WERSJA 1.0 MAJ 2026

Pakiet wzorcowych dokumentów dot. Systemu Zarządzania Bezpieczeństwem Informacji

OPRACOWANIE:
Grupa robocza ds. Cyfryzacji i Cyberbezpieczeństwa
Śląskiego Związku Gmin i Powiatów

ŚLĄSKI ZWIĄZEK GMIN I POWIATÓW
35 lat

Spis treści

1. Instrukcja poruszania się po wzorcowych dokumentach Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) 13

2. Przewodnik wdrożeniowy Systemu Zarządzania Bezpieczeństwem Informacji 19

2.1 Cel dokumentu 19
2.2 Zakres stosowania 19
2.3 Architektura dokumentacji SZBI 20
2.4 Zasada nadrzędności Polityki 20
2.5 Role systemowe i ich mapowanie 21
2.6 Przykładowe mapowanie ról 21
2.7 Elementy konfigurowalne (parametry wdrożeniowe) 22
2.8 Kroki wdrożeniowe 22
2.9 Minimalne artefakty dowodowe 23
2.10 Typowe błędy wdrożeniowe 23
2.11 Wniosek końcowy 24

3. Polityka Bezpieczeństwa Informacji 26

3.1 Cel Polityki 26
3.2 Podstawa prawna 27
3.3 Opis Postępowania / kontekst organizacji 28
3.3.1 Zrozumienie organizacji i jej kontekstu 28
3.3.2 Określenie stron zainteresowanych 32
3.4 Określenie zakresu systemu zarządzania bezpieczeństwem informacji 35
3.5 Przywództwo i zaangażowanie 35
3.6 Polityka 36
3.7 Role, odpowiedzialność i uprawnienia 36
3.8 Planowanie – działania odnoszące się do ryzyk i szans 36
3.9 Cele bezpieczeństwa informacji i planowanie ich osiągnięcia 37

3.10 Wsparcie / zasoby 37
3.11 Kompetencje 37
3.12 Komunikacja 38
3.13 Udokumentowane informacje / opracowywanie i aktualizowanie 38
3.14 Nadzór nad udokumentowanymi informacjami 38
3.15 Działania operacyjne / planowanie i nadzór nad działaniami operacyjnymi 39
3.16 Szacowanie ryzyka w bezpieczeństwie informacji 39
3.17 Postępowanie z ryzykiem w bezpieczeństwie informacji 39
3.18 Ocena wyników / monitorowanie, pomiary, analiza i ocena 39
3.19 Audyt wewnętrzny 40
3.20 Przegląd zarządzania 40
3.21 Doskonalenie / niezgodności i działania korygujące 41
3.22 Ciągłe doskonalenie 41

4. Słownik pojęć używanych w ramach dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji 42

4.1 Cel 42
4.2 Opis postępowania – układ alfabetyczny 42
4.3 Uwagi 49
4.4 Metryka 49

5. Analiza ryzyka 50

5.1 Cel 50
5.2 Zakres stosowania 50
5.3 Odpowiedzialność za procedurę 50
5.4 Opis postępowania 51
5.4.1 Zasady ogólne metodyki analizy ryzyka 51
5.4.2 Identyfikacja ryzyka 51
5.4.3 Ocena skutków 52
5.4.4 Istotność zagrożenia 52
5.4.5 Ocena prawdopodobieństwa 52
5.4.6 Ocena poziomu ryzyka 52

5.4.7 Apetyt na ryzyko i akceptacja ryzyka 52
5.4.8 Postępowanie z ryzykiem 53
5.4.9 Właściciel ryzyka 53
5.4.10 Wskaźniki i mierniki ryzyka 53
5.5 Cykle szacowania ryzyka 54
5.6 Metryka 54
5.7 Uwagi 54
5.8 Załączniki 54

6. Bezpieczeństwo w cyklu życia systemów ICT 58

6.1 Cel 58
6.2 Zakres stosowania 58
6.3 Odpowiedzialności za procedurę 59
6.4 Opis postępowania 59
6.4.1 Etap planowania i inicjowania systemu 59
6.4.2 Etap projektowania i pozyskania 60
6.4.3 Etap wdrażania i uruchamiania 60
6.4.4 Etap eksploatacji i utrzymania 60
6.4.5 Etap zmian i rozwoju systemu 60
6.4.6 Etap wycofania i likwidacji systemu 61
6.5 Uwagi 61
6.6 Metryka 61

7. Bezpieczeństwo fizyczne i środowiskowe 62

7.1 Cel 62
7.2 Zakres stosowania 62
7.3 Odpowiedzialności za procedurę 63
7.4 Opis postępowania 63
7.4.1 Kontrola dostępu do obszarów 63
7.4.2 Wykazy obszarów 64
7.4.3 Separacja stref 64
7.4.4 Zasilanie 64

7.4.5 Warunki środowiskowe 65
7.4.6 Redundancja urządzeń wspomagających warunki środowiskowe 65
7.5 Uwagi 65
7.6 Metryka 65
7.7 Załączniki 66

8. Bezpieczeństwo zasobów ludzkich – edukacja i podnoszenie świadomości 67

8.1 Cel 67
8.2 Zakres stosowania 67
8.3 Odpowiedzialności za procedurę 68
8.4 Opis postępowania 68
8.4.1 Weryfikacja personelu 68
8.4.2 Zobowiązania do zachowania poufności 69
8.4.3 Umowy o zachowaniu poufności 69
8.4.4 Rozdział obowiązków 69
8.4.5 Szkolenia z zakresu bezpieczeństwa informacji 69
8.4.6 Założenia systemu szkoleń 70
8.4.7 Planowanie szkoleń 70
8.4.8 Realizacja szkoleń okresowych 70
8.4.9 Dowody realizacji szkoleń 71
8.4.10 Pomiar efektywności i kampanie świadomościowe 71
8.4.11 Zasady zakończenia współpracy i odejść 71
8.5 Uwagi 72
8.6 Metryka 72

9. Bezpieczeństwo łańcucha dostaw 73

9.1 Cel 73
9.2 Zakres stosowania 73
9.3 Odpowiedzialności za procedurę 73
9.4 Opis postępowania 74
9.4.1 Wstępna ocena dostawców i łańcucha dostaw 74
9.4.2 Ocena ryzyka związanych z dostawcami 74

9.4.3 Wymagania umowne i warunki świadczenia usług 75
9.4.4 Plany wyjścia i ciągłość współpracy 75
9.4.5 Okresowa ocena dostawców i podwykonawców 75
9.4.6 Nadzór nad poziomem świadczenia usług 76
9.5 Uwagi 76
9.6 Metryka 76
9.7 Załączniki 76

10. Procedura dot. ciągłości działania systemów technologii informacyjno-komunikacyjnych wykorzystywanych w JST 83

10.1 Cel 83
10.2 Zakres stosowania 83
10.3 Odpowiedzialności za procedurę 83
10.4 Opis postępowania 84
10.4.1 Zasady ogólne zapewnienia ciągłości działania 84
10.4.2 Analiza wpływu na działalność 84
10.4.3 Określenie parametrów odtworzeniowych 85
10.4.4 Minimalne konfiguracje i zasoby niezbędne do działania 85
10.4.5 Scenariusze awaryjne 85
10.4.6 Działania w sytuacji zakłócenia ciągłości działania 85
10.4.7 Odtwarzanie systemów i powrót do normalnego funkcjonowania 86
10.4.8 Testowanie planów ciągłości działania 86
10.5 Uwagi 86
10.6 Metryka 87
10.7 Załączniki 87
10.8 Uwagi 87

11. Monitorowanie ICT 89

11.1 Cel 89
11.2 Zakres stosowania 89
11.3 Odpowiedzialności za procedurę 89
11.4 Opis postępowania 90

11.4.1 Rejestrowanie zdarzeń w systemach technologii informacyjno-komunikacyjnych 90
11.4.2 Typy zdarzeń rejestrowanych dla usług 90
11.4.3 Wskaźniki progowe i wykrywanie nieprawidłowości 91
11.4.4 Centralne gromadzenie i analiza zdarzeń 91
11.4.5 Nadzór operacyjny nad bezpieczeństwem systemów 92
11.4.6 Przechowywanie i ochrona rejestrów zdarzeń 92
11.5 Uwagi 92
11.6 Metryka 92

12. Audyty wewnętrzne i zewnętrzne w JST 93

12.1 Cel 93
12.2 Zakres stosowania 93
12.3 Odpowiedzialności za procedurę 93
12.4 Opis postępowania 94
12.4.1 Program audytów 94
12.4.2 Audyty wewnętrzne 94
12.4.3 Audyty zewnętrzne 95
12.4.4 Testy penetracyjne i audyty techniczne 95
12.4.5 Ocena wyników audytów 95
12.4.6 Działania poaudytowe 95
12.4.7 Zlecanie audytów podmiotom zewnętrznym 96
12.4.8 Kompetencje i niezależność audytora 96
12.5 Uwagi 97
12.6 Metryka 97

13. Cyberhigiena systemów technologii informacyjno-komunikacyjnych wykorzystywanych w JST 98

13.1 Cel 98
13.2 Zakres stosowania 98
13.3 Odpowiedzialności za procedurę 98
13.4 Opis postępowania 99
13.4.1 Ogólne zasady cyberhigieny systemów 99

13.4.2 Bezpieczna konfiguracja systemów 99
13.4.3 Zarządzanie poprawkami 100
13.4.4 Utrzymanie spójności konfiguracji 100
13.4.5 Monitorowanie skuteczności cyberhigieny 100
13.5 Uwagi 100
13.6 Metryka 101

14. Zasady stosowania mechanizmów kryptograficznych oraz zarządzania kluczami kryptograficznymi w JST 102

14.1 Cel 102
14.2 Zakres stosowania 102
14.3 Odpowiedzialności za procedurę 103
14.4 Opis postępowania 103
14.4.1 Ogólne zasady stosowania kryptografii 103
14.4.2 Szyfrowanie danych przechowywanych 104
14.4.3 Szyfrowanie danych przesyłanych 104
14.4.4 Zabezpieczenia przy przesyłaniu danych w usługach internetowych 104
14.4.5 Zabezpieczenia w komunikacji za pomocą poczty elektronicznej 104
14.4.6 Zarządzanie kluczami kryptograficznymi 105
14.4.7 Nadzór i doskonalenie stosowania kryptografii 105
14.5 Uwagi 105
14.6 Metryka 106
14.7 Załączniki 106

15. Bezpieczna komunikacja MFA 107

15.1 Cel 107
15.2 Zakres stosowania 107
15.3 Odpowiedzialności za procedurę 107
15.4 Opis postępowania 108
15.4.1 Zasady komunikacji w autoryzowanych kanałach 108
15.4.2 Ochrona poufności i integralności komunikacji 108
15.4.3 Uwierzytelnianie użytkowników i kontrola dostępu 108

15.4.4 Bezpieczna komunikacja z wykorzystaniem sieci publicznej 109
15.4. Bezpieczna komunikacja w systemach dostępnych przez sieć publiczną 109
15.4.6 Nadzór nad komunikacją i doskonalenie zabezpieczeń 109
15.5 Uwagi 110
15.6 Metryka 110

16. Aktywa w JST 111

16.1 Cel 111
16.2 Zakres stosowania 111
16.3 Odpowiedzialności za procedurę 111
16.4 Opis postępowania 112
16.4.1 Identyfikacja i inwentaryzacja aktywów 112
16.4.2 Inwentaryzacja sprzętu i aktywów majątkowych 112
16.4.3 Inwentaryzacja oprogramowania 112
16.4.4 Inwentaryzacja danych i informacji 113
16.4.5 Klasyfikacja danych i informacji 113
16.4.6 Oznaczanie danych i informacji 113
16.4.7 Postępowanie z aktywami i danymi 113
16.5 Metryka 114
16.6 Uwagi 114
16.7 Załączniki 114

17. Kontrola dostępu 117

17.1 Cel 117
17.2 Zakres stosowania 117
17.3 Odpowiedzialności za procedurę 117
17.4 Opis postępowania 118
17.4.1 Zarządzanie tożsamościami użytkowników 118
17.4.2 Nadawanie dostępów 118
17.4.3 Modyfikacja i przegląd dostępów 119
17.4.4 Cofanie dostępów 119
17.4.5 Uwierzytelnianie użytkowników 119

17.4.6 Kontrola i rozliczalność dostępu 119
17.4.7 Dostępy uprzywilejowane 120
17.4.8 Zasady tworzenia i stosowania haseł użytkowników 120
17.4.9 Zasady tworzenia i stosowania haseł administracyjnych 121
17.4.10 Uwierzytelnianie wieloskładnikowe 121
17.4.11 Polityka haseł dla systemów dostępnych w sieci Internet 122
17.5 Uwagi 122
17.6 Metryka 122
17.7 Załączniki 122

18. Podatność JST na zagrożenia 125

18.1 Cel 125
18.2 Zakres stosowania 125
18.3 Odpowiedzialności za procedurę 125
18.4 Opis postępowania 126
18.4.1 Identyfikacja i ujawnianie podatności 126
18.4.2 Analiza i ocena podatności 126
18.4.3 Postępowanie z podatnościami 127
18.4.4 Usuwanie podatności 127
18.4.5 Monitorowanie zagrożeń 127
18.4.6 Doskonalenie zarządzania podatnościami i zagrożeniami 128
18.5 Metryka 128

19. Incydenty w JST 129

19.1 Cel 129
19.2 Zakres stosowania 129
19.3 Odpowiedzialności za procedurę 129
19.4 Opis postępowania 130
19.4.1 Zasady ogólne zarządzania incydentami 130
19.4.2 Zgłaszanie zdarzeń i incydentów 130
19.4.3 Rejestracja i wstępna ocena zdarzenia 131
19.4.4 Kwalifikacja zdarzenia i decyzja o dalszym postępowaniu 131

19.4.5 Obsługa incydentu i ograniczanie skutków 132
19.4.6 Zabezpieczenie i archiwizacja materiału dowodowego 132
19.4.7 Eskalacja do organów zewnętrznych 132
19.4.8 Usunięcie przyczyn incydentu i przywrócenie działania 133
19.4.9 Analiza i wyciąganie wniosków 133
19.4.10 Archiwizacja materiału dowodowego 133
19.5 Metryka 133
19.6 Uwagi 133
19.7 Załączniki 134

20. Kopie zapasowe 135

20.1 Cel 135
20.2 Zakres stosowania 135
20.3 Odpowiedzialności za procedurę 135
20.4 Opis postępowania 136
20.4.1 Zasady ogólne wykonywania kopii zapasowych 136
20.4.2 Harmonogram i częstotliwość wykonywania kopii zapasowych 136
20.4.3 Oznaczanie kopii zapasowych 137
20.4.4 Przechowywanie i kolokacja kopii zapasowych 137
20.4.5 Kopie zapasowe przechowywane w trybie odłączonym 137
20.4.6 Testowanie kopii zapasowych 138
20.4.7 Postępowanie w przypadku odtwarzania danych 138
20.5 Załączniki 138
20.6 Uwagi 138
20.7 Metryka 138

ŚLĄSKI ZWIĄZEK GMIN I POWIATÓW

WERSJA 1.0 MAJ 2026

INSTRUKCJA PORUSZANIA SIĘ PO WZORCOWYCH DOKUMENTACH DOT. SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI (SZBI)

OPRACOWANIE:
Grupa robocza ds. Cyfryzacji i Cyberbezpieczeństwa
Śląskiego Związku Gmin i Powiatów

1. Instrukcja poruszania się po wzorcowych dokumentach Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)

Instrukcja poruszania się po wzorcowych dokumentach Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) stanowi zbiór uporządkowanych wytycznych i rekomendacji, dotyczących korzystania z dokumentacji związanej z bezpieczeństwem informacji w organizacji, jaka została wypracowana przez Grupę roboczą ds. Cyfryzacji i Cyberbezpieczeństwa, działającą przy Śląskim Związku Gmin i Powiatów.

Grupa robocza ds. Cyfryzacji i Cyberbezpieczeństwa powstała pod koniec 2024 r. W jej skład weszli przedstawiciele zarówno mniejszych gmin, jak i dużych miast na prawach powiatu oraz powiatów:

1) **p. Piotr Absalon (UM Radlin) – Przewodniczący Grupy, redaktor opracowania,**
2) p. Beata Wanic (UM Zabrze) – Zastępca Przewodniczącego,
3) p. Dariusz Łużny (UM Bielsko-Biała),
4) p. Stanisław Kawecki (UM Cieszyn),
5) p. Magdalena Mickielewicz (UM Gliwice),
6) p. Zbigniew Gamza (UM Marklowice),
7) p. Joanna Szymańska (UM Mszana),
8) p. Dagmara Dzida (UG Pilchowice),
9) p. Arkadiusz Świrski (UG Pilchowice),
10) p. Leszek Żogała (SP Gliwice),
11) p. Michał Lorek (SP Wodzisław Śląski),
12) p. Piotr Gawron (UG Psary),
13) p. Liliana Moskała-Zydra (UM Ruda Śląska),
14) p. Przemysław Szulc (UM Rybnik),
15) p. Ewelina Włoch (UM Rybnik),
16) p. Adam Fisior (UM Siemianowice Śląskie),
17) p. Aleksandra Gajda (UM Tarnowskie Góry),

18) p. Sławomir Niesłony (UM Tarnowskie Góry),

19) p. Paweł Walczak (UM Tychy),

20) p. Sebastian Wika (UM Tychy),

21) **p. Tomasz Banasik – ekspert zewnętrzny ds. bezpieczeństwa informacji, redaktor opracowania.**

Celem prac Grupy było wypracowanie spójnej, możliwie kompletnej oraz zgodnej z przepisami znowelizowanej ustawy o krajowym systemie cyberbezpieczeństwa dokumentacji będącej istotnym elementem SZBI. Dokumentacja ta ma charakter uniwersalny i może być – po odpowiednim dostosowaniu – używana, jako punkt odniesienia przy projektowaniu i wdrażaniu SZBI, niezależnie od wielkości czy specyfiki jednostki samorządu terytorialnego.

Niniejsza instrukcja definiuje strukturę dokumentacji oraz wskazuje kluczowe elementy poszczególnych procedur. Należy mieć świadomość, że prezentowana dokumentacja jest istotnym elementem w budowie SZBI, nie stanowi jednak SZBI rozumianego jako zbiór procesów, zasad, narzędzi i struktur organizacyjnych, których celem jest zapewnienie bezpieczeństwa informacji w sposób systematyczny i mierzalny.

Aby system funkcjonował konieczne jest:

a) **zaangażowanie kierownictwa** – Wójt / Burmistrz / Prezydent miasta / Starosta musi zatwierdzić kierunkową strategię działania, zapewnić niezbędne przydzielone zasoby i formalnie zaakceptować poziom ryzyka, który jednostka jest w stanie ponieść. Kierownik jednostki powinien w drodze zarządzenia wprowadzić system w podległym urzędzie;

b) **stworzenie polityki bezpieczeństwa informacji** – przygotowana przez Grupę dokumentacja dostosowana do lokalnych uwarunkowań i uzupełniona o niezbędne rejestry i instrukcje spełnia to zadanie;

c) **przeprowadzenie analizy ryzyka i identyfikacji zagrożeń** – w przekazywanej dokumentacji dostępna jest procedura oraz wstępnie wypełnione narzędzie do analizy ryzyka w urzędzie;

d) **opracowanie i wdrożenie zabezpieczeń** – na podstawie analizy ryzyka dobierane są odpowiednie środki techniczne i organizacyjne. W ten sposób planowana jest prewencja oraz działania zaradcze, takie jak opracowanie planów odzyskiwania po awarii i planów ciągłości działania, mających na celu minimalizację potencjalnego wpływu incydentów na

funkcjonowanie jednostki. W dokumentacji uwzględnione zostały ogólne procedury dotyczące utrzymania ciągłości działania i reakcji na incydenty;

e) **szkolenie pracowników** – niezbędne jest prowadzenie szkoleń, które zwiększają wzrost świadomości pracowników w zakresie rozpoznawania zagrożeń, bezpiecznego korzystania z systemów informatycznych i dokumentów w elektronicznej postaci. Dokumentacja zawiera procedurę dotyczącą zasobów ludzkich i edukacji personelu;

f) **prowadzenie audytów i przeglądów systemu** – regularne przeglądy, testy oraz audyty wewnętrzne pomagają utrzymać wysoką jakość systemu, wykrywać niezgodności i wdrażać działania korygujące. Dokumentacja zawiera procedurę opisującą audyty wewnętrzne i zewnętrzne.

W ramach przekazanego przez Śląski Związek Gmin i Powiatów pakietu wzorcowych dokumentów dot. Systemu Zarządzania Bezpieczeństwem Informacji znajdą Państwo:

1) **Przewodnik Wdrożeniowy SZBI** – jest to dokument, który opisuje strukturę dokumentacji i proponowany przebieg wdrożenia SZBI,
2) **Słownik pojęć używanych w ramach dokumentacji SZBI dla JST** – dokument, który porządkuje słownictwo stosowane w cyberbezpieczeństwie,
3) **Analizę ryzyka wraz z załącznikiem w postaci arkusza służącego do szacowania ryzyka** – zestaw dokumentów pozwalający na przeprowadzenie analizy ryzyka w jednostce. Grupa przyjęła, że ryzyko będzie analizowane dla poszczególnych usług ICT świadczonych przez urzędy, za pomocą produktów ICT.
4) **Procedury:**
    a) bezpieczeństwo w cyklu życia systemów ICT,
    b) bezpieczeństwo fizyczne i środowiskowe,
    c) bezpieczeństwo zasobów ludzkich, edukacja i podnoszenia świadomości,
    d) bezpieczeństwo łańcucha dostaw,
    e) ciągłość działania systemów technologii informacyjno-komunikacyjnych wykorzystywanych w JST,
    f) monitorowanie technologii informacyjno-komunikacyjnych,
    g) prowadzenie audytu wewnętrznego i zewnętrznego w JST,

h) cyberhigiena systemów technologii informacyjno-komunikacyjnych wykorzystywanych w JST,
i) zasady stosowania mechanizmów kryptograficznych oraz zarządzania kluczami kryptograficznymi w JST,
j) bezpieczna komunikacja MFA,
k) aktywa w JST,
l) kontrola dostępu,
m) podatność JST na zagrożenia,
n) incydenty w JST,
o) kopie zapasowe.

5) **Dokumenty dołączone do dokumentacji:**
   a) arkusz określający częstotliwości prowadzenia działań w ramach SZBI oraz zestawienie procedur wraz z podstawami prawnymi – działania w ramach ISO-NIS2-UOKSC (zakres procedur),
   b) załącznik nr 2 *Arkusz szacowania ryzyka ICT*.

Powyższe dokumenty należy nieznacznie zmodyfikować dostosowując je do specyfiki swojego urzędu. Procedury zawierają informacje o dokumentach niższego rzędu (instrukcjach, rejestrach), które można / należy wdrożyć w poszczególnych obszarach. W niektórych jednostkach, ze względu na ich specyfikę może być konieczne wdrożenie także innych, dodatkowych procedur, jak również uwzględnienie podczas analizy ryzyka dodatkowych usług lub produktów ICT, które nie zostały zidentyfikowane przez Grupę. Przykładem takiego produktu ICT jest sztuczna inteligencja, której wykorzystanie w świadczonych usługach niewątpliwie stanowi zagrożenie, które należy uwzględnić podczas analizy ryzyka. Jest możliwa także sytuacja odwrotna polegająca na tym, że jednostka nie świadczy niektórych z usług ICT lub świadczy je nie wykorzystując produktów ICT uwzględnionych w analizie ryzyka. W takim przypadku można odpowiednio te usługi lub produkty usunąć z analizy.

Przedstawiony pakiet dokumentów stanowi uporządkowaną podstawę do budowy i rozwijania dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji w organizacji. Jego zastosowanie sprzyja nie tylko ujednoliceniu formy i zakresu dokumentów, ale również

zwiększa skuteczność zarządzania bezpieczeństwem poprzez jasne określenie zasad, odpowiedzialności i procesów.

Należy podkreślić, że dokumentacja SZBI nie jest elementem statycznym – powinna podlegać regularnym przeglądom i aktualizacjom, wynikającym zarówno ze zmian organizacyjnych, technologicznych, jak i ewolucji zagrożeń czy wymagań prawnych. Utrzymanie jej aktualności oraz adekwatności do rzeczywistych potrzeb organizacji jest kluczowe dla zapewnienia skuteczności całego systemu.

Dokumentacja powinna być rozwijana i dostosowywana do specyfiki danej jednostki, stanowiąc narzędzie wspierające zarówno wdrożenie SZBI, jak i jego dalsze doskonalenie. W praktyce jej wartość przejawia się w możliwości konsekwentnego stosowania przyjętych standardów oraz w ułatwieniu komunikacji pomiędzy interesariuszami zaangażowanymi w obszar bezpieczeństwa informacji.

Ostatecznie, dobrze zaprojektowana i zarządzana dokumentacja stanowi istotny filar budowania kultury bezpieczeństwa informacji, wspierając organizację w osiąganiu jej celów oraz minimalizowaniu ryzyka operacyjnego, czego Zespół Redakcyjny niniejszej instrukcji życzy wszystkim samorządom członkowskim Śląskiego Związku Gmin i Powiatów.

