



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



System Zarządzania Bezpieczeństwem Informacji (SZBI)				
	Nazwa dokumentu SZBI:	Wykaz dokumentacji SZBI		
	Numer:	Załącznik nr 1 do Zarządzenia Nr 51/2026 r. Starosty Powiatu Żyrardowskiego z dnia 28 maja 2026 r.	Data obowiązywania zgodna z Zarządzeniem Nr 51/2026 r. Starosty Powiatu Żyrardowskiego	01.09.2026 r.
	Klauzula:	DO UŻYTKU WEWNĘTRZNEGO	Wersja:	1.0
	Zatwierdził:	Starosta Powiatu Żyrardowskiego		

Wykaz dokumentacji SZBI

wraz z określeniem uprawnień do dostępu

Zadanie współfinansowane ze środków Unii Europejskiej
w ramach Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC)
Priorytet II: Zaawansowane usługi cyfrowe
Działanie 2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa.
Projekt „Cyberbezpieczny Samorząd ”

HISTORIA ZMIAN

Numer wersji	Data zmiany	Opis zmiany	Autor
1.0	15-12-2025	Utworzenie dokumentu	- Starostwo Powiatowe w Żyrardowie Wydział Informatyzacji i Ochrony Danych - InBASE Sp. z o.o.

Lp.	Oznaczenie dokumentu numer załącznika do zarządzenia	Nazwa dokumentu	Dostęp
1.	Załącznik nr 1	Wykaz dokumentacji SZBI	Wszyscy Pracownicy, Współpracownicy
2.	Załącznik nr 2	Polityka bezpieczeństwa informacji Załącznik nr 1 – powołanie Administratora Systemów Informatycznych oraz Zastępców Administratora Systemów Informatycznych	Wszyscy Pracownicy, Współpracownicy
3.	Załącznik nr 3	Polityka ochrony danych osobowych - Załącznik nr 1 – Wyciąg polityki bezpieczeństwa danych osobowych dla podmiotów zewnętrznych; - Załącznik nr 2 – Rejestr czynności przetwarzania danych osobowych; - Załącznik nr 3 – Rejestr kategorii czynności przetwarzania; - Załącznik nr 4 – Obowiązek informacyjny - wzór; - Załącznik nr 5 – Klauzula zgody przetwarzania danych osobowych - wzór; - Załącznik nr 6 – Umowa powierzenia przetwarzania danych osobowych - wzór; - Załącznik nr 7 – Kwestionariusz pytań dla podmiotu przetwarzającego dane osobowe; - Załącznik nr 8 – Upoważnienie do przetwarzania danych osobowych - wzór; - Załącznik nr 9 – Oświadczenie o zachowaniu poufności osoby upoważnionej do przetwarzania danych osobowych - wzór; - Załącznik nr 10 – Rejestru osób upoważnionych do przetwarzania danych osobowych - wzór; - Załącznik nr 11 – Formularz dla osoby, która zgłasza chęć skorzystania z praw jej przysługujących; - Załącznik nr 12 – Raport z incydentu naruszenia ochrony danych osobowych; - Załącznik nr 13 – Powołanie Inspektora Ochrony Danych (IOD) - wzór; - Załącznik nr 14 – Plan audytów wewnętrznych systemu ochrony danych osobowych	Wszyscy Pracownicy, Współpracownicy
4.	Załącznik nr 4	Regulamin bezpieczeństwa informacji - Załącznik nr 1 – Kontekst organizacji - Załącznik nr 2 – Plan ciągłości działania - wzór - Załącznik nr 3 – Zestaw mierników – wzór - Załącznik nr 4 – Program osiągnięcia celów SZBI - wzór	Wszyscy Pracownicy, Współpracownicy
5.	Załącznik nr 5	Regulamin bezpieczeństwa teleinformatycznego (IT) - Załącznik nr 1 – Wzór protokołu zdawczo-odbiorczego - Załącznik nr 2 - Wzór protokołu niszczenia	Wszyscy Pracownicy, Współpracownicy
6.	Załącznik nr 6	Analiza ryzyka - uwzględniająca poszczególne zasoby (Załączniki 1-40 do analizy ryzyka)	Zespół ds. SZBI, Najwyższe kierownictwo, Koordynator SZBI, ASI, IOD, Informatycy, Dyrektorzy wydziałów
7.	Załącznik nr 7	Procedura klasyfikacji informacji	Wszyscy Pracownicy, Współpracownicy
8.	Załącznik nr 8	Procedura nadzoru nad udokumentowanymi informacjami	Wszyscy Pracownicy, Współpracownicy
9.	Załącznik nr 9	Procedura zarządzania bezpieczeństwem fizycznym i środowiskowym Załącznik nr 1 - Wzór protokołu wydania klucza - wzór	Zespół ds. SZBI, Najwyższe kierownictwo, Koordynator SZBI, ASI, IOD, Informatycy, Dyrektorzy wydziałów, Ochrona fizyczna Starostwa
10.	Załącznik nr 10	Procedura zarządzania bezpieczeństwem zasobów ludzkich - Załącznik nr 1 – Oświadczenie o zachowaniu poufności - Załącznik nr 2 – Lista obecności na szkoleniu – wzór	Zespół ds. SZBI, Najwyższe kierownictwo, Koordynator SZBI, ASI, IOD, Informatycy, Dyrektorzy wydziałów, Kadry

