

**ZARZĄDZENIE NR 100/2026**  
**BURMISTRZA LUBNIEWIC**

z dnia 2 stycznia 2026 r.

**w sprawie wprowadzenia Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miejskim  
w Lubniewicach**

Na podstawie 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 z dnia 2024.05.22.) zarządza się, co następuje:

**§ 1.**

1. W Urzędzie Miejskim w Lubniewicach w celu utrzymania podstawowych atrybutów bezpieczeństwa Systemu Przetwarzania Informacji, w szczególności poufności, dostępności i integralności informacji wprowadza się System Zarządzania Bezpieczeństwem Informacji (w skrócie dalej: SZBI) oraz prowadzi związaną z nim dokumentację.
2. Na dokumentację SZBI składają się procedury, wykazy, polityki i instrukcje, gwarantujące poufności, dostępności i integralności informacji przetwarzanych w Urzędzie Miejskim w Lubniewicach wymienione w załączniku nr 1 do niniejszego zarządzenia.

**§ 2.**

Zobowiązuję pracowników komórek organizacyjnych Urzędu do realizacji zadań wynikających z wprowadzenia systemu zarządzania bezpieczeństwem informacji oraz kierowników do nadzoru nad zapoznaniem z SZBI pracowników podległych im komórek organizacyjnych. Pracownicy Urzędu Miejskiego w Lubniewicach zobowiązani są do zapoznania się z dokumentacją SZBI oraz do przestrzegania procedur w niej zawartych.

**§ 3.**

Wdrożenie oraz utrzymanie dokumentacji SZBI powierza się Administratorowi Systemu Informatycznego oraz Inspektorowi Ochrony Danych Osobowych w zakresie dokumentacji dotyczącej ochrony danych osobowych.

**§ 4.**

Na podstawie art. 5 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2022 r. poz. 902 z późn. zm.), wyklucza się z jawności treść dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji, o której mowa w§ 1 ust. 1 i 2.

**§ 5.**

Nadzór nad wykonaniem zarządzenia powierza się Sekretarzowi Gminy.

**§ 6.**

Zarządzenie wchodzi w życie z dniem podjęcia.

Burmistrz Lubniewic

**Radosław Sosnowski**

Załącznik Nr 1 do zarządzenia nr 100/2026

Burmistrza Lubniewic

z dnia 2 stycznia 2026 r.

SZBI - 00 Polityka Bezpieczeństwa Informacji (Rdzeń Systemu SZBI)

Lp.	Oznaczenie i tytuł dokumentu
1.	SZBI-00-01 Polityka Bezpieczeństwa Informacji
2.	SZBI-00-02-Pojęcia i definicje
3.	SZBI-00-03-Deklaratywna polityka bezpieczeństwa informacji
4.	SZBI-00-04-Kontekst-zakres-cele bezpieczeństwa
5.	SZBI-00-06-Utrzymanie i doskonalenie systemu zarządzania bezpieczeństwem informacji
6.	SZBI-01-03b-Upoważnienie do przetwarzania
7.	SZBI-01-04-Oświadczenie o poufności
8.	SZBI-06-1 Cele i plany bezpieczeństwa
9.	SZBI-06-2 Proces Analiza ryzyka i plan postępowania
10.	SZBI-06-2b-Deklaracja Stosowania (SoA)
11.	SZBI-06-2a Arkusz analizy ryzyka
12.	SZBI-07-3 Procedura nadzoru nad udokumentowanymi informacjami
13.	SZBI-07-6 Ramowy plan szkolenia i warsztatów z podstaw cyberbezpieczeństwa oraz dokumentacji
14.	SZBI-09-1 Proces monitorowania, pomiarów, analizy i oceny
15.	SZBI-09-1-a Ewidencja obszarów monitorowania i pomiarów
16.	SZBI-09-2 Procedura audytu wewnętrznego
17.	SZBI-09-2-2 Plan audytu wewnętrznego
18.	SZBI-09-2-1 Program audytu wewnętrznego
19.	SZBI-09-2-3 Raport z audytu wewnętrznego
20.	SZBI-09-4 Procedura przeglądu zarządzania
21.	SZBI-09-4-1 Raport z przeglądu zarządzania
22.	SZBI-10-1 Procedura zarządzania niezgodnościami
23.	SZBI-10-1a Rejestr niezgodności i działań korygujących

