

**ZARZADZENIE NR 115/2026
BURMISTRZA ŚRODY ŚLĄSKIEJ
z dnia 5 czerwca 2026 r.**

w sprawie wprowadzenia Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miejskim w Środzie Śląskiej oraz ustalenia okresu dostosowawczego

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), art. 8 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2026 r. poz. 20 i 252), art. 24 ust. 1 i 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 (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.) oraz § 19 ust. 1–3 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. 2024 r. poz. 773), a także z uwzględnieniem Polskiej Normy PN-EN ISO/IEC 27001:2023, zarządza się, co następuje:

§ 1. Wprowadza się System Zarządzania Bezpieczeństwem Informacji w Urzędzie Miejskim w Środzie Śląskiej, zwany dalej „SZBI”, w celu zapewnienia odpowiedniego poziomu bezpieczeństwa informacji, w tym poufności, integralności i dostępności.

§ 2. 1. SZBI stanowi podsystem systemu kontroli zarządczej i obejmuje wszelkie informacje przetwarzane w Urzędzie Miejskim w Środzie Śląskiej lub na potrzeby innych podmiotów, bez względu na ich formę oraz miejsce przetwarzania.

2. Z zakresu stosowania SZBI wyłącza się informacje niejawne.

3. Wykaz dokumentacji SZBI stanowi załącznik nr 1 do niniejszego zarządzenia.

§ 3. 1. Odpowiedzialności i uprawnienia oraz akceptowalny poziom użycia aktywów określają Regulamin Organizacyjny Urzędu Miejskiego w Środzie Śląskiej, udzielone upoważnienia, pełnomocnictwa oraz inne regulacje opracowane, wdrożone i ogłoszone przez Burmistrza Środy Śląskiej.

2. Za nadzór nad całością SZBI odpowiada Zespół do spraw Systemu Zarządzania Bezpieczeństwem Informacji, zwany dalej „Zespołem ds. SZBI”.

3. W skład Zespołu ds. SZBI wchodzi:

- a. Inspektor Ochrony Danych (IOD), z głosem doradczym,
- b. Administrator Systemów Informatycznych (ASI),
- c. Pełnomocnik ds. Cyberbezpieczeństwa – Przewodniczący Zespołu.

4. Przewodniczący Zespołu kieruje pracami Zespołu.

5. Zespół ds. SZBI podlega bezpośrednio Burmistrzowi.

6. Zespół ds. SZBI jest uprawniony do:

- a. opiniowania instrukcji, procedur oraz innych zapisów wchodzących w zakres dokumentacji SZBI i przedkładania ich do zatwierdzenia,
- b. monitorowania, przeglądu i doskonalenia dokumentacji SZBI,
- c. monitorowania zmiany kontekstu SZBI,
- d. monitorowania postępu wdrożenia SZBI względem harmonogramu okresu dostosowawczego.

7. Dokumentację SZBI zatwierdza Burmistrz Środy Śląskiej albo Sekretarz Gminy działający na podstawie jego upoważnienia.

8. Za procesy SZBI oraz powiązane z nimi aktywa informacyjne odpowiadają ich właściciele wskazani w załączniku „Inwentaryzacja zasobów”, którego wzór stanowi załącznik do Polityki Bezpieczeństwa Informacji.

9. Aktualizacja załącznika „Inwentaryzacja zasobów” nie wymaga wydania lub zmiany niniejszego zarządzenia.

10. Za aktywa wspierające odpowiadają pracownicy, wykonawcy, podwykonawcy i zleceńbiorycy, którym na mocy regulaminu organizacyjnego, przekazania mienia, zakresu zadań, umów lub porozumień powierzono zarządzanie danym aktywem.
11. Za bezpieczeństwo informacji odpowiada każdy pracownik oraz podmioty, którym powierzono informacje, w tym dostawcy usług.
12. Za bezpieczeństwo fizyczne odpowiada komendant Straży Miejskiej.

