych osób.

5. Zadania IOD określa art. 39 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) (Dz. Urz. UE L 119 z 04.05.2016, str. 1).

6. Pełnomocnik do spraw bezpieczeństwa cyberprzestrzeni:

1) utrzymuje kontakty GUM z podmiotami krajowego systemu cyberbezpieczeństwa, w rozumieniu ustawy o krajowym systemie cyberbezpieczeństwa;

2) planuje, inicjuje i realizuje działania wynikające z przepisów dotyczących bezpieczeństwa cyberprzestrzeni, w tym związane z przygotowywaniem i testowaniem planów awaryjnych;

3) identyfikuje i analizuje ryzyka w obszarze cyberbezpieczeństwa;

4) zgłasza incydent, nie później niż w ciągu 24 godzin od momentu wykrycia, do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV;

5) koordynuje obsługę incydentu cyberbezpieczeństwa i incydentu krytycznego w GUM oraz zapewnia ich obsługę we współpracy z właściwym CSIRT MON, CSIRT NASK lub CSIRT GOV, przekazując niezbędne dane, w tym dane osobowe;

6) zapewnia pracownikom i interesantom dostęp do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami;

7) przygotowuje roczny raport o stanie bezpieczeństwa cyberprzestrzeni i przedstawia go Kierownictwu GUM do 31 stycznia roku następującego po roku, którego dotyczy raport.

7. Zadania Pełnomocnika do spraw ochrony informacji niejawnych określa art. 15 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2024 r. poz. 632 i 1222).

8. Audytor wewnętrzny GUM zapewnia przeprowadzenie audytu SZBI.

9. Kierownik komórki organizacyjnej GUM właściwej do spraw ochrony fizycznej zapewnia zabezpieczenia fizyczne, techniczne i organizacyjne aktywów.

10. Kierownik komórki organizacyjnej GUM właściwej do spraw informatyki zapewnia bezpieczeństwo systemów teleinformatycznych GUM i łączności telefonicznej w GUM, oraz budowę, rozwój i utrzymanie tych systemów, a także środki techniczne i organizacyjne umożliwiające przetwarzanie informacji w tych systemach.

11. Kierownik komórki organizacyjnej GUM właściwej do spraw bezpieczeństwa zapewnia bezpieczeństwo informacji w sytuacjach kryzysowych.

12. Kierownik komórki organizacyjnej GUM właściwej do spraw udostępniania informacji zapewnia bezpieczeństwo informacji udostępnianej na wniosek.

13. Kierownik komórki organizacyjnej GUM właściwej do spraw promocji działa zgodnie z regulacjami wewnętrznymi oraz zapewnia bezpieczeństwo informacji udostępnianej w mediach społecznościowych, stronach internetowych GUM i w Biuletynie Informacji Publicznej GUM.

14. Kierownik komórki organizacyjnej GUM właściwej do spraw wsparcia nowych technologii odpowiada za bezpieczeństwo informacji w wytwarzanym oprogramowaniu.

15. Kierownicy komórek organizacyjnych GUM, w zakresie swojej właściwości, odpowiadają za:

1) wdrożenie i przestrzeganie polityki;

2) zapoznanie podmiotów trzecich, o których mowa w § 19, z niniejszym zarządzeniem oraz odebranie oświadczenia, o których mowa w § 25 ust. 2, od tych podmiotów lub ich pracowników;

3) ochronę aktywów;

4) stałe monitorowanie poziomu bezpieczeństwa informacji w obszarze pracy podległych pracowników oraz innych osób wykonujących pracę pod ich nadzorem, w tym także osób wykonujących pracę na podstawie zawartych umów;

5) szacowanie ryzyka bezpieczeństwa informacji;

6) realizację procedur zapewniających ciągłość funkcjonowania komórki w sytuacjach awaryjnych i kryzysowych;

7) umożliwienie pracownikom udziału w organizowanych szkoleniach z zakresu bezpieczeństwa informacji.

16. Za bezpieczeństwo informacji w projektach odpowiada Kierownik Projektu.

§ 22. 1. Użytkownicy odpowiadają w szczególności za:

1) przestrzeganie polityki;

2) ochronę aktywów, w zakresie swojej właściwości, w tym dokumentów i nośników informacji wynoszonych poza siedzibę GUM w celu realizacji zadań służbowych;

3) niezwłoczne reagowanie w przypadku wystąpienia lub podejrzenia wystąpienia incydentu oraz postępowanie zgodnie z wewnętrznymi regulacjami w tym zakresie;

4) zabezpieczanie informacji przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów prawa oraz nieuprawnioną zmianą, utratą, uszkodzeniem lub zniszczeniem;

5) zachowanie w tajemnicy informacji pozyskanych w ramach wykonywania obowiązków służbowych w GUM oraz przestrzegania zasad bezpiecznego ich przetwarzania, w tym w systemach teleinformatycznych, w zakresie nadanych uprawnień lub wskazanym w upoważnieniu do przetwarzania danych osobowych.