Redakcja materiałów:

Biuro Śląskiego Związku Gmin i Powiatów:

Przemysław Antkowiak, Patrycja Brol, Katarzyna Kamieniobrodzka-Bartosik

ŚLĄSKI ZWIĄZEK GMIN I POWIATÓW

35 lat

Przewodnik wdrożeniowy / implementacyjny Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)

OPRACOWANIE:

Grupa robocza ds. Cyfryzacji i Cyberbezpieczeństwa Śląskiego Związku Gmin i Powiatów

Wersja 1.0 Maj 2026

2. Przewodnik wdrożeniowy Systemu Zarządzania Bezpieczeństwem Informacji

2.1 Cel dokumentu

Celem niniejszego Przewodnika wdrożeniowego jest umożliwienie **jednolitego, uporządkowanego i bezpiecznego wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)** w różnych typach organizacji, w oparciu o zestaw dokumentów referencyjnych (Polityka Bezpieczeństwa Informacji oraz procedury wykonawcze).

Dokument pełni rolę **instrukcji implementacyjnej**, wyjaśniającej:

a) jak dostosować dokumentację SZBI do konkretnej organizacji,
b) które elementy są obowiązkowe, a które konfigurowalne,
c) jakie kroki należy wykonać, aby system funkcjonował jako spójne rozwiązanie organizacyjne.

Przewodnik nie zastępuje Polityki Bezpieczeństwa Informacji ani procedur – **stanowi dokument pomocniczy**, wspierający ich prawidłowe wdrożenie.

2.2 Zakres stosowania

Przewodnik może być stosowany w szczególności przez:

a) jednostki samorządu terytorialnego,
b) jednostki organizacyjne sektora finansów publicznych,
c) spółki komunalne i spółki prawa handlowego,
d) instytucje kultury, placówki oświatowe,
e) inne podmioty publiczne przetwarzające informacje i dane osobowe.

Na potrzeby dokumentacji wdrożeniowej używa się pojęcia **„Organizacja”** jako określenia podmiotu wdrażającego SZBI.

2.3 Architektura dokumentacji SZBI

System Zarządzania Bezpieczeństwem Informacji opiera się na hierarchicznej strukturze dokumentów:

Poziom 1 – dokument nadrzędny – Polityka Bezpieczeństwa Informacji,

Poziom 2 – dokumenty wykonawcze – procedury SZBI (np. incydenty, kopie zapasowe, kontrola dostępu, ciągłość działania, audyty itp.),

Poziom 3 – instrukcje, rejestry i formularze, np.:

a) rejestr incydentów,
b) rejestr ryzyka,
c) rejestr kopii zapasowych,
d) ewidencje dostępów, audytów, szkoleń,
e) instrukcja wykonywania kopii zapasowych.

Poziom 4 – zapisy:

a) raporty,
b) protokoły,
c) wyniki testów,
d) potwierdzenia wykonania działań.

Każdy niższy poziom dokumentacji **wynika z poziomu wyższego** i nie może pozostawać z nim w sprzeczności.

2.4 Zasada nadrzędności Polityki

Polityka Bezpieczeństwa Informacji stanowi formalną podstawę obowiązywania całego SZBI.

Procedury, instrukcje, rejestry i formularze:

a) są dokumentami wykonawczymi do Polityki,
b) obowiązują na podstawie jej zatwierdzenia,
c) nie wymagają odrębnego powielania podstaw prawnych.

2.5 Role systemowe i ich mapowanie

W dokumentach SZBI role są definiowane funkcyjnie, a nie personalnie. Każda Organizacja przypisuje je do własnej struktury.

2.6 Przykładowe mapowanie ról

Rola systemowa	Przykłady w organizacjach
Kierownik organizacji	Prezydent / Wójt / Zarząd / Dyrektor
Osoba odpowiedzialna	Pełnomocnik SZBI / CISO
Komórka IT	Dział IT / Administrator systemów / Outsourcing
Właściciel aktywa	Kierownik jednostki / właściciel procesu
IOD	Inspektor Ochrony Danych

Organizacja powinna:

a) formalnie wskazać role,
b) określić ich odpowiedzialności,
c) udokumentować przypisania (zarządzenie, zakres czynności).

2.7 Elementy konfigurowalne (parametry wdrożeniowe)

Część zapisów SZBI ma charakter parametryczny i wymaga dostosowania.

Typowe parametry do ustalenia:

a) częstotliwość audytów,
b) częstotliwość testów kopii zapasowych i ciągłości działania,
c) czasy reakcji na incydenty,
d) okresy przechowywania logów,
e) poziomy klasyfikacji informacji,
f) zakres monitorowania.

Rekomenduje się utworzenie jednej tabeli parametrów SZBI, zatwierdzanej przez kierownictwo, która może bazować na dokumencie “Działania w ramach ISO-NIS2-UOKSC” (plik składowy do opracowanej dokumentacji SZBI).

2.8 Kroki wdrożeniowe

Etap 1 – przygotowanie:

a) zapoznanie kierownictwa z Polityką,
b) decyzja o wdrożeniu SZBI,
c) wyznaczenie ról systemowych.

Etap 2 – dostosowanie dokumentacji:

a) uzupełnienie nazwy, adresów, stanowiska,
b) dopasowanie terminologii do Organizacji,
c) ustalenie parametrów konfiguracyjnych.

Etap 3 – zatwierdzenie:

a) wydanie zarządzenia zatwierdzającego Politykę i procedury,

b) zapewnienie dostępności dokumentów dla pracowników.

Etap 4 – uruchomienie operacyjne:

a) uruchomienie rejestrów,

b) rozpoczęcie monitorowania,

c) szkolenia pracowników.

Etap 5 – nadzór i doskonalenie:

a) przeprowadzenie pierwszego audytu,

b) przegląd zarządzania,

c) aktualizacja dokumentacji.

2.9 Minimalne artefakty dowodowe

Funkcjonalnie SZBI jako system wymaga od Organizacji wygenerowania co najmniej:

a) rejestru ryzyka w oparciu o ***arkusz szacowania ryzyka ICT (Excel – plik zewnętrzny)*** – **załącznik do procedury Analizy Ryzyka ICT**,

b) rejestru usług ICT i produktów ICT w oparciu o ***arkusz szacowania ryzyka ICT (Excel – plik zewnętrzny)*** **– załącznik do procedury Analizy Ryzyka ICT**,

c) rejestru incydentów,

d) raportu z audytów,

e) raportu z przeglądu zarządzania,

f) ewidencji szkoleń,

g) rejestru kopii zapasowych.

Brak zapisów oznacza brak działania systemu – nawet przy dobrej dokumentacji.

2.10 Typowe błędy wdrożeniowe

Przykłady najczęściej występujących błędów

a) traktowanie SZBI wyłącznie jako „zestawu dokumentów”,
b) brak realnego przypisania ról,
c) brak zapisów i rejestrów,
d) brak zaangażowania kierownictwa,
e) kopiowanie dokumentów bez dostosowania.

2.11 Wniosek końcowy

Dokumentacja SZBI, do której odnosi się niniejszy Przewodnik, **może być skutecznie wdrażana w różnych organizacjach**, pod warunkiem:

a) zachowania nadrzędności Polityki,
b) formalnego przypisania ról,
c) uzupełnienia parametrów konfiguracyjnych,
d) zapewnienia nadzoru i zapisów.

Przewodnik ten stanowi narzędzie umożliwiające **powtarzalne, bezpieczne i audytowane wdrożenie SZBI jako rozwiązania systemowego**.

ŚLĄSKI ZWIĄZEK GMIN I POWIATÓW

35 lat

WERSJA 1.0 MAJ 2026

Polityka Bezpieczeństwa Informacji

OPRACOWANIE:

Grupa robocza ds. Cyfryzacji i Cyberbezpieczeństwa Śląskiego Związku Gmin i Powiatów

3. Polityka Bezpieczeństwa Informacji

3.1 Cel Polityki

1) Celem niniejszej Polityki jest określenie zasad oraz procesów mających na celu funkcjonowanie systemu zarządzania bezpieczeństwem informacji w tym zapewnienie ochrony przetwarzanych informacji i danych osobowych w kontekście realizacji zadań administracji publicznej oraz świadczenia usług dla mieszkańców.
2) Wszystkie terminy i definicje dla wszystkich dokumentów systemu ujęte są w Słowniku SZBI.
3) Niniejsza Polityka Bezpieczeństwa Informacji została ustanowiona i wdrożona w JST *[nazwa jednostki – do uzupełnienia przez JST]* jako kluczowy element Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).
4) Polityka wspiera cele działalności JST polegające na zapewnieniu wysokiej jakości usług publicznych, z uwzględnieniem bezpieczeństwa informacji w procesach zarządzania i obsługi mieszkańców oraz partnerów Urzędu.
5) System Zarządzania Bezpieczeństwem Informacji w JST obejmuje:
    a) ochronę poufności, integralności i dostępności danych w procesach administracyjnych, usługach cyfrowych i komunikacji zewnętrznej,
    b) zapewnienie ciągłości działania w razie wystąpienia incydentu mającego wpływ na dostępność świadczonych usług na zasadach przyjętych w ramach oceny ryzyka,
    c) identyfikację i zarządzanie aktywami informacyjnymi, w tym systemami informatycznymi, dokumentacją papierową i elektroniczną oraz infrastrukturą wspierającą,
    d) spełnianie wymagań prawnych i regulacyjnych dotyczących ochrony danych osobowych, cyberbezpieczeństwa i informacji publicznych.
6) Cele SZBI obejmują:
    a) minimalizowanie ryzyka naruszenia bezpieczeństwa danych,
    b) zapewnienie ciągłości pracy i świadczenia usług na akceptowalnym poziomie,

c) zapewnienie mieszkańcom i innym stronom zainteresowanym zaufania do procesów przetwarzania informacji.

3.2 Podstawa prawna

1) Niniejsza Polityka Bezpieczeństwa Informacji jest podstawowym dokumentem opisującym System Zarządzania Bezpieczeństwem Informacji wdrożony w Jednostce Samorządu Terytorialnego (dalej JST). Dokument ten definiuje ramy dla zarządzania bezpieczeństwem informacji zgodnie z obowiązującą normą PN-ISO/IEC 27001, przepisami prawnymi, w szczególności:
   a) ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa,
   b) ustawą z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne,
   c) rozporządzeniem 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.
2) Polityka Bezpieczeństwa Informacji uwzględnia również wymagania:
   a) dyrektywy Parlamentu Europejskiego i Rady z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dalej jako dyrektywa NIS 2),
   b) rozporządzenie Parlamentu Europejskiego i Rady 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 tzw. RODO).

3.3 Zakres Stosowania

Niniejsza Polityka ma zastosowanie w Jednostce Samorządu Terytorialnego (JST) *[nazwa i adres – do uzupełnienia przez JST]* i obowiązuje wszystkie systemy informatyczne, ICT,

pracowników oraz osoby dopuszczone do przetwarzania danych niezależnie od ich kategorii oraz rodzaju.

Odpowiedzialność za Politykę

a) Kierownik JST ponosi odpowiedzialność za zapewnienie funkcjonowania systemu zarządzania bezpieczeństwem informacji, w tym za zatwierdzenie, wdrożenie oraz egzekwowanie niniejszej polityki.
b) Osoba odpowiedzialna za bezpieczeństwo informacji, odpowiada za nadzór nad stosowaniem Polityki, jej spójność z innymi regulacjami wewnętrznymi oraz monitorowanie skuteczności stosowanych środków bezpieczeństwa.
c) Kierownik komórki odpowiedzialnej za obsługę informatyczną odpowiada za techniczną realizację wymagań bezpieczeństwa na wszystkich etapach cyklu życia systemów technologii informacyjno-komunikacyjnych.
d) Kierownicy komórek organizacyjnych odpowiadają za stosowanie polityki w odniesieniu do systemów wykorzystywanych w podległych im obszarach działalności oraz w odniesieniu do pracowników.
e) Pracownicy JST są zobowiązani do przestrzegania zasad określonych w SZBI w zakresie wynikającym z powierzonych im obowiązków.

Opis Postępowania / kontekst organizacji

3.3.1 Zrozumienie organizacji i jej kontekstu

JST uwzględnia czynniki wewnętrzne i zewnętrzne mające wpływ na realizację swoich działań i funkcjonowanie SZBI.

CZYNNIKI ZEWNĘTRZNE

Rodzaj czynnika	Charakterystyka czynnika	Sposób monitorowania	Odpowiedzialność za monitorowanie
Sytuacja polityczna			
Polityka krajowa	- zmiany w polityce rządu - stabilność polityczna w kraju	- bieżące śledzenie sytuacji politycznej - analiza zmian legislacyjnych	*[uzupełnienie stanowiska przez JST]*
Polityka samorządowa	- decyzje władz wojewódzkich - współpraca z innymi jednostkami samorządu	- monitorowanie decyzji władz samorządowych	*[uzupełnienie stanowiska przez JST]*
Przepisy prawne			
Ustawy i rozporządzenia	- zmiany w przepisach prawa	- regularne przeglądy prawne - współpraca z radcą prawnym	*[uzupełnienie stanowiska przez JST]*
Sytuacja gospodarcza i otoczenie ekonomiczne			
Budżet	- stan finansów - wpływy z podatków i opłat	- analiza budżetu - monitorowanie wpływów i wydatków	*[uzupełnienie stanowiska przez JST]*
Dotacje i subwencje	- środki z budżetu państwa - fundusze unijne	- monitorowanie dostępnych programów finansowania	*[uzupełnienie stanowiska przez JST]*
Otoczenie technologiczne			
Nowe technologie	- rozwój IT - cyfryzacja usług publicznych	- śledzenie trendów technologicznych - udział w szkoleniach	*[uzupełnienie stanowiska przez JST]*
Cyberzagrożenia	- ataki hakerskie - wirusy i malware - socjotechniki	- systemy monitoringu bezpieczeństwa IT - audyty bezpieczeństwa	*[uzupełnienie stanowiska przez JST]*
Otoczenie społeczne			
Społeczność lokalna	- oczekiwania mieszkańców - aktywność obywatelska	- liczba wniosków i skarg - konsultacje społeczne	*[uzupełnienie stanowiska przez JST]*

Otoczenie instytucji kontrolnych			
Kontrole zewnętrzne	- m.in. NIK, RIO, UODO - audyty zewnętrzne	- przygotowanie do kontroli - analiza raportów pokontrolnych	*[uzupełnienie stanowiska przez JST]*
Audyty wewnętrzne	- wymagania ISO 27001 - inne normy i standardy - przepisy prawne	- audyty wewnętrzne i zewnętrzne - przeglądy SZBI	*[uzupełnienie stanowiska przez JST]*
Otoczenie rynkowe			
Dostawcy i partnerzy	- firmy świadczące usługi dla JST - partnerstwa publiczno-prywatne	- ocena i wybór dostawców - monitorowanie realizacji umów	*[uzupełnienie stanowiska przez JST]*

CZYNNIKI WEWNĘTRZNE

Rodzaj czynnika	Charakterystyka czynnika	Sposób monitorowania	Odpowiedzialność za monitorowanie
Zasoby ludzkie			
Pracownicy JST i polityka personalna	- kompetencje i doświadczenie - rotacja kadry - rekrutacja - motywowanie pracowników	- okresowe oceny pracy pracowników - planowanie szkoleń - monitorowanie stanu zatrudnienia	*[uzupełnienie stanowiska przez JST]*
Wiedza			
Procedury i instrukcje	- dokumentacja wewnętrzna - wiedza organizacji	- aktualizacja dokumentacji - zarządzanie wiedzą	*[uzupełnienie stanowiska przez JST]*
Doświadczenie	- realizacja zadań publicznych - historie projektów	- analiza zakończonych projektów - wyciąganie wniosków	*[uzupełnienie stanowiska przez JST]*
Kultura organizacji			
Wartości i etyka pracy	- zaangażowanie pracowników - postawy proaktywne	- szkolenia - oceny pracownicze	*[uzupełnienie stanowiska przez JST]*

		- działalność Komisji ds. Etyki - samokontrola	
Świadomość bezpieczeństwa	- znajomość procedur - zachowania w sytuacjach zagrożenia	- szkolenia z zakresu bezpieczeństwa - testy i ćwiczenia - samokontrola	*[uzupełnienie stanowiska przez JST]*
Struktura organizacyjna i podział zadań			
Schemat organizacyjny	- podległości służbowe - zakresy obowiązków	- regularne przeglądy struktury - aktualizacja zakresów obowiązków	*[uzupełnienie stanowiska przez JST]*
Procedury decyzyjne	- sposób podejmowania decyzji - uprawnienia i odpowiedzialność	- audyty wewnętrzne - analiza procesów	*[uzupełnienie stanowiska przez JST]*
Infrastruktura i systemy informatyczne			
Sprzęt i oprogramowanie	- komputery, serwery - systemy operacyjne i aplikacje	- inwentaryzacja sprzętu - aktualizacje systemów	*[uzupełnienie stanowiska przez JST]*
Sieci i komunikacja	- sieci LAN/WAN - urządzenia sieciowe	- monitorowanie sieci - testy penetracyjne	*[uzupełnienie stanowiska przez JST]*
Finanse			
Budżet JST	- plan finansowy - wydatki	- planowanie budżetu - monitorowanie wydatków	*[uzupełnienie stanowiska przez JST]*
Zarządzanie kosztami	- optymalizacja wydatków - efektywne wykorzystanie zasobów	- analiza kosztów - audyty finansowe	*[uzupełnienie stanowiska przez JST]*
Dokumentacja			
Polityki i procedury dotyczące bezpieczeństwa informacji	- polityka bezpieczeństwa - instrukcje wewnętrzne	- przeglądy dokumentacji - audyty wewnętrzne	*[uzupełnienie stanowiska przez JST]*

Zarządzanie dokumentacją	- archiwizacja - dostęp do dokumentów	- system zarządzania dokumentami - kontrola dostępu	*[uzupełnienie stanowiska przez JST]*
Strategie i cele			
Plan strategiczny	- misja i wizja JST - cele długoterminowe	- przeglądy strategiczne - monitorowanie realizacji celów	*[uzupełnienie stanowiska przez JST]*
Cele operacyjne	- zadania roczne - projekty i inicjatywy	- raportowanie okresowe - spotkania zespołów	*[uzupełnienie stanowiska przez JST]*
Metody pracy			
Praca zdalna	- elastyczne godziny pracy - praca poza obszarem bezpiecznym	- monitorowanie dostępu zdalnego - szkolenia z bezpieczeństwa	*[uzupełnienie stanowiska przez JST]*
Dostawcy i podwykonawcy			
Usługi zewnętrzne	- usługi remontowe i serwisowe - zewnętrzna obsługa prawna	- ocena i wybór dostawców - monitorowanie realizacji umów	*[uzupełnienie stanowiska przez JST]*
Umowy i kontrakty	- warunki współpracy - klauzule bezpieczeństwa	- przeglądy umów - audyty dostawców	*[uzupełnienie stanowiska przez JST]*

3.3.2 Określenie stron zainteresowanych

JST określa strony zainteresowane istotne z punktu widzenia funkcjonowania systemu zarządzania bezpieczeństwem informacji oraz wymagania tych stron zainteresowanych.

Lp.	Strona zainteresowana	Wymagania strony zainteresowanej
1.	**Petenci**	- ochrona danych osobowych - bezpieczeństwo informacji dotyczących usług miejskich - dostęp do wiarygodnych i aktualnych informacji

		- transparentność działań JST - szybkie i bezpieczne załatwianie spraw urzędowych
2.	**Pracownicy**	- bezpieczne środowisko pracy - ochrona danych osobowych pracowników - dostęp do niezbędnych informacji w celu wykonywania obowiązków - szkolenia z zakresu bezpieczeństwa informacji - jasne procedury i polityki - oczekiwania finansowe
3.	**Władze JST**	- efektywne zarządzanie bezpieczeństwem informacji - zgodność z przepisami prawa i regulacjami - raportowanie o stanie SZBI - minimalizacja ryzyka incydentów bezpieczeństwa - wdrożenie strategii JST w zakresie bezpieczeństwa informacji
4.	**Organy nadzoru i regulacyjne (np. UODO, NIK)**	- zgodność z obowiązującymi przepisami i regulacjami - dostęp do dokumentacji oraz do zasobów JST - wdrożenie i utrzymanie odpowiednich środków bezpieczeństwa - współpraca podczas kontroli i audytów - terminowe realizowanie zaleceń pokontrolnych
5.	**Dostawcy usług i kontrahenci**	- bezpieczne przetwarzanie udostępnianych informacji - zachowanie poufności danych - jasne zasady współpracy w zakresie bezpieczeństwa informacji - umowy o poufności i klauzule bezpieczeństwa - terminowe informowanie o zmianach wpływających na bezpieczeństwo
6.	**Społeczność lokalna i organizacje społeczne**	- transparentność działań JST - ochrona informacji - ułatwiony dostęp do informacji publicznej - reagowanie na zgłaszane uwagi i wnioski - współpraca w zakresie inicjatyw społecznych

7.	**Media lokalne**	- dostęp do rzetelnych i aktualnych informacji - ochrona informacji niejawnych i poufnych - współpraca w zakresie komunikacji kryzysowej - szybkie udzielanie odpowiedzi na zapytania - organizacja konferencji prasowych i briefingów
8.	**Inne jednostki administracji publicznej**	- wymiana informacji w bezpieczny sposób - zgodność z jednolitymi standardami bezpieczeństwa - współpraca w zakresie ochrony danych - uzgadnianie wspólnych procedur - współpraca w projektach ponadlokalnych
9.	**Instytucje finansujące (np. fundusze unijne)**	- zgodność z wymogami dotacyjnymi w zakresie bezpieczeństwa informacji - raportowanie zgodnie z wymaganiami - odpowiednie zarządzanie dokumentacją projektową - zapewnienie trwałości projektów - przestrzeganie terminów i zobowiązań umownych
10.	**Audytorzy zewnętrzni**	- dostęp do niezbędnej dokumentacji SZBI - współpraca podczas audytów - wdrażanie zaleceń poaudytowych - transparentność działań w zakresie SZBI - zapewnienie dowodów zgodności z normami i standardami
11.	**Przedsiębiorcy i inwestorzy**	- bezpieczeństwo informacji udostępnianych JST - transparentność procedur administracyjnych - ochrona tajemnicy przedsiębiorstwa - szybkość i efektywność załatwiania spraw - jasne i stabilne regulacje prawne
12.	**Służby ratunkowe i porządkowe**	- szybki dostęp do niezbędnych informacji w sytuacjach kryzysowych - bezpieczeństwo systemów komunikacji i informacji - współpraca w zakresie planowania

		i reagowania na sytuacje nadzwyczajne - regularne aktualizowanie procedur awaryjnych
13.	**Organizacje pozarządowe (NGO)**	- dostęp do informacji publicznej - ochrona danych osobowych w ramach współpracy - transparentność działań JST - wsparcie w realizacji projektów społecznych - współpraca w zakresie edukacji i promocji bezpieczeństwa informacji
14.	**Organizacje branżowe i stowarzyszenia samorządowe**	- wymiana doświadczeń i dobrych praktyk - udział w inicjatywach na rzecz bezpieczeństwa informacji - zgodność z rekomendacjami branżowymi - współpraca w zakresie legislacji i standardów

3.4 Określenie zakresu systemu zarządzania bezpieczeństwem informacji

1) Zakres Polityki Bezpieczeństwa obejmuje zarządzanie bezpieczeństwem informacji we wszystkich procesach JST, w szczególności w zakresie:
   a) obsługi interesantów,
   b) zarządzania systemami IT,
   c) ochrony danych osobowych przetwarzanych przez JST.
2) JST realizuje swoje zadania w lokalizacjach tj: *[Adresy – do uzupełnienia przez JST]*.

3.5 Przywództwo i zaangażowanie

Kierownik JST zobowiązuje się do:

a) zapewnienia zasobów niezbędnych do wdrożenia, utrzymania i doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji (SZBI),
b) promowania podejścia opartego na ryzyku i jego minimalizacji w zakresie przetwarzania informacji,

c) realizacji celów bezpieczeństwa informacji w sposób spójny z celami JST, określonymi w ramach kontroli zarządczej,
d) komunikowania znaczenia SZBI pracownikom oraz zaangażowania ich w procesy związane z bezpieczeństwem informacji.

3.6 Polityka

Polityka Bezpieczeństwa Informacji została opracowana i zatwierdzona przez kierownika JST *[zadanie JST – podać nazwę stanowiska]*, jest dostępna dla wszystkich pracowników i stron zainteresowanych *[zadanie JST – podać miejsce]*, a także na stronie internetowej *[zadanie JST – podać adres, jeżeli dotyczy]*.

3.7 Role, odpowiedzialność i uprawnienia

Kierownik JST sprawuje nadzór nad funkcjonowaniem i doskonaleniem Systemu Zarządzania Bezpieczeństwem Informacji. Odpowiedzialność i uprawnienia pracowników dotyczące przestrzegania i doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji zostały określone w zakresie czynności, regulaminie organizacyjnym, poszczególnych dokumentach systemu, poprzez imienne upoważnienia do wykonywania określonych czynności (np. związanych z przetwarzaniem danych osobowych) oraz w innych zarządzeniach wewnętrznych.

3.8 Planowanie – działania odnoszące się do ryzyk i szans

1) JST prowadzi systematyczną analizę ryzyk związanych z bezpieczeństwem informacji.
2) Szczegółowa analiza przeprowadzana jest w oparciu o Procedurę Zarządzania Ryzykiem, która stanowi odrębną regulację Systemu Zarządzania.
3) Wyniki dokumentowane są w Arkuszu oceny ryzyka, którego wzór stanowi załącznik do Procedury Zarządzania Ryzykiem oraz odnoszą się do zabezpieczeń stosowanych w JST.