§ 4. 1. Odpowiedzialność za funkcjonowanie SZBI ponosi kierownik podmiotu zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa.

2. Zadania administratora danych osobowych (ADO) wykonuje Burmistrz Środy Śląskiej. Wyznacza się role: Inspektora Ochrony Danych (IOD), Administratora Systemów Informatycznych (ASI) oraz Pełnomocnika ds. Cyberbezpieczeństwa, zgodnie z dokumentacją SZBI. Role obowiązują od dnia wejścia w życie zarządzenia.

§ 5. 1. System Zarządzania Bezpieczeństwem Informacji podlega corocznemu przeglądowi w ramach systemu kontroli zarządczej oraz ciągłemu doskonaleniu, a także przeglądowi po każdej istotnej zmianie organizacyjnej lub technicznej oraz po poważnym incydencie.

2. Efektywność zarządzania systemem bezpieczeństwa informacji oparta jest o wskaźniki i mierniki ustalane w ramach systemu kontroli zarządczej.
3. Kierownicy Wydziałów Urzędu Miejskiego w Środzie Śląskiej uwzględniają stan bezpieczeństwa wykorzystywanych aktywów informacyjnych w obszarach kontroli zarządczej, w ramach corocznej samooceny.

§ 6. Ustala się następującą systematykę zarządzania bezpieczeństwem informacji:

1. Polityka Systemu Zarządzania Bezpieczeństwem Informacji – polityka nadrzędna wobec innych regulacji obszaru bezpieczeństwa informacji, z wyłączeniem ochrony informacji niejawnych;
2. polityki niższego rzędu – polityki, standardy, zasady, wytyczne, regulaminy i inne regulacje obejmujące część obszaru bezpieczeństwa informacji lub systemu;
3. procedury, instrukcje, programy – reguły postępowania i sposoby wypełniania polityk.

§ 7. 1. Wprowadza się czterostopniową klasyfikację informacji:

- 1) publiczne,
 - 2) do użytku wewnętrznego,
 - 3) do użytku służbowego,
 - 4) strzeżone.
2. Szczegółowe zasady klasyfikowania i oznaczania informacji określa polityka klasyfikacji informacji (SZBI-KLS-01).
 3. Zasady oznaczania stosuje się do dokumentów tworzonych od dnia wejścia w życie zarządzenia. Dokumenty wcześniejsze podlegają klasyfikacji sukcesywnie w okresie dostosowawczym.

§ 8. 1. Od dnia wejścia w życie niniejszego zarządzenia bezwzględnie obowiązują, bez okresu dostosowawczego, następujące zasady i procedury – jako niezbędne dla bieżącego bezpieczeństwa:

- 1) obowiązek niezwłocznego zgłoszenia incydentu bezpieczeństwa Pełnomocnikowi ds. Cyberbezpieczeństwa oraz Administratorowi Systemów Informatycznych przez każdego, kto incydent wykrył, oraz obsługa incydentu zgodnie z procedurą zarządzania incydentami bezpieczeństwa;
 - 2) obowiązek ochrony danych osobowych zgodnie z RODO oraz zgłoszenia naruszenia ochrony danych osobowych Prezesowi Urzędu Ochrony Danych Osobowych w terminie 72 godzin od stwierdzenia naruszenia;
 - 3) zakaz ujawniania informacji klasy strzeżone oraz zasady dostępu do nich;
 - 4) obowiązek zachowania poufności przez pracowników i podmioty zewnętrzne.
2. Zgłaszanie incydentów poważnych właściwemu zespołowi CSIRT – wczesne ostrzeżenie w terminie 24 godzin i zgłoszenie incydentu poważnego w terminie 72 godzin od wykrycia oraz sprawozdanie końcowe w terminie miesiąca – następuje w terminach i trybie określonych w ustawie o krajowym systemie cyberbezpieczeństwa, od dnia uzyskania przez Urząd dostępu do systemu teleinformatycznego służącego zgłaszaniu incydentów.
 3. Terminy, o których mowa w ust. 1 pkt 2 oraz w ust. 2, biegną niezależnie od siebie.