2. Odpowiedzialność użytkowników w zakresie, o którym mowa w ust. 1, dotyczy również bezpieczeństwa aktywów wykorzystywanych do wykonywania pracy zdalnej.

§ 23. Ujawnianie, zniszczenie lub zmiana informacji, w tym jej fałszowanie, stanowi naruszenie obowiązków pracowniczych i może podlegać sankcjom określonym w przepisach powszechnie obowiązujących.

Rozdział 5
Budowanie świadomości użytkowników

§ 24.1. Budowanie świadomości i zapewnienie kompetencji w zakresie bezpieczeństwa informacji jest realizowane w następujący sposób:

1) komórka organizacyjna GUM właściwa do spraw kadrowych wraz z IOD zapewnia, aby każdy pracownik GUM oraz inna osoba wykonująca prace pod nadzorem została zapoznana z regulacjami wewnętrznymi z zakresu bezpieczeństwa informacji oraz przeszkolona z zakresu ochrony danych osobowych;

2) co najmniej raz na 18 miesięcy każdy pracownik GUM jest zobowiązany do udziału w szkoleniu z zakresu bezpieczeństwa informacji.

2. Oprócz działań wymienionych w ust. 1, Zespół może przeprowadzać okresowe działania informacyjne oraz aktualizujące wiedzę i umiejętności pracowników w zakresie bezpieczeństwa informacji.

§ 25.1. Za zapoznanie z polityką odpowiada, w przypadku:

1) nowo zatrudnionego pracownika, osoby odbywającej praktykę, staż lub wolontariat – komórka organizacyjna GUM właściwa do spraw kadrowych;

2) pracownika wykonującego obowiązki wynikające ze stosunku pracy na rzecz GUM – kierownik komórki organizacyjnej GUM, w której jest zatrudniony, z uwzględnieniem pkt 1;

3) osób świadczących usługi realizujące dostawy oraz wykonujących roboty budowlane na rzecz GUM na podstawie umowy cywilnoprawnej, w tym umowy zlecenia lub umowy o dzieło, ekspertów oraz pracowników podmiotów zewnętrznych realizujących zadania na rzecz GUM – kierownik komórki organizacyjnej GUM odpowiedzialnej za realizację umowy albo nadzorujący realizację zadań na rzecz GUM.

2. Użytkownicy, którzy po raz pierwszy uzyskają dostęp do systemów teleinformatycznych oraz innych aktywów GUM po wejściu w życie niniejszego zarządzenia, składają, niezwłocznie po uzyskaniu tego dostępu, oświadczenie o zapoznaniu się z jego treścią, o zobowiązaniu się do przestrzegania zawartych w nim zasad oraz o zachowaniu w tajemnicy informacji prawnie chronionych, a także sposobów zabezpieczenia tych informacji. Wzór oświadczenia określa załącznik nr 1 do zarządzenia. Oświadczenie użytkownicy przekazują w systemie EZD do komórki organizacyjnej GUM właściwej do spraw bezpieczeństwa. W przypadku braku dostępu do systemu EZD oświadczenie przekazywane jest w formie papierowej.

Rozdział 6
Klasyfikacja informacji

§ 26. 1. Proces klasyfikacji informacji przetwarzanych przez GUM koordynuje Zespół.

2. Informacje przetwarzane przez GUM są klasyfikowane według następujących kategorii:

1) informacje publiczne – informacje, których obowiązek udostępniania wynika z przepisów prawa, w szczególności informacje publiczne w rozumieniu ustawy o dostępie do informacji publicznej; informacje udostępniane w szczególności na stronach internetowych GUM i w Biuletynie Informacji Publicznej GUM;

2) informacje prawnie chronione – informacje stanowiące dane osobowe podlegające ochronie na mocy przepisów o ochronie danych osobowych, informacje przekazane GUM przez przedsiębiorcę, co do których podjął on działania w celu zachowania ich w poufności, w szczególności nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą (tajemnica przedsiębiorstwa), informacje chronione na mocy ustawy o ochronie informacji niejawnych oraz inne informacje chronione z mocy prawa;

3) informacje wewnętrznie chronione – informacje wewnętrzne GUM, wytworzone w GUM lub na jego rzecz, niewchodzące w zakres informacji zaklasyfikowanych do pozostałych grup. Są to informacje ogólnie dostępne wewnątrz GUM oraz przeznaczone do użytku wewnętrznego.

§ 27. 1. W przypadku wątpliwości Zespołu dotyczącej zaklasyfikowania informacji w danej kategorii decyzje podejmują, w zakresie swoich kompetencji, Prezes GUM albo Dyrektor Generalny GUM.