3.9 Cele bezpieczeństwa informacji i planowanie ich osiągnięcia

W oparciu o obowiązującą Politykę Bezpieczeństwa Informacji, JST wyznacza cele bezpieczeństwa informacji oraz mierniki ich osiągnięcia. Cele ujęte w Polityce Bezpieczeństwa Informacji i ciągłości działania określają ramy konieczne do ustanowienia mierzalnych celów systemu pod kątem zapewnienia bezpieczeństwa informacji. Cele są dokumentowane w ramach przeglądów zarządzania i okresowo rozliczane.

3.10 Wsparcie / zasoby

Zasoby konieczne do utrzymania i doskonalenia systemu zarządzania bezpieczeństwem informacji obejmują następujące grupy zasobów:

a) pracownicy JST,
b) infrastruktura (techniczna, teleinformatyczna),
c) warunki działalności (wyposażenie pomieszczeń, zapewnienie bezpiecznych i higienicznych warunków pracy),
d) wiedza organizacji (szkolenia wewnętrzne i zewnętrzne).

3.11 Kompetencje

JST regularnie zapewnia swoim pracownikom szkolenia w zakresie bezpieczeństwa informacji, obejmujące:

a) przepisy prawa (KRI, RODO, ustawa o ochronie danych osobowych),
b) działania zapobiegające incydentom bezpieczeństwa,
c) obsługę systemów IT i procedury ochrony danych,
d) metody zarządzania i wykorzystania infrastruktury IT z uwzględnieniem aktualnej wiedzy na temat zabezpieczeń i cyberzagrożeń.

3.12 Komunikacja

Komunikowanie w zakresie SZBI odbywa się w sposób określony w zasadach funkcjonowania kontroli zarządczej w JST w zakresie mechanizmów przekazywania ważnych informacji w obrębie struktury organizacyjnej oraz z podmiotami zewnętrznymi.

3.13 Udokumentowane informacje / opracowywanie i aktualizowanie

1) W zależności od rodzaju dokumentu SZBI przyjmuje się następujące postępowanie:
   a) każdy nowy dokument opracowywany jest na zgodnie z obowiązującym szablonem dokumentacji,
   b) każda polityka, procedura i standard powinny posiadać tabelkę ,,Karta zmian" na ostatniej stronie dokumentu,
   c) obowiązujące dokumenty w aktualnej wersji dostępne są dla pracowników w *[zadanie JST – wskazać lokalizację]*.
2) Wszystkie zmiany dokumentów są zatwierdzane przez kierownika JST.
3) Nadzór nad dokumentami w systemie prowadzony jest przez *[zadanie JST – podać stanowisko]* lub inną osobę wskazaną.
4) Co najmniej raz w roku następuje przegląd dokumentacji pod kątem jej prawidłowości, aktualności oraz przydatności i adekwatności.
5) Propozycje zmian w dokumentach są zgłaszane za pośrednictwem formularza Karta wniosku o zmianę bezpośrednio *[zadanie JST – podać stanowisko]*, który nadzoruje zmianę, oraz komunikuje ją pracownikom. Zmiany w dokumentach zatwierdza Prezydent miasta/ Burmistrz/ Wójt / Starosta / Kierownik jednostki.

3.14 Nadzór nad udokumentowanymi informacjami

Nadzór nad dokumentacją SZBI sprawuje *[zadanie JST – podać stanowisko]* w zakresie dostępu i postępowania z dokumentami stosuje się postanowienia przyjętej klasyfikacji informacji oraz reguły i uprawnienia nadane zgodnie z wewnętrznymi regulacjami.

3.15 Działania operacyjne / planowanie i nadzór nad działaniami operacyjnymi

W celu spełnienia wymagań normy JST realizuje następujące procesy:

a) audytowanie SZBI,
b) zarządzanie ryzykiem,
c) zarządzanie incydentami,
d) zarządzanie ciągłością działania,
e) zarzadzanie cyklem życia produktów ICT.

3.16 Szacowanie ryzyka w bezpieczeństwie informacji

1) JST dokonuje szacowania ryzyka bezpieczeństwa informacji minimum raz w roku zgodnie z wytycznymi *Procedury zarządzania ryzykiem* oraz niniejszej Polityki. Istnieje możliwość przeprowadzenia dodatkowej analizy ryzyka w przypadku zaplanowania i / lub wdrożenia zmian, które mają wpływ na bezpieczeństwo informacji lub stwierdzenia incydentów bezpieczeństwa informacji.
2) Wyniki szacowania ryzyka są dokumentowane w arkuszu *Arkusz szacowania ryzyka ICT*.

3.17 Postępowanie z ryzykiem w bezpieczeństwie informacji

W ramach szacowania ryzyka, JST wdraża plany postępowania z ryzykiem dla stwierdzonych wysokich poziomów ryzyka, co odnotowuje w *Arkusz szacowania ryzyka ICT*. Wyniki analizy są dokumentowane i są omawiane podczas przeglądu zarządzania.

3.18 Ocena wyników / monitorowanie, pomiary, analiza i ocena

Zgodnie z zapisami niniejszej Polityki, monitorowanie SZBI odbywa się poprzez:

a) monitorowanie osiągania celów,

b) monitorowanie procesów,
c) audyty wewnętrzne,
d) przegląd zarządzania.

3.19 Audyt wewnętrzny

1) Nie rzadziej niż raz w roku wykonywany jest audyt bezpieczeństwa informacji, pod kątem spełnienia wymagań KRI oraz UoKSC. Zakres audytu może zostać poszerzony o wymagania normy ISO 27001.
2) Audyt może być przeprowadzony przez pracownika JST lub wyspecjalizowany podmiot zewnętrzny, pod warunkiem posiadania odpowiednich kompetencji.
3) Z każdego audytu sporządzany jest raport, który jest przedstawiany kierownikowi JST, który podejmuje decyzję dotyczącą wdrożenia ewentualnych rekomendacji z audytu oraz wskazuje osoby odpowiedzialne za realizację rekomendacji i przydziela niezbędne zasoby.
4) Wyniki audytów i rodzaje podjętych działań w następstwie audytów podlegają dokumentowaniu w ramach przeglądu zarządzania.

3.20 Przegląd zarządzania

1) *[Zadanie JST – podać stanowisko]* opracowuje nie rzadziej niż raz w roku raport z przeglądu zarządzania na podstawie informacji otrzymanych od kierowników komórek organizacyjnych zaangażowanych w funkcjonowanie SZBI. W raporcie uwzględnia się:
   a) stan realizacji działań, które zostały podjęte w następstwie wcześniejszych przeglądów systemu,
   b) wymagane lub podjęte zmiany w kontekście organizacji,
   c) wyniki realizacji celów bezpieczeństwa informacji,
   d) informacje o stwierdzonych niezgodnościach i podjętych działaniach korygujących w ich następstwie (również z uwzględnieniem incydentów bezpieczeństwa informacji),
   e) informacje o wynikach prowadzonych kontroli w ramach bieżącego monitorowania systemu zarządzania bezpieczeństwem informacji (wyniki mogą uwzględniać np. zmianę dokumentów, wdrożenie nowych zabezpieczeń),

f) wyniki przeprowadzonych audytów wewnętrznych,
g) wyniki szacowania ryzyka,
h) możliwość ciągłego doskonalenia.

2) Raport przedstawiany jest i omawiany z kierownictwem JST.
3) Przegląd zarządzania jest przeprowadzany *[w II kwartale każdego roku]*.

3.21 Doskonalenie / niezgodności i działania korygujące

1) W JST wszyscy pracownicy są zobowiązani do reagowania i zgłaszania niezgodności. Każde zdarzenie, które według pracownika może stanowić niespełnienie wymagań wdrożonego SZBI powinno być natychmiastowo zgłoszone do przełożonego.
2) Zgłoszenia można dokonać w zgodnie z przyjętymi regulacjami w zakresie zarządzania incydentami.
3) Wszystkie podjęte działania w następstwie niezgodności powinny być dokumentowane w ramach przeglądu zarządzania i w rejestrze incydentów wraz z datą zamknięcia działań oraz oceną skuteczności.

3.22 Ciągłe doskonalenie

Wszystkie podejmowane w JST działania w ramach systemu zarządzania bezpieczeństwem informacji mają na celu jego ciągłe doskonalenie. W celu doskonalenia procesów w ramach systemu, podejmowane są działania obejmujące m.in.

a) przegląd dokumentacji systemowej (w szczególności polityki bezpieczeństwa informacji i przyjętych celów bezpieczeństwa informacji),
b) wyniki prowadzonych przeglądów zarządzania (w szczególności działania podjęte w następstwie tych przeglądów),
c) wyniki prowadzonych audytów wewnętrznych (w szczególności działania podjęte w następstwie tych przeglądów).

4. Słownik pojęć używanych w ramach dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji

4.1 Cel

Celem niniejszego dokumentu jest określenie słownika pojęć używanych w ramach dokumentacji SZBI w JST. Słownik bazuje na definicjach ujętych w normie ISO27000. Podstawy prawne określone są w dokumencie Polityki Bezpieczeństwa. Słownik ma zastosowanie dla wszystkich regulacji SZBI. Osoba odpowiedzialna za bezpieczeństwo informacji odpowiada za spójność
z innymi regulacjami wewnętrznymi oraz aktualność słownika.

4.2 Opis postępowania – układ alfabetyczny

1) **Akceptacja ryzyka** – świadome przyjęcie skutków określonego ryzyka bez podejmowania dodatkowych działań zabezpieczających.
2) **Aktywa (informacyjne)** – każdy zasób mający wartość dla organizacji, który wymaga ochrony. Aktywami są m.in. informacje, systemy teleinformatyczne, urządzenia sprzętowe, oprogramowanie, infrastruktura, a także ludzie i ich kompetencje – wszystkie elementy, od których zależy przetwarzanie informacji i realizacja zadań organizacji.
3) **Analiza wpływu na działalność (BIA – Business Impact Analysis)** – systematyczne badanie, jak potencjalne zakłócenia funkcjonowania systemów ICT wpływają na realizację kluczowych procesów i usług organizacji. Analiza ta identyfikuje procesy krytyczne, wspierające je systemy oraz skutki ich niedostępności, stanowiąc podstawę planowania priorytetów odtwarzania systemów i wymagań dotyczących ich dostępności.
4) **Analiza ryzyka** – systematyczny, udokumentowany i powtarzalny proces identyfikowania ryzyka dla bezpieczeństwa informacji, analizowania ich przyczyn i skutków oraz oceny prawdopodobieństwa ich wystąpienia.

5) **Apetyt na ryzyko** – ustalony przez kierownictwo poziom ryzyka, jaki organizacja jest gotowa zaakceptować w związku ze swoją działalnością. Wyrażony jest często poprzez ogólne kryteria oceny ryzyka lub progi akceptowalności.
6) **Audyt (bezpieczeństwa informacji)** – niezależny i obiektywny przegląd oraz ocena procesów, procedur, mechanizmów i zabezpieczeń związanych z bezpieczeństwem informacji w organizacji.
7) **Audyt wewnętrzny** – audyt realizowany przez samą organizację (lub na jej zlecenie) w celu wewnętrznej oceny zgodności i skuteczności Systemu Zarządzania Bezpieczeństwem Informacji.
8) **Audyt zewnętrzny** – audyt przeprowadzany przez niezależną, uprawnioną jednostkę spoza organizacji w celu uzyskania obiektywnej oceny poziomu bezpieczeństwa informacji i zgodności z wymaganiami.
9) **Autentyczność informacji** – cecha informacji polegająca na pewności co do tożsamości źródła oraz prawdziwości treści informacji. Autentyczność oznacza, że dany podmiot (osoba, system) jest tym, za kogo się podaje, a dane nie zostały zmodyfikowane w nieautoryzowany sposób – nadawca i odbiorca informacji mogą zweryfikować swoje tożsamości i mieć pewność, że informacja jest oryginalna.
10) **Bezpieczna konfiguracja systemów** – stan oraz zbiór ustawień systemu teleinformatycznego zapewniający jego bezpieczne funkcjonowanie.
11) **Bezpieczeństwo dostawców (bezpieczeństwo łańcucha dostaw)** – zespół zasad i działań mających na celu zapewnienie, że dostawcy zewnętrzni produktów, usług lub procesów nie wprowadzają zagrożeń dla bezpieczeństwa informacji i ciągłości działania organizacji.
12) **Bezpieczeństwo fizyczne** – stosowanie środków organizacyjnych i technicznych do ochrony obiektów, pomieszczeń i infrastruktury, w których przetwarzane są informacje, przed zagrożeniami fizycznymi.
13) **Bezpieczeństwo informacji** – stan, w którym informacje są odpowiednio chronione przed zagrożeniami, tak aby zachować ich poufność, integralność i dostępność. Bezpieczeństwo informacji obejmuje zabezpieczenia organizacyjne, techniczne i prawne, chroniące informacje przed nieautoryzowanym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zakłóceniem.

14) **Bezpieczeństwo środowiskowe** – ochrona systemów informacyjnych i infrastruktury technicznej przed zagrożeniami wynikającymi z czynników środowiskowych i awarii infrastrukturalnych. Obejmuje utrzymanie odpowiednich warunków środowiskowych w pomieszczeniach serwerowni i innych miejscach przetwarzania informacji (np. temperatura, wilgotność, czystość zasilania elektrycznego) oraz wdrażanie mechanizmów zapobiegających ich przekroczeniu.
15) **Bezpieczeństwo zasobów ludzkich** – stosowanie zasad i praktyk mających na celu uwzględnienie wymogów bezpieczeństwa informacji w procesach zarządzania personelem na wszystkich etapach zatrudnienia i współpracy. Obejmuje to m.in. weryfikację wiarygodności i kwalifikacji kandydatów przed zatrudnieniem (screening), zawieranie z pracownikami i współpracownikami umów o zachowaniu poufności, wyraźne określanie i rozdział obowiązków służbowych w sposób minimalizujący ryzyko nadużyć, stałe podnoszenie świadomości bezpieczeństwa wśród personelu oraz bezpieczne procedury zakończenia współpracy (np. odbiór identyfikatorów, odebranie dostępu do systemów).
16) **Bezpieczeństwo wbudowane** – zasada „security by design", czyli podejście do projektowania systemów informacyjnych uwzględniające mechanizmy bezpieczeństwa od samego początku jako integralną część systemu. Bezpieczeństwo wbudowane oznacza, że już na etapie planowania i projektowania nowego systemu ICT określa się wymagania bezpieczeństwa (techniczne i organizacyjne) oraz implementuje odpowiednie zabezpieczenia, zamiast dodawać je dopiero po wdrożeniu.
17) **Bezpieczeństwo domyślne** – zasada ustawiania bezpiecznych domyślnych konfiguracji i ustawień systemów ICT („security by default"). Polega na tym, że każdy nowy system lub usługa jest domyślnie skonfigurowana w sposób maksymalnie bezpieczny, wymagając aktywnego działania, aby wprowadzić mniej bezpieczne ustawienia (a nie odwrotnie).
18) **Ciągłe doskonalenie** – zasada, zgodnie z którą System Zarządzania Bezpieczeństwem Informacji powinien być nieustannie oceniany i usprawniany.
19) **Ciągłość działania** – zdolność organizacji do nieprzerwanego świadczenia kluczowych usług i realizacji podstawowych funkcji (lub szybkiego ich wznowienia) na akceptowalnym poziomie w przypadku wystąpienia zakłóceń, takich jak awarie, incydenty czy sytuacje kryzysowe.

20) **Cyberhigiena** – zbiór standardowych praktyk i działań utrzymujących systemy informacyjno-komunikacyjne w czystości i bezpiecznym stanie na co dzień, analogicznie do higieny osobistej. Cyberhigiena obejmuje m.in. stosowanie ustandaryzowanych bezpiecznych konfiguracji systemów, regularne aktualizowanie oprogramowania i zarządzanie poprawkami, usuwanie lub wyłączanie zbędnych funkcji i usług, monitorowanie stanu zabezpieczeń oraz bieżące eliminowanie wykrytych podatności.
21) **Cykl życia systemu ICT** – kolejne etapy istnienia systemu technologii informacyjno-komunikacyjnej od jego inicjatywy do wycofania z eksploatacji. W typowym cyklu życia wyróżnia się fazy: planowania i pozyskania (analiza potrzeb, definiowanie wymagań, wybór rozwiązania), projektowania (uwzględniającego zasady bezpieczeństwa wbudowanego i domyślnego), wdrażania i uruchamiania, eksploatacji i utrzymania (monitorowanie, aktualizacje, reagowanie na incydenty), wprowadzania zmian i rozwoju systemu oraz fazę wycofania z użytkowania i likwidacji.
22) **Dostępność informacji** – właściwość polegająca na zapewnieniu uprawnionym użytkownikom dostępu do informacji i zasobów wtedy, kiedy jest to potrzebne, bez nieuzasadnionej zwłoki.
23) **Działanie korygujące** – działanie podejmowane w celu wyeliminowania przyczyny stwierdzonej niezgodności lub innego niepożądanego zjawiska i zapobieżenia jego ponownemu wystąpieniu.
24) **Incydent bezpieczeństwa informacji** – pojedyncze zdarzenie lub seria niepożądanych i nieoczekiwanych zdarzeń, które naruszają lub mogą naruszać bezpieczeństwo informacji w organizacji.
25) **Integralność informacji** – właściwość zapewniająca, że informacje i systemy nie zostały zmienione lub zniszczone w sposób nieautoryzowany. Integralność oznacza dokładność, kompletność i spójność danych – dane zachowują swój pierwotny, prawidłowy stan i nie nastąpiła w nich żadna niedozwolona modyfikacja.
26) **Kontrola dostępu** – zestaw mechanizmów i reguł służących ograniczaniu dostępu do informacji, systemów lub fizycznych obszarów wyłącznie do podmiotów uprawnionych. Kontrola dostępu zapewnia, że tylko osoby (lub procesy) o odpowiednich uprawnieniach

mogą korzystać z określonych zasobów, i to tylko w zakresie niezbędnym do wykonania swoich zadań (zgodnie z zasadą minimalnych uprawnień).

27) **Łańcuch dostaw** – powiązany system podmiotów i procesów zaangażowanych w dostarczanie produktów, usług lub informacji od dostawców początkowych aż do ostatecznej organizacji (odbiorcy).
28) **Monitorowanie systemów ICT** – ciągły proces obserwacji, rejestrowania i analizowania zdarzeń zachodzących w systemach informacyjno-komunikacyjnych organizacji, w celu wykrycia potencjalnych incydentów bezpieczeństwa informacji lub nieprawidłowości oraz zapewnienia właściwego poziomu nadzoru nad infrastrukturą.
29) **Mechanizm kontrolny (środek bezpieczeństwa)** – patrz: pkt 44) Środek bezpieczeństwa informacji. *(Uwaga: w terminologii ISO zamiast terminu „kontrola" używa się określenia środek lub mechanizm bezpieczeństwa – definicja w pkt 44) Środek bezpieczeństwa).*
30) **Niezgodność** – stwierdzone odstępstwo od wymagań lub zasad przyjętych w systemie zarządzania (w tym w SZBI).
31) **Ograniczone zaufanie (Zero Trust)** – koncepcja architektury bezpieczeństwa, według której żadna osoba, urządzenie ani sieć nie jest automatycznie godna pełnego zaufania, nawet jeśli znajduje się wewnątrz granic sieci organizacji.
32) **Ocena ryzyka** – określenie szacunkowego poziomu ryzyka poprzez analizę prawdopodobieństwa wystąpienia konkretnego incydentu oraz potencjalnego skutku tego incydentu dla organizacji. Ocena ryzyka następuje po identyfikacji zagrożeń i podatności, aby zmierzyć, które ryzyka są najpoważniejsze.
33) **Ochrona danych osobowych** – *zob. Polityka bezpieczeństwa informacji (aspekt RODO)*.
34) **Plan wyjścia (zakończenia współpracy z dostawcą)** – ustalony plan działania na wypadek zakończenia lub zerwania współpracy z kluczowym dostawcą, mający na celu zabezpieczenie ciągłości działania organizacji i ochrony jej informacji.
35) **Podatność** – słabość lub luka w zabezpieczeniach aktywu (systemu, procesu, procedury lub innego zasobu), która może zostać wykorzystana przez zagrożenie. Podatnością może być błąd w oprogramowaniu, brak aktualnej poprawki, źle skonfigurowany system, niewystarczające procedury lub brak świadomości użytkowników.

36) **Polityka bezpieczeństwa informacji** – nadrzędny dokument wewnętrzny organizacji określający cele, założenia i ogólne zasady postępowania w obszarze bezpieczeństwa informacji. Polityka wyraża zobowiązanie kierownictwa do ochrony informacji i wyznacza ramy dla ustanowienia SZBI.
37) **Postępowanie z ryzykiem (zarządzanie ryzykiem)** – podejmowanie działań w odpowiedzi na zidentyfikowane ryzyko, w celu obniżenia go do akceptowalnego poziomu lub usunięcia nieakceptowalnych zagrożeń.
38) **Poufność informacji** – właściwość zapewniająca, że informacja nie jest ujawniana ani dostępna dla nieupoważnionych osób, podmiotów lub procesów. Zachowanie poufności oznacza ochronę tajności informacji – tylko osoby posiadające odpowiednie uprawnienia (wynikające z obowiązków służbowych lub nadanych ról) mogą mieć dostęp do określonych danych.
39) **Przegląd zarządzania** – okresowe, formalne spotkanie najwyższego kierownictwa organizacji, podczas którego dokonywana jest ocena funkcjonowania i skuteczności systemu zarządzania (w tym Systemu Zarządzania Bezpieczeństwem Informacji).
40) **Raport audytowy** – dokument podsumowujący ustalenia audytu bezpieczeństwa informacji (wewnętrznego lub zewnętrznego).
41) **Rejestr ryzyk** – oficjalna, zorganizowana dokumentacja wszystkich zidentyfikowanych ryzyk bezpieczeństwa informacji w organizacji, wraz z ich oceną i historią postępowania.
42) **Rozdział obowiązków** – zasada organizacyjna polegająca na takim podziale ról i przydzielaniu zadań pracownikom, by zapobiec skoncentrowaniu nadmiernych uprawnień lub czynności krytycznych w rękach jednej osoby.
43) **Rozliczalność** – zdolność systemu do przypisania konkretnych działań konkretnym podmiotom oraz zapewnienia dowodów pozwalających rozliczyć te podmioty z wykonanych operacji. Rozliczalność w bezpieczeństwie informacji oznacza, że można jednoznacznie ustalić kto, kiedy, jaką czynność wykonał na określonych danych lub systemach.
44) **Środek bezpieczeństwa informacji (zabezpieczenie)** – każde narzędzie, mechanizm, proces lub procedura, które służą redukcji ryzyka związanego z bezpieczeństwem informacji. Środki bezpieczeństwa mogą mieć charakter techniczny (np. firewall,

oprogramowanie antywirusowe, kopie zapasowe, szyfrowanie danych), organizacyjny (np. polityki i procedury, podział obowiązków, szkolenia), personalny (np. weryfikacja personelu, świadomość pracowników) czy fizyczny (np. kontrola dostępu do budynków, szafy pancerne).

45) **Świadomość bezpieczeństwa informacji** – poziom wiedzy, zrozumienia i odpowiedzialności pracowników (oraz współpracowników) dotyczący ochrony informacji i potencjalnych zagrożeń. Wysoka świadomość bezpieczeństwa oznacza, że personel zna polityki i procedury bezpieczeństwa, rozumie, dlaczego są one ważne oraz potrafi rozpoznawać sytuacje mogące stanowić zagrożenie (np. próby phishingu, podejrzane zachowania) i odpowiednio na nie reagować. Budowanie świadomości odbywa się poprzez regularne szkolenia z zakresu bezpieczeństwa informacji, kampanie informacyjne, testy socjotechniczne, przypomnienia i zaangażowanie kierownictwa w promowanie kultury bezpieczeństwa.
46) **Zagrożenie** – potencjalna przyczyna incydentu, która może wyrządzić szkodę systemowi lub organizacji. Zagrożenie to każdy czynnik (osoba, zjawisko, zdarzenie, stan) mający negatywny wpływ na bezpieczeństwo informacji, jeśli się urzeczywistni.
47) **Zarządzanie ciągłością działania** – część ogólnego systemu zarządzania, polegająca na planowaniu, wdrażaniu i utrzymywaniu rozwiązań zapewniających ciągłość kluczowych procesów organizacji w razie wystąpienia poważnych zakłóceń.
48) **Zarządzanie incydentami bezpieczeństwa informacji** – proces rejestrowania, analizowania i reagowania na incydenty w obszarze bezpieczeństwa informacji, mający na celu opanowanie sytuacji kryzysowej i ograniczenie jej negatywnych skutków, a następnie wyciągnięcie wniosków na przyszłość.
49) **Zarządzanie ryzykiem bezpieczeństwa informacji** – skoordynowane działania związane z kierowaniem i nadzorowaniem organizacji w odniesieniu do ryzyka dla bezpieczeństwa informacji. Obejmuje cały cykl postępowania z ryzykiem: ustanowienie kontekstu (określenie kryteriów oceny ryzyka, zakresu i zakresu odpowiedzialności), identyfikację ryzyka (ustalenie co zagraża którym aktywom i jak), analizę i ocenę ryzyka (oszacowanie prawdopodobieństw i skutków w celu nadania priorytetów) oraz wybór i wdrożenie opcji postępowania z ryzykiem (wdrożenie zabezpieczeń, akceptacja itp.).

50) **Zdarzenie bezpieczeństwa informacji** – zaobserwowane zdarzenie lub sytuacja, która może wskazywać na naruszenie polityki bezpieczeństwa lub mechanizmów ochronnych organizacji, lub świadczyć o wcześniej nieznanym stanie mogącym mieć znaczenie dla bezpieczeństwa.

4.3 Uwagi

Regulacja nie powinna być rozszerzana – należy ją aktualizować o nowe pojęcia używane w SZBI.

