ZARZĄDZENIE Nr 55/26
WÓJTA GMINY KIWITY
z dnia 24 czerwca 2026 r.

w sprawie wprowadzenia dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Gminy Kiwity

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2025 r. poz. 1436), art. 13 ust. 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2025 r. poz. 1703 i 1301) oraz § 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), rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (RODO), ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2019 r. poz. 1781), zarządzam co następuje:

§ 1. 1 Wprowadzam do stosowania w Urzędzie Gminy Kiwity dokumentację Systemu Zarządzania Bezpieczeństwem Informacji, w celu zapewnienia efektywnego zarządzania bezpieczeństwem informacji, chroniąc poufność, integralność i dostępność danych, a także zapewniając ciągłość działania procesów wspierających świadczenie usług publicznych.
2. Na dokumentację Systemu Zarządzania Bezpieczeństwem Informacji, o której mowa w ust.1, składają się dokumenty wymienione w spisie dokumentów Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Gminy Kiwity, stanowiącym załącznik nr 1 do Zarządzenia.

§ 2. Dokumentacja, o której mowa w § 1, stanowi wewnętrzną regulację i nie podlega publikacji.

§ 3. Aktualizacja oraz dostosowywanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji nie wymaga wydawania odrębnych zarządzeń.

§ 4. Wszystkie osoby zatrudnione w Urzędzie Gminy Kiwity zobowiązane są do zapoznania się i przestrzegania zapisów SZBI.

§ 5. 1. Wyznacza się Panią Annę Bułkowską na Pełnomocnika ds. Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w Urzędzie Gminy Kiwity.

2. Pełnomocnik ds. Systemu Zarządzania Bezpieczeństwem Informacji odpowiada za wdrożenie, koordynację i nadzorowanie realizacji polityk i procedur bezpieczeństwa informacji, a także raportowanie stanu bezpieczeństwa do kierownictwa.

§ 6. Za wdrożenie i nadzór nad SZBI odpowiada Najwyższe Kierownictwo Urzędu Gminy Kiwity.

§ 7. Wykonanie zarządzenia oraz nadzór nad Systemem Zarządzania Bezpieczeństwem Informacji powierzam Sekretarzowi Gminy.

§ 8. Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT
Jacek Pawlik

Załączniki:

1. Spis dokumentów Systemu Zarządzania Bezpieczeństwem Informacji

RADCA PRAWNY
Bogusława Dworzańska

WYKAZ
DOKUMENTÓW, DRUKÓW, FORMULARZY I ZAPISÓW SZBI

L.p.	Oznaczenie/ Symbol	Nazwa dokumentu	
1	D1	Polityka Bezpieczeństwa Informacji	
2	D1-1	Przeglądy zarządzania	
3	D1-2	Cele SZBI - ustanowienie i pomiary	
4	D1-3	Kontekst organizacji	
5	D1-3-1		Wykaz aktów prawnych
6	D1-4	Klasyfikacja informacji, nadzór nad dokumentacją i zapisami SZBI	
7	D1-4-1		Wykaz dokumentów, druków, formularzy i zapisów SZBI
8	D1-4-2		Wykaz klasyfikacji informacji
9	D1-5	Bezpieczeństwo fizyczne i środowiskowe	
10	D1-5-1		Polityka kluczy
11	D1-6	Kanały komunikacji - zasady bezpiecznej komunikacji	
12	D1-7	Polityka czystego biurka i czystego ekranu	
13	D1-8	Polityka czystego ekranu	
14	D1-P1	Polityka zarządzania incydentami BI	
15	D1-P1-1		Procedura nadzoru nad zdarzeniami, incydentami BI i niezgodnościami
16	D1-P1-2		Identyfikacja zdarzeń, incydentów, niezgodności i naruszeń
17	D1-P1-3		Rejestr incydentów i niezgodności
18	D1-P1-4		Macierz klasyfikacji incydentów
19	D1-P1-5		Macierz eskalacji i ścieżki komunikacji
20	D1-P1-6		Formularz zgłoszenia incydentu CSIRT GOV
21	D1-P1-7		Lista kontaktów alarmowych i CSIRT
22	D1-P2	Procedura monitorowania	

23	D1-P3	Procedura zarządzania ryzykiem	
24	D1-P3-1		Arkusz analizy ryzyka
25	D1-P4	Procedura audytów wewnętrznych	
26	D1-P4-1		Program audytów
27	D1-P4-2		Karta audytu
28	D1-P4-3		Ankieta badania podmiotu
29	D1-P4-4		Lista kontrolna audytu wewnętrznego na zgodność z normą ISO 27001
30	D1-P5	Procedura szkoleń i podnoszenie świadomości	
31	D1-P6	Procedura zarządzania personelem	
32	D1-P7	Procedura kontaktów z organami władzy	
33	D1-P8	Procedura zarządzania umowami	
34	D1-P9	Zasady stosowania odstępstw	
35	D1-P9-1		Rejestr odstępstw
36	D1-DS	Deklaracja stosowania Zabezpieczeń	
37	D2	Polityka Ochrony Danych	
38	D2-1	Wzór Rejestru czynności przetwarzania	
39	D2-2	Wzór Rejestru kategorii czynności przetwarzania	
40	D2-3	Wzór Klauzuli informacyjnej	
41	D2-4	Wzór Umowy powierzenia przetwarzania danych	
42	D2-5	Tabela zmian w dokumentach	
43	D2-P1	Procedura dopuszczenia osoby do pracy	
44	D2-P1-1		Obowiązek informacyjny - RODO
45	D2-P1-2		Zgoda na przetwarzanie danych osobowych
46	D2-P1-3		Ewidencja odbioru oświadczeń

