

ZARZĄDZENIE NR 69.2026
WÓJTA GMINY DZIERŻĄNIA
z dnia 24 lipca 2026 r.

**w sprawie wprowadzenia Systemu Zarządzania Bezpieczeństwem Informacji
w Urzędzie Gminy w Dzierżąni oraz systemu teleinformatycznego do obsługi zgłoszeń
i prowadzenia dokumentacji SZBI**

Na podstawie art. 33 ust. 3 i ust. 5 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2026 r. poz. 662) oraz § 19 i 20 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), w związku z art. 24, art. 28 i art. 32 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (RODO), zarządza się, co następuje:

§ 1. Wprowadzenie Systemu Zarządzania Bezpieczeństwem Informacji

1. Wprowadza się w Urzędzie Gminy w Dzierżąni System Zarządzania Bezpieczeństwem Informacji (SZBI), oparty na wymaganiach normy PN-EN ISO/IEC 27001 oraz przepisach o Krajowych Ramach Interoperacyjności.
2. Na dokumentację SZBI składają się polityki, procedury, instrukcje, wzory i rejestry wyszczególnione w „D1-6-1 Wykaz dokumentów, druków, formularzy i zapisów SZBI”
3. Dokumentacja SZBI obowiązuje wszystkich pracowników Urzędu, praktykantów, stażystów oraz — w zakresie wynikającym z umów — podmioty zewnętrzne realizujące zadania na rzecz Urzędu.

§ 2. System teleinformatyczny obsługi zgłoszeń i dokumentacji SZBI

1. Do wsparcia funkcjonowania SZBI wprowadza się system teleinformatyczny Softpublica zwany dalej „Systemem”, służący w szczególności do:
 - 1) przyjmowania i obsługi zgłoszeń serwisowych oraz zgłoszeń zdarzeń i incydentów bezpieczeństwa informacji,
 - 2) prowadzenia Rejestru incydentów i niezgodności (D1-P1-3),
 - 3) opracowywania, wersjonowania, zatwierdzania, udostępniania i archiwizacji dokumentacji SZBI,
 - 4) prowadzenia rejestrów i zapisów SZBI, w tym wykazu osób pełniących kluczowe role w SZBI (D1-2).
2. System jest udostępniany i utrzymywany przez Software & Service Sebastian Rajca, NIP 5671574127 zwany dalej „Usługodawcą”, na podstawie umowy nr ORG.272.12.2026 z dnia 21.07.2026 oraz umowy powierzenia przetwarzania danych osobowych.
3. Zasady korzystania z Systemu, w tym zasady uwierzytelniania, klasyfikacji i ochrony informacji w nim przetwarzanych, określa dokumentacja SZBI, w szczególności dokumenty D1-6, D1-8, D1-P1-1, D3 i D3-P3.

§ 3. Kanały zgłoszeń

1. Podstawowym kanałem zgłaszania zgłoszeń serwisowych oraz zdarzeń i incydentów bezpieczeństwa informacji przez pracowników Urzędu jest System.
2. Kanałami zapasowymi, stosowanymi w szczególności w przypadku niedostępności Systemu lub sieci teleinformatycznej Urzędu, są kanały określone w procedurze D1-P1-1: telefonicznie (23 661 59 02 wew. 36), pocztą elektroniczną (sekretarz@dzierzaznia.pl) oraz osobiście. Zgłoszenia przyjęte kanałami zapasowymi wprowadza się do Systemu niezwłocznie po ustaniu przyczyny ich zastosowania.

§ 4. Rejestr incydentów i niezgodności

Rejestr incydentów i niezgodności prowadzi się w postaci elektronicznej w Systemie, na zasadach określonych w procedurze D1-P1-1, z dostępem ograniczonym do osób upoważnionych zgodnie z nadanymi uprawnieniami. Unikalny identyfikator zgłoszenia nadawany jest automatycznie przez System, a działania użytkowników w Systemie są rejestrowane.

§ 5. Obsługa zgłoszeń przez Usługodawcę

1. Przyjęcie, rejestrację i wstępną klasyfikację zgłoszeń (pierwsza linia obsługi) realizuje Usługodawca na podstawie umowy, o której mowa w § 2 ust. 2, z zachowaniem czasów reakcji w niej określonych.
2. Zastrzega się do wyłącznej kompetencji Urzędu:
 - a) ostateczną klasyfikację incydentu oraz decyzje o eskalacji — Pełnomocnik ds. SZBI,
 - b) ocenę i obsługę naruszeń ochrony danych osobowych, w tym zgłoszenia do Prezesa UODO — Inspektor Ochrony Danych we współpracy z Administratorem Danych,
 - c) zgłoszenia do CSIRT NASK — osoba wyznaczona do kontaktów z CSIRT,
 - d) zawiadomienie organów ścigania — Kierownik jednostki.

§ 6. Czynności ewidencyjne i aktualizacja dokumentacji

Zobowiązuje się: Administratora Systemu Informatycznego — do dokonania wpisów w rejestrze dostawców usług ICT (D3-P4-1), w rejestrze zasobów teleinformatycznych oraz w wykazie podmiotów zewnętrznych korzystających z dostępu zdalnego; Sekretarza Gminy — do dokonania wpisów w rejestrze umów powierzenia (D2-1) oraz w rejestrze czynności przetwarzania danych osobowych (D2-2); Pełnomocnika ds. SZBI — do ujęcia Systemu w analizie ryzyka oraz w analizie BIA (D4-1) wraz z parametrami RTO/RPO zgodnymi z umową, o której mowa w § 2 ust. 2 — w terminie 14 dni od dnia wejścia w życie zarządzenia.

§ 7. Zapoznanie pracowników

1. Pełnomocnik ds. SZBI zapewnia zakomunikowanie dokumentacji SZBI wszystkim pracownikom Urzędu w trybie określonym w dokumencie D1-6; fakt zapoznania się z dokumentacją podlega udokumentowaniu.
2. Przed produkcyjnym uruchomieniem Systemu wszyscy pracownicy Urzędu zostaną zapoznani z zasadami korzystania z Systemu, w tym z kanałem zgłaszania zdarzeń i incydentów bezpieczeństwa informacji. Instruktaż przeprowadza Usługodawca lub osoba wyznaczona przez Sekretarza Gminy; fakt zapoznania dokumentuje się zgodnie z procedurą D1-P5.

§ 8. Utrata mocy

Traci moc Zarządzenie Nr 48/2019 Wójta Gminy Dzierżążnia z dnia 12 listopada 2019 roku w sprawie wprowadzenia Polityki Ochrony Danych Osobowych w Urzędzie Gminy w Dzierżążni.

§ 9. Wykonanie

Wykonanie zarządzenia powierza się Sekretarzowi Gminy oraz Pełnomocnikowi ds. SZBI.

§ 10. Wejście w życie

Zarządzenie wchodzi w życie z dniem podpisania.

Wójt Gminy Dzierżążnia

mgr inż. Adam Sobiecki



UZASADNIENIE

Obowiązek ustanowienia, wdrożenia i doskonalenia systemu zarządzania bezpieczeństwem informacji w podmiotach realizujących zadania publiczne wynika z § 20 rozporządzenia w sprawie Krajowych Ram Interoperacyjności. Opracowana dokumentacja SZBI od pierwszego wydania uwzględnia wykorzystanie systemu teleinformatycznego wspierającego funkcjonowanie SZBI: system zapewnia unikalną identyfikację i rozliczalność zgłoszeń, prowadzenie rejestru incydentów i niezgodności z dostępem ograniczonym zgodnie z klasyfikacją informacji, wersjonowanie i ewidencję dokumentacji oraz automatyczne dane wejściowe do przeglądów zarządzania i pomiaru skuteczności (mierniki procedury D1-P2). Wymagania dla usług świadczonych w modelu chmurowym, określone w rozdziale XVI dokumentu D3 Polityka bezpieczeństwa teleinformatycznego, zostały odzwierciedlone w umowie z Usługodawcą oraz w umowie powierzenia przetwarzania danych osobowych, a zasady uwierzytelniania do Systemu — w dokumentach D3-P3 i D1-8. Wprowadzenie SZBI oraz Systemu jednym aktem zapewnia spójność dokumentacji od dnia jej wejścia w życie.

*RTO i RPO to dwa główne wskaźniki w informatyce, które pomagają firmom zaplanować działanie na wypadek awarii. RTO (Recovery Time Objective) to maksymalny czas potrzebny na naprawę i włączenie systemu po awarii, a RPO (Recovery Point Objective) to maksymalna ilość danych, jaką firma może bezpowrotnie stracić (mierzona w czasie od ostatniej kopii zapasowej)