4.4 Metryka

Lp.	Zakres zmiany	Data przyjęcia i podstawa stosowania
1.	Utworzenie dokumentu	00-00-2026 Zarządzenie …

5. Analiza ryzyka

5.1 Cel

Celem niniejszej procedury jest ustanowienie jednolitych, spójnych i powtarzalnych zasad identyfikacji, analizy, oceny, postępowania oraz przeglądu ryzyka związanych z bezpieczeństwem informacji oraz funkcjonowaniem systemów i usług teleinformatycznych w JST. Procedura ma na celu zapewnienie ochrony poufności, integralności i dostępności informacji, ciągłości realizacji zadań publicznych JST, ograniczenie skutków zdarzeń niepożądanych oraz wsparcie podejmowania świadomych decyzji zarządczych w obszarze cyberbezpieczeństwa. Podstawy prawne określone są w dokumencie Polityki Bezpieczeństwa.

5.2 Zakres stosowania

1) Procedura ma zastosowanie do wszystkich komórek organizacyjnych JST, wszystkich pracowników, współpracowników oraz podmiotów realizujących zadania na rzecz JST, którzy uczestniczą w planowaniu, eksploatacji, utrzymaniu lub nadzorze nad systemami i usługami teleinformatycznymi.
2) Procedura obejmuje wszystkie systemy teleinformatyczne, usługi ICT, procesy organizacyjne, dane, zasoby techniczne oraz zasoby ludzkie, które mają wpływ na realizację zadań publicznych JST.

5.3 Odpowiedzialność za procedurę

1) Kierownik JST odpowiada za zatwierdzenie metodyki analizy ryzyka, określenie akceptowalnego poziomu ryzyka, podejmowanie decyzji o akceptacji ryzyka oraz zapewnienie zasobów niezbędnych do realizacji procedury.
2) Pełnomocnik do spraw bezpieczeństwa informacji lub inna wyznaczona osoba odpowiada za koordynację procesu analizy ryzyka, nadzór nad spójnością metodyki, prowadzenie rejestru ryzyka oraz raportowanie wyników kierownictwu JST.

3) Właściciele usług, systemów i aktywów odpowiadają za identyfikację zagrożeń, ocenę skutków i prawdopodobieństwa, wskazywanie istniejących zabezpieczeń oraz proponowanie działań ograniczających ryzyko.
4) Komórka odpowiedzialna za obsługę teleinformatyczną zapewnia wsparcie merytoryczne w zakresie identyfikacji podatności technicznych, oceny skutków technicznych oraz wdrażania działań ograniczających ryzyko.

5.4 Opis postępowania

5.4.1 Zasady ogólne metodyki analizy ryzyka

1) Analiza ryzyka w JST jest procesem systematycznym, udokumentowanym i cyklicznym. Metodyka opiera się na identyfikacji zagrożeń dla usług i systemów teleinformatycznych, ocenie skutków ich materializacji oraz ocenie prawdopodobieństwa ich wystąpienia, a następnie na wyznaczeniu poziomu ryzyka i określeniu sposobu postępowania z ryzykiem.
2) Analiza ryzyka jest przeprowadzana w sposób zapewniający porównywalność wyników pomiędzy różnymi obszarami JST oraz możliwość monitorowania zmian poziomu ryzyka w czasie.

5.4.2 Identyfikacja ryzyka

1) Dla każdej usługi teleinformatycznej oraz każdego systemu ICT identyfikuje się elementy niezbędne do ich funkcjonowania, w tym zasoby techniczne, organizacyjne oraz ludzkie. Dodatkowo identyfikuje się zagrożenia, które mogą mieć negatywny wpływ na poufność, integralność lub dostępność informacji oraz na ciągłość realizacji zadań publicznych JST.
2) Identyfikacja ryzyka uwzględnia charakter przetwarzanych informacji, znaczenie usługi dla JST, zależności pomiędzy systemami oraz powiązania z dostawcami zewnętrznymi.

5.4.3 Ocena skutków

1) Dla każdego zidentyfikowanego zagrożenia określa się wpływ na poufność, integralność i dostępność informacji. Każdy z tych atrybutów jest oceniany w sposób jednoznaczny, a następnie wyznaczany jest łączny poziom skutku materializacji zagrożenia.
2) Ocena skutków uwzględnia konsekwencje organizacyjne, prawne, finansowe oraz wizerunkowe dla JST, a także wpływ na realizację zadań publicznych i prawa obywateli.

5.4.4 Istotność zagrożenia

Dla każdego ostatecznie ocenionego zagrożenia określa się jego istotność biorąc pod uwagę klasyfikację (istotność) aktywa lub danych.

5.4.5 Ocena prawdopodobieństwa

1) Dla każdego zagrożenia określa się prawdopodobieństwo jego wystąpienia, biorąc pod uwagę istniejące podatności, historię incydentów, aktualne zagrożenia w cyberprzestrzeni oraz poziom zastosowanych zabezpieczeń organizacyjnych i technicznych.
2) Ocena prawdopodobieństwa jest dokonywana w sposób ujednolicony i umożliwiający porównywanie ryzyk pomiędzy różnymi obszarami JST.

5.4.6 Ocena poziomu ryzyka

1) Poziom ryzyka jest wyznaczany jako wynik połączenia oceny skutków oraz oceny prawdopodobieństwa. Dla każdego ryzyka przypisywany jest poziom ryzyka, który stanowi podstawę do dalszych decyzji dotyczących postępowania z ryzykiem.
2) Ryzyka są klasyfikowane w sposób umożliwiający jednoznaczne określenie, które z nich są akceptowalne, a które wymagają działań ograniczających lub decyzji kierownictwa JST.

5.4.7 Apetyt na ryzyko i akceptacja ryzyka

1) Kierownik JST określa poziom akceptowalnego ryzyka, zwany apetytem na ryzyko, uwzględniając charakter działalności JST, obowiązki prawne oraz oczekiwania interesariuszy.

2) Ryzyka mieszczące się w granicach apetytu na ryzyko mogą zostać zaakceptowane, co musi zostać udokumentowane. Ryzyka przekraczające poziom akceptowalny wymagają podjęcia działań ograniczających lub innych decyzji zarządczych.

5.4.8 Postępowanie z ryzykiem

1) Dla ryzyk nieakceptowalnych określa się sposób postępowania, który może obejmować ograniczenie ryzyka poprzez wdrożenie zabezpieczeń, unikanie ryzyka poprzez zmianę sposobu realizacji procesu lub przeniesienie ryzyka na inny podmiot.
2) Dla każdego działania określa się odpowiedzialność, termin realizacji oraz mierniki pozwalające na ocenę skuteczności podjętych działań.
3) Osobą odpowiedzialną za ryzyko i plan postępowania jest właściciel ryzyka, którym domyślnie jest właściciel aktywa.

5.4.9 Właściciel ryzyka

1) Dla każdego ryzyka należy wskazać właściciela. Właściciel ryzyka bierze udział w analizie ryzyka oraz jest merytorycznie odpowiedzialny za obszar jego występowania (w tym obszar biznesowy).

   Właściciel ryzyka odpowiada za:

   a) udział w analizie ryzyka, w szczególności określeniu zagrożeń,
   b) weryfikację oceny ryzyka,
   c) nadzór nad mechanizmami mitygacji ryzyka.

5.4.10 Wskaźniki i mierniki ryzyka

W JST stosuje się wskaźniki umożliwiające monitorowanie poziomu ryzyka, skuteczności zabezpieczeń oraz postępu działań ograniczających ryzyko. Wskaźniki te są wykorzystywane do raportowania kierownictwu JST oraz do podejmowania decyzji doskonalących system zarządzania bezpieczeństwem informacji.

5.5 Cykle szacowania ryzyka

1) Analiza ryzyka jest przeprowadzana okresowo, nie rzadziej niż raz w roku, a także każdorazowo w przypadku istotnych zmian organizacyjnych, technologicznych, prawnych lub po wystąpieniu poważnych incydentów bezpieczeństwa.
2) Cykliczność analizy zapewnia aktualność ocen ryzyka oraz dostosowanie zabezpieczeń do zmieniających się zagrożeń.
3) Analiza ryzyka jest zatwierdzana przez kierownictwo JST oraz podlega przeglądowi w ramach przeglądu zarządzania.

5.6 Metryka

Lp.	Zakres zmiany	Data przyjęcia i podstawa stosowania
1.	Utworzenie dokumentu	00-00-2026 Zarządzenie …

5.7 Uwagi

Regulacja nie musi być rozszerzana – możliwe obszary doprecyzowania (przykładowe) to szczegółowy plan postępowania z ryzykiem rezydualnym.

5.8 Załączniki

1) Załącznik nr 1 Instrukcja oceny ryzyka ICT
2) Załącznik nr 2 Arkusz szacowania ryzyka ICT (Excel – plik zewnętrzny)

Załącznik nr 1 Instrukcja oceny ryzyka ICT

Identyfikacja

Dla każdej usługi ICT należy wskazać główne elementy które są wymagane do świadczenia danej usługi. Elementy te mogą obejmować zarówno aktywa osobowe, teleinformatyczne jak i organizacyjne (produkty ICT oraz możliwe składowe o ile mają wpływ na ocenę ryzyka) oraz zidentyfikować istotne zagrożenia. W opisie „Wpływ na poufność / integralność / dostępność" krótko uzasadnić skutki.

Ocena skutku

a) Dla każdego zagrożenia należy przypisać wartości binarne:

Poufność (C) możliwa wartość: 0/1

Integralność (I) możliwa wartość: 0/1

Dostępność (A) możliwa wartość: 0/1

Następnie wyliczyć skutek ich materializacji S = C + I + A oraz uwzględnić istotność zagrożenia I

b) Istotność zagrożenia posiada domyślną wartość „1", która nie zmienia skutku obliczonego w powyższym wzorze. Wysokość skutku może zostać zmodyfikowana w zależności od jego istotności dla danego aktywa / produktu lub usługi ICT. Wstawiając wartość istotności zagrożenia „2" – ISTOTNE lub „3" – BARDZO ISTOTNE skutek S wyniesie odpowiednio „2" lub „3" niezależnie od wartości wcześniej obliczonej zgodnie z powyższym wzorem.
Wartościom liczbowym skutku odpowiadają odpowiednio wartości tekstowe:

1 → MAŁY

2 → ŚREDNI

3→ WYSOKI

Ocena prawdopodobieństwa

a) Określić wartość prawdopodobieństwa P na skali:

MAŁE = 1 (sporadyczne / mało realne)

ŚREDNIE = 2 (możliwe)

WYSOKIE = 3 (prawdopodobne)

b) Przy ocenie prawdopodobieństwa należy uwzględnić podatności, historię incydentów (w tym ujawnionych spoza Organizacji / Urzędu), wiedzę ekspercką oraz wdrożone zabezpieczenia.

Ocena ryzyka

Posiadając wiedzę na temat skutków danego zdarzenia (z uwzględnieniem istotności) oraz prawdopodobieństwa jego wystąpienia należy wyliczyć wartość ryzyka R według następującego wzoru:

R= P × S

oraz przypisać poziomy ryzyka:

1–2 → **MAŁE**

3–4 → **ŚREDNIE**

6–9 → **WYSOKIE**

Macierz Ryzyka (P × S)

RYZYKO	**1 – MAŁE**	**2 – ŚREDNIE**	**3 – WYSOKIE**
1 – MAŁE	1 – MAŁE	2 – MAŁE	3 – ŚREDNIE
2 – ŚREDNIE	2 – MAŁE	4 – ŚREDNIE	6 – WYSOKIE
3 – WYSOKIE	3 – ŚREDNIE	6 – WYSOKIE	9 – WYSOKIE

Legenda macierzy:

a) MAŁE (zielone) – akceptowalne,
b) ŚREDNIE (żółte) – wymagają planu działań,
c) WYSOKIE (czerwone) – natychmiastowe działania i nadzór kierownictwa.

Postępowanie z ryzykiem

a) Dla ryzyk na poziomie ŚREDNIM i WYSOKIM należy określić działania (redukcja / unikanie / przeniesienie) ze wskazaniem właściciela danego ryzyka, terminu i zastosowanego miernika efektu / postępu.
b) Ryzyko MAŁE można akceptować – należy to odnotować.

6. Bezpieczeństwo w cyklu życia systemów ICT

6.1 Cel

Celem niniejszej procedury jest ustanowienie jednolitych, systemowych i spójnych zasad zapewnienia bezpieczeństwa systemów technologii informacyjno-komunikacyjnych funkcjonujących w JST w całym ich cyklu życia, począwszy od etapu planowania i pozyskania, poprzez projektowanie, wdrażanie, eksploatację, utrzymanie, modyfikację, aż do etapu wycofania z użytkowania oraz likwidacji. Procedura ma na celu zapewnienie ochrony poufności, integralności, dostępności oraz autentyczności informacji przetwarzanych w systemach technologii informacyjno-komunikacyjnych JST, a także zapewnienie odporności tych systemów na zdarzenia mogące negatywnie wpływać na realizację zadań publicznych, ciągłość działania urzędu oraz zaufanie obywateli. Podstawy prawne określone są w dokumencie Polityki Bezpieczeństwa.

6.2 Zakres stosowania

1) Procedura ma zastosowanie do wszystkich systemów technologii informacyjno-komunikacyjnych wykorzystywanych przez JST, niezależnie od ich lokalizacji, formy technicznej, sposobu finansowania, modelu utrzymania oraz stopnia krytyczności.
2) Procedura obowiązuje wszystkie komórki organizacyjne JST, w szczególności:
   a) komórki realizujące zadania merytoryczne z wykorzystaniem systemów informacyjnych,
   b) komórki odpowiedzialne za obsługę informatyczną i techniczną,
   c) komórki odpowiedzialne za bezpieczeństwo informacji,
   d) kierownictwo JST oraz osoby pełniące funkcje kierownicze.
3) Procedura ma zastosowanie również do systemów utrzymywanych lub obsługiwanych przez podmioty zewnętrzne, jeżeli systemy te przetwarzają informacje JST lub są wykorzystywane do realizacji zadań publicznych.

6.3 Odpowiedzialności za procedurę

1) Kierownik JST ponosi odpowiedzialność za zapewnienie funkcjonowania systemu zarządzania bezpieczeństwem informacji, w tym za zatwierdzenie, wdrożenie oraz egzekwowanie niniejszej procedury.
2) Osoba odpowiedzialna za bezpieczeństwo informacji odpowiada za nadzór nad stosowaniem procedury, jej spójność z innymi regulacjami wewnętrznymi oraz monitorowanie skuteczności stosowanych środków bezpieczeństwa.
3) Kierownik komórki odpowiedzialnej za obsługę informatyczną odpowiada za techniczną realizację wymagań bezpieczeństwa na wszystkich etapach cyklu życia systemów technologii informacyjno-komunikacyjnych.
4) Kierownicy komórek organizacyjnych odpowiadają za stosowanie procedury w odniesieniu do systemów wykorzystywanych w podległych im obszarach działalności.
5) Pracownicy JST są zobowiązani do przestrzegania zasad określonych w procedurze w zakresie wynikającym z powierzonych im obowiązków.

6.4 Opis postępowania

6.4.1 Etap planowania i inicjowania systemu

1) Każdy nowy system technologii informacyjno-komunikacyjnej planowany do wdrożenia w JST podlega identyfikacji potrzeb biznesowych oraz ocenie wpływu na realizację zadań publicznych.
2) Na etapie planowania określa się wymagania bezpieczeństwa informacji, uwzględniając charakter przetwarzanych danych, znaczenie systemu dla ciągłości działania JST oraz obowiązujące wymagania prawne i regulacyjne.
3) Planowanie systemu obejmuje również uwzględnienie ryzyk związanych z jego funkcjonowaniem w całym cyklu życia, w tym ryzyk wynikających z zależności od dostawców, rozwiązań technicznych oraz czynników organizacyjnych.

6.4.2 Etap projektowania i pozyskania

1) Projektowanie systemu technologii informacyjno-komunikacyjnej uwzględnia zasadę bezpieczeństwa wbudowanego oraz bezpieczeństwa domyślnego.
2) Wymagania bezpieczeństwa są integralnym elementem dokumentacji projektowej, umów, specyfikacji technicznych oraz warunków zamówień publicznych.
3) Na etapie pozyskania zapewnia się, aby rozwiązania techniczne umożliwiały wdrożenie mechanizmów kontroli dostępu, rejestrowania zdarzeń, ochrony przed nieuprawnionym dostępem oraz odporności na awarie.

6.4.3 Etap wdrażania i uruchamiania

1) Przed uruchomieniem systemu przeprowadza się działania weryfikujące zgodność wdrożenia z założonymi wymaganiami bezpieczeństwa.
2) System jest konfigurowany w sposób ograniczający dostęp do funkcji i danych wyłącznie do osób upoważnionych, zgodnie z zasadą minimalnych uprawnień.
3) Uruchomienie systemu następuje po formalnym potwierdzeniu gotowości do bezpiecznej eksploatacji.

6.4.4 Etap eksploatacji i utrzymania

1) W trakcie eksploatacji systemy technologii informacyjno-komunikacyjnych podlegają stałemu nadzorowi pod kątem bezpieczeństwa informacji.
2) Zapewnia się regularne wykonywanie działań utrzymaniowych, w tym aktualizacji, przeglądów konfiguracji oraz monitorowania zdarzeń istotnych dla bezpieczeństwa.
3) Wszelkie incydenty lub zdarzenia mogące negatywnie wpłynąć na bezpieczeństwo systemu są identyfikowane, analizowane oraz obsługiwane zgodnie z obowiązującymi procedurami reagowania.

6.4.5 Etap zmian i rozwoju systemu

1) Każda zmiana w systemie technologii informacyjno-komunikacyjnej, w tym zmiana funkcjonalna, techniczna lub organizacyjna, podlega ocenie pod kątem wpływu na bezpieczeństwo informacji.

2) Zmiany są planowane i wdrażane w sposób kontrolowany, z zachowaniem ciągłości działania oraz spójności zabezpieczeń.
3) Dokumentacja systemu jest aktualizowana w celu odzwierciedlenia wprowadzonych zmian.

6.4.6 Etap wycofania i likwidacji systemu

1) Wycofanie systemu z użytkowania odbywa się w sposób zaplanowany i udokumentowany.
2) Przed likwidacją zapewnia się ochronę informacji poprzez ich archiwizację, migrację lub trwałe usunięcie, zgodnie z obowiązującymi przepisami oraz wewnętrznymi regulacjami JST.
3) Zasoby techniczne wykorzystywane przez system są zwalniane lub niszczone w sposób uniemożliwiający odzyskanie informacji.

6.5 Uwagi

1) Regulacja nie musi być rozszerzana, możliwe obszary doprecyzowania (przykładowe):
   a) instrukcja wdrażania komponentów ICT (np. instalacji stacji roboczej, implementacji polityk),
   b) instrukcja wycofywania komponentów ICT (np. metoda likwidacji wycofanych / uszkodzonych nośników).

UWAGA: Za udokumentowaną informację uważa się również instrukcje audio-wizualne np. w postaci filmów pokazujących krok po kroku wykonanie zdania.

6.6 Metryka

Lp.	Zakres zmiany	Data przyjęcia i podstawa stosowania
1.	Utworzenie dokumentu	00-00-2026 Zarządzenie …

7. Bezpieczeństwo fizyczne i środowiskowe

7.1 Cel

Celem niniejszej procedury jest ustanowienie kompleksowych, jednolitych i trwałych zasad zapewnienia bezpieczeństwa fizycznego oraz środowiskowego w JST w odniesieniu do zasobów wykorzystywanych do przetwarzania informacji oraz realizacji zadań publicznych. Procedura ma na celu ochronę informacji, systemów technologii informacyjno-komunikacyjnych, infrastruktury technicznej oraz personelu JST przed zagrożeniami wynikającymi z nieuprawnionego dostępu fizycznego, niekorzystnych warunków środowiskowych, przerw w zasilaniu oraz innych zdarzeń mogących zakłócić poufność, integralność i dostępność informacji, a także ciągłość funkcjonowania JST. Podstawy prawne określone są w dokumencie Polityki Bezpieczeństwa.

7.2 Zakres stosowania

1) Procedura ma zastosowanie do wszystkich obiektów, pomieszczeń oraz obszarów użytkowanych przez JST, w których przetwarzane są informacje lub zlokalizowane są zasoby wspierające przetwarzanie informacji.
2) Procedura obejmuje w szczególności:
   a) budynki i pomieszczenia biurowe,
   b) pomieszczenia techniczne,
   c) obszary przeznaczone do przechowywania dokumentacji i nośników informacji,
   d) infrastrukturę zasilania oraz środowiska wspomagające funkcjonowanie systemów.
3) Procedura obowiązuje wszystkie komórki organizacyjne JST, kierownictwo, pracowników oraz osoby trzecie przebywające na terenie JST w zakresie wynikającym z ich roli i uprawnień.

7.3 Odpowiedzialności za procedurę

1) Kierownik JST odpowiada za zapewnienie warunków organizacyjnych i finansowych umożliwiających realizację niniejszej procedury.
2) Osoba odpowiedzialna za bezpieczeństwo informacji sprawuje nadzór nad spójnością procedury z systemem zarządzania bezpieczeństwem informacji oraz monitoruje jej skuteczność.
3) Kierownik komórki odpowiedzialnej za administrację obiektami i infrastrukturą techniczną odpowiada za wdrażanie i utrzymanie środków bezpieczeństwa fizycznego i środowiskowego.
4) Kierownicy komórek organizacyjnych odpowiadają za przestrzeganie zasad procedury w obszarach im podległych.
5) Pracownicy JST są zobowiązani do stosowania zasad bezpieczeństwa fizycznego i środowiskowego zgodnie z niniejszą procedurą.

7.4 Opis postępowania

7.4.1 Kontrola dostępu do obszarów

1) Określa się następujące obszary przetwarzania danych:
   a) **obszary ściśle chronione** – obszary obejmujące krytyczną infrastrukturę ICT oraz dane, do których dostęp mają wyłącznie osoby upoważnione.

Do obszarów zalicza się:

Serwerownie

Archiwa

[… wskazać – do samodzielnego uzupełnienia przez JST…]

Obszary służbowe

[… wskazać – do samodzielnego uzupełnienia przez JST …]

Obszary publiczne

[… wskazać – do samodzielnego uzupełnienia przez JST …]

2) Dostęp fizyczny do obiektów i pomieszczeń JST podlega kontroli w sposób adekwatny do znaczenia przetwarzanych informacji oraz krytyczności realizowanych w nich zadań.
3) Dostęp do obszarów JST jest przyznawany wyłącznie osobom uprawnionym i ograniczony do zakresu niezbędnego do wykonywania obowiązków służbowych.
4) Zasady dostępu uwzględniają rozróżnienie pomiędzy personelem JST a osobami trzecimi – zapewniają możliwość identyfikacji i rozliczalności dostępu fizycznego.

7.4.2 Wykazy obszarów

1) W JST prowadzi się aktualne wykazy obszarów, w których przetwarzane są informacje lub zlokalizowana jest infrastruktura wspierająca ich przetwarzanie.
2) Obszary te są klasyfikowane zgodnie z ich znaczeniem dla bezpieczeństwa informacji oraz ciągłości działania JST.
3) Wykazy obszarów podlegają okresowym przeglądom i aktualizacji w przypadku zmian organizacyjnych, technicznych lub lokalowych.

7.4.3 Separacja stref

1) Obszary JST są dzielone na strefy bezpieczeństwa o zróżnicowanym poziomie ochrony fizycznej.
2) Separacja stref ma na celu ograniczenie ryzyka nieuprawnionego dostępu do informacji oraz infrastruktury krytycznej.
3) Przemieszczanie się pomiędzy strefami odbywa się zgodnie z ustalonymi zasadami kontroli dostępu i nadzoru.

7.4.4 Zasilanie

1) JST zapewnia stabilne i bezpieczne źródła zasilania dla infrastruktury technicznej wspierającej przetwarzanie informacji.
2) Systemy zasilania są zaprojektowane i utrzymywane w sposób minimalizujący ryzyko przerw w dostępności usług i danych.
3) Zasilanie podlega regularnemu nadzorowi i utrzymaniu w celu zapewnienia ciągłości funkcjonowania JST.

7.4.5 Warunki środowiskowe

1) Warunki środowiskowe w pomieszczeniach, w których znajdują się zasoby przetwarzające informacje, są utrzymywane na poziomie zapewniającym ich bezpieczne i stabilne funkcjonowanie.
2) JST monitoruje czynniki środowiskowe mogące negatywnie wpłynąć na infrastrukturę techniczną i informacje.
3) Działania związane z utrzymaniem warunków środowiskowych są planowane i realizowane w sposób ciągły.

7.4.6 Redundancja urządzeń wspomagających warunki środowiskowe

1) JST zapewnia odpowiedni poziom redundancji urządzeń wspomagających utrzymanie właściwych warunków środowiskowych dla infrastruktury przetwarzającej informacje.
2) Redundancja ma na celu ograniczenie skutków awarii pojedynczych elementów infrastruktury oraz zapewnienie ciągłości działania.
3) Urządzenia wspomagające podlegają regularnym przeglądom oraz utrzymaniu technicznemu.

7.5 Uwagi

Regulacja nie musi być rozszerzana, możliwe obszary doprecyzowania (przykładowe) to szczegółowe schematy dostępu do pomieszczeń / obiektów / szaf itd.