SZBI - A05 Polityka bezpieczeństwa organizacyjnego (Kontrola A.5)

Lp.	Oznaczenie i tytuł dokumentu
1.	SZBI-A05-00-Polityka bezpieczeństwa organizacyjnego
2.	SZBI-A05-01-1 Polityka dotycząca mediów społecznościowych
3.	SZBI-A05-01-2 Polityka bezpieczeństwa HR
4.	SZBI-A05-04-1 Regulamin sygnalistów
5.	SZBI-A05-05-1 Lista kontaktów z organami
6.	SZBI-A05-06-1 Lista kontaktów grup eksperckich
7.	SZBI-A05-07-1 Polityka wywiadu w zakresie identyfikacji zagrożeń
8.	SZBI-A05-07-3 Raport informacji o zagrożeniach
9.	SZBI-A05-08-1 Procedura bezpieczeństwa informacji w zarządzaniu projektami
10.	SZBI-A05-09-1a Ewidencja - inwentaryzacja sprzętu IT ITC
11.	SZBI-A05-09-1b Ewidencja - inwentaryzacja aktywów
12.	SZBI-A05-09-1 Polityka zarządzania aktywami informacyjnymi
13.	SZBI-A05-10-1 Polityka dozwolonego użycia
14.	SZBI-A05-10-2 Polityka dostępu do Internetu
15.	SZBI-A05-10-3 Zasady korzystania z poczty elektronicznej

16.	SZBI-A05-10-5 Procedura zarządzania zagubionymi lub skradzionymi urządzeniami
17.	SZBI-A05-10-6 Polityka współpracy online
18.	SZBI-A05-11-1 Obiegówka
19.	SZBI-A05-12-1 Procedura klasyfikacji informacji
20.	SZBI-A05-13-1 Procedura oznaczania informacji
21.	SZBI-A05-14-1 Procedura transferu informacji poufnych
22.	SZBI-A05-14-2 Umowa transferu informacji poufnej
23.	SZBI-A05-15-1 Polityka kontroli dostępu
24.	SZBI-A05-18-1 Proces zarządzania uprawnieniami użytkowników
25.	SZBI-A05-18-1a Wniosek zarządzania uprawnieniami użytkowników
26.	SZBI-A05-18-1b Ewidencja osób upoważnionych
27.	SZBI-A05-19-1 Polityka bezpieczeństwa informacji w relacjach z dostawcami
28.	SZBI-A05-21-1 Zarządzanie bezpieczeństwem informacji w łańcuchu dostaw
29.	SZBI-A05-22-1a Arkusz oceny dostawców
30.	SZBI-A05-22-1 Procedura oceny bezpieczeństwa dostawców
31.	SZBI-A05-23-1 Polityka bezpieczeństwa usług w chmurze
32.	SZBI-A05-23-2 Kwestionariusz oceny usługi chmurowej
33.	SZBI-A05-24-1 Plan reagowania na incydenty Ransomware
34.	SZBI-A05-24-2 Plan reagowania na incydenty DoS
35.	SZBI-A05-25-1 Procedura oceny zdarzeń związanych z bezpieczeństwem informacji
36.	SZBI-A05-26-1 Procedura reagowania na incydenty bezpieczeństwa informacji
37.	SZBI-A05-27-1 Raport po incydencie
38.	SZBI-A05-30-4 Plan ciągłości działania
39.	SZBI-A05-30-5 Harmonogram testowania ciągłości ICT
40.	SZBI-A05-30-6 Plan testu ciągłości ICT
41.	SZBI-A05-30-7 Raport z testu ciągłości ICT
42.	SZBI-A05-31-1 Procedura dotycząca wymagań prawnych i regulacyjnych
43.	SZBI-A05-31-2 Rejestr wymagań prawnych i kontraktowych
44.	SZBI-A05-32-1 Polityka zgodności z prawem własności intelektualnej i prawami autorskimi
45.	SZBI-A05-33-1 Polityka ochrony dokumentów

