ZARZĄDZENIE NR 72/2026
WÓJTA GMINY ZŁOTA
z dnia 4 września 2026 r.

w sprawie ustanowienia i wprowadzenia do stosowania Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Gminy Złota

Na podstawie art. 33 ust. 3 i 5 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2026 r. poz. 662), w związku z art. 8 ust. 3 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2026 r. poz. 20 z późn. zm.) oraz § 19 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), zarządza się, co następuje:

§ 1.

1. Ustanawia się i wprowadza do stosowania w Urzędzie Gminy Złota System Zarządzania Bezpieczeństwem Informacji, zwany dalej „SZBI".
2. SZBI obejmuje działania związane z zarządzaniem bezpieczeństwem informacji w zakresie określonym w jego dokumentacji.
3. SZBI jest opisany w dokumentacji obejmującej w szczególności polityki, zasady, procedury, rejestry, formularze oraz inne dokumenty niezbędne do jego funkcjonowania.

§ 2.

1. Dokumentacja podlega bieżącemu utrzymaniu, przeglądowi, aktualizacji i doskonaleniu zgodnie z zasadami przyjętymi w ramach SZBI.
2. Zmiany, aktualizacje, zastępowanie lub wycofywanie poszczególnych dokumentów nie wymagają zmiany niniejszego zarządzenia.

§ 3.

Pracownicy Urzędu Gminy Złota oraz inne osoby wykonujące zadania na rzecz Urzędu są zobowiązani do stosowania zasad i wymagań SZBI w zakresie właściwym dla wykonywanych zadań, pełnionych funkcji oraz posiadanych uprawnień.

§ 4.

Nadzór nad stosowaniem SZBI w Urzędzie Gminy Złota powierza się sekretarzowi gminy w zakresie administracyjnym i informatykowi urzędowemu w zakresie technicznym

§ 5.

Zarządzenie wchodzi w życie z dniem 4 września 2026 r.

WÓJT
mgr inż. Waldemar Podsiadło

WYKAZ DOKUMENTACJI SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI (SZBI):

1. Księga Systemu Zarządzania Bezpieczeństwem Informacji
2. Polityka bezpieczeństwa informacji
3. Procedura nadzoru nad udokumentowaną informacją
4. Metodyka szacowania i postępowania z ryzykiem bezpieczeństwa informacji
5. Procedura zarządzania wymaganiami i oceny zgodności
6. Procedura oceny i doskonalenia SZBI
7. Zasady zarządzania informacją i aktywami
8. Zasady bezpiecznego korzystania z informacji i zasobów
9. Zasady zarządzania tożsamościami, uwierzytelnianiem i dostępem
10. Zasady bezpieczeństwa personelu, kompetencji i świadomości
11. Zasady bezpieczeństwa dostawców i usług zewnętrznych
12. Zasady zarządzania zdarzeniami i incydentami bezpieczeństwa
13. Zasady bezpieczeństwa fizycznego i środowiskowego
14. Zasady konfiguracji, eksploatacji i monitoringu IT
15. Zasady bezpieczeństwa sieci, komunikacji i kryptografii
16. Zasady projektów, cyklu życia systemów i zarządzania zmianą
17. Zasady ciągłości działania i gotowości ICT
18. Klasyfikacja, postępowanie, retencji i usuwania informacji
19. Model dostępu i uprawnień
20. Profil bezpieczeństwa technicznego
21. Instrukcje postepowania w razie incydentu
22. Pakiet BIA, planów ciągłości i odtwarzania ICT
23. Wymagania i kryteria oceny dostawców
24. Macierz obsady ról, zastępstw, komunikacji i kontaktów operacyjnych
25. Rejestr kontekstu, stron zainteresowanych, wymagań i oceny zgodności
26. Rejestr ryzyk i szans dotyczących SZBI
27. Rejestr ryzyk bezpieczeństwa informacji i plan postępowania z ryzykiem
28. Deklaracja Stosowania (SoA)
29. Plan celów, mierników, wyników i działań SZBI
30. Katalog udokumentowanej informacji, źródeł dowodów i retencji
31. Zintegrowany rejestr aktywów i zależności
32. Rejestr oceny bezpieczeństwa dostawców i usług zewnętrznych
33. Rejestr zdarzeń i incydentów
34. Rejestr kompetencji, szkoleń i świadomości
35. Program audytów i dokumentacja audytów wewnętrznych
36. Rejestr przeglądów zarządzania
37. Rejestr niezgodności i działań korygujących
38. Rejestr odstępstw i czasowej akceptacji ryzyka
39. Rejestr testów ciągłości i odtwarzania