

Poz. 15

ZARZĄDZENIE
GENERALNEGO DYREKTORA
OCHRONY ŚRODOWISKA

z dnia 19 czerwca 2026 r.

**w sprawie ustanowienia i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji
w Generalnej Dyrekcji Ochrony Środowiska**

Na podstawie § 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 z 2025 r. poz. 1158) zarządza się, co następuje:

§ 1. W Generalnej Dyrekcji Ochrony Środowiska ustanawia się i wdraża System Zarządzania Bezpieczeństwem Informacji, który obejmuje dokumentację Systemu Zarządzania Bezpieczeństwem Informacji, a także strukturę organizacyjną, planowane działania i zasoby.

§ 2. Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Generalnej Dyrekcji Ochrony Środowiska obejmuje w szczególności:

- 1) Politykę Bezpieczeństwa Informacji – stanowiącą załącznik do zarządzenia;
- 2) Księgę Bezpieczeństwa Informacji;
- 3) Politykę Przetwarzania Danych Osobowych;
- 4) Procedurę bezpieczeństwa fizycznego;
- 5) Procedurę bezpieczeństwa teleinformatycznego;
- 6) Procedurę identyfikacji informacji oraz oceny ryzyka i postępowania z ryzykiem dotyczącym utraty poufności, integralności i dostępności;
- 7) Procedurę zarządzania uprawnieniami;

8) Procedurę zarządzania zdarzeniami i incydentami.

§ 3. Dokumentację Systemu Zarządzania Bezpieczeństwem Informacji w Generalnej Dyrekcji Ochrony Środowiska, z wyłączeniem Polityki Bezpieczeństwa Informacji, o której mowa w § 2 pkt 1, wprowadza do stosowania Dyrektor Generalny Generalnej Dyrekcji Ochrony Środowiska odrębnym zarządzeniem.

§ 4. Traci moc zarządzenie Nr 14 Generalnego Dyrektora Ochrony Środowiska z dnia 17 listopada 2022 r. w sprawie ustanowienia i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji w Generalnej Dyrekcji Ochrony Środowiska (Dz. Urz. GDOŚ poz. 15).

§ 5. Zarządzenie wchodzi w życie z dniem 1 lipca 2026 r.

GENERALNY DYREKTOR

Piotr Otawski
Generalny Dyrektor Ochrony Środowiska
/ – podpisany cyfrowo/

OCHRONY ŚRODOWISKA

Załącznik do Zarządzenia Generalnego
Dyrektora Ochrony Środowiska z dnia 19
czerwca 2026 r.

Polityka Bezpieczeństwa Informacji

§ 1. **Informacje ogólne**

1. Polityka Bezpieczeństwa Informacji służy określeniu zasad i procedur w Generalnej Dyrekcji Ochrony Środowiska zapewniających ochronę danych i informacji przed ich utratą, nieuprawnionym dostępem i nadużyciami.
2. Polityka Bezpieczeństwa Informacji opisuje w szczególności zabezpieczenia i rozwiązania wdrożone na podstawie wymagań normy PN-EN ISO/IEC 27001, przepisów prawa powszechnie obowiązującego, w tym ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, regulacji wewnętrznych Generalnej Dyrekcji Ochrony Środowiska, wymagań wynikających z zawartych umów oraz wyników przeprowadzanej analizy ryzyka dla zinwentaryzowanych aktywów.

§ 2. **Zakres Systemu Zarządzania Bezpieczeństwem Informacji**

System Zarządzania Bezpieczeństwem Informacji oraz związane z nim procedury i zasady mają zastosowanie do wszystkich procesów i zadań Generalnej Dyrekcji Ochrony Środowiska realizowanych przez wszystkich pracowników, zgodnie z obowiązującą strukturą organizacyjną wynikającą z regulaminu organizacyjnego Generalnej Dyrekcji Ochrony Środowiska.

