Zarządzenie Nr 45/2026
Wójta Gminy Ruda Maleniecka
z dnia 17 lipca 2026 r.

w sprawie ustanowienia Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) oraz wprowadzenia jego dokumentacji w Urzędzie Gminy w Rudzie Malenieckiej

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, z późn. zm.), w związku z § 19 ust. 1 i 2 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), a także mając na uwadze wymagania wynikające z:

1. Dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającej rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającej dyrektywę (UE) 2016/1148 (dyrektywa NIS 2),
2. rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO),
3. ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (z późn. zm.), w tym zmian wprowadzonych ustawą z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (Dz. U. z 2026 r. poz. 252),
4. PN-EN ISO/IEC 27001:2023-08 – Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Systemy zarządzania bezpieczeństwem informacji – Wymagania,
5. PN-EN ISO/IEC 27701:2021-09,
6. PN-EN ISO/IEC 27002:2023-01,
7. PN ISO/IEC 27005:2022-10,
8. PN-EN ISO 22301:2020-04,
9. PN-EN ISO/IEC 27017:2021-07,
10. Narodowych Standardów Cyberbezpieczeństwa (NSC), stanowiących rekomendacje standaryzujące w zakresie bezpieczeństwa informacji i systemów informacyjnych, **zarządzam, co następuje:**

§ 1

Wprowadzenie dokumentacji SZBI

1. Wprowadza się do stosowania w Urzędzie Gminy w Rudzie Malenieckiej dokumentację Systemu Zarządzania Bezpieczeństwem Informacji, zwaną dalej „Dokumentacją SZBI" albo „SZBI".
2. Dokumentacja SZBI funkcjonuje w powiązaniu z Polityką ochrony danych osobowych oraz innymi regulacjami dotyczącymi przetwarzania danych osobowych w Urzędzie Gminy w Rudzie Malenieckiej.
3. Dokumentacja SZBI stanowi zbiór zatwierdzonych zasad, polityk, procedur, instrukcji, rejestrów, formularzy i innych zapisów służących zapewnieniu poufności, integralności, dostępności i autentyczności informacji przetwarzanych w Urzędzie, a także ciągłości działania i właściwego zarządzania ryzykiem.
4. Wykaz dokumentów wchodzących w skład Dokumentacji SZBI w obszarze zabezpieczeń organizacyjnych, zabezpieczeń zasobów ludzkich, zabezpieczeń fizycznych i technologicznych określa **Załącznik nr 1 do niniejszego zarządzenia.**
5. Dokumentacja, o której mowa w § 1 ust. 3, stanowi wewnętrzną regulację i nie podlega publikacji.
6. Dokumentacja SZBI podlega okresowym przeglądom oraz aktualizacji, w szczególności w przypadku zmian przepisów prawa, wymagań normatywnych, struktury organizacyjnej, procesów, systemów teleinformatycznych, wyników analizy ryzyka, audytów, incydentów bezpieczeństwa lub innych zmian mających wpływ na bezpieczeństwo informacji.

§ 2

Zakres obowiązywania

1. Dokumentacja SZBI wprowadzona niniejszym zarządzeniem obejmuje obszar zabezpieczeń organizacyjnych, zabezpieczeń zasobów ludzkich, zabezpieczeń fizycznych i technologicznych oraz ma zastosowanie do wszystkich komórek organizacyjnych Urzędu Gminy w Rudzie Malenieckiej, wszystkich procesów realizowanych przez Urząd oraz informacji przetwarzanych w związku z wykonywaniem zadań publicznych i obsługą administracyjną Urzędu.
2. Postanowienia Dokumentacji SZBI obowiązują wszystkich pracowników Urzędu, osoby zatrudnione na podstawie umów cywilnoprawnych, stażystów, praktykantów, wolontariuszy oraz inne osoby, którym udzielono dostępu do informacji, zasobów lub systemów teleinformatycznych Urzędu – w zakresie wynikającym z charakteru wykonywanych czynności i nadanych uprawnień.
3. Wymagania SZBI stosuje się odpowiednio do podmiotów zewnętrznych świadczących usługi na rzecz Urzędu, jeżeli w ramach realizacji tych usług uzyskują one dostęp do informacji, infrastruktury, systemów teleinformatycznych lub danych osobowych Urzędu, z uwzględnieniem postanowień zawartych umów.

§ 3

Obowiązki pracowników i komórek organizacyjnych

1. Kierownicy komórek organizacyjnych odpowiadają, w zakresie swojej właściwości, za wdrażanie i egzekwowanie wymagań Dokumentacji SZBI, identyfikowanie ryzyk, zgłaszanie potrzeb aktualizacji zabezpieczeń oraz zapewnienie, aby podlegli pracownicy zostali zapoznani z właściwymi dla nich zasadami i procedurami.
2. Każda osoba objęta zakresem SZBI jest zobowiązana do zapoznania się z Dokumentacją SZBI w zakresie niezbędnym do wykonywania powierzonych obowiązków, przestrzegania ustanowionych zasad bezpieczeństwa, ochrony powierzonych informacji i zasobów oraz niezwłocznego zgłaszania incydentów, podatności, naruszeń lub podejrzeń naruszenia bezpieczeństwa.
3. Osoby posiadające uprawnienia administracyjne lub uprzywilejowane oraz osoby odpowiedzialne za utrzymanie systemów teleinformatycznych wykonują swoje obowiązki z zachowaniem zasady minimalnych uprawnień, rozliczalności działań i rozdzielenia obowiązków, zgodnie z Dokumentacją SZBI.
4. Inspektor Ochrony Danych wykonuje zadania wynikające z RODO z zachowaniem niezależności przewidzianej w art. 38 RODO oraz współpracuje z osobami odpowiedzialnymi za bezpieczeństwo informacji w zakresie, w jakim działania SZBI dotyczą ochrony danych osobowych.
5. Koordynowanie, przegląd i aktualizację Dokumentacji SZBI będą realizowały osoby upoważnione wyznaczone przez Wójta Gminy Ruda Maleniecka,
6. Fakt zapoznania się z Dokumentacją SZBI może być potwierdzany w sposób przyjęty w Urzędzie, w szczególności w formie pisemnego lub elektronicznego oświadczenia, potwierdzenia udziału w szkoleniu albo potwierdzenia udostępnienia dokumentacji w systemie wewnętrznym.