11.	Załącznik nr 11	Procedura reagowania na incydenty bezpieczeństwa informacji	Wszyscy Pracownicy, Współpracownicy
12.	Załącznik nr 12	Procedura audytu wewnętrznego • Załącznik nr 1 – Program audytów – wzór • Załącznik nr 2 – Plan audytów – wzór • Załącznik nr 3 – Raport z audytu – wzór	Zespół ds. SZBI, Najwyższe kierownictwo, Koordynator SZBI, ASI, IOD, Audytorzy wewn.
13.	Załącznik nr 13	Procedura zarządzania niezgodnościami, działaniami korygującymi i doskonalącymi • Załącznik nr 1 – Rejestr niezgodności • Załącznik nr 2 – Karta działań korygujących	Zespół ds. SZBI, Najwyższe kierownictwo, Koordynator SZBI, ASI, IOD, Informatycy, Dyrektorzy wydziałów
14.	Załącznik nr 14	Procedura nadawania, modyfikacji, odbierania uprawnień do zasobów informatycznych	Wszyscy Pracownicy, Współpracownicy
15.	Załącznik nr 15	Zestawienie odpowiedzialności w ramach SZBI	Wszyscy Pracownicy, Współpracownicy
16.	Załącznik nr 16	Zasady komunikacji w ramach SZBI	Wszyscy Pracownicy, Współpracownicy
17.	Załącznik nr 17	Deklaracja stosowania	Zespół ds. SZBI, Najwyższe kierownictwo, Koordynator SZBI, ASI, IOD, Informatycy,
18.	Załącznik nr 18	Rejestr Aktywów	Zespół ds. SZBI, Najwyższe kierownictwo, Koordynator SZBI, ASI, IOD, Informatycy, Dyrektorzy wydziałów,
19.	Załącznik nr 19	Plany ciągłości działania	Zespół ds. SZBI, Najwyższe kierownictwo, Koordynator SZBI, ASI, IOD, Informatycy, Dyrektorzy wydziałów,

Powszechny dostęp (Wszyscy Pracownicy, Współpracownicy): Przypisany do procedur operacyjnych, które każdy urzędnik musi stosować na co dzień (Klasyfikacja informacji, Nadzór nad dokumentami, Zgłaszanie incydentów, Odpowiedzialność i Komunikacja).

Dyrektorzy wydziałów: Muszą znać dokumenty zarządcze (Analiza ryzyka, Zarządzanie ludźmi/kadrami, Rejestr aktywów ich wydziału), aby skutecznie nadzorować podległych pracowników i zarządzać ciągłością pracy wydziału.

Koordynator SZBI, IOD, ASI oraz Najwyższe kierownictwo: Posiadają pełny wgląd we wszystkie dokumenty o charakterze analitycznym, rejestrowym i deklaracyjnym, ponieważ odpowiadają za strategiczne bezpieczeństwo jednostki.

Zespół ds. SZBI: Jako ciało kolegialne, które zatwierdza i cyklicznie przegląda system, posiada dostęp do **każdego** dokumentu w tabeli. Członkowie zespołu muszą mieć pełen obraz sytuacji, aby oceniać ryzyka (Załącznik nr 6) oraz wdrażać działania korygujące (Załącznik nr 13).

Informatycy (ASI): Zostali wprost przypisani jako współwłaściciele procedur technicznych. Muszą bezwzględnie znać zasady zarządzania uprawnieniami (Załącznik nr 14), zabezpieczenia serwerowni (Załącznik nr 9), Rejestr aktywów (Załącznik nr 18) oraz procedury odtwarzania systemów po awarii w Planie ciągłości działania (Załącznik nr 19).

Ochrona fizyczna Starostwa: Ograniczona do procedury bezpieczeństwa fizycznego (Załącznik nr 9).