**SZBI - A06 Polityka bezpieczeństwa zasobami ludzkimi HR (Kontrola A.6)**

<b>Lp.</b>	<b>Oznaczenie i tytuł dokumentu</b>
1.	SZBI-A06-0-0 Polityka bezpieczeństwa zasobami ludzkimi HR
2.	SZBI-A06-06-1 Ewidencja umów poufności
3.	SZBI-A06-06-2 Umowa o zachowaniu poufności (NDA)
4.	SZBI-A06-06-4 Proces dyscyplinarny
5.	SZBI-A06-07-1 Polityka pracy zdalnej
6.	SZBI-A06-07-2 Regulamin pracy zdalnej
7.	SZBI-A06-07-3 Informacja BHP przy wykonywaniu pracy zdalnej przez pracowników
8.	SZBI-A06-08-1 Procedura raportowania zdarzeń bezpieczeństwa informacji

**SZBI - A07 Polityka bezpieczeństwa fizycznego (Kontrola A.7)**

<b>Lp.</b>	<b>Oznaczenie i tytuł dokumentu</b>
1	SZBI-A07-0-0 Polityka bezpieczeństwa fizycznego
2	SZBI-A07-01-1 Fizyczne strefy bezpieczeństwa
3	SZBI-A07-01-1a Polityka kluczy
4	SZBI-A07-02-1 Standardy projektowania zabezpieczeń fizycznych
5	SZBI-A07-03-1 Procedura dostępu do centrum danych
6	SZBI-A07-04-1 Polityka monitoringu wizyjnego

7	SZBI-A07-06-1 Praca w obszarach bezpiecznych
8	SZBI-A07-09-1 Procedura wynoszenia sprzętu i aktywów poza organizację
9	SZBI-A07-10-1 Procedura zarządzania nośnikami wymiennymi
10	SZBI-A07-10-1a Ewidencja nośników zawierających dane chronione
11	SZBI-A07-10-2 Procedura przesyłania nośników fizycznych
12	SZBI-A07-14-1 Procedura niszczenia nośników
13	SZBI-A07-14-1a Protokół zniszczenia nośników
14	SZBI-A07-7-1 Polityka czystego biurka i czystego ekranu

SZBI - A08 Instrukcja zarządzania systemami informatycznymi (IZSI) (Kontrola A.8)

Lp.	Oznaczenie i tytuł dokumentu
1.	SZBI-A08-0-0 Instrukcja zarządzania systemami informatycznymi (IZIS)
2.	SZBI-A08-01-1 Polityka zarządzania urządzeniami mobilnymi
3.	SZBI-A08-01-2 Polityka BYOD
4.	SZBI-A08-03-1 Polityka dynamicznej kontroli dostępu
5.	SZBI-A08-06-1 Zarządzanie pojemnością
6.	SZBI-A08-07-1 Procedura ochrony przed złośliwym oprogramowaniem
7.	SZBI-A08-08-1 Polityka zarządzania podatnościami technicznymi
8.	SZBI-A08-08-2 Procedura oceny podatności technicznej
9.	SZBI-A08-09-1 Polityka zarządzania konfiguracją
10.	SZBI-A08-09-3 Szablon konfiguracji sprzętu mobilnego
11.	SZBI-A08-09-3a Szablony zarządzania konfiguracją
12.	SZBI-A08-10-1 Polityka usuwania informacji
13.	SZBI-A08-11-1 Polityka maskowania danych
14.	SZBI-A08-11-2 Proces maskowania danych
15.	SZBI-A08-12-1 Polityka zapobiegania wyciekom danych
16.	SZBI-A08-13-1 Polityka backupów - tworzenia kopii zapasowych
17.	SZBI-A08-13-1a Procedura backupów
18.	SZBI-A08-14-1 Polityka zarządzania dostępnością
19.	SZBI-A08-15-1 Polityka rejestrowania i monitorowania
20.	SZBI-A08-16-1 Polityka monitorowania
21.	SZBI-A08-17-1 Synchronizacja zegarów
22.	SZBI-A08-18-1 Rejestr uprzywilejowanych programów narzędziowych
23.	SZBI-A08-19-1 Polityka oprogramowania
24.	SZBI-A08-20-1 Polityka bezpieczeństwa sieci
25.	SZBI-A08-23-1 Polityka filtrowania sieci
26.	SZBI-A08-24-1 Polityka kryptograficzna
27.	SZBI-A08-29-1 Lista kontrolna testów akceptacyjnych
28.	SZBI-A08-32-1 Proces zarządzania zmianami

Burmistrz Lubniewic

**Radosław Sosnowski**