§ 4

Aktualizacja dokumentacji

1. Aktualizacja dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) odbywa się zgodnie z zasadami określonymi w dokumentacji SZBI i nie wymaga każdorazowo wydawania odrębnego zarządzenia.
2. Dokumentowanie zmian odbywa się poprzez dokonanie odpowiedniego zapisu w historii zmian dokumentu.

§ 5

Postanowienia końcowe i wejście w życie

1. Zobowiązuje się kierowników komórek organizacyjnych do zapewnienia zapoznania podległych pracowników z treścią niniejszego zarządzenia oraz właściwymi elementami Dokumentacji SZBI.
2. Nadzór nad wykonaniem niniejszego zarządzenia powierza się Sekretarzowi Gminy.

4. Zarządzenie wchodzi w życie z dniem 17 lipca 2026 r.

Załącznik nr 1
do Zarządzenia Nr 45/2026
Wójta Gminy Ruda Maleniecka
z dnia 17 lipca 2026 r.

WYKAZ DOKUMENTACJI SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI (SZBI)

w Urzędzie Gminy w Rudzie Malenieckiej

Dokumentacja SZBI obejmuje poniższe dokumenty nadrzędne. Poszczególne wymagania bezpieczeństwa informacji zostały przypisane do dokumentów w sposób zapewniający objęcie wszystkich obszarów zabezpieczeń organizacyjnych, zabezpieczeń zasobów ludzkich, zabezpieczeń fizycznych i technologicznych. Dokumenty mogą zawierać załączniki, formularze, rejestry i instrukcje operacyjne, które stanowią ich integralne uzupełnienie.

Lp.	Nazwa dokumentu SZBI	Zakres regulacji	Realizowane punkty wymagań SZBI
1.	**Polityka Bezpieczeństwa Informacji z załącznikami w tym wykaz ról i odpowiedzialności w SZBI**	Dokument nadrzędny SZBI określający cele, zasady, zakres i strukturę systemu, role i odpowiedzialności, nadzór kierownictwa, wymagania zgodności, zasady przeglądów oraz powiązanie SZBI z ochroną danych osobowych.	1, 2, 3, 11, 12, 13
2.	**Procedura zarządzania ryzykiem bezpieczeństwa informacji**	Zasady identyfikowania aktywów, zagrożeń i podatności, szacowania i oceny ryzyka, postępowania z ryzykiem oraz uwzględniania bezpieczeństwa informacji w projektach i zmianach organizacyjnych.	4, 5
3.	**Procedura zarządzania dostępem i klasyfikacji informacji**	Zasady klasyfikowania i oznaczania informacji oraz przyznawania, zmiany, okresowego przeglądu i odbierania praw dostępu; zasady ograniczania dostępu i bezpiecznego uwierzytelniania.	6, 7, 31, 32
4.	**Procedura bezpieczeństwa dostawców i usług chmurowych**	Wymagania bezpieczeństwa w relacjach z dostawcami, zasady oceny i nadzoru nad dostawcami, wymagania umowne, powierzenie przetwarzania danych oraz zasady wyboru, korzystania i zakończenia korzystania z usług chmurowych.	8, 9

5.	**Procedura zarządzania incydentami bezpieczeństwa informacji**	Zasady zgłaszania, rejestrowania, klasyfikowania, oceny, podejmowania decyzji, reagowania i dokumentowania incydentów; współpraca z procesem obsługi naruszeń ochrony danych osobowych i wyciąganie wniosków po incydentach.	10
6.	**Regulamin bezpieczeństwa informacji dla pracowników i współpracowników**	Zasady bezpieczeństwa związane z zatrudnieniem i współpracą, obowiązki osób, poufność, szkolenia i świadomość, odpowiedzialność za naruszenia, obowiązki po zmianie lub zakończeniu współpracy, praca zdalna, czyste biurko i czysty ekran oraz podstawowe zasady korzystania z zasobów Urzędu.	14, 15, 16, 17, 18, 19, 24
7.	**Polityka bezpieczeństwa cyfrowego**	Zasady ochrony fizycznej pomieszczeń i zasobów oraz zabezpieczeń technologicznych, w tym urządzeń końcowych, nośników, kopii zapasowych, sieci, konfiguracji, oprogramowania, ochrony przed złośliwym oprogramowaniem, wyciekiem danych, kryptografii, usuwania informacji oraz bezpiecznego cyklu życia i zmian systemów.	20, 21, 22, 23, 25, 26, 27, 28, 29, 30, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42

1. Wskazane dokumenty stanowią dokumenty główne SZBI. Szczegółowe formularze, rejestry, instrukcje mogą być prowadzone jako załączniki lub dokumenty wykonawcze.
2. W obszarze prywatności i ochrony danych osobowych stosuje się również odrębną dokumentację ochrony danych osobowych obowiązującą w Urzędzie, w szczególności Politykę Ochrony Danych Osobowych oraz procedury wynikające z RODO.
3. Zakres dokumentów podlega okresowemu przeglądowi i aktualizacji w przypadku zmian prawnych, organizacyjnych, technologicznych, wyników analizy ryzyka, audytów lub incydentów bezpieczeństwa.