

**w sprawie ustanowienia Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)  
w Urzędzie Gminy Zawidz**

Na podstawie art. 30 ust. 1 oraz art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U. z 2024 r. poz. 609 z późn. zm.) oraz w związku z realizacją wymagań wynikających z:

- normy PN-EN ISO/IEC 27001:2022 – Systemy zarządzania bezpieczeństwem informacji,
  - rozporządzeniem Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności,
  - oraz art. 32 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO),
- zarządzam, co następuje:

**§ 1.**

Ustanawia się w Urzędzie Gminy Zawidz System Zarządzania Bezpieczeństwem Informacji (SZBI), którego celem jest zapewnienie odpowiedniego poziomu ochrony informacji – w tym danych osobowych – przetwarzanych w Urzędzie, zgodnie z wymaganiami prawa oraz dobrymi praktykami bezpieczeństwa informacji.

**§ 2.**

1. Zakres Systemu Zarządzania Bezpieczeństwem Informacji obejmuje:
  1. wszystkie komórki organizacyjne Urzędu Gminy Zawidz
  2. wszystkich pracowników i współpracowników realizujących zadania na rzecz Urzędu Gminy Zawidz,
  3. dane i informacje przetwarzane w formie papierowej i elektronicznej,
  4. systemy teleinformatyczne, sieci komputerowe i urządzenia mobilne wykorzystywane do przetwarzania informacji,
  5. obiekty i pomieszczenia, w których przetwarzane są informacje.
2. SZBI obejmuje także zasady bezpiecznego korzystania z usług informatycznych, dostępów zewnętrznych, zarządzania kopiami zapasowymi oraz utrzymania ciągłości działania (BCP/DRP).

### § 3.

1. System Zarządzania Bezpieczeństwem Informacji realizowany jest poprzez wdrożenie i stosowanie następujących dokumentów systemowych:
  1. Polityk bezpieczeństwa informacji (SZBI.POL.001 – SZBI.POL.010),
  2. Procedur bezpieczeństwa informacji (SZBI.PRO.001 – SZBI.PRO.003),
  3. Instrukcji bezpieczeństwa informacji (SZBI.INS.001 – SZBI.INS.004),
  4. Załączników i rejestrów
  5. Słownika pojęć i definicji (SZBI.WSP.001).
2. Dokumenty określają szczegółowe zasady organizacyjne, techniczne i proceduralne dotyczące bezpieczeństwa informacji.
3. Wersje obowiązujące dokumentów udostępniane są w repozytorium SZBI prowadzonym przez Pełnomocnika ds. SZBI.

### § 4.

1. Nadzór nad funkcjonowaniem i utrzymaniem SZBI powierzam Pełnomocnikowi ds. Systemu Zarządzania Bezpieczeństwem Informacji, powołanemu na podstawie odrębnego zarządzenia.
2. Pełnomocnik ds. SZBI odpowiada w szczególności za:
  1. koordynację wdrożenia i aktualizacji systemu,
  2. utrzymanie repozytorium dokumentacji SZBI,
  3. prowadzenie rejestrów oraz koordynację analizy ryzyka,
  4. organizację szkoleń i budowanie świadomości pracowników,
  5. raportowanie Wójtowi wyników audytów, przeglądów i mierników bezpieczeństwa.

### § 5.

1. Wszystkich pracowników urzędu zobowiązuje do przestrzegania zasad i wymagań określonych w dokumentach Systemu Zarządzania Bezpieczeństwem Informacji.
2. Kierownicy komórek organizacyjnych są odpowiedzialni za wdrożenie i stosowanie postanowień SZBI w zakresie działalności swoich wydziałów.

### § 6.

1. System Zarządzania Bezpieczeństwem Informacji jest utrzymywany w sposób ciągły i doskonalony zgodnie z cyklem PDCA (plan–do–check–act).
2. Przegląd funkcjonowania SZBI dokonywany jest co najmniej raz w roku i udokumentowany w „Protokole z przeglądu zarządzania” (SZBI.POL.001-ZA2).

**§ 7.**

Z dniem wejścia w życie niniejszego zarządzenia traci moc „Polityka Ochrony Danych Osobowych” ustanowiona Zarządzeniem nr 47/2025 z dnia 12.11.2025 r. Postanowienia nowego Systemu Zarządzania Bezpieczeństwem Informacji obejmują zagadnienia ochrony danych osobowych w ramach Polityki Ochrony Danych Osobowych (SZBI.POL.010).

**§ 8.**

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT GMINY  
  
Kamil Jan Różański