UCHWAŁA NR XV/45/2026
ZARZĄDU CELOWEGO ZWIĄZKU GMIN
„EKO-LOGICZNI"
z dnia 29 kwietnia 2026 r.

w sprawie wprowadzenia Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w Biurze Celowego Związku Gmin „Eko-Logiczni"

Na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t. j. Dz.U. z 2025 r., poz. 1703 z późn. zm.), w związku z § 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. z 2024 r. poz. 773), art. 8 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t. j. Dz.U. z 2026 r. poz. 20 z późn. zm.),

Zarząd Celowego Związku Gmin
uchwala, co następuje

§ 1.

1. Wprowadza się do stosowania w Biurze Celowego Związku Gmin „Eko-Logiczni" System Zarządzania Bezpieczeństwem Informacji (SZBI).
2. System Zarządzania Bezpieczeństwem Informacji obejmuje informacje, procesy, zasoby informacyjne oraz systemy teleinformatyczne wykorzystywane w Biurze Celowego Związku Gmin „Eko-Logiczni".
3. System Zarządzania Bezpieczeństwem Informacji (SZBI) zapewnienia efektywne zarządzanie bezpieczeństwem informacji, chroniąc poufność, integralność i dostępność danych, a także zapewniając ciągłość działania procesów wspierających świadczenie usług publicznych.

§ 2.

1. Wprowadza się dokumentację Systemu Zarządzania Bezpieczeństwem Informacji.
2. Wykaz dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji stanowi załącznik do niniejszego Zarządzenia.
3. Dokumentacja SZBI funkcjonuje w powiązaniu z Polityką ochrony danych osobowych oraz innymi regulacjami dotyczącymi przetwarzania danych osobowych w Biurze Celowego Związku Gmin „Eko-Logiczni".

§ 3.

1. Aktualizacja dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) odbywa się zgodnie z zasadami określonymi w dokumentacji SZBI i nie wymaga każdorazowo wydawania odrębnej uchwały.
2. Zmiany dokumentacji podlegają rejestracji w Rejestrze zmian oraz nadzorowi.

§ 4.

1. Wyznacza się Koordynatora Systemu Zarządzania Bezpieczeństwem Informacji odpowiedzialnego za nadzór nad funkcjonowaniem SZBI, w osobie Pana Pawła Trojanowskiego.
2. Do zadań Koordynatora należy w szczególności:
   1) koordynowanie wdrożenia i utrzymania SZBI,
   2) nadzór nad aktualnością dokumentacji,
   3) współpraca z Administratorem Systemów Informatycznych (ASI) oraz Inspektorem Ochrony Danych (IOD),
   4) inicjowanie działań doskonalących.

§ 5.

1. Zobowiązuje się Kierowników Działów do zapoznania podległych pracowników z postanowieniami niniejszej uchwały oraz nadzorowania przestrzegania dokumentacji SZBI.
2. Nieprzestrzeganie zasad zawartych w dokumentacji SZBI jest naruszeniem obowiązków pracowniczych.
3. Przestrzeganie przepisów z zakresu bezpieczeństwa informacji jest obowiązkiem każdego pracownika, a także innych osób realizujących zadania w związku z dostępem do informacji, w tym stażyści, praktykanci, strony umów cywilnych.
4. Każdy pracownik podejmujący pracę jest zobowiązany do zapoznania się z przepisami dotyczącymi bezpieczeństwa informacji.

§ 6.

1. System Zarządzania Bezpieczeństwem Informacji podlega:
   1) audytom wewnętrznym,
   2) przeglądom zarządzania,
   3) ciągłemu doskonaleniu.
2. Przeglądy zarządzania przeprowadzane są nie rzadziej niż raz w roku.

§ 7.

1. Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji stanowi dokumentację wewnętrzną i nie podlega publikacji.
2. Uchwała wchodzi w życie z dniem podjęcia.

Jerzy Kocój
Przewodniczący Zarządu
Celowego Związku Gmin
„Eko-Logiczni"

WYKAZ DOKUMENTACJI

Systemu Zarządzania

Bezpieczeństwem Informacji (SZBI)
w Biurze Celowego Związku Gmin „Eko-Logiczni"

1. Polityka bezpieczeństwa informacji.
2. Zasady korzystania z systemów informatycznych przez użytkowników.
3. Polityka zarządzania uprawnieniami.
4. Ewidencja zasobów informacyjnych.
5. Analiza ryzyka.
6. Procedura kopii zapasowych.
7. Procedura pracy zdalnej.
8. Procedura przeglądu systemu zarządzania bezpieczeństwem informacji (SZBI).
9. Procedura zarządzania incydentami bezpieczeństwa informacji.
10. Mapowanie procedury tworzenia i zarządzania kopiami zapasowymi do wymagań krajowych ram interoperacyjności (KRI)
11. Rejestr incydentów bezpieczeństwa.