2. W przypadkach indywidualnych, w zakresie swoich kompetencji, Prezes GUM albo Dyrektor Generalny GUM mogą podjąć decyzję o zmianie kategorii danej informacji.

§ 28. Informacje mogą być sklasyfikowane na czas określony, przy czym czas ten rozumie się jako konkretny termin, okres albo zdarzenie, które wystąpi, ale którego przewidzenie w czasie jest niemożliwe.

§ 29. Zespół prowadzi wykaz informacji przetwarzanych przez GUM, którego wzór określa załącznik nr 2 do zarządzenia, i aktualizuje go co najmniej raz w roku.

Rozdział 7
Przeglądy i analiza ryzyka SZBI

§ 30. Za stałe monitorowanie zmian przepisów prawa oraz zgodność regulacji wewnętrznych w obszarze:

1) ochrony danych osobowych – odpowiada IOD;

2) bezpieczeństwa teleinformatycznego oraz cyberbezpieczeństwa, w tym zarządzania incydentami – odpowiada pełnomocnik do spraw bezpieczeństwa cyberprzestrzeni;

3) ochrony informacji niejawnych – odpowiada pełnomocnik do spraw ochrony informacji niejawnych.

§ 31. 1. W SZBI identyfikacja i analiza ryzyka jest obligatoryjna i przeprowadza się ją zgodnie z odrębnymi regulacjami wewnętrznymi.

2. Identyfikacja i analiza ryzyka powinna być dodatkowo realizowana przez Zespół zgodnie z potrzebami, w szczególności przed opracowaniem dokumentacji bezpieczeństwa dla danego obszaru lub systemu oraz po wystąpieniu istotnych zmian w danym obszarze lub systemie.

§ 32. 1. Co najmniej raz w roku Zespół organizuje przegląd dokumentacji tworzącej SZBI, pod kątem przydatności, adekwatności i skuteczności przyjętych rozwiązań oraz podejmowanych działań przy uwzględnianiu analizy stwierdzonych incydentów.

2. Wyniki przeglądu oraz rekomendacja działań GUM są przedstawiane przez Zespół Kierownictwu GUM.

§ 33. 1. Zespół sporządza roczne raporty o funkcjonowaniu SZBI, stanowiące element przeglądu zarządzania SZBI, na podstawie wyników przeprowadzonych audytów i kontroli, analizy incydentów w obszarze bezpieczeństwa informacji,

analizy ryzyka, zmian wynikających z przepisów prawa, a także innych zdarzeń mających wpływ na bezpieczeństwo informacji.

2. Raport jest przedstawiany przez Zespół Kierownictwu GUM do 31 stycznia roku następującego po roku, którego dotyczy raport.

Rozdział 8
Przepisy przejściowe i końcowe

§ 34. Do spraw z zakresu polityki, wszczętych i niezakończonych przed dniem wejścia w życie niniejszego zarządzenia, stosuje się przepisy dotychczasowe.

§ 35. Traci moc zarządzenie nr 2 Prezesa Głównego Urzędu Miar z dnia 12 czerwca 2023 r. w sprawie ustalenia polityki bezpieczeństwa informacji Głównego Urzędu Miar.

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

Prezes Głównego Urzędu Miar: *Jacek Semaniak*

(podpisano elektronicznie)

Załączniki do zarządzenia nr 1
Prezesa Głównego Urzędu Miar
z dnia 27 stycznia 2025 r.
(Dz. Urz. GUM poz. 6)

Załącznik nr 1

**Oświadczenie o zapoznaniu się
z polityką bezpieczeństwa informacji Głównego Urzędu Miar**

Niniejszym oświadczam, że zapoznałem(am) się z treścią zarządzenia nr 1 Prezesa Głównego Urzędu Miar z dnia … w sprawie polityki bezpieczeństwa informacji Głównego Urzędu Miar i zobowiązuję się do przestrzegania zawartych w niej zasad.
Ponadto zobowiązuję się do zachowania w tajemnicy informacji prawnie chronionych, do których mam lub będę miał(a) dostęp w związku z wykonywaniem przeze mnie obowiązków pracowniczych lub innych wykonywanych na rzecz Głównego Urzędu Miar, a także sposobów zabezpieczenia tych informacji, zarówno w trakcie wykonywania zadań, jak i po ich zakończeniu.

…….
(data, imię i nazwisko, podpis
lub akceptacja w systemie EZD)

Załącznik nr 2

Klasyfikacja informacji w Głównym Urzędzie Miar					
Lp.	**Kategoria informacji** /na podstawie JRWA/	**Informacje publiczne** /stale (**S+**), czasowo (**S-**)/	**Informacje wewnętrznie chronione** /stale (**W+**), czasowo (**W-**)/	**Informacje prawnie chronione** (**U**)	**Wyłączenia** /dla **S-** i **W-**/