§ 3. **Definicje**

Ilekcroć w Polityce Bezpieczeństwa Informacji jest mowa o:

- 1) aktywach informacyjnych – należy przez to rozumieć wszelkie informacje w formie papierowej, elektronicznej i innej, przetwarzane (w tym zbierane, utrwalane, przechowywane, opracowywane, zmieniane, udostępniane, transmitowane, przekazywane i usuwane) w sposób tradycyjny lub w systemach teleinformatycznych, będące własnością, wykorzystywane bądź administrowane przez GDOŚ, które posiadają wartość materialną lub prawną;
- 2) ciągłym doskonaleniu – należy przez to rozumieć zobowiązanie do zwiększania skuteczności oraz ulepszania i aktualizowania w GDOŚ SZBI;
- 3) ciągłości działania – należy przez to rozumieć zdolność GDOŚ do ciągłego dostarczania usług w akceptowalnych ramach czasowych przy zdefiniowanej wcześniej zdolności do działania w czasie zakłócenia;
- 4) GDOŚ – należy przez to rozumieć Generalną Dyrekcję Ochrony Środowiska;
- 5) infrastrukturze informacyjnej i teleinformatycznej – należy przez to rozumieć środowisko techniczne, dla którego GDOŚ zapewnia ciągłość działania i które obejmuje systemy i aplikacje teleinformatyczne wykorzystywane w działalności GDOŚ;

- 6) Kierownictwie GDOŚ – należy przez to rozumieć Generalnego Dyrektora Ochrony Środowiska, Zastępcę Generalnego Dyrektora Ochrony Środowiska, Dyrektora Generalnego GDOŚ, dyrektorów komórek organizacyjnych oraz Głównego Księgowego dysponenta drugiego stopnia;
- 7) Pełnomocniku do spraw Bezpieczeństwa Informacji (PBI) – należy przez to rozumieć osobę wyznaczoną przez Dyrektora Generalnego GDOŚ, która sprawuje nadzór nad wszystkimi czynnościami w obszarze zarządzania bezpieczeństwem informacji w GDOŚ;
- 8) PN-EN ISO/IEC 27001 – należy przez to rozumieć normę standaryzującą SZBI, z której wymaganiami SZBI GDOŚ powinien być zgodny;
- 9) Systemie Zarządzania Bezpieczeństwem Informacji (SZBI) – należy przez to rozumieć ustanowiony, wdrożony i nadzorowany system, którego celem jest osiągnięcie najwyższego poziomu ochrony informacji, poprzez realizację m.in. poufności, integralności i dostępności;
- 10) właścicielach ryzyk – należy przez to rozumieć osoby wyznaczone i odpowiedzialne za odpowiednie zabezpieczenie zinwentaryzowanych i sklasyfikowanych aktywów informacyjnych.

§ 4.

Deklaracja Kierownictwa GDOŚ

1. Kierownictwo GDOŚ zobowiązuje się do dołożenia wszelkich starań w celu realizacji założeń niniejszej Polityki Bezpieczeństwa Informacji, zapewnienia odpowiednich warunków organizacyjnych, środków finansowych i wymagań niezbędnych do osiągnięcia jej celów oraz osiągnięcia najwyższego poziomu ochrony informacji poprzez zaangażowanie całej GDOŚ (pracowników i kadry kierowniczej) w zapewnienie skuteczności oraz ciągłe doskonalenie SZBI.
2. Kierownictwo GDOŚ, uznając informacje za jedno z kluczowych aktywów organizacji, ustanawia, wdraża i nadzoruje Politykę Bezpieczeństwa Informacji, obejmującą wszystkie aktywa oraz procesy związane z przetwarzaniem informacji, a także infrastrukturę informacyjną i teleinformatyczną wykorzystywaną w działalności GDOŚ.
3. Polityka ta stanowi wyraz zobowiązania GDOŚ wobec interesariuszy do zapewnienia oraz ciągłego doskonalenia bezpieczeństwa informacji w ramach realizowanych zadań.

§ 5.

Cel i zakres stosowania

1. Celem Polityki Bezpieczeństwa Informacji w GDOŚ jest określenie ogólnych wymagań i zasad ochrony informacji, które stanowią podstawę dla wszystkich dokumentów związanych z bezpieczeństwem informacji oraz dla funkcjonowania SZBI. Przedstawia ona przyjęte podejście do ochrony informacji, zasady zabezpieczania aktywów informacyjnych oraz odwołuje się do szczegółowych procedur i instrukcji obowiązujących w ramach SZBI.