47	D2-P1-4			Lista uczestników szkolenia z zakresu ochrony danych osobowych
48	D2-P1-5			Upoważnienie i polecenie przetwarzania danych osobowych
49	D2-P1-5a			Upoważnienie i polecenie przetwarzania danych osobowych szczególnej kategorii
50	D2-P1-5b			Upoważnienie i polecenie przetwarzania danych osobowych (ZFŚS)
51	D2-P1-6			Zgoda na przebywanie o obszarze przetwarzania danych osobowych
52	D2-P1-7			Oświadczenie o zachowaniu poufności
53	D2-P1-8			Zgoda na przetwarzanie danych osobowych (publikacja wizerunku)
54	D2-P1-9			Oświadczenie pracownika w sprawie prywatnego numeru telefonu i adresu e-mail
55	D2-P1-10			Obowiązek informacyjny RODO - pracownik
56	D2-P1-11			Obowiązek informacyjny RODO - osoby zatrudnione na podstawie umowy cywilnoprawnej
57	D2-P1-12			Obowiązek informacyjny RODO - stażyści i praktykanci
58	D2-P1-13			Obowiązek informacyjny RODO - w stosunku do osób korzystających z ZFŚS
59	D2-P2		Procedura realizacji obowiązku informacyjnego	
60	D2-P2-1			Treść stopki email dotycząca przetwarzania danych
61	D2-P3		Procedura realizacji praw osób fizycznych	
62	D2-P3-1			Wzór odpowiedzi dotyczącej wydłużenia terminu
63	D2-P3-2			Wzór odpowiedzi na wniosek
64	D2-P3-3			Wzór informacji o usunięciu danych osobowych
65	D2-P4		Procedura zarządzania zmianą, zapewnienia ochrony danych w fazie projektowania i domyślnej ochrony danych u administratora	
66	D2-P5		Procedura wynoszenia dokumentacji i sprzętu IT u administratora	
67	D2-P5-1			Wzór zgody na wynoszenie sprzętu IT poza miejsce pracy
68	D2-P5-2			Wzór zgody na wynoszenie dokumentów poza budynki administratora
69	D2-P6		Procedura zapewnienia prawidłowego przetwarzania danych przy korzystaniu ze sprzętu IT i systemów	
70	D2-P6-1			Rejestr sprzętu IT
71	D2-P6-2			Rejestr systemów
72	D2-P7		Procedura korzystania ze sprzętu IT i systemów u administratora	

73	D2-P7-1			Zgoda na korzystanie ze sprzętu IT
74	D2-P7-2			Rejestr zgód na korzystanie ze sprzętu IT u Administratora
75	D2-P7-3			Rejestr wydanego sprzętu IT
76	D2-P7-4			Zgoda na wynoszenie sprzętu IT poza miejsce pracy
77	D2-P7-5			Rejestr zgód na wynoszenie sprzętu IT poza miejsce pracy
78	D2-P7-6			Zgoda na korzystanie z prywatnego sprzętu IT
79	D2-P7-7			Rejestr zgód na korzystanie z prywatnego sprzętu IT
80	D2-P7-8			Zgoda na korzystanie z systemów
81	D2-P7-9			Rejestr zgód na korzystanie z systemów
82	D2-P8		Procedura zgłaszania incydentów	
83	D2-P8-1			Formularz zgłoszenia i oceny incydentu
84	D2-P8-2			Zgłoszenie incydentu dotyczącego przetwarzania danych osobowych przez klienta
85	D2-P9		Procedura prowadzenia ewidencji naruszeń ochrony danych osobowych u administratora	
86	D2-P9-1			Ewidencja naruszeń ochrony danych osobowych
87	D2-P10		Procedura oceny powagi naruszenia	
88	D2-P11		Procedura, metodologia analizy Ryzyka RODO	
89	D3	Polityka bezpieczeństwa teleinformatycznego		
90	D3-1		Dziennik administratora systemu informatycznego	
91	D3-2		Plan zarządzania podatnościami	
92	D3-3		Logowanie zdarzeń w SI	
93	D3-4		Zasady pracy w SI	
94	D3-5		Zasady projektowania bezpiecznych systemów	
95	D3-6		Ochrona kryptograficzna	
96	D3-7		Bezpieczeństwo teleinformatyczne i bezpieczna komunikacja	
97	D3-7-1			Instrukcja adresowania i zabezpieczania wiadomości email

98	D3-8		Polityka usuwania danych i likwidacji nośników	
99	D3-9		Instrukcja zarządzania e-usługami	
100	D3-10		Polityka AI	
101	D3-P1		Procedura zarządzania dostępem i uprawnieniami	
102	D3-P1-1			Wniosek o dostęp do DO i do SI
103	D3-P2		Zarządzanie zmianą i aktualizacjami	
104	D3-P3		Polityka haseł i uwierzytelniania	
105	D3-P4		Procedura zarządzania ICT	
106	D3-P4-1		Rejestr dostawców usług ICT	
107	D4	Polityka Ciągłości Działania		
108	D4-1		Analiza BIA	
109	D4-2		Plan odtworzenia po awarii	
110	D4-P1		Procedura Zarządzania Ciągłością Działania	
111	D4-P1-1			Wzór raportu z testów PCD
112	D4-P2		Procedura zarządzania kopiami zapasowymi	
113	D4-P2-1			Rejestr kopii zapasowych
114	D4-P2-2			Testy kopii zapasowych
115	D5	Wykaz dokumentów, druków, formularzy i zapisów SZBI		