7.6 Metryka

Lp.	Zakres zmiany	Data przyjęcia i podstawa stosowania
1.	Utworzenie dokumentu	00-00-2026 Zarządzenie …

7.7 Załączniki

Załącznik nr 1 Ewidencja wejść osób trzecich do obszarów chronionych

Lp.	Data	Godzina	Osoba / Firma	Cel wejścia

8. Bezpieczeństwo zasobów ludzkich – edukacja i podnoszenie świadomości

8.1 Cel

Celem niniejszej procedury jest ustanowienie spójnych, kompleksowych i trwałych zasad zapewnienia bezpieczeństwa informacji w obszarze zarządzania zasobami ludzkimi w JST na wszystkich etapach współpracy z personelem, począwszy od etapu poprzedzającego nawiązanie stosunku pracy lub innej formy współpracy, poprzez okres jej trwania, aż do momentu zakończenia zatrudnienia lub współpracy. Procedura ma na celu ograniczenie ryzyka dla poufności, integralności i dostępności informacji wynikających z działań lub zaniechań osób wykonujących zadania na rzecz JST, zapewnienie właściwego poziomu świadomości bezpieczeństwa informacji oraz ochronę interesu publicznego poprzez odpowiedzialne i kontrolowane zarządzanie dostępem do informacji i systemów. Podstawy prawne określone są w dokumencie Polityki Bezpieczeństwa.

8.2 Zakres stosowania

1) Procedura ma zastosowanie do wszystkich osób wykonujących zadania na rzecz JST, niezależnie od podstawy prawnej zatrudnienia lub współpracy.
2) Procedura obejmuje pracowników JST, osoby pełniące funkcje kierownicze, osoby czasowo delegowane, stażystów oraz inne osoby, którym powierzono dostęp do informacji lub zasobów JST.
3) Procedura ma zastosowanie również do osób współpracujących z JST za pośrednictwem podmiotów zewnętrznych, w zakresie wynikającym z powierzonych im zadań i dostępu do informacji.

8.3 Odpowiedzialności za procedurę

1) Kierownik JST odpowiada za ustanowienie i egzekwowanie zasad bezpieczeństwa zasobów ludzkich oraz za zapewnienie ich zgodności z obowiązującymi wymaganiami prawnymi i regulacyjnymi.
2) Osoba odpowiedzialna za bezpieczeństwo informacji sprawuje nadzór nad spójnością niniejszej procedury z systemem zarządzania bezpieczeństwem informacji oraz monitoruje jej skuteczność.
3) Komórka organizacyjna odpowiedzialna za sprawy kadrowe odpowiada za realizację czynności związanych z weryfikacją personelu, dokumentacją zobowiązań do zachowania poufności oraz procesami zakończenia współpracy.
4) Kierownicy komórek organizacyjnych odpowiadają za właściwy rozdział obowiązków, nadzór nad personelem oraz zapewnienie przestrzegania zasad bezpieczeństwa informacji w podległych obszarach.
5) Osoby wykonujące zadania na rzecz JST są zobowiązane do przestrzegania zasad bezpieczeństwa informacji określonych w niniejszej procedurze.

8.4 Opis postępowania

8.4.1 Weryfikacja personelu

1) Przed dopuszczeniem osoby do wykonywania zadań na rzecz JST przeprowadza się weryfikację jej wiarygodności w zakresie adekwatnym do planowanego zakresu obowiązków i dostępu do informacji zgodnie z obowiązującymi przepisami prawa oraz w zakresie uprawnień JST.
2) Weryfikacja personelu ma na celu potwierdzenie spełnienia wymagań formalnych, kompetencyjnych oraz etycznych niezbędnych do bezpiecznego wykonywania powierzonych zadań.
3) Zakres i sposób weryfikacji są dokumentowane i realizowane z poszanowaniem obowiązujących przepisów prawa.

8.4.2 Zobowiązania do zachowania poufności

1) Osoby wykonujące zadania na rzecz JST są zobowiązane do zachowania poufności informacji uzyskanych w związku z realizacją powierzonych im obowiązków.
2) Zobowiązanie do zachowania poufności ma charakter formalny i obowiązuje zarówno w okresie trwania współpracy, jak i po jej zakończeniu.
3) Zakres zobowiązań do zachowania poufności jest adekwatny do rodzaju i wrażliwości informacji, do których dana osoba uzyskuje dostęp.
4) Wzór dokumentu oświadczenia o zachowaniu poufności stanowi załącznik. *[do samodzielnego uzupełnienia przez JST]*

8.4.3 Umowy o zachowaniu poufności

1) W JST zawierane są odrębne umowy o zachowaniu poufności z osobami, którym powierzany jest dostęp do informacji o szczególnym znaczeniu oraz osobami nie zatrudnionymi na umowę o pracę.
2) Umowy o zachowaniu poufności określają zakres informacji objętych ochroną, obowiązki stron oraz konsekwencje naruszenia zobowiązań.
3) Zawarcie umowy o zachowaniu poufności jest warunkiem dopuszczenia do realizacji określonych zadań.

8.4.4 Rozdział obowiązków

1) W JST stosuje się zasadę rozdziału obowiązków w celu ograniczenia ryzyka nadużyć, błędów oraz nieuprawnionych działań.
2) Zakres obowiązków poszczególnych osób jest określany w sposób jednoznaczny i udokumentowany.
3) Rozdział obowiązków uwzględnia potrzebę zapewnienia kontroli wzajemnej oraz ciągłości realizacji zadań.

8.4.5 Szkolenia z zakresu bezpieczeństwa informacji

1) Osoby rozpoczynające współpracę z JST są objęte szkoleniem z zakresu bezpieczeństwa informacji, cyberbezpieczeństwa oraz ochrony danych osobowych.

2) Szkolenia mają na celu zapoznanie personelu z zasadami ochrony informacji, odpowiedzialnością wynikającą z dostępu do informacji oraz obowiązującymi procedurami.
3) Udział w szkoleniu jest dokumentowany i stanowi warunek pełnego dopuszczenia do wykonywania obowiązków.

8.4.6 Założenia systemu szkoleń

1) JST ustanawia system edukacji i podnoszenia świadomości w zakresie bezpieczeństwa informacji jako element stały i integralny systemu zarządzania bezpieczeństwem informacji.
2) Zakres i poziom działań edukacyjnych są dostosowane do ról, odpowiedzialności oraz dostępu do informacji poszczególnych grup pracowników.
3) Działania edukacyjne obejmują zarówno przekazywanie wiedzy, jak i kształtowanie postaw sprzyjających odpowiedzialnemu i bezpiecznemu postępowaniu z informacjami.

8.4.7 Planowanie szkoleń

1) W JST opracowuje się plan szkoleń z zakresu bezpieczeństwa informacji i cyberbezpieczeństwa.
2) Plan szkoleń określa zakres tematyczny, grupy docelowe, częstotliwość realizacji oraz formy działań edukacyjnych.
3) Plan szkoleń jest okresowo aktualizowany w celu uwzględnienia zmian w przepisach prawa, zagrożeniach, strukturze organizacyjnej oraz stosowanych rozwiązaniach technicznych.

8.4.8 Realizacja szkoleń okresowych

1) Szkolenia są realizowane w sposób zapewniający zrozumienie przekazywanych treści oraz ich odniesienie do obowiązków wykonywanych przez pracowników.
2) Oprócz szkoleń podstawowych JST prowadzi inne działania ukierunkowane na podnoszenie świadomości w zakresie bezpieczeństwa informacji.
3) Działania edukacyjne są prowadzone w sposób ciągły, a nie wyłącznie jednorazowy.

8.4.9 Dowody realizacji szkoleń

1) JST prowadzi dokumentację potwierdzającą realizację szkoleń i innych działań edukacyjnych.
2) Dokumentacja obejmuje informacje o zakresie szkolenia, terminie realizacji oraz uczestnikach.
3) Dowody realizacji szkoleń są przechowywane w sposób umożliwiający ich wykorzystanie do celów audytowych, kontrolnych oraz zarządczych.

8.4.10 Pomiar efektywności i kampanie świadomościowe

1) JST dokonuje okresowej oceny skuteczności działań edukacyjnych w zakresie bezpieczeństwa informacji.
2) Ocena efektywności obejmuje analizę poziomu wiedzy i świadomości pracowników oraz ich wpływu na ograniczenie ryzyk związanych z bezpieczeństwem informacji.
3) Wyniki pomiarów efektywności są wykorzystywane do doskonalenia planów szkoleń oraz metod edukacyjnych.
4) W JST mogą być prowadzone testy wiedzy w zakresie bezpieczeństwa informacji w celu weryfikacji skuteczności szkoleń.
5) JST realizuje okresowe kampanie informacyjne i świadomościowe mające na celu utrwalanie właściwych postaw oraz przypominanie o obowiązujących zasadach bezpieczeństwa.
6) Działania te są planowane i realizowane w sposób spójny z systemem zarządzania bezpieczeństwem informacji.

8.4.11 Zasady zakończenia współpracy i odejść

1) Zakończenie zatrudnienia lub współpracy z JST podlega sformalizowanej procedurze mającej na celu ochronę informacji i zasobów JST.
2) W ramach procesu odejścia zapewnia się zwrot wszelkich powierzonych zasobów, w tym zasobów niematerialnych związanych z dostępem do informacji.
3) Dostępy do informacji i systemów są cofane w sposób uporządkowany i terminowy, zgodnie z ustalonymi zasadami bezpieczeństwa.

8.5 Uwagi

Regulacja nie musi być rozszerzana, możliwe obszary doprecyzowania:

a) okresowe plany szkoleń,

b) lista obecności na szkoleniu,

c) Instrukcja dostępu do szkoleń / instrukcja obsługi platformy szkoleniowej

8.6 Metryka

Lp.	Zakres zmiany	Data przyjęcia i podstawa stosowania
1.	Utworzenie dokumentu	00-00-2026 Zarządzenie …

9. Bezpieczeństwo łańcucha dostaw

9.1 Cel

Celem niniejszej procedury jest ustanowienie jednolitych, kompleksowych i systemowych zasad oceny dostawców oraz zarządzania bezpieczeństwem łańcucha dostaw w JST, w sposób zapewniający ochronę informacji, ciągłość realizacji zadań publicznych oraz odporność JST na zakłócenia wynikające z zależności od podmiotów zewnętrznych. Procedura ma na celu identyfikację, ocenę oraz kontrolę ryzyk związanych z dostawcami produktów, usług i procesów wykorzystywanych przez JST, zarówno na etapie ich wyboru, jak i w trakcie trwania współpracy, z uwzględnieniem całego łańcucha dostaw. Podstawy prawne określone są w dokumencie Polityki Bezpieczeństwa.

9.2 Zakres stosowania

1) Procedura ma zastosowanie do wszystkich dostawców, podwykonawców oraz innych podmiotów zewnętrznych, które dostarczają JST produkty, usługi lub realizują procesy mające wpływ na bezpieczeństwo informacji, ciągłość działania lub realizację zadań publicznych. Procedura ma zastosowanie do zamówień, które ze względu na swoją specyfikę uzasadniają stosowanie podwyższonych wymagań w obszarze bezpieczeństwa.
2) Procedura obejmuje cały cykl współpracy z dostawcami, w tym etap wstępnej oceny, zawierania umów, monitorowania realizacji usług, okresowej oceny oraz zakończenia współpracy.
3) Procedura obowiązuje wszystkie komórki organizacyjne JST uczestniczące w procesach zakupowych, kontraktowych, nadzorczych oraz związanych z bezpieczeństwem informacji.
4) Procedura nie narusza przepisów ustawy Prawo zamówień publicznych.

9.3 Odpowiedzialności za procedurę

1) Kierownik JST odpowiada za zapewnienie funkcjonowania systemu oceny dostawców i łańcucha dostaw zgodnie z niniejszą procedurą.

2) Osoba odpowiedzialna za bezpieczeństwo informacji sprawuje nadzór nad uwzględnieniem wymagań bezpieczeństwa informacji w relacjach z dostawcami oraz nad spójnością procedury z systemem zarządzania bezpieczeństwem informacji.
3) Komórki organizacyjne odpowiedzialne za zamówienia, umowy i współpracę z dostawcami odpowiadają za stosowanie procedury na etapie wyboru i nadzoru nad dostawcami.
4) Kierownicy komórek merytorycznych odpowiadają za bieżącą ocenę jakości i bezpieczeństwa usług świadczonych przez dostawców w obszarach im podległych.

9.4 Opis postępowania

9.4.1 Wstępna ocena dostawców i łańcucha dostaw

1) Przed nawiązaniem współpracy z dostawcą JST przeprowadza wstępną ocenę dostawcy, a w uzasadnionych przypadkach, jego łańcucha dostaw.
2) Wstępna ocena obejmuje analizę zdolności dostawcy do realizacji przedmiotu współpracy w sposób bezpieczny, zgodny z wymaganiami prawnymi, organizacyjnymi i technicznymi JST.
3) W ramach oceny analizuje się posiadane przez dostawcę certyfikaty, stosowane normy oraz inne potwierdzenia dojrzałości organizacyjnej i technicznej w zakresie bezpieczeństwa informacji i ciągłości działania.
4) Ocena obejmuje również analizę kompletności oferowanego rozwiązania lub usługi, w tym zdolność dostawcy do zapewnienia wszystkich elementów niezbędnych do prawidłowej realizacji umowy.
5) JST dokonuje oceny zdolności finansowej i organizacyjnej dostawcy w zakresie zapewniającym stabilność i ciągłość świadczenia usług przez cały okres współpracy.

9.4.2 Ocena ryzyka związanych z dostawcami

1) Dla dostawców mających istotny wpływ na bezpieczeństwo informacji lub realizację zadań publicznych JST przeprowadza ocenę ryzyka związanego z ich udziałem w procesach JST.
2) Ocena ryzyka uwzględnia zależność JST od dostawcy, możliwość zastąpienia dostawcy, wpływ potencjalnych zakłóceń oraz ryzyka wynikające z dalszych ogniw łańcucha dostaw.

3) Wyniki oceny ryzyka są dokumentowane i wykorzystywane przy podejmowaniu decyzji o nawiązaniu lub kontynuowaniu współpracy.
4) Wyniki oceny ryzyka są przedstawiane do podpisu wraz z umową i są zatwierdzane przez osoby podpisujące umowę.

9.4.3 Wymagania umowne i warunki świadczenia usług

1) Umowy zawierane z dostawcami określają wymagania dotyczące bezpieczeństwa informacji, ciągłości świadczenia usług oraz odpowiedzialności stron.
2) Umowy zawierają warunki dotyczące poziomu świadczenia usług, w tym wymagania jakościowe, dostępnościowe oraz organizacyjne.
3) W umowach określa się zasady korzystania z podwykonawców oraz obowiązek zapewnienia przez dostawcę, aby podwykonawcy spełniali wymagania JST w zakresie bezpieczeństwa informacji.
4) Umowy regulują również zasady postępowania w przypadku incydentów oraz obowiązki informacyjne dostawcy wobec JST.

9.4.4 Plany wyjścia i ciągłość współpracy

1) JST zapewnia, aby współpraca z dostawcami była planowana w sposób umożliwiający kontrolowane i bezpieczne zakończenie współpracy.
2) Dla usług i produktów o istotnym znaczeniu opracowuje się warunki umożliwiające przeniesienie usług, danych lub procesów do innego dostawcy lub do struktur własnych JST.
3) Plany wyjścia uwzględniają ochronę informacji, zachowanie ciągłości działania oraz ograniczenie ryzyka organizacyjnego i finansowego.
4) JST okresowo analizuje ryzyko wynikające z umowy oraz plany wycofania się z usługi lub zapewnienia ciągłości działania w przypadku jej nieświadczenia.

9.4.5 Okresowa ocena dostawców i podwykonawców

1) W trakcie trwania współpracy JST prowadzi okresową ocenę dostawców – w uzasadnionych przypadkach podwykonawców.

2) Okresowa ocena obejmuje analizę jakości i terminowości realizowanych usług, poziomu spełnienia wymagań umownych oraz zgodności z wymaganiami bezpieczeństwa informacji.
3) Wyniki okresowych ocen są dokumentowane i wykorzystywane przy podejmowaniu decyzji dotyczących dalszej współpracy, renegocjacji warunków lub zakończenia umowy.

9.4.6 Nadzór nad poziomem świadczenia usług

1) JST sprawuje bieżący nadzór nad poziomem świadczenia usług przez dostawców w zakresie określonym w umowach.
2) Nadzór obejmuje monitorowanie realizacji zobowiązań, reagowanie na niezgodności oraz podejmowanie działań korygujących.
3) W przypadku stwierdzenia istotnych naruszeń lub obniżenia poziomu bezpieczeństwa JST podejmuje działania mające na celu ograniczenie ryzyka oraz zapewnienie ciągłości realizacji zadań publicznych.

9.5 Uwagi

Regulacja nie musi być rozszerzana – możliwe obszary doprecyzowania (przykładowe):

a) instrukcja szczegółowej oceny dostawców / poddostawców,
b) kryteria akceptowalności oceny,
c) rejestr podwykonawców ICT.

9.6 Metryka

Lp.	Zakres zmiany	Data przyjęcia i podstawa stosowania
1.	Utworzenie dokumentu	00-00-2026 Zarządzenie …

9.7 Załączniki

1) Załącznik nr 1 Szablon umowy NDA
2) Załącznik nr 2 Szablon oceny wstępnej wykonawcy oraz analizy ryzyka

Załącznik nr 1 Szablon umowy NDA

[do opracowania / stosowania we własnym zakresie – poniżej szablon]

UMOWA O ZACHOWANIU POUFNOŚCI

(Non-Disclosure Agreement – NDA)

zawarta w dniu …… r. w ……, pomiędzy:

[Pełna nazwa Jednostki Samorządu Terytorialnego],
z siedzibą w ……,
adres: ……,
NIP: ……, REGON: ……,
reprezentowaną przez:
……
zwaną dalej „JST” lub „Stroną Ujawniającą”,

a

[Pełna nazwa podmiotu / imię i nazwisko],
z siedzibą / miejscem zamieszkania w ……,
adres: ……,
NIP / PESEL: ……,
reprezentowaną / reprezentowanym przez:
……
zwaną / zwanym dalej „Stroną Otrzymującą”,

łącznie zwanymi dalej „Stronami”, a każda z osobna „Stroną”.

§ 1 Cel umowy

1. Celem niniejszej umowy jest określenie zasad ochrony informacji poufnych ujawnianych Stronie Otrzymującej w związku z:
   1) realizacją zadań publicznych JST,
   2) współpracą projektową, usługową lub doradczą,

3) dostępem do systemów informatycznych, dokumentacji lub infrastruktury JST.

2. Umowa stanowi realizację obowiązków JST wynikających w szczególności z:
   1) normy ISO/IEC 27001,
   2) dyrektywy NIS2 (UE) 2022/2555,
   3) ustawy o krajowym systemie cyberbezpieczeństwa,
   4) przepisów o ochronie danych osobowych oraz informacji niejawnych, o ile mają zastosowanie.

§ 2 Definicje

1. Informacje Poufne – wszelkie informacje, niezależnie od formy ich utrwalenia (pisemnej, ustnej, elektronicznej lub innej), które:
   1) dotyczą JST lub podmiotów z nią współpracujących,
   2) nie stanowią informacji publicznej,
   3) posiadają wartość informacyjną, organizacyjną, prawną, finansową, techniczną lub operacyjną.
2. Za Informacje Poufne uznaje się w szczególności:
   1) informacje o systemach teleinformatycznych, architekturze sieci, zabezpieczeniach,
   2) dane przetwarzane w systemach JST, w tym dane osobowe,
   3) dokumentację wewnętrzną, procedury, polityki bezpieczeństwa,
   4) informacje o incydentach bezpieczeństwa i podatnościach,
   5) informacje objęte analizą ryzyka lub planami ciągłości działania.
3. Incydent bezpieczeństwa – zdarzenie naruszające lub mogące naruszać poufność, integralność lub dostępność informacji.

§ 3 Zakres obowiązku poufności

1. Strona Otrzymująca zobowiązuje się do:
   1) zachowania w poufności wszystkich Informacji Poufnych,
   2) niewykorzystywania Informacji Poufnych w celach innych niż określone w § 1,
   3) nieujawniania Informacji Poufnych osobom trzecim bez uprzedniej pisemnej zgody JST.

2. Obowiązek poufności obejmuje również informacje uzyskane pośrednio lub w wyniku dostępu do systemów JST.
3. Strona Otrzymująca ponosi odpowiedzialność za działania lub zaniechania osób, którym udostępniła Informacje Poufne.

§ 4 Środki bezpieczeństwa informacji

1. Strona Otrzymująca zobowiązuje się stosować środki techniczne i organizacyjne nie niższe niż wymagane przez:
   1) ISO/IEC 27001,
   2) postanowienia dyrektywy NIS2, ustawę KSC, a także przepisy wykonawcze do tych aktów prawnych,
   3) wewnętrzne regulacje JST, o ile zostały jej przekazane.
2. W szczególności Strona Otrzymująca zobowiązuje się do:
   1) kontroli dostępu do Informacji Poufnych,
   2) zabezpieczenia systemów przed nieuprawnionym dostępem,
   3) stosowania zasad minimalizacji dostępu,
   4) niezwłocznego zgłaszania incydentów bezpieczeństwa.

§ 5 Zgłaszanie incydentów

1. Strona Otrzymująca zobowiązuje się niezwłocznie, nie później niż w ciągu 24 godzin, poinformować JST o każdym:
   1) naruszeniu poufności informacji,
   2) podejrzeniu incydentu bezpieczeństwa,
   3) utracie, kradzieży lub nieuprawnionym ujawnieniu informacji.
2. Zgłoszenie powinno zawierać co najmniej opis zdarzenia, zakres informacji oraz podjęte działania.

§ 6 Wyłączenia z obowiązku poufności

Obowiązek poufności nie dotyczy informacji, które:

1. były publicznie dostępne w chwili ich ujawnienia,

2. stały się publiczne bez naruszenia niniejszej umowy,
3. zostały ujawnione na podstawie bezwzględnie obowiązujących przepisów prawa lub prawomocnego orzeczenia sądu.

§ 7 Czas trwania obowiązku poufności

1. Umowa wchodzi w życie z dniem podpisania.
2. Obowiązek zachowania poufności obowiązuje przez okres [np. 5 lat] od dnia zakończenia współpracy, chyba że przepisy prawa wymagają dłuższego okresu ochrony.

§ 8 Odpowiedzialność

1. Naruszenie postanowień niniejszej umowy może skutkować:

1) odpowiedzialnością cywilną,
2) odpowiedzialnością dyscyplinarną,
3) odpowiedzialnością administracyjną lub karną, zgodnie z obowiązującymi przepisami.

2. JST zastrzega sobie prawo dochodzenia odszkodowania na zasadach ogólnych.

§ 9 Postanowienia końcowe

1. Wszelkie zmiany umowy wymagają formy pisemnej pod rygorem nieważności.
2. W sprawach nieuregulowanych zastosowanie mają przepisy prawa polskiego.
3. Spory wynikłe z umowy będą rozstrzygane przez sąd właściwy miejscowo dla siedziby JST.
4. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

Podpisy Stron:

Załącznik nr 2 Szablon oceny wstępnej wykonawcy – kluczowe zagadnienia

1) **Obszar organizacyjny (rejestrowy, reprezentacyjny)**
   a) Czy podmiot jest zarejestrowany w odpowiednim rejestrze (KRS, CEIDG lub równoważnym)?
   b) Czy struktura własnościowa i organizacyjna podmiotu jest przejrzysta oraz udokumentowana?
   c) Czy osoby reprezentujące podmiot posiadają umocowanie do zawierania umów w imieniu organizacji?
   d) Czy wobec podmiotu toczą się postępowania upadłościowe, restrukturyzacyjne lub likwidacyjne?
   e) Czy podmiot posiada wdrożone podstawowe polityki organizacyjne (np. regulamin organizacyjny, zasady odpowiedzialności)?
2) **Obszar technologiczny (certyfikaty, poufność informacji)**
   a) Czy podmiot posiada certyfikaty lub deklaruje zgodność z uznanymi normami bezpieczeństwa (np. ISO/IEC 27001, ISO 22301)?
   b) Czy stosowane są środki techniczne zapewniające poufność, integralność i dostępność informacji (np. szyfrowanie, kontrola dostępu)?
   c) Czy podmiot posiada procedury reagowania na incydenty bezpieczeństwa informacji?
   d) Czy dane przetwarzane są wyłącznie w środowiskach spełniających wymogi bezpieczeństwa (lokalnie lub w chmurze)?
   e) Czy podmiot regularnie aktualizuje systemy informatyczne i stosuje zabezpieczenia przed zagrożeniami cybernetycznymi?
3) **Obszar finansowy (sytuacja materialna)**
   a) Czy podmiot posiada stabilną sytuację finansową umożliwiającą realizację umowy przez cały okres jej obowiązywania?
   b) Czy w ostatnich latach podmiot generował dodatni wynik finansowy lub posiada zabezpieczone źródła finansowania?
   c) Czy wobec podmiotu prowadzone są postępowania egzekucyjne lub istnieją istotne zaległości publicznoprawne?

d) Czy podmiot posiada ubezpieczenie odpowiedzialności cywilnej związanej z zakresem świadczonych usług?

e) Czy ryzyko niewypłacalności podmiotu można uznać za niskie lub umiarkowane?

4) Obszar kompetencyjny (kompetencje, personel)

a) Czy podmiot zatrudnia pracowników lub współpracowników posiadających wymagane kwalifikacje do realizacji usługi?

b) Czy kluczowy personel posiada certyfikaty, uprawnienia lub doświadczenie adekwatne do zakresu umowy?

c) Czy organizacja zapewnia ciągłość kompetencji (np. zastępowalność kluczowych osób)?

d) Czy pracownicy są szkoleni w zakresie bezpieczeństwa informacji i ochrony danych?

e) Czy ryzyko błędów wynikających z braku kompetencji można uznać za niskie?