§ 9. 1. Ustala się okres dostosowawczy do dnia 3 kwietnia 2027 r., w którym Wydział Urzędu Miejskiego w Środzie Śląskiej dostosują swoje procesy do pełnych wymogów SZBI.

2. Wdrożenie zapisów SZBI w okresie dostosowawczym następuje etapami, zgodnie z harmonogramem stanowiącym załącznik nr 2 do niniejszego zarządzenia.

3. W zakresie nieobjętym jeszcze wdrożeniem, a niewymienionym w § 8, do czasu zakończenia danego etapu dopuszcza się stosowanie dotychczasowych zasad, o ile nie naruszają one przepisów prawa powszechnie obowiązującego.

§ 10. 1. Zespół ds. SZBI monitoruje postęp wdrożenia względem harmonogramu i informuje kierownika podmiotu o ewentualnych zagrożeniach dla dotrzymania terminów.

2. Bieżące czynności monitorujące w imieniu Zespołu może wykonywać Pełnomocnik ds. Cyberbezpieczeństwa.

3. Po zakończeniu okresu dostosowawczego Zespół ds. SZBI sporządza protokół potwierdzający pełne wdrożenie SZBI.

§ 11. 1. Dokumentację SZBI ogłasza się w sposób umożliwiający dostęp pracownikom Urzędu Miejskiego w Środzie Śląskiej, w zakresie odpowiadającym zakresowi ich zadań oraz klasyfikacji poszczególnych dokumentów.

2. Pracownicy zapoznają się z dokumentacją SZBI właściwą dla zajmowanego stanowiska w terminie 14 dni od dnia jej ogłoszenia i potwierdzają to na formularzu stanowiącym załącznik do Polityki Bezpieczeństwa Informacji.

3. Strony zainteresowane posiadają dostęp do dokumentacji SZBI wyłącznie w zakresie niezbędnym do realizacji zadań wykonywanych dla Urzędu Miejskiego w Środzie Śląskiej.

§ 12. 1. Wykonanie zarządzenia w zakresie monitorowania wdrożenia powierza się Zespołowi ds. SZBI.

2. Wykonanie zarządzenia powierza się Sekretarzowi Gminy.

3. Zarządzenie wchodzi w życie z dniem podpisania, z uwzględnieniem okresu dostosowawczego określonego w § 9.

BURMISTRZ

Elżbieta Czarnota

Wykaz dokumentów Systemu Zarządzania Bezpieczeństwem Informacji

Przewodniki (5)

1. Przewodnik ADO IOD
2. Przewodnik Administrator IT
3. Przewodnik Kierownik
4. Przewodnik Pracownik
5. Przewodnik Pracownik Zdalny

Polityki nadrzędne (15)

6. PBI 1 0 Polityka Bezpieczeństwa Informacji
7. PBI ZAL 01 Inwentaryzacja zasobów
8. PBI ZAL 02 NDA
9. PBI ZAL 03 Deklaracja stosowania
10. PBI ZAL 04 Kontekst organizacyjny
11. PBI ZAL 05 Protokół przeglądu SZBI
12. PBI ZAL 06 Utrzymanie SZBI
13. PBI ZAL 07 Plan zmian SZBI
14. PBI ZAL 08 Program audytu
15. PBI ZAL 09 Potwierdzenie PBI
16. PBI ZAL 10 Harmonogram szkoleń
17. PBI ZAL 11 Kanały komunikacji
18. PBI ZAL 12 Procedura przesyłania informacji
19. PBI ZAL 13 Polityka kluczy
20. PBI ZAL 14 Polityka przechowywania danych

Procedury SZBI (41)