2. Do najważniejszych celów realizowanych poprzez SZBI należą:

- 1) zapewnienie poufności, integralności, dostępności i rozliczalności przetwarzanych informacji – niezależnie od ich formy i systemów, w których są przetwarzane;
- 2) zapewnienie ciągłości działania infrastruktury informacyjnej i teleinformatycznej GDOŚ;
- 3) minimalizowanie skutków wystąpienia zagrożeń dla bezpieczeństwa informacji, wynikających z działań celowych, jak i zdarzeń losowych;
- 4) zapewnienie zgodności z obowiązującymi wymaganiami;
- 5) gotowość do podejmowania działań w sytuacjach kryzysowych;
- 6) budowanie i utrwalanie kultury bezpieczeństwa informacji poprzez podnoszenie świadomości i rozwój kompetencji pracowników GDOŚ.

3. Cele SZBI realizowane są poprzez następujące środki:

- 1) odpowiednią strukturę organizacyjną gwarantującą jasny podział i koordynację zadań oraz odpowiedzialności w zakresie bezpieczeństwa informacji;
- 2) inwentaryzację i klasyfikację aktywów informacyjnych z uwzględnieniem ich rodzaju i znaczenia dla działalności GDOŚ;
- 3) wyznaczenie właścicieli ryzyk odpowiedzialnych za zabezpieczenie wskazanego ryzyka;
- 4) stosowanie Polityki Bezpieczeństwa Informacji oraz związanej z nią pozostałej dokumentacji SZBI przez wszystkich pracowników GDOŚ;
- 5) określenie zasad przetwarzania informacji oraz lokalizacji, w których procesy te są realizowane;
- 6) regularne przeglądy i aktualizacje dokumentacji SZBI;
- 7) dążenie do utrzymania zgodności SZBI z wymaganiami PN-EN ISO/IEC 27001;
- 8) ciągłe doskonalenie SZBI w GDOŚ.

§ 6.

Niezgodności i odstępstwa od systemu

Wszelkie niezgodności oraz odstępstwa od zasad i standardów przyjętych w SZBI w GDOŚ wymagają akceptacji PBI, Dyrektora Generalnego GDOŚ oraz Generalnego Dyrektora Ochrony Środowiska. Dla każdego odstępstwa należy opracować plan postępowania, określający sposób jego monitorowania i eliminacji. Za opracowanie planu odpowiada PBI.

§ 7.

Dokumentacja SZBI

W skład dokumentacji SZBI wchodzi następujące rodzaje dokumentów:

- 1) Polityka Bezpieczeństwa Informacji – jako dokument strategiczny, określający kierunek działania i ogólne zasady obowiązujące w GDOŚ w zakresie bezpieczeństwa informacji. Polityka Bezpieczeństwa Informacji ma charakter deklaracyjny;
- 2) wprowadzone zarządzeniem Dyrektora Generalnego GDOŚ:
 - a) Księga Bezpieczeństwa Informacji,
 - b) Polityka Przetwarzania Danych Osobowych,
 - c) procedury;
- 3) pozostałe dokumenty operacyjne i ewidencyjne:
 - a) instrukcje – dokumenty operacyjne, zawierające szczegółowy opis wykonania konkretnej czynności (np. konfiguracja systemu, sposób obsługi urządzenia),
 - b) rejestry – dokumenty ewidencyjne, w których zapisywane są informacje wymagane przepisami prawa lub przez SZBI (np. rejestr incydentów, rejestr aktywów);
- 4) opracowywane przez PBI i przekazywane do korzystania podręczniki – dokumenty wspierające stosowanie SZBI, pełniące rolę materiału pomocniczego dla pracowników i kadry kierowniczej, zawierające praktyczne wskazówki, opisy dobrych praktyk i przykłady odnoszące się do wdrożonych polityk i procedur.