5) Obszar reputacyjny (referencje / opinie rynkowe)

a) Czy podmiot może przedstawić referencje od obecnych lub wcześniejszych klientów?

b) Czy dostępne opinie rynkowe wskazują na rzetelność i terminowość realizowanych usług?

c) Czy w przeszłości odnotowano istotne incydenty reputacyjne (np. naruszenia danych, spory publiczne)?

d) Czy podmiot jest postrzegany jako wiarygodny partner biznesowy w swojej branży?

e) Czy ryzyko reputacyjne związane z zawarciem umowy jest akceptowalne?

6) Obszar samodzielności realizacji usługi

a) Czy podmiot jest w stanie świadczyć usługę samodzielnie, bez angażowania dalszych podwykonawców?

b) Jeżeli wykorzystywani są podwykonawcy, czy są oni identyfikowani i podlegają kontroli?

c) Czy podmiot posiada procedury zarządzania podwykonawcami?

d) Czy odpowiedzialność za działania dalszych podwykonawców jest jednoznacznie określona?

e) Czy model realizacji usługi nie powoduje istotnego zwiększenia ryzyka operacyjnego lub prawnego?

10. Procedura dot. ciągłości działania systemów technologii informacyjno-komunikacyjnych wykorzystywanych w JST

10.1 Cel

Celem niniejszej procedury jest ustanowienie kompleksowych, spójnych i systemowych zasad zapewnienia ciągłości działania systemów technologii informacyjno-komunikacyjnych wykorzystywanych w JST, w szczególności w sytuacjach zakłóceń, awarii, incydentów bezpieczeństwa lub zdarzeń nadzwyczajnych. Procedura ma na celu zagwarantowanie nieprzerwanej lub możliwie najszybszej realizacji zadań publicznych JST, ochronę interesu publicznego oraz ograniczenie skutków zdarzeń wpływających na dostępność, integralność i poufność informacji oraz usług świadczonych przez JST. Podstawy prawne określone są w dokumencie Polityki Bezpieczeństwa.

10.2 Zakres stosowania

1) Procedura ma zastosowanie do wszystkich systemów technologii informacyjno-komunikacyjnych wykorzystywanych przez JST do realizacji zadań publicznych.
2) Procedura obejmuje systemy krytyczne, wspierające oraz pomocnicze, a także infrastrukturę techniczną, dane i zasoby niezbędne do ich funkcjonowania.
3) Procedura obowiązuje wszystkie komórki organizacyjne JST, kierownictwo, pracowników oraz osoby trzecie realizujące zadania na rzecz JST w zakresie wynikającym z powierzonych im obowiązków.

10.3 Odpowiedzialności za procedurę

1) Kierownik JST odpowiada za ustanowienie, wdrożenie oraz utrzymanie systemu zapewnienia ciągłości działania systemów technologii informacyjno-komunikacyjnych.

2) Osoba odpowiedzialna za bezpieczeństwo informacji koordynuje działania związane z planowaniem, wdrażaniem i doskonaleniem ciągłości działania w obszarze technologii informacyjno-komunikacyjnych.
3) Komórka organizacyjna odpowiedzialna za obsługę informatyczną odpowiada za techniczne przygotowanie systemów, utrzymanie konfiguracji minimalnych oraz realizację działań odtworzeniowych.
4) Kierownicy komórek organizacyjnych odpowiadają za współpracę przy analizie wpływu zakłóceń oraz za zapewnienie ciągłości procesów merytorycznych.
5) Pracownicy JST są zobowiązani do przestrzegania zasad ciągłości działania oraz do stosowania się do poleceń wydawanych w sytuacjach awaryjnych.

10.4 Opis postępowania

10.4.1 Zasady ogólne zapewnienia ciągłości działania

1) JST zapewnia ciągłość działania systemów technologii informacyjno-komunikacyjnych jako integralny element systemu zarządzania bezpieczeństwem informacji.
2) Zapewnienie ciągłości działania opiera się na identyfikacji procesów krytycznych, analizie ryzyk oraz planowaniu działań zapobiegawczych i odtworzeniowych.
3) Działania w zakresie ciągłości działania są proporcjonalne do znaczenia systemów i usług dla realizacji zadań publicznych.

10.4.2 Analiza wpływu na działalność

1) JST przeprowadza analizę wpływu zakłóceń systemów technologii informacyjno-komunikacyjnych na realizację zadań publicznych.
2) Analiza obejmuje identyfikację procesów krytycznych, systemów je wspierających oraz skutków ich niedostępności.
3) Wyniki analizy wpływu na działalność stanowią podstawę do określenia priorytetów odtwarzania systemów oraz wymagań dotyczących ich dostępności.

10.4.3 Określenie parametrów odtworzeniowych

1) Dla systemów technologii informacyjno-komunikacyjnych JST określa dopuszczalny czas przerwy w działaniu oraz dopuszczalny zakres utraty danych.
2) Parametry te są ustalane na podstawie analizy wpływu zakłóceń oraz znaczenia systemów dla realizacji zadań JST.
3) Określone parametry są dokumentowane i uwzględniane w planach ciągłości działania.

10.4.4 Minimalne konfiguracje i zasoby niezbędne do działania

1) JST definiuje minimalne konfiguracje techniczne systemów niezbędne do utrzymania podstawowych funkcji.
2) Minimalne konfiguracje obejmują zasoby sprzętowe, programowe, sieciowe oraz dane wymagane do uruchomienia systemów w trybie awaryjnym.
3) Konfiguracje minimalne są utrzymywane w stanie aktualnym oraz okresowo weryfikowane.

10.4.5 Scenariusze awaryjne

1) JST opracowuje scenariusze postępowania na wypadek wystąpienia zdarzeń zakłócających funkcjonowanie systemów technologii informacyjno-komunikacyjnych.
2) Scenariusze awaryjne uwzględniają różne rodzaje zakłóceń, w tym awarie techniczne, incydenty bezpieczeństwa oraz zdarzenia losowe.
3) Każdy scenariusz określa role, odpowiedzialności, kolejność działań oraz sposób komunikacji.

10.4.6 Działania w sytuacji zakłócenia ciągłości działania

1) W przypadku wystąpienia zakłócenia JST podejmuje działania zgodnie z właściwym scenariuszem awaryjnym.
2) Działania obejmują zabezpieczenie zasobów, uruchomienie konfiguracji minimalnych oraz odtworzenie kluczowych funkcji systemów.
3) Przebieg działań jest dokumentowany w celu zapewnienia rozliczalności i możliwości późniejszej analizy.

10.4.7 Odtwarzanie systemów i powrót do normalnego funkcjonowania

1) Odtwarzanie systemów odbywa się zgodnie z ustalonymi priorytetami oraz parametrami odtworzeniowymi.
2) Po przywróceniu podstawowych funkcji systemów JST realizuje działania mające na celu pełne odtworzenie środowiska pracy.
3) Powrót do normalnego funkcjonowania jest potwierdzany po weryfikacji poprawności działania systemów.

10.4.8 Testowanie planów ciągłości działania

1) JST prowadzi okresowe testy planów ciągłości działania systemów technologii informacyjno-komunikacyjnych.
2) Testy mają na celu sprawdzenie skuteczności procedur, przygotowania personelu oraz adekwatności konfiguracji minimalnych.
3) Wyniki testów są dokumentowane i analizowane.

10.5 Uwagi

Regulacja nie musi być rozszerzana o wszystkie pozycje, możliwe obszary doprecyzowania (przykładowe):

a) scenariusze postępowania (obowiązkowe),
b) MAC – Minimalna akceptowalna konfiguracja zasobów ICT niezbędnych do uruchomienia planów,
c) BIA – analiza wpływu na pracę określająca dopuszczalne przestoje i czasy odtworzenia,
d) lista osób koniecznych do uruchomienia planu,
e) lista osób zewnętrznych (tzw. interesantów) których trzeba koniecznie poinformować w przypadku incydentu,
f) lista mediów, które można poinformować o incydencie.

10.6 Metryka

Lp.	Zakres zmiany	Data przyjęcia i podstawa stosowania
1.	Utworzenie dokumentu	00-00-2026 Zarządzenie …

10.7 Załączniki

Załącznik nr 1 Procedura na wypadek zdarzenia w obszarze Cyberbezpieczeństwa *[do samodzielnego uzupełnienia przez JST]*.

10.8 Uwagi

Urząd powinien rozważyć wprowadzenie w obszarze ICT planów określonych w art. 26 rozporządzenia wykonawczego PE 1775/2024 – w szczególności wszystkie następujące scenariusze:

1) cyberataki i pracę awaryjną w trakcie przełączania się z głównej infrastruktury ICT na nadmiarowe zdolności, kopie zapasowe i urządzenia redundantne,
2) scenariusze, w których jakość pełnienia krytycznej lub istotnej funkcji pogarsza się do niedopuszczalnego poziomu lub funkcja ta przestaje być pełniona, a także należycie uwzględniają potencjalny wpływ niewypłacalności lub innych rodzajów awarii któregokolwiek z odnośnych zewnętrznych dostawców usług ICT,
3) częściowe lub całkowite awarie obiektów, w tym obiektów biurowych i lokali przedsiębiorstwa, oraz ośrodków przetwarzania danych,
4) poważną awarię zasobów ICT lub infrastruktury łączności,
5) niedostępność krytycznej liczby pracowników lub członków personelu odpowiedzialnych za zagwarantowanie ciągłości operacji,
6) wpływ zdarzeń związanych ze zmianą klimatu i degradacją środowiska, klęsk żywiołowych, pandemii i ataków fizycznych, w tym włamań i ataków terrorystycznych,

7) niestabilność polityczną i społeczną, w tym, w stosownych przypadkach, w jurysdykcji zewnętrznego dostawcy usług ICT oraz w lokalizacji, w której dane są przechowywane i przetwarzane,
8) ataki wewnętrzne,
9) przerwy w dostawie energii elektrycznej na szeroką skalę.

11. Monitorowanie ICT

11.1 Cel

Celem niniejszej procedury jest ustanowienie jednolitych, kompleksowych i systemowych zasad monitorowania oraz rejestrowania zdarzeń zachodzących w systemach technologii informacyjno-komunikacyjnych wykorzystywanych przez JST, w sposób zapewniający wczesne wykrywanie zdarzeń niepożądanych, skuteczne reagowanie na incydenty oraz możliwość analizy zdarzeń mających wpływ na bezpieczeństwo informacji i ciągłość realizacji zadań publicznych. Procedura ma na celu zapewnienie rozliczalności działań podejmowanych w systemach technologii informacyjno-komunikacyjnych, zwiększenie odporności JST na zagrożenia oraz spełnienie wymagań w zakresie nadzoru nad bezpieczeństwem informacji i cyberbezpieczeństwem. Podstawy prawne określone są w dokumencie Polityki Bezpieczeństwa.

11.2 Zakres stosowania

1) Procedura ma zastosowanie do wszystkich systemów technologii informacyjno-komunikacyjnych wykorzystywanych przez JST, niezależnie od ich lokalizacji, architektury technicznej oraz sposobu utrzymania.
2) Procedura obejmuje systemy świadczące usługi na rzecz JST, systemy wspierające realizację zadań publicznych oraz infrastrukturę techniczną służącą do przetwarzania informacji.
3) Procedura obowiązuje wszystkie komórki organizacyjne JST odpowiedzialne za eksploatację, utrzymanie, nadzór oraz bezpieczeństwo systemów technologii informacyjno-komunikacyjnych.

11.3 Odpowiedzialności za procedurę

1) Kierownik JST odpowiada za zapewnienie organizacyjnych i technicznych warunków umożliwiających skuteczne monitorowanie i rejestrowanie zdarzeń w systemach technologii informacyjno-komunikacyjnych.

2) Osoba odpowiedzialna za bezpieczeństwo informacji sprawuje nadzór nad zgodnością działań monitorujących z systemem zarządzania bezpieczeństwem informacji oraz nad wykorzystaniem wyników monitorowania do zarządzania ryzykiem.
3) Komórka organizacyjna odpowiedzialna za obsługę informatyczną odpowiada za wdrożenie, utrzymanie oraz prawidłowe funkcjonowanie mechanizmów monitorowania i rejestrowania zdarzeń.
4) Kierownicy komórek organizacyjnych odpowiadają za współpracę w zakresie identyfikacji zdarzeń istotnych dla realizowanych usług.
5) Pracownicy JST są zobowiązani do respektowania zasad monitorowania oraz do niepodejmowania działań mogących zakłócić prawidłowe funkcjonowanie mechanizmów rejestrowania zdarzeń.

11.4 Opis postępowania

11.4.1 Rejestrowanie zdarzeń w systemach technologii informacyjno-komunikacyjnych

1) Systemy technologii informacyjno-komunikacyjnych JST są objęte obowiązkiem rejestrowania zdarzeń istotnych z punktu widzenia bezpieczeństwa informacji, ciągłości działania oraz rozliczalności.
2) Rejestry zdarzeń obejmują zdarzenia związane z funkcjonowaniem usług, dostępem do systemów, przetwarzaniem informacji oraz zmianami w konfiguracji systemów.
3) Zakres rejestrowanych zdarzeń jest dostosowany do charakteru danej usługi, jej znaczenia dla JST oraz poziomu ryzyka związanego z jej funkcjonowaniem.
4) Rejestry zdarzeń są prowadzone w sposób umożliwiający ich późniejszą analizę, korelację oraz wykorzystanie w postępowaniach wyjaśniających.

11.4.2 Typy zdarzeń rejestrowanych dla usług

1) Dla każdej usługi świadczonej przy użyciu systemów technologii informacyjno-komunikacyjnych określa się kategorie zdarzeń podlegających rejestrowaniu.

2) Kategorie zdarzeń obejmują zdarzenia eksploatacyjne, zdarzenia związane z bezpieczeństwem informacji oraz zdarzenia mogące wskazywać na nieprawidłowe lub nieautoryzowane działania.
3) Zakres rejestrowania zdarzeń jest okresowo weryfikowany w celu zapewnienia jego adekwatności do aktualnych zagrożeń i wymagań organizacyjnych.

11.4.3 Wskaźniki progowe i wykrywanie nieprawidłowości

1) JST określa wskaźniki progowe dla zdarzeń rejestrowanych w systemach technologii informacyjno-komunikacyjnych.
2) Wskaźniki progowe służą do identyfikacji sytuacji mogących świadczyć o naruszeniu bezpieczeństwa informacji, obniżeniu jakości usług lub zagrożeniu ciągłości działania.
3) Przekroczenie ustalonych progów skutkuje uruchomieniem działań analitycznych oraz w uzasadnionych przypadkach, procedur reagowania na incydenty.
4) Wskaźniki progowe podlegają okresowemu przeglądowi i dostosowaniu do zmieniających się warunków technicznych i organizacyjnych.

11.4.4 Centralne gromadzenie i analiza zdarzeń

1) JST zapewnia funkcjonowanie rozwiązania umożliwiającego centralne gromadzenie, korelację oraz analizę zdarzeń pochodzących z wielu systemów technologii informacyjno-komunikacyjnych.
2) Centralna analiza zdarzeń umożliwia identyfikację zależności pomiędzy zdarzeniami, wykrywanie anomalii oraz ocenę skali i skutków potencjalnych zagrożeń.
3) Wyniki analizy są wykorzystywane do bieżącego zarządzania bezpieczeństwem informacji oraz do doskonalenia mechanizmów ochronnych.
4) Wszystkie dzienniki zdarzeń są przechowywane przez okres co najmniej dwóch lat, zgodnie z obowiązującymi JST przepisami prawa.

11.4.5 Nadzór operacyjny nad bezpieczeństwem systemów

1) JST zapewnia zorganizowany nadzór operacyjny nad bezpieczeństwem systemów technologii informacyjno-komunikacyjnych, realizowany w sposób ciągły lub okresowy, w zależności od krytyczności systemów.
2) Nadzór obejmuje obserwację zdarzeń, analizę alertów oraz koordynację działań w przypadku wykrycia zagrożeń.
3) Nadzór operacyjny może być realizowany przez wyspecjalizowane struktury organizacyjne JST lub przez podmioty zewnętrzne działające na podstawie zawartych umów, przy zachowaniu odpowiedzialności JST za bezpieczeństwo informacji.

11.4.6 Przechowywanie i ochrona rejestrów zdarzeń

1) Rejestry zdarzeń są przechowywane przez okres umożliwiający realizację celów bezpieczeństwa, audytu oraz rozliczalności, zgodnie z obowiązującymi przepisami i regulacjami wewnętrznymi.
2) Dostęp do rejestrów zdarzeń jest ograniczony do osób upoważnionych i podlega kontroli.
3) Rejestry zdarzeń są chronione przed nieuprawnioną modyfikacją, usunięciem lub ujawnieniem.

11.5 Uwagi

Regulacja nie musi być rozszerzana, możliwe obszary doprecyzowania (przykładowe):

a) obszary monitoringu oraz wskaźniki pomiaru (akceptowalności),
b) rejestr – zakres monitorowania, czas retencji logów itd.

11.6 Metryka

Lp.	Zakres zmiany	Data przyjęcia i podstawa stosowania
1.	Utworzenie dokumentu	00-00-2026 Zarządzenie …

12. Audyty wewnętrzne i zewnętrzne w JST

12.1 Cel

Celem niniejszej procedury jest ustanowienie jednolitych, systemowych i udokumentowanych zasad planowania, realizacji oraz wykorzystywania wyników audytów wewnętrznych i zewnętrznych w JST, w sposób zapewniający stałą ocenę skuteczności środków bezpieczeństwa informacji, zgodności z obowiązującymi wymaganiami prawnymi i normatywnymi oraz ciągłe doskonalenie systemu zarządzania bezpieczeństwem informacji. Procedura ma na celu zapewnienie, aby audyty stanowiły narzędzie nadzorcze i doskonalące, umożliwiające identyfikację niezgodności, słabości oraz obszarów wymagających poprawy, a także potwierdzenie adekwatności i skuteczności stosowanych zabezpieczeń organizacyjnych, technicznych i fizycznych. Podstawy prawne określone są w dokumencie Polityki Bezpieczeństwa.

12.2 Zakres stosowania

1) Procedura ma zastosowanie do wszystkich obszarów działalności JST objętych systemem zarządzania bezpieczeństwem informacji.
2) Procedura obejmuje audyty wewnętrzne realizowane przez JST oraz audyty zewnętrzne realizowane przez uprawnione i niezależne podmioty.
3) Procedura dotyczy również audytów specjalistycznych, w tym audytów technicznych oraz testów bezpieczeństwa systemów technologii informacyjno-komunikacyjnych.
4) Procedura obowiązuje wszystkie komórki organizacyjne JST oraz osoby uczestniczące w planowaniu, realizacji i obsłudze audytów.

12.3 Odpowiedzialności za procedurę

1) Kierownik JST odpowiada za zapewnienie realizacji audytów wewnętrznych i zewnętrznych oraz za wykorzystanie ich wyników w procesie zarządzania bezpieczeństwem informacji.

2) Osoba odpowiedzialna za bezpieczeństwo informacji odpowiada za opracowanie programu audytów, koordynację ich realizacji oraz nadzór nad wdrażaniem działań korygujących i doskonalących.
3) Komórki organizacyjne JST są zobowiązane do współpracy w trakcie audytów oraz do udostępniania informacji i dokumentacji niezbędnej do ich przeprowadzenia.
4) Audytorzy wewnętrzni odpowiadają za rzetelne, obiektywne i niezależne przeprowadzenie audytów zgodnie z zatwierdzonym programem.
5) Podmioty zewnętrzne realizujące audyty odpowiadają za wykonanie powierzonych czynności zgodnie z umową oraz obowiązującymi standardami zawodowymi i wymaganiami JST.

12.4 Opis postępowania

12.4.1 Program audytów

1) W JST ustanawia się program audytów obejmujący audyty wewnętrzne i zewnętrzne.
2) Program audytów określa zakres, cele, częstotliwość oraz priorytety audytów, z uwzględnieniem wyników analizy ryzyk, znaczenia poszczególnych procesów oraz wcześniejszych wyników audytów.
3) Program audytów jest zatwierdzany przez kierownika JST i podlega okresowemu przeglądowi oraz aktualizacji.

12.4.2 Audyty wewnętrzne

1) Audyty wewnętrzne są planowane i realizowane w celu oceny zgodności funkcjonowania JST z przyjętymi regulacjami wewnętrznymi, wymaganiami normy ISO 27001 oraz obowiązującymi przepisami prawa.
2) Audyty wewnętrzne są prowadzone w sposób niezależny i obiektywny, przez osoby posiadające odpowiednie kompetencje.
3) Zakres audytu wewnętrznego obejmuje ocenę procesów, zabezpieczeń, dokumentacji oraz praktyk organizacyjnych związanych z bezpieczeństwem informacji.

12.4.3 Audyty zewnętrzne

1) Audyty zewnętrzne są zlecane w celu uzyskania niezależnej oceny poziomu bezpieczeństwa informacji oraz zgodności z wymaganiami prawnymi i normatywnymi.
2) Decyzja o zleceniu audytu zewnętrznego uwzględnia krytyczność obszarów objętych audytem oraz potrzebę obiektywnej weryfikacji.
3) Zakres audytu zewnętrznego jest określany w umowie i uzgadniany z JST przed rozpoczęciem prac.

12.4.4 Testy penetracyjne i audyty techniczne

1) W ramach audytów bezpieczeństwa systemów technologii informacyjno-komunikacyjnych JST przewiduje się realizację testów penetracyjnych oraz innych audytów technicznych.
2) Testy te mają na celu ocenę odporności systemów na zagrożenia oraz identyfikację podatności mogących prowadzić do naruszenia bezpieczeństwa informacji.
3) Zakres, harmonogram oraz zasady realizacji testów są planowane w sposób zapewniający bezpieczeństwo i ciągłość działania JST.

12.4.5 Ocena wyników audytów

1) Wyniki audytów wewnętrznych i zewnętrznych są dokumentowane w raportach audytowych.
2) Raporty zawierają ustalenia audytu, w tym stwierdzone niezgodności, obserwacje oraz wnioski dotyczące skuteczności stosowanych zabezpieczeń.
3) Wyniki audytów są analizowane przez kierownictwo JST oraz osobę odpowiedzialną za bezpieczeństwo informacji w celu określenia niezbędnych działań, które należy przeprowadzić natychmiast w przypadku niesatysfakcjonującego wyniku audytu lub w ramach przeglądu zarządzania SZBI.

12.4.6 Działania poaudytowe

1) Na podstawie wyników audytów JST określa działania korygujące i doskonalące.
2) Działania te są planowane, realizowane oraz monitorowane w sposób zapewniający usunięcie przyczyn stwierdzonych niezgodności.

3) Skuteczność działań poaudytowych podlega weryfikacji w ramach kolejnych audytów lub przeglądów.

12.4.7 Zlecanie audytów podmiotom zewnętrznym

1) Zlecanie audytów podmiotom zewnętrznym odbywa się z zachowaniem zasad przejrzystości, bezstronności oraz ochrony informacji JST.
2) Podmioty zewnętrzne są wybierane z uwzględnieniem ich kompetencji, doświadczenia oraz zdolności do zapewnienia poufności informacji.
3) Umowy z podmiotami zewnętrznymi regulują zakres audytu, obowiązki stron oraz zasady postępowania z informacjami uzyskanymi w trakcie audytu.

12.4.8 Kompetencje i niezależność audytora

1) Audyty wewnętrzne i zewnętrzne w JST są realizowane wyłącznie przez osoby lub podmioty posiadające kompetencje niezbędne do rzetelnej, obiektywnej i profesjonalnej oceny systemu zarządzania bezpieczeństwem informacji oraz stosowanych środków bezpieczeństwa.
2) Kompetencje audytora obejmują wiedzę z zakresu:
   a) zasad zarządzania bezpieczeństwem informacji,
   b) obowiązujących przepisów prawa w zakresie cyberbezpieczeństwa i ochrony informacji,
   c) norm i dobrych praktyk dotyczących bezpieczeństwa informacji,
   d) funkcjonowania systemów technologii informacyjno-komunikacyjnych oraz procesów organizacyjnych JST.
3) Audytor posiada doświadczenie umożliwiające ocenę adekwatności, skuteczności i spójności zabezpieczeń organizacyjnych, technicznych i fizycznych, w odniesieniu do ryzyk występujących w JST.
4) JST wymaga od Audytora zewnętrznego posiadania certyfikatu określonego Rozporządzeniem Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U. 2018 poz. 1999).

5) Audytor realizujący audyt wewnętrzny jest niezależny od obszaru działalności podlegającego audytowi i nie uczestniczy w projektowaniu, wdrażaniu ani utrzymywaniu ocenianych zabezpieczeń lub procesów.
6) Niezależność audytora oznacza brak konfliktu interesów, który mógłby wpłynąć na bezstronność, obiektywność lub wiarygodność wyników audytu.
7) Audytor nie podlega naciskom organizacyjnym, służbowym ani osobistym, które mogłyby mieć wpływ na przebieg audytu lub formułowanie jego wyników.
8) W przypadku audytów zewnętrznych JST zapewnia wybór podmiotu audytującego, który jest niezależny organizacyjnie i kapitałowo od JST oraz od dostawców ocenianych rozwiązań, usług lub procesów.
9) Kompetencje i niezależność audytora są weryfikowane przed rozpoczęciem audytu, w szczególności na etapie planowania audytu oraz zawierania umowy z podmiotem zewnętrznym.
10) Audytor jest zobowiązany do zachowania poufności informacji uzyskanych w trakcie audytu oraz do wykorzystywania ich wyłącznie do celów realizacji audytu.
11) JST zapewnia, aby osoby pełniące rolę audytorów wewnętrznych miały możliwość stałego podnoszenia kwalifikacji oraz aktualizowania wiedzy w zakresie bezpieczeństwa informacji i cyberbezpieczeństwa.