21. SZBI-AI-01 Instrukcja stosowania systemów AI
22. SZBI-BYOD-01 Polityka BYOD
23. SZBI-DPIA-01 Procedura DPIA
24. SZBI-EDR-01 Ochrona końcówek i monitoring
25. SZBI-EDR-02 Zapis regulamin i klauzule pracownicze
26. SZBI-INC-02 Procedura zarządzania incydentami
27. SZBI-KLS-01 Polityka klasyfikacji informacji
28. SZBI-ONB-01 Procedura onboarding offboarding
29. SZBI-PZ-02 Regulamin pracy zdalnej okazjonalnej
30. SZBI-PZ-02 Za1 Wniosek o pracę zdalną
31. SZBI-PZ-02 Za2 Odmowa wniosku
32. SZBI-PZ-02 Za3 Oświadczenie pracownika
33. SZBI-PZ-02 Za4 Wniosek zaprzestanie
34. SZBI-PZ-02 Za5 Wycofanie zgody
35. SZBI-PZ-02 Za6 Protokół odbiorczy
36. SZBI-PZ-02 Za7 Protokół zdawczy
37. SZBI-PZ-02 Za8 Informacja BHP
38. SZBI-PZ-02 Za9 Ocena ryzyka zawodowego
39. SZBI-RYZ-01 Analiza zagrożeń i ryzyka
40. SZBI-RYZ-02 Wnioski i plan postępowania z ryzykiem
41. SZBI-RYZ-03 Karta ryzyka SZBI

42. SZBI-RYZ-04 Metodyka ENISA szacowania ryzyka
43. SZBI-RYZ-05 Procedura Integracji Metodyk Ryzyka
44. SZBI-RYZ-05 ZaIA Most Zabezpieczeń ENISA
45. SZBI-RYZ-05 ZaIB Klauzula SARBI
46. SZBI-RYZ-05 ZaIC Klauzula ARDO
47. SZBI-SCH-02 Schemat postępowania niezgodności
48. SZBI-SLA-01 Zarządzanie jakością usług IT
49. SZBI-SLOWNIK-01 Słownik pojęć SZBI
50. SZBI-TI-01 Threat Intelligence
51. SZBI-ZAST-01 Procedura zastępstw ról
52. SZBI 1 7 NARDO Procedura naruszenia danych
53. SZBI AZ 01 Architektura zabezpieczeń
54. SZBI CM 01 Polityka zarządzania zmianami IT
55. SZBI IAM 01 Polityka zarządzania dostępem
56. SZBI INC 01 Szablony zgłoszenia CSIRT
57. SZBI KK 01 Plan komunikacji kryzysowej
58. SZBI LD 01 Polityka łańcucha dostaw
59. SZBI ND 01 Polityka nośników danych
60. SZBI PZ 01 Polityka pracy zdalnej
61. SZBI SZ 01 Program szkoleń i test wiedzy

Ochrona danych osobowych (RODO) (17)

62. RODO PDO 02 Umowa powierzenia
63. RODO PDO 06 Oświadczenie poufności
64. RODO PDO 07 DPIA
65. RODO PDO 08 Wykaz budynków i pomieszczeń
66. RODO PDO 10 Sprawozdanie doraźne
67. RODO PDO 11 Klauzule informacyjne RODO
68. RODO PDO 12 Sprawozdanie planowe
69. RODO PDO 14 Procedura RCP
70. RODO PDO 18 Umowa współadministrowanie
71. RODO PDO 19 Wykaz podstaw prawnych kraje trzecie
72. RODO PDO 1 0 Polityka Ochrony Danych Osobowych
73. RODO PDO 20a Prawa osób fizycznych
74. RODO PDO 20b Wzory odpowiedzi na żądania
75. RODO PDO 20c Wzory zawiadomień ADO
76. RODO PDO 21 Wniosek o udostępnienie danych
77. RODO PDO 22 Privacy by Design
78. RODO PDO PRZEWODNIK Rejestry RODO

Bezpieczeństwo IT (21)

79. IZSI 1 5 Instrukcja Zarządzania Systemami Informatycznymi
80. IZSI 1 6 URAW Procedura nadawania uprawnień
81. IZSI ZAL 01 Lista aktywów
82. IZSI ZAL 02 Lista jednostek podległych
83. IZSI ZAL 03 Lista administratorów
84. IZSI ZAL 04 Regulamin użytkownika SI
85. IZSI ZAL 05 Regulamin użytkownika komputerów przenośnych
86. IZSI ZAL 06 Regulamin użytkownik zdalnego dostępu
87. IZSI ZAL 09 Polityka uwierzytelniania administratorów
88. IZSI ZAL 10 Zarządzanie podatnościami
89. IZSI ZAL 11 Czyste biurko i ekran
90. IZSI ZAL 12 Protokół zdawczo odbiorczy
91. IZSI ZAL 13 Regulamin dostępu zewnętrznych
92. IZSI ZAL 14 Zasady haseł

- 93. IZSI ZAL 15 Zasady szyfrowania
- 94. IZSI ZAL 16 Poczta i Internet
- 95. IZSI ZAL 17 Chmura obliczeniowa
- 96. IZSI ZAL 18 Zestawienie systemów IT
- 97. IZSI ZAL 19 Polityka kopii zapasowych
- 98. IZSI ZAL 20 Wniosek o nadanie uprawnień IT
- 99. SZBI-WYT-01 Wytoczne klasyfikacji aktywów

Ciągłość działania (10)

- 100. BCP-1.4.1 Protokół testu całości działania
- 101. BCP-1.4.2 Procedura BCMS Active Directory
- 102. BCP-1.4.3 Procedura BCMS Aplikacja bazodanowa
- 103. BCP-1.4.4 Procedura BCMS Przełącznik sieciowy
- 104. BCP-1.4.5 Procedura BCMS Macierz dyskowa
- 105. BCP-1.4.6 Procedura BCMS Aktualizacje
- 106. BCP-1.4.7 Procedura BCMS Serwer
- 107. BCP-1.4.8 Plany awaryjne scenariusze krytyczne
- 108. BCP-1.4.9 Procedura BCMS EZD ePUAP
- 109. BCP-1.4 Plan całości działania

Reagowanie na zagrożenia (6)

- 110. PR-1.8.1 Plan reagowania vishing deepfake
- 111. PR-1.8.2 Plan reagowania phishing ASI
- 112. PR-1.8.3 Plan reagowania phishing użytkownik
- 113. PR-1.8.4 Plan reagowania ransomware ASI
- 114. PR-1.8.5 Plan reagowania smishing użytkownik
- 115. PR-1.8 Plany reagowania na cyberzagrożenia

Role i obowiązki (7)

- 116. SZBI-POMOC-ADO Lista zadań ADO
- 117. SZBI-POMOC-ASI Lista zadań ASI
- 118. SZBI-POMOC-DIP-01 Poradnik dostęp informacja publiczna
- 119. SZBI-POMOC-IOD Lista zadań IOD
- 120. SZBI-POMOC-KIER Lista zadań Kierownika
- 121. SZBI-POMOC-KSC Lista zadań Pełnomocnik KSC
- 122. SZBI-POMOC-PRAC Obowiązki Pracownika

Rejestry i zapisy (4)

- 123. IZSI ZAL 08 Rejestr uprawnień
- 124. SZBI-REJ-01 Rejestr naruszeń bezpieczeństwa
- 125. SZBI-REJ-02 Raport działań niezgodności
- 126. SZBI-RR-01 Rejestr ryzyka SZBI

Karty operacyjne (8)

- 127. Karta KB-01 Phishing A
- 128. Karta KB-01 Phishing B
- 129. Karta KB-02 Incydent A
- 130. Karta KB-02 Incydent B
- 131. Karta KB-03 Naruszenie RODO A
- 132. Karta KB-03 Naruszenie RODO B
- 133. Karta KB-04 Awaria A
- 134. Karta KB-04 Awaria B

Onboarding / Offboarding (3)

- 135. Oświadczenie zapoznania
- 136. Pakiet onboardingowy
- 137. Zestaw minimum pracownika

Wspólne IT i jednostki podległe (7)

- 138. WSP-01 Porozumienie o wspólnym systemie IT
- 139. WSP-02 Umowa powierzenia przetwarzania
- 140. WSP-03 Macierz RACI podział odpowiedzialności
- 141. WSP-04 Klauzula przejęcia zabezpieczeń IT
- 142. WSP-05 Procedura incydentów architektura wspólną
- 143. WSP-06 Zakres odpowiedzialności jednostki
- 144. WSP-07 Polityka bezpieczeństwa poczty

Podmioty zewnętrzne (4)

- 145. SZBI-POMOC-ZEW-01 Poradnik udostępnianie podmioty zewnętrzne
- 146. SZBI-ZEW-01 Protokół udostępnienia
- 147. SZBI-ZEW-02 Oświadczenie podmiotu
- 148. SZBI-ZEW-03 Rejestr udostępnień

Model operacyjny i audyt (2)

- 149. SZBI-GLPI-01 Instrukcja GLPI NIS2 SZBI
- 150. SZBI-OPS-01 Model operacyjny

Szablon dla jednostki podległej (7)

- 151. JEDN-INC-01 Procedura i rejestr incydentów
- 152. JEDN-INW-01 Inwentaryzacja stacji roboczych
- 153. JEDN-PBI-1.0 Polityka Bezpieczeństwa Informacji jednostki
- 154. JEDN-Przewodnik dla jednostki podległej
- 155. JEDN-RCP-01 Rejestr czynności przetwarzania
- 156. JEDN-RYZ-01 Analiza ryzyka jednostki
- 157. JEDN-SZK-01 Szkolenia pracowników jednostki

Harmonogram etapowego wdrożenia SZBI w okresie dostosowawczym

Etap	Zakres / działania	Dokumenty SZBI	Termin
1	Powołanie Zespołu ds. SZBI, przyjęcie Polityki Bezpieczeństwa Informacji, klasyfikacja informacji	PBI-1.0, SZBI-KLS-01	do podpisania zarządzenia
2	Weryfikacja danych w wykazie podmiotów kluczowych i podmiotów ważnych, wyznaczenie i zgłoszenie osób do kontaktu	—	do 3 października 2026 r.
3	Inwentaryzacja zasobów i systemów, przypisanie właścicieli aktywów	PBI-ZAL-01, IZSI-ZAL-18	do 31 grudnia 2026 r.
4	Analiza ryzyka i plan postępowania z ryzykiem	SZBI-RYZ-01, SZBI-RYZ-02, SZBI-RR-01	do 31 grudnia 2026 r.
5	Procedury dostępu i uprawnień, rejestr kont	IZSI-1.6-URAW, SZBI-IAM-01, IZSI-ZAL-08	do 28 lutego 2027 r.
6	Procedury kopii zapasowych i ciągłości działania	IZSI-ZAL-19, BCP-1.4	do 28 lutego 2027 r.
7	Procedury incydentów, reagowania i podatności	SZBI-INC-02, IZSI-ZAL-10	do 15 marca 2027 r.
8	Szkolenia pracowników, potwierdzenia zapoznania, szkolenie kierownika podmiotu	SZBI-SZ-01, PBI-ZAL-10, PBI-ZAL-09	do 31 marca 2027 r. (sukcesywnie)
9	Audyt wewnętrzny, protokół pełnego wdrożenia	PBI-ZAL-08	do 3 kwietnia 2027 r.