12.5 Uwagi

Regulacja nie musi być rozszerzana, możliwe obszary doprecyzowania (przykładowe):

a) plan audytów,
b) wykaz audytorów z kompetencjami w obszarze ICT.

12.6 Metryka

Lp.	Zakres zmiany	Data przyjęcia i podstawa stosowania
1.	Utworzenie dokumentu	00-00-2026 Zarządzenie …

13. Cyberhigiena systemów technologii informacyjno-komunikacyjnych wykorzystywanych w JST

13.1 Cel

Celem niniejszej procedury jest ustanowienie jednolitych, systemowych i trwałych zasad zapewnienia cyberhigieny systemów technologii informacyjno-komunikacyjnych wykorzystywanych w JST, w całym okresie ich eksploatacji. Procedura ma na celu ograniczenie podatności systemów na zagrożenia, zwiększenie ich odporności na incydenty cyberbezpieczeństwa oraz zapewnienie właściwego poziomu ochrony poufności, integralności i dostępności informacji poprzez stosowanie ustandaryzowanych, bezpiecznych konfiguracji oraz skutecznego zarządzania poprawkami. Podstawy prawne określone są w dokumencie Polityki Bezpieczeństwa.

13.2 Zakres stosowania

1) Procedura obejmuje pracowników JST, osoby pełniące funkcje kierownicze, osoby czasowo delegowane, stażystów oraz inne osoby, którym powierzono dostęp do informacji lub zasobów JST.
2) Procedura obejmuje wszystkie systemy teleinformatyczne, usługi ICT, procesy organizacyjne, dane, zasoby techniczne oraz zasoby ludzkie, które mają wpływ na realizację zadań publicznych JST.

13.3 Odpowiedzialności za procedurę

1) Kierownik JST odpowiada za zapewnienie warunków organizacyjnych i finansowych umożliwiających realizację zasad cyberhigieny systemów technologii informacyjno-komunikacyjnych.
2) Osoba odpowiedzialna za bezpieczeństwo informacji sprawuje nadzór nad spójnością niniejszej procedury z systemem zarządzania bezpieczeństwem informacji oraz nad skutecznością stosowanych środków ochronnych.

3) Komórka organizacyjna odpowiedzialna za obsługę informatyczną odpowiada za wdrażanie i utrzymanie bezpiecznych konfiguracji systemów oraz za realizację procesu zarządzania poprawkami.
4) Kierownicy komórek organizacyjnych odpowiadają za współpracę w zakresie planowania działań wpływających na funkcjonowanie systemów oraz za zapewnienie, aby użytkownicy przestrzegali obowiązujących zasad.
5) Pracownicy JST są zobowiązani do użytkowania systemów zgodnie z ustalonymi zasadami cyberhigieny oraz do niepodejmowania działań mogących obniżyć poziom ich bezpieczeństwa.

13.4 Opis postępowania

13.4.1 Ogólne zasady cyberhigieny systemów

1) JST zapewnia, aby wszystkie systemy technologii informacyjno-komunikacyjnych były konfigurowane i utrzymywane w sposób minimalizujący ryzyko potencjalnych zagrożeń, co dalej rozumie się pod pojęciem „Cyberhigieny”.
2) Cyberhigiena systemów stanowi element stały procesu zarządzania bezpieczeństwem informacji i jest uwzględniana na etapie projektowania, wdrażania oraz eksploatacji systemów.
3) Stosowane konfiguracje oraz praktyki utrzymaniowe są oparte na zasadzie ograniczonego zaufania oraz minimalizacji funkcji i usług niezbędnych do realizacji zadań JST.

13.4.2 Bezpieczna konfiguracja systemów

1) JST ustanawia wymagania dotyczące bezpiecznej konfiguracji systemów technologii informacyjno-komunikacyjnych.
2) Konfiguracja systemów zapewnia wyłączenie lub ograniczenie funkcji, usług i mechanizmów, które nie są niezbędne do realizacji ich przeznaczenia.
3) Ustawienia systemowe są dobierane w sposób zapewniający ochronę przed nieuprawnionym dostępem, nieautoryzowaną modyfikacją oraz niezamierzonym ujawnieniem informacji.

4) Bezpieczne konfiguracje są dokumentowane oraz okresowo weryfikowane pod kątem ich aktualności i skuteczności.

13.4.3 Zarządzanie poprawkami

1) JST ustanawia proces zarządzania poprawkami dla systemów technologii informacyjno-komunikacyjnych.
2) Proces zarządzania poprawkami obejmuje identyfikację dostępnych poprawek, ocenę ich wpływu na bezpieczeństwo oraz planowanie ich wdrażania.
3) Poprawki mające istotne znaczenie dla bezpieczeństwa są wdrażane w możliwie najkrótszym czasie, z uwzględnieniem konieczności zapewnienia ciągłości działania JST.
4) Wdrażanie poprawek jest realizowane w sposób kontrolowany i udokumentowany.

13.4.4 Utrzymanie spójności konfiguracji

1) JST zapewnia utrzymanie spójności konfiguracji systemów w całym okresie ich eksploatacji.
2) Zmiany konfiguracji są wprowadzane w sposób zaplanowany, kontrolowany i zgodny z obowiązującymi procedurami.
3) Po wprowadzeniu zmian konfiguracja systemu podlega weryfikacji pod kątem zgodności z wymaganiami cyberhigieny.

13.4.5 Monitorowanie skuteczności cyberhigieny

1) JST okresowo ocenia skuteczność stosowanych praktyk cyberhigieny systemów technologii informacyjno-komunikacyjnych.
2) Ocena obejmuje analizę podatności, zgodność konfiguracji z przyjętymi wymaganiami, wytycznymi producentów oraz skuteczność procesu zarządzania poprawkami.
3) Wyniki oceny są wykorzystywane do doskonalenia konfiguracji systemów oraz procesów utrzymaniowych.

13.5 Uwagi

Regulacja nie musi być rozszerzana, możliwe obszary doprecyzowania (przykładowe):

a) instrukcje implementacji polityk lokalnych (np. GPO),

b) zasady ograniczeń przepływów w sieciach,

c) inne ograniczenia i doprecyzowania we wszystkich obszarach zabezpieczeń.

13.6 Metryka

Lp.	Zakres zmiany	Data przyjęcia i podstawa stosowania
1.	Utworzenie dokumentu	00-00-2026 Zarządzenie …

14. Zasady stosowania mechanizmów kryptograficznych oraz zarządzania kluczami kryptograficznymi w JST

14.1 Cel

Celem niniejszej procedury jest ustanowienie jednolitych, systemowych i bezpiecznych zasad stosowania mechanizmów kryptograficznych oraz zarządzania kluczami kryptograficznymi w JST, w sposób zapewniający ochronę poufności, integralności i autentyczności informacji przetwarzanych, przechowywanych oraz przesyłanych z wykorzystaniem systemów technologii informacyjno-komunikacyjnych. Procedura ma na celu ograniczenie ryzyk związanych z nieuprawnionym dostępem do informacji, ich ujawnieniem, modyfikacją lub utratą, a także zapewnienie zgodności działań JST z wymaganiami systemu zarządzania bezpieczeństwem informacji oraz przepisami dotyczącymi cyberbezpieczeństwa. Podstawy prawne określone są w dokumencie Polityki Bezpieczeństwa.

14.2 Zakres stosowania

1) Procedura ma zastosowanie do wszystkich informacji przetwarzanych przez JST w postaci elektronicznej, niezależnie od ich rodzaju, nośnika, lokalizacji oraz sposobu przetwarzania.
2) Procedura obejmuje wszystkie systemy technologii informacyjno-komunikacyjnych wykorzystywane w JST, w tym systemy służące do przechowywania danych, transmisji danych oraz komunikacji elektronicznej.
3) Procedura obowiązuje wszystkie komórki organizacyjne JST oraz wszystkie osoby mające dostęp do informacji lub systemów objętych stosowaniem mechanizmów kryptograficznych.

14.3 Odpowiedzialności za procedurę

1) Kierownik JST odpowiada za zapewnienie warunków organizacyjnych i finansowych umożliwiających stosowanie mechanizmów kryptograficznych zgodnie z niniejszą procedurą.
2) Osoba odpowiedzialna za bezpieczeństwo informacji sprawuje nadzór nad zasadnością, spójnością i skutecznością stosowania kryptografii oraz nad zgodnością niniejszej procedury z systemem zarządzania bezpieczeństwem informacji.
3) Komórka organizacyjna odpowiedzialna za obsługę informatyczną odpowiada za techniczne wdrożenie mechanizmów kryptograficznych oraz za bezpieczne zarządzanie kluczami kryptograficznymi.
4) Kierownicy komórek organizacyjnych odpowiadają za zapewnienie stosowania zasad szyfrowania informacji w podległych im obszarach działalności.
5) Pracownicy JST są zobowiązani do stosowania mechanizmów kryptograficznych zgodnie z obowiązującymi zasadami oraz do ochrony powierzonych im kluczy i zabezpieczeń.

14.4 Opis postępowania

14.4.1 Ogólne zasady stosowania kryptografii

1) JST stosuje mechanizmy kryptograficzne jako podstawowy środek ochrony informacji o istotnym znaczeniu dla realizacji zadań publicznych oraz ochrony interesu publicznego.
2) Stosowanie kryptografii jest uzależnione od klasyfikacji informacji, wyników analizy ryzyk oraz wymagań prawnych i organizacyjnych.
3) Mechanizmy kryptograficzne są dobierane w sposób zapewniający adekwatny poziom bezpieczeństwa przez cały okres użytkowania informacji.
4) JST prowadzi rejestr wydanych i użytkowanych certyfikatów będący załącznikiem do niniejszej regulacji.

14.4.2 Szyfrowanie danych przechowywanych

1) Informacje przechowywane w systemach JST, które wymagają ochrony przed nieuprawnionym dostępem, są zabezpieczane poprzez szyfrowanie danych w stanie spoczynku.
2) Szyfrowanie danych przechowywanych obejmuje zarówno zasoby systemowe, jak i nośniki danych wykorzystywane do pracy bieżącej oraz archiwizacji.
3) Dostęp do danych chronionych kryptograficznie jest możliwy wyłącznie dla osób uprawnionych, po spełnieniu wymagań uwierzytelniających i autoryzacyjnych.

14.4.3 Szyfrowanie danych przesyłanych

1) Informacje przesyłane pomiędzy systemami JST lub pomiędzy JST, a innymi podmiotami są zabezpieczane poprzez szyfrowanie danych w trakcie transmisji.
2) Szyfrowanie transmisji danych obejmuje komunikację realizowaną za pośrednictwem sieci publicznych oraz sieci wewnętrznych.
3) Mechanizmy zabezpieczające transmisję zapewniają ochronę przed podsłuchem, modyfikacją danych oraz podszywaniem się pod strony komunikacji.

14.4.4 Zabezpieczenia przy przesyłaniu danych w usługach internetowych

1) JST zapewnia, aby usługi udostępniane z wykorzystaniem technologii internetowych były chronione mechanizmami kryptograficznymi zapewniającymi bezpieczną wymianę danych.
2) Dane przekazywane pomiędzy użytkownikami a systemami JST są chronione przed nieuprawnionym dostępem oraz ingerencją w ich treść.
3) Stosowane zabezpieczenia są konfigurowane i utrzymywane w sposób zapobiegający wykorzystaniu słabych lub przestarzałych mechanizmów kryptograficznych.

14.4.5 Zabezpieczenia w komunikacji za pomocą poczty elektronicznej

1) Informacje przesyłane za pomocą poczty elektronicznej, które wymagają ochrony poufności, są zabezpieczane poprzez stosowanie mechanizmów kryptograficznych lub co najmniej zabezpieczenia silnym hasłem zgodnie z przyjętymi zasadami tworzenia haseł.

2) Pliki zawierające dane chronione są dodatkowo zabezpieczane w sposób uniemożliwiający dostęp do ich treści osobom nieuprawnionym.
3) Zasady zabezpieczania korespondencji elektronicznej są dostosowane do poziomu wrażliwości przesyłanych informacji.

14.4.6 Zarządzanie kluczami kryptograficznymi

1) JST ustanawia zasady bezpiecznego tworzenia, przechowywania, wykorzystywania, odnawiania oraz unieważniania kluczy kryptograficznych.
2) Klucze kryptograficzne są chronione przed nieuprawnionym ujawnieniem, skopiowaniem lub modyfikacją.
3) Dostęp do kluczy kryptograficznych jest ograniczony wyłącznie do osób upoważnionych, w zakresie niezbędnym do realizacji ich obowiązków.
4) Cykl życia kluczy kryptograficznych jest dokumentowany i nadzorowany w celu zapewnienia ciągłości ochrony informacji zgodnie z prowadzoną ewidencją.

14.4.7 Nadzór i doskonalenie stosowania kryptografii

1) JST okresowo, w ramach audytów wewnętrznych ocenia skuteczność stosowanych mechanizmów kryptograficznych oraz zasad zarządzania kluczami.
2) Ocena obejmuje zgodność z wymaganiami bezpieczeństwa informacji, aktualność stosowanych rozwiązań oraz odporność na znane zagrożenia.
3) Wyniki ocen są wykorzystywane do doskonalenia stosowanych zabezpieczeń kryptograficznych.

14.5 Uwagi

Regulacja nie musi być rozszerzana, możliwe obszary doprecyzowania (przykładowe):

a) wykaz stosowanych kluczy kryptograficznych z zastosowaniem i parametrami,
b) wykaz osób posiadających klucze kryptograficzne z zastosowaniem i parametrami,
c) wykaz osób posiadających certyfikaty kwalifikowane wraz z dostępami,
d) wykaz pieczęci kryptograficznych.

14.6 Metryka

Lp.	Zakres zmiany	Data przyjęcia i podstawa stosowania
1.	Utworzenie dokumentu	00-00-2026 Zarządzenie …

14.7 Załączniki

Załącznik nr 1 Wykaz kluczy kryptograficznych

Lp.	Nazwa klucza	Zastosowanie	Wydany dla	Ważny do	Odpowiedzialność	Uwagi

15. Bezpieczna komunikacja MFA

15.1 Cel

Celem niniejszej procedury jest ustanowienie jednolitych, systemowych i bezpiecznych zasad prowadzenia komunikacji w JST, w szczególności komunikacji realizowanej z wykorzystaniem systemów technologii informacyjno-komunikacyjnych oraz sieci publicznych. Procedura ma na celu zapewnienie ochrony poufności, integralności, dostępności oraz autentyczności informacji przekazywanych w procesach komunikacyjnych, ograniczenie ryzyk związanych z nieuprawnionym dostępem do treści komunikacji oraz zapewnienie zgodności z wymaganiami systemu zarządzania bezpieczeństwem informacji i przepisami dotyczącymi cyberbezpieczeństwa. Podstawy prawne określone są w dokumencie Polityki Bezpieczeństwa.

15.2 Zakres stosowania

1) Procedura ma zastosowanie do wszystkich form komunikacji realizowanej w JST w związku z wykonywaniem zadań publicznych.
2) Procedura obejmuje komunikację wewnętrzną oraz zewnętrzną, prowadzoną przy użyciu systemów informatycznych, sieci teleinformatycznych oraz usług dostępnych z wykorzystaniem sieci publicznej.
3) Procedura obowiązuje wszystkie komórki organizacyjne JST, kierownictwo, pracowników oraz osoby trzecie, którym powierzono prowadzenie komunikacji w imieniu JST.

15.3 Odpowiedzialności za procedurę

1) Kierownik JST odpowiada za zapewnienie warunków organizacyjnych i technicznych umożliwiających bezpieczną komunikację w JST.
2) Osoba odpowiedzialna za bezpieczeństwo informacji sprawuje nadzór nad spójnością zasad bezpiecznej komunikacji z systemem zarządzania bezpieczeństwem informacji oraz nad ich skutecznością.

3) Komórka organizacyjna odpowiedzialna za obsługę informatyczną odpowiada za wdrożenie i utrzymanie technicznych środków zabezpieczających komunikację.
4) Kierownicy komórek organizacyjnych odpowiadają za stosowanie zasad bezpiecznej komunikacji w podległych im obszarach.
5) Pracownicy JST są zobowiązani do prowadzenia komunikacji zgodnie z niniejszą procedurą oraz do korzystania wyłącznie z autoryzowanych kanałów komunikacji.

15.4 Opis postępowania

15.4.1 Zasady komunikacji w autoryzowanych kanałach

1) Komunikacja służbowa w JST jest prowadzona wyłącznie za pośrednictwem kanałów komunikacyjnych zatwierdzonych przez JST.
2) Autoryzowane kanały komunikacji są dobierane w sposób uwzględniający rodzaj przekazywanych informacji, ich wrażliwość oraz poziom ryzyka związanego z komunikacją.
3) Korzystanie z nieautoryzowanych kanałów komunikacji do celów służbowych jest niedozwolone.

15.4.2 Ochrona poufności i integralności komunikacji

1) JST zapewnia, aby komunikacja realizowana z wykorzystaniem systemów informatycznych była chroniona przed nieuprawnionym dostępem oraz ingerencją w jej treść.
2) Ochrona komunikacji obejmuje stosowanie mechanizmów kryptograficznych zapewniających poufność i integralność danych na całej drodze ich przekazu pomiędzy nadawcą a odbiorcą.
3) Mechanizmy ochronne są dobierane w sposób zapewniający odporność na znane zagrożenia oraz adekwatny poziom bezpieczeństwa.

15.4.3 Uwierzytelnianie użytkowników i kontrola dostępu

1) Dostęp do systemów wykorzystywanych do komunikacji w JST jest chroniony poprzez stosowanie silnych mechanizmów uwierzytelniania.

2) W systemach o podwyższonym znaczeniu dla bezpieczeństwa informacji stosuje się uwierzytelnianie wieloskładnikowe.
3) Uprawnienia do korzystania z systemów komunikacyjnych są przyznawane zgodnie z zakresem obowiązków użytkownika i podlegają okresowej weryfikacji.

15.4.4 Bezpieczna komunikacja z wykorzystaniem sieci publicznej

1) Systemy JST dostępne z wykorzystaniem sieci publicznej są zabezpieczone w sposób zapewniający bezpieczną komunikację z użytkownikami.
2) Komunikacja realizowana za pośrednictwem sieci publicznej jest chroniona przed podsłuchem, modyfikacją oraz podszywaniem się pod strony komunikacji.
3) Dostęp do systemów udostępnianych w sieci publicznej jest ograniczony do osób uprawnionych i realizowany zgodnie z obowiązującymi zasadami bezpieczeństwa.

15.4.5 Bezpieczna komunikacja w systemach dostępnych przez sieć publiczną

1) JST zapewnia, aby systemy informatyczne udostępniane użytkownikom zewnętrznym lub wewnętrznym przez sieć publiczną były projektowane i utrzymywane z uwzględnieniem zasad bezpiecznej komunikacji.
2) Wymiana informacji pomiędzy systemami oraz pomiędzy użytkownikami a systemami jest zabezpieczona mechanizmami chroniącymi przed nieuprawnionym dostępem i utratą danych.
3) Konfiguracja systemów jest okresowo weryfikowana w celu utrzymania odpowiedniego poziomu bezpieczeństwa komunikacji.

15.4.6 Nadzór nad komunikacją i doskonalenie zabezpieczeń

1) JST sprawuje nadzór nad funkcjonowaniem systemów i kanałów komunikacyjnych w zakresie bezpieczeństwa informacji.
2) Zdarzenia mogące wskazywać na naruszenie bezpieczeństwa komunikacji są analizowane i obsługiwane zgodnie z obowiązującymi procedurami.
3) Wyniki analiz są wykorzystywane do doskonalenia zasad bezpiecznej komunikacji oraz stosowanych zabezpieczeń.

15.5 Uwagi

Regulacja nie musi być rozszerzana, możliwe obszary doprecyzowania (przykładowe):

a) wykaz kanałów komunikacji wraz ze stosowanymi zabezpieczeniami,

b) wykaz stosowanych narzędzi MFA oraz ich wykorzystania w systemach,

c) wykaz osób posiadających dostęp oraz zasoby MFA.

15.6 Metryka

Lp.	Zakres zmiany	Data przyjęcia i podstawa stosowania
1.	Utworzenie dokumentu	00-00-2026 Zarządzenie …

16. Aktywa w JST

16.1 Cel

Celem niniejszej procedury jest ustanowienie jednolitych, systemowych i udokumentowanych zasad zarządzania aktywami wykorzystywanymi w JST, w szczególności aktywami informacyjnymi, sprzętowymi oraz programowymi, w całym ich cyklu życia. Procedura ma na celu zapewnienie, aby wszystkie aktywa JST były jednoznacznie zidentyfikowane, zinwentaryzowane, przypisane do właścicieli oraz chronione w sposób adekwatny do ich znaczenia dla realizacji zadań publicznych, bezpieczeństwa informacji oraz ciągłości działania JST. Podstawy prawne określone są w dokumencie Polityki Bezpieczeństwa.

16.2 Zakres stosowania

1) Procedura ma zastosowanie do wszystkich aktywów wykorzystywanych przez JST w realizacji zadań publicznych.
2) Procedura obejmuje w szczególności:
   a) sprzęt teleinformatyczny oraz inny sprzęt techniczny,
   b) oprogramowanie systemowe i użytkowe,
   c) dane i informacje przetwarzane przez JST,
   d) aktywa majątkowe wykorzystywane do przetwarzania lub przechowywania informacji.
3) Procedura obowiązuje wszystkie komórki organizacyjne JST oraz wszystkie osoby korzystające z aktywów JST lub odpowiedzialne za ich utrzymanie.

16.3 Odpowiedzialności za procedurę

1) Kierownik JST odpowiada za ustanowienie i funkcjonowanie systemu zarządzania aktywami oraz za zapewnienie zasobów niezbędnych do jego realizacji.
2) Osoba odpowiedzialna za bezpieczeństwo informacji sprawuje nadzór nad spójnością zarządzania aktywami z systemem zarządzania bezpieczeństwem informacji.

3) Komórki organizacyjne JST odpowiadają za identyfikację, ewidencjonowanie oraz właściwe użytkowanie aktywów wykorzystywanych w ich obszarze działania.
4) Właściciele aktywów odpowiadają za ich właściwe wykorzystanie, ochronę oraz zgodność z zasadami określonymi w niniejszej procedurze.
5) Pracownicy JST są zobowiązani do korzystania z aktywów zgodnie z ich przeznaczeniem oraz obowiązującymi zasadami bezpieczeństwa.

16.4 Opis postępowania

16.4.1 Identyfikacja i inwentaryzacja aktywów

1) JST prowadzi systematyczną i aktualną inwentaryzację wszystkich aktywów wykorzystywanych do realizacji zadań publicznych.
2) Inwentaryzacja obejmuje sprzęt, oprogramowanie, dane oraz aktywa majątkowe związane z przetwarzaniem informacji.
3) Każde aktywo jest jednoznacznie identyfikowane oraz ujmowane w odpowiednich rejestrach prowadzonych przez JST.
4) Rejestry aktywów są aktualizowane w przypadku nabycia, modyfikacji, przeniesienia lub wycofania aktywa z użytkowania.
5) Określa się właścicieli aktywów.

16.4.2 Inwentaryzacja sprzętu i aktywów majątkowych

1) Sprzęt ICT wykorzystywany przez JST podlega ewidencji obejmującej jego rodzaj, przeznaczenie oraz lokalizację (zgodnie z wymaganiami §19 Rozporządzenia KRI).
2) Aktywa majątkowe związane z przetwarzaniem informacji są identyfikowane i przypisywane do właściwych komórek organizacyjnych.
3) Odpowiedzialność za sprzęt jest jednoznacznie przypisana do właściciela lub użytkownika.

16.4.3 Inwentaryzacja oprogramowania

1) JST prowadzi ewidencję oprogramowania wykorzystywanego w systemach technologii informacyjno-komunikacyjnych.

2) Ewidencja obejmuje informacje umożliwiające identyfikację oprogramowania oraz jego powiązanie z systemami i sprzętem.
3) Oprogramowanie jest użytkowane wyłącznie zgodnie z jego przeznaczeniem oraz obowiązującymi zasadami organizacyjnymi JST.

16.4.4 Inwentaryzacja danych i informacji

1) Dane i informacje przetwarzane przez JST są traktowane jako aktywa o szczególnym znaczeniu.
2) JST identyfikuje dane oraz miejsca ich przetwarzania i przechowywania.
3) Każde aktywo / proces przetwarzania danych posiada przypisanego właściciela odpowiedzialnego za jego ochronę i właściwe przetwarzanie.

16.4.5 Klasyfikacja danych i informacji

1) JST ustanawia zasady klasyfikacji danych i informacji w celu określenia wymaganego poziomu ich ochrony.
2) Klasyfikacja uwzględnia znaczenie informacji dla realizacji zadań publicznych, skutki ich ujawnienia, modyfikacji lub utraty.
3) Poziom ochrony informacji jest dostosowany do nadanej klasy.

16.4.6 Oznaczanie danych i informacji

1) Dane i informacje podlegające klasyfikacji są oznaczane w sposób umożliwiający ich jednoznaczną identyfikację.
2) Oznaczenia są stosowane w dokumentach, systemach oraz nośnikach danych zgodnie z przyjętymi zasadami.
3) Oznaczenie informacji stanowi podstawę do stosowania odpowiednich środków ochrony.

16.4.7 Postępowanie z aktywami i danymi

1) Aktywa JST są użytkowane, przechowywane i przekazywane w sposób zapewniający ich ochronę przed utratą, zniszczeniem lub nieuprawnionym dostępem.

2) Dane i informacje są przetwarzane zgodnie z nadaną klasyfikacją oraz obowiązującymi procedurami bezpieczeństwa.
3) Wycofanie aktywów z użytkowania odbywa się w sposób kontrolowany i udokumentowany, z zapewnieniem ochrony informacji.

16.5 Metryka

Lp.	Zakres zmiany	Data przyjęcia i podstawa stosowania
1.	Utworzenie dokumentu	00-00-2026 Zarządzenie …

16.6 Uwagi

Regulacja nie musi być rozszerzana, możliwe obszary doprecyzowania (przykładowe) to szczegółowy wykaz aktywów ICT (może być przechowywany w formie zewnętrznych systemów), właściciele, kolokacja itd.

16.7 Załączniki

Załącznik nr 1 Klasyfikacja informacji

Załącznik nr 1 Klasyfikacja informacji

1) **Informacje publiczne:**
   a) strony WWW,
   b) serwis BIP,
   c) …
2) **Informacje służbowe:**
   a) regulaminy i procedury,
   b) …
3) **Informacje prawnie chronione:**
   a) dane osobowe,
   b) dane finansowe,
   c) system Pesel („źródło”),
   d) …

Postępowanie z informacją

Kategoria Informacji	Informacje Publiczne	Informacje Prawnie Chronione	Informacje Służbowe
Oznaczanie	Nie jest wymagane specjalne oznaczenie poufności.	W uzasadnionych przypadkach mogą być stosowane etykiety z klauzulami "Poufne", "Dane Osobowe" itp.	W uzasadnionych przypadkach mogą być stosowane etykiety z klauzulami "Informacja Służbowa" lub "Do użytku wewnętrznego"
Przechowywanie	Przechowywać w ogólnodostępnych systemach Urzędu.	Przechowywać w zabezpieczonych systemach z kontrolą dostępu.	Przechowywać w systemach dostępnych dla pracowników Urzędu.

	Dostępne na stronach internetowych Urzędu lub w BIP.	Fizycznie w zamkniętych szafach lub pomieszczeniach.	Fizycznie w biurach, szafach biurowych.
Kopiowanie	Dozwolone bez ograniczeń z zachowaniem integralności danych.	Kopiowanie tylko za zgodą przełożonego i zgodnie z przepisami prawa. Kopie muszą być zabezpieczone tak jak oryginały.	Kopiowanie dozwolone w ramach potrzeb służbowych. Kopie powinny być chronione przed dostępem osób nieuprawnionych.
Usuwanie	Usuwanie zgodnie z ogólnymi zasadami archiwizacji.	Usuwanie poprzez trwałe niszczenie (niszczarka, nadpisanie danych). Zgodnie z instrukcją kancelaryjną.	Usuwanie zgodnie z wewnętrznymi procedurami archiwizacji i niszczenia dokumentów.
Udostępnianie Wewnętrzne	Dostępne dla wszystkich pracowników Urzędu.	Udostępniane tylko pracownikom posiadającym odpowiednie uprawnienia. Wymagana ewidencja udostępniania.	Dostępne dla pracowników Urzędu zgodnie z potrzebą wykonywania obowiązków.
Udostępnianie Zewnętrzne	Udostępniane bez ograniczeń, zgodnie z przepisami o dostępie do informacji publicznej.	Udostępnianie wyłącznie uprawnionym podmiotom na podstawie przepisów prawa lub umów. W uzasadnionych przypadkach może być wymagana umowa powierzenia przetwarzania danych lub klauzula poufności.	Udostępnianie na zewnątrz wymaga zgody przełożonego lub jest zabronione. W razie konieczności, wymagane jest podpisanie klauzuli poufności przez odbiorcę.

17. Kontrola dostępu

17.1 Cel

Celem niniejszej procedury jest ustanowienie jednolitych, systemowych i bezpiecznych zasad zarządzania tożsamościami oraz dostępami do systemów technologii informacyjno-komunikacyjnych i zasobów informacyjnych w JST. Procedura ma na celu zapewnienie, aby dostęp do informacji oraz systemów JST był przyznawany wyłącznie osobom uprawnionym, w zakresie niezbędnym do realizacji powierzonych im obowiązków, z zachowaniem zasad poufności, integralności, dostępności oraz rozliczalności działań użytkowników. Podstawy prawne określone są w dokumencie Polityki Bezpieczeństwa.

17.2 Zakres stosowania

1) Procedura ma zastosowanie do wszystkich systemów technologii informacyjno-komunikacyjnych wykorzystywanych przez JST, niezależnie od ich rodzaju, lokalizacji oraz sposobu utrzymania.
2) Procedura obejmuje wszystkich użytkowników systemów JST, w tym pracowników, kadrę kierowniczą oraz osoby trzecie, którym przyznano dostęp do systemów lub informacji JST.
3) Procedura ma zastosowanie do całego cyklu życia tożsamości użytkownika, począwszy od jej utworzenia, poprzez okres aktywnego korzystania z dostępu, aż do jego cofnięcia.

17.3 Odpowiedzialności za procedurę

1) Kierownik JST odpowiada za zapewnienie organizacyjnych i technicznych warunków umożliwiających skuteczne zarządzanie tożsamościami i dostępami.
2) Osoba odpowiedzialna za bezpieczeństwo informacji sprawuje nadzór nad spójnością niniejszej procedury z systemem zarządzania bezpieczeństwem informacji oraz nad skutecznością stosowanych mechanizmów kontroli dostępu.

3) Komórka organizacyjna odpowiedzialna za obsługę informatyczną odpowiada za techniczne wdrożenie mechanizmów zarządzania tożsamościami i dostępami oraz za ich bieżące utrzymanie.
4) Komórka odpowiedzialna za sprawy kadrowe odpowiada za przekazywanie informacji niezbędnych do prawidłowego nadawania, modyfikowania i cofania dostępów.
5) Kierownicy komórek organizacyjnych odpowiadają za wnioskowanie o nadanie, zmianę lub odebranie dostępów użytkownikom podległych im obszarów.
6) Użytkownicy systemów JST są zobowiązani do korzystania z przyznanych dostępów zgodnie z ich przeznaczeniem oraz do ochrony swoich danych uwierzytelniających.

17.4 Opis postępowania

17.4.1 Zarządzanie tożsamościami użytkowników

1) Każda osoba korzystająca z systemów JST posiada jednoznacznie zidentyfikowaną nazwę użytkownika (tożsamość).
2) Tożsamość użytkownika jest tworzona w sposób umożliwiający jednoznaczne przypisanie działań wykonywanych w systemach do konkretnej osoby.
3) Tworzenie tożsamości użytkownika następuje wyłącznie na podstawie udokumentowanego upoważnienia oraz informacji o zakresie obowiązków danej osoby.

17.4.2 Nadawanie dostępów

1) Dostępy do systemów i informacji JST są nadawane zgodnie z zasadą minimalnego zakresu uprawnień.
2) Zakres przyznanych dostępów jest bezpośrednio powiązany z zakresem obowiązków służbowych użytkownika.
3) Nadanie dostępu następuje po formalnym zatwierdzeniu przez kierownika komórki organizacyjnej oraz realizowane jest przez upoważnione osoby.

17.4.3 Modyfikacja i przegląd dostępów

1) Zmiana zakresu obowiązków użytkownika skutkuje niezwłoczną weryfikacją i dostosowaniem jego dostępów.
2) Wyniki przeglądów dostępów są dokumentowane i wykorzystywane do eliminowania zbędnych lub nadmiernych uprawnień.

17.4.4 Cofanie dostępów

1) Dostępy do systemów i informacji JST są cofane niezwłocznie po ustaniu podstawy do ich posiadania.
2) Cofnięcie dostępów obejmuje wszystkie systemy i zasoby, do których użytkownik miał przyznane uprawnienia.
3) Proces cofania dostępów jest realizowany w sposób uporządkowany i udokumentowany.

17.4.5 Uwierzytelnianie użytkowników

1) Dostęp do systemów JST jest chroniony mechanizmami uwierzytelniania zapewniającymi właściwy poziom bezpieczeństwa.
2) W systemach o podwyższonym znaczeniu dla bezpieczeństwa informacji stosuje się uwierzytelnianie wieloskładnikowe.
3) Dane uwierzytelniające użytkowników są chronione przed nieuprawnionym ujawnieniem, wykorzystaniem lub modyfikacją.

17.4.6 Kontrola i rozliczalność dostępu

1) JST zapewnia rejestrowanie działań użytkowników w systemach w zakresie umożliwiającym ich rozliczalność.
2) Rejestry dostępu są wykorzystywane do monitorowania zgodności korzystania z systemów z obowiązującymi zasadami.
3) Nieuprawnione próby dostępu lub naruszenia zasad są analizowane i obsługiwane zgodnie z obowiązującymi procedurami.
4) JST przeprowadza okresowe przeglądy przyznanych dostępów w celu potwierdzenia ich aktualności i zasadności.

17.4.7 Dostępy uprzywilejowane

1) Dostępy o podwyższonych uprawnieniach (np. administracyjne) są przyznawane w sposób szczególnie kontrolowany.
2) JST prowadzi ewidencję kont uprzywilejowanych.
3) Zakres i czas trwania dostępów uprzywilejowanych jest ograniczony do niezbędnego minimum.
4) Korzystanie z dostępów uprzywilejowanych podlega wzmożonemu nadzorowi i rejestrowaniu.

17.4.8 Zasady tworzenia i stosowania haseł użytkowników

1) JST ustanawia jednolite zasady tworzenia, stosowania oraz ochrony haseł użytkowników systemów technologii informacyjno-komunikacyjnych, jako podstawowego mechanizmu uwierzytelniania.
2) Hasła użytkowników są traktowane jako informacje poufne i podlegają ochronie przed ujawnieniem, przechwyceniem lub nieuprawnionym wykorzystaniem.
3) Użytkownicy są zobowiązani do samodzielnego tworzenia i przechowywania haseł w sposób uniemożliwiający dostęp do nich osobom trzecim.
4) Hasła użytkowników muszą zapewniać odpowiedni poziom odporności na próby odgadnięcia, przełamania lub wykorzystania w atakach automatycznych.
5) Określa się następujące zasady haseł:
   a) długość hasła,
   b) złożoność hasła,
   c) minimalny okres zmiany,
   d) maksymalny okres zmiany,
   e) historię haseł.
6) Zabrania się współdzielenia haseł pomiędzy użytkownikami oraz wykorzystywania tego samego hasła w różnych systemach JST.

17.4.9 Zasady tworzenia i stosowania haseł administracyjnych

1) Hasła administracyjne są traktowane jako informacje o podwyższonym znaczeniu dla bezpieczeństwa JST.
2) Dostępy administracyjne są zabezpieczane hasłami o zwiększonym poziomie złożoności i odporności na ataki.
3) Hasła administracyjne są przyznawane wyłącznie osobom upoważnionym, w zakresie niezbędnym do realizacji powierzonych im zadań.
4) Przechowywanie oraz wykorzystywanie haseł administracyjnych odbywa się w sposób ograniczający ryzyko ich ujawnienia lub nieuprawnionego użycia.
5) Użycie haseł administracyjnych podlega wzmożonemu nadzorowi oraz rejestrowaniu.
6) Określa się następujące zasady haseł:
   a) długość hasła,
   b) złożoność hasła,
   c) minimalny okres zmiany,
   d) maksymalny okres zmiany,
   e) historię haseł.

17.4.10 Uwierzytelnianie wieloskładnikowe

1) JST stosuje uwierzytelnianie wieloskładnikowe jako obowiązkowy mechanizm ochrony dostępu do systemów o istotnym znaczeniu dla bezpieczeństwa informacji wszędzie tam, gdzie jego zastosowanie jest możliwe.
2) Uwierzytelnianie wieloskładnikowe jest stosowane w szczególności dla:
   a) dostępów administracyjnych,
   b) systemów dostępnych z wykorzystaniem sieci publicznej,
   c) systemów przetwarzających informacje o podwyższonej wrażliwości.
3) Mechanizmy uwierzytelniania wieloskładnikowego są dobierane w sposób zapewniający wysoki poziom bezpieczeństwa oraz odporność na przejęcie pojedynczego składnika uwierzytelniającego.

17.4.11 Polityka haseł dla systemów dostępnych w sieci Internet

1) Systemy JST dostępne z wykorzystaniem sieci Internet podlegają zaostrzonym zasadom uwierzytelniania i ochrony haseł (stosowane polityki nie mogą być niższe niż polityki dla kont administracyjnych).
2) Dostęp do systemów dostępnych w sieci Internet wymaga stosowania mechanizmów kryptograficznych oraz uwierzytelniania wieloskładnikowego.
3) Hasła stosowane w systemach dostępnych w sieci Internet muszą zapewniać wysoki poziom odporności na ataki zdalne.
4) Dostępy administracyjne do systemów dostępnych w sieci Internet są zawsze zabezpieczone uwierzytelnianiem wieloskładnikowym.
5) Konfiguracja mechanizmów uwierzytelniania w systemach dostępnych w sieci Internet podlega regularnej weryfikacji pod kątem bezpieczeństwa.

17.5 Uwagi

Regulacja nie musi być rozszerzana, możliwe obszary doprecyzowania (przykładowe):

a) instrukcja obsługi systemu zgłoszeniowego do zmiany uprawnień,
b) wnioski o zmianę uprawnień,
c) lista osób z uprawnieniami,
d) lista osób z uprawnieniami administratora,
e) lista osób trzecich (spoza JST) mająca dostęp do systemów.

17.6 Metryka

Lp.	Zakres zmiany	Data przyjęcia i podstawa stosowania
1.	Utworzenie dokumentu	00-00-2026 Zarządzenie …

17.7 Załączniki

1) Załącznik nr 1 Wniosek o nadanie uprawnień
2) Załącznik nr 2 Karta nadania / wycofania uprawnień

3) Załącznik nr 3 Ewidencja kont administracyjnych

Załącznik nr 1 – Wniosek o nadanie uprawnień

WNIOSEK O NADANIE UPRAWNIEŃ

Imię i nazwisko pracownika: .....

Stanowisko: .....

Cel dostępu: .....

Zakres wymaganych uprawnień: .....

Okres trwania uprawnień: .....

Data i miejsce: .....

Podpis wnioskującego: .....

Zatwierdzenie:

[ ] Przełożony

[ ] Administrator / Dyrektor / Administrator systemu

Podpis i data: .....

Załącznik nr 2 – Karta nadania / wycofania uprawnień

KARTA NADANIA / WYCOFANIA UPRAWNIEŃ

Imię i nazwisko użytkownika: .....

Data nadania uprawnień: .....

Data cofnięcia uprawnień: .....

Zakres nadanych uprawnień: .....

Administrator 1 (nadający uprawnienia): .....

Podpis: ..... Data: .....

Administrator 2 (opcjonalnie): .....

Podpis: ..... Data: .....

Potwierdzenie użytkownika:

[ ] Odbyto instruktaż z zakresu zasad bezpieczeństwa i obsługi systemu

Data i podpis użytkownika: .....

Załącznik nr 3 Ewidencja kont administracyjnych

Lp.	Nazwa konta	Zastosowanie	Wydany dla	Ważny do	Do zasobu	Uwagi

18. Podatność JST na zagrożenia

18.1 Cel

Celem niniejszej procedury jest ustanowienie jednolitych, systemowych i udokumentowanych zasad identyfikowania, ujawniania, analizowania, obsługi oraz usuwania podatności, a także reagowania na zagrożenia bezpieczeństwa informacji w JST. Procedura ma na celu ograniczenie ryzyk dla poufności, integralności i dostępności informacji oraz zapewnienie odporności JST na zagrożenia poprzez terminowe i skuteczne działania organizacyjne i techniczne, zgodne z wymaganiami systemu zarządzania bezpieczeństwem informacji oraz przepisami dotyczącymi cyberbezpieczeństwa.

Podstawy prawne określone są w dokumencie Polityki Bezpieczeństwa.

18.2 Zakres stosowania

1) Procedura ma zastosowanie do wszystkich systemów technologii informacyjno-komunikacyjnych, urządzeń, oprogramowania oraz informacji wykorzystywanych przez JST.
2) Procedura obejmuje podatności i zagrożenia identyfikowane w środowisku technicznym JST, jak również informacje o podatnościach pochodzące ze źródeł zewnętrznych.
3) Procedura obowiązuje wszystkie komórki organizacyjne JST, kierownictwo, pracowników oraz osoby trzecie wykonujące zadania na rzecz JST w zakresie wynikającym z powierzonych im obowiązków.

18.3 Odpowiedzialności za procedurę

1) Kierownik JST odpowiada za zapewnienie warunków organizacyjnych i zasobów niezbędnych do skutecznego zarządzania podatnościami i zagrożeniami.
2) Osoba odpowiedzialna za bezpieczeństwo informacji sprawuje nadzór nad spójnością niniejszej procedury z systemem zarządzania bezpieczeństwem informacji oraz nad skutecznością jej stosowania.

3) Komórka organizacyjna odpowiedzialna za obsługę informatyczną odpowiada za identyfikację podatności technicznych, wdrażanie działań naprawczych oraz reagowanie na zagrożenia w środowisku technicznym.
4) Kierownicy komórek organizacyjnych odpowiadają za zgłaszanie zauważonych nieprawidłowości oraz współpracę przy realizacji działań wynikających z niniejszej procedury.
5) Pracownicy JST są zobowiązani do niezwłocznego zgłaszania podejrzeń wystąpienia podatności lub zagrożeń bezpieczeństwa informacji.

18.4 Opis postępowania

18.4.1 Identyfikacja i ujawnianie podatności

1) JST zapewnia systematyczną identyfikację podatności mogących mieć wpływ na bezpieczeństwo informacji oraz ciągłość realizacji zadań publicznych.
2) Podatności mogą być identyfikowane w wyniku działań własnych JST, informacji pochodzących od dostawców, podmiotów zewnętrznych lub użytkowników systemów.
3) JST ustanawia zasady bezpiecznego i uporządkowanego ujawniania informacji o podatnościach, zapewniające ochronę przed ich niekontrolowanym rozpowszechnianiem.
4) Informacje o podatnościach są rejestrowane i analizowane w sposób umożliwiający podjęcie adekwatnych działań.

18.4.2 Analiza i ocena podatności

1) Zidentyfikowane podatności podlegają analizie w celu określenia ich wpływu na bezpieczeństwo informacji oraz realizację zadań JST.
2) Klasyfikacja podatności oraz wpływu opiera się na klasyfikacji CVE dla każdej z podatności.
3) Analiza uwzględnia znaczenie systemu lub informacji, których dotyczy podatność, oraz możliwe skutki jej wykorzystania.

4) Wyniki analizy stanowią podstawę do określenia priorytetów działań oraz wyboru sposobu postępowania z podatnością.

18.4.3 Postępowanie z podatnościami

1) JST określa sposób postępowania z każdą zidentyfikowaną podatnością.
2) Postępowanie obejmuje decyzję o usunięciu podatności, ograniczeniu jej skutków lub zastosowaniu innych środków ochronnych.
3) Działania podejmowane w związku z podatnościami są planowane i realizowane w sposób zapewniający ciągłość działania JST.
4) W przypadku braku możliwości podjęcia działań w związku z ujawnionymi podatnościami, podatności oceniane są w ramach analizy ryzyk oraz podlegają przeglądom przez kierownictwo JST.

18.4.4 Usuwanie podatności

1) Usuwanie podatności jest realizowane w możliwie najkrótszym czasie, adekwatnie do poziomu ryzyk.
2) Działania naprawcze są wdrażane w sposób kontrolowany i zgodny z obowiązującymi procedurami.
3) Po usunięciu podatności przeprowadza się weryfikację skuteczności podjętych działań.

18.4.5 Monitorowanie zagrożeń

1) JST prowadzi bieżące monitorowanie zagrożeń mogących mieć wpływ na bezpieczeństwo systemów i informacji.
2) Monitorowanie obejmuje analizę zdarzeń, sygnałów ostrzegawczych oraz informacji o aktualnych zagrożeniach.
3) Informacje o zagrożeniach są wykorzystywane do aktualizacji działań ochronnych oraz doskonalenia zabezpieczeń.

18.4.6 Doskonalenie zarządzania podatnościami i zagrożeniami

1) JST okresowo dokonuje przeglądu skuteczności działań w zakresie zarządzania podatnościami i zagrożeniami.
2) Wyniki przeglądów są wykorzystywane do aktualizacji procedur, zabezpieczeń oraz planów działań.
3) Zarządzanie podatnościami i zagrożeniami stanowi proces ciągły i integralny element systemu zarządzania bezpieczeństwem informacji.

18.5 Metryka

Lp.	Zakres zmiany	Data przyjęcia i podstawa stosowania
1.	Utworzenie dokumentu	00-00-2026 Zarządzenie …

19. Incydenty w JST

19.1 Cel

Celem niniejszej procedury jest ustanowienie pełnych, jednoznacznych i systemowych zasad postępowania w przypadku wystąpienia incydentów bezpieczeństwa informacji oraz incydentów dotyczących systemów technologii informacyjno-komunikacyjnych w JST. Procedura ma na celu zapewnienie skutecznego wykrywania, zgłaszania, oceny, obsługi, eskalacji oraz dokumentowania incydentów, a także ograniczenie ich skutków dla poufności, integralności i dostępności informacji, ciągłości realizacji zadań publicznych oraz interesu publicznego. Podstawy prawne określone są w dokumencie Polityki Bezpieczeństwa.

19.2 Zakres stosowania

1) Procedura ma zastosowanie do wszystkich incydentów bezpieczeństwa informacji oraz incydentów związanych z funkcjonowaniem systemów technologii informacyjno-komunikacyjnych wykorzystywanych przez JST.
2) Procedura obejmuje incydenty mogące mieć wpływ na realizację zadań publicznych, bezpieczeństwo informacji, ciągłość działania oraz zaufanie obywateli.
3) Procedura obowiązuje wszystkie komórki organizacyjne JST, kierownictwo, pracowników oraz osoby trzecie wykonujące zadania na rzecz JST w zakresie wynikającym z powierzonych im obowiązków.

19.3 Odpowiedzialności za procedurę

1) Kierownik JST odpowiada za zapewnienie organizacyjnych, kadrowych i technicznych warunków umożliwiających skuteczne zarządzanie incydentami.
2) Osoba odpowiedzialna za bezpieczeństwo informacji koordynuje proces zarządzania incydentami, nadzoruje jego zgodność z przepisami prawa oraz odpowiada za kontakt z właściwymi organami zewnętrznymi.

3) Komórka organizacyjna odpowiedzialna za obsługę informatyczną odpowiada za techniczną obsługę incydentów, w tym identyfikację przyczyn, ograniczanie skutków oraz przywracanie prawidłowego funkcjonowania systemów.
4) Kierownicy komórek organizacyjnych odpowiadają za niezwłoczne zgłaszanie incydentów oraz współpracę w procesie ich obsługi.
5) Pracownicy JST są zobowiązani do natychmiastowego zgłaszania wszelkich podejrzeń wystąpienia incydentu bezpieczeństwa informacji.

19.4 Opis postępowania

19.4.1 Zasady ogólne zarządzania incydentami

1) Zarządzanie incydentami bezpieczeństwa informacji oraz systemów technologii informacyjno-komunikacyjnych w JST odbywa się w sposób uporządkowany, skoordynowany i udokumentowany.
2) Każde zdarzenie mogące mieć wpływ na bezpieczeństwo informacji, ciągłość działania, jakość usług lub zgodność z przepisami prawa podlega analizie w ramach niniejszej procedury.
3) Zdarzenia są klasyfikowane w szczególności jako zdarzenia nieistotne, incydenty bezpieczeństwa informacji, naruszenia ochrony danych osobowych, niezgodności lub sytuacje nadzwyczajne.
4) Proces zarządzania incydentami obejmuje pełny cykl życia incydentu, od momentu jego zgłoszenia do momentu zamknięcia oraz wdrożenia działań zapobiegawczych.

19.4.2 Zgłaszanie zdarzeń i incydentów

1) Każda osoba zobowiązana do przestrzegania regulacji wewnętrznych JST ma obowiązek niezwłocznego zgłoszenia zdarzenia mogącego naruszyć bezpieczeństwo informacji lub ciągłość działania.
2) Zgłoszenie przekazywane jest do Pełnomocnika ds. systemu zarządzania bezpieczeństwem informacji w formie pisemnej, w sposób umożliwiający zachowanie udokumentowanych informacji.

3) W sytuacjach wymagających natychmiastowej reakcji dopuszcza się zgłoszenie innym kanałem komunikacji, z obowiązkiem niezwłocznego uzupełnienia zgłoszenia w formie pisemnej.
4) Zdarzenia wykryte automatycznie przez systemy informatyczne podlegają analizie przez administratora systemów informatycznych i niezwłocznie przekazywane są do Pełnomocnika do spraw systemu zarządzania bezpieczeństwem informacji.

19.4.3 Rejestracja i wstępna ocena zdarzenia

1) Każde zgłoszone zdarzenie jest rejestrowane w centralnym rejestrze zdarzeń i incydentów prowadzonym przez JST.
2) Pełnomocnik do spraw systemu zarządzania bezpieczeństwem informacji, we współpracy z administratorem systemów informatycznych, dokonuje wstępnej oceny zdarzenia.
3) Wstępna ocena obejmuje określenie charakteru zdarzenia, jego potencjalnych skutków oraz wpływu na bezpieczeństwo informacji, ciągłość działania i dane osobowe.
4) W przypadku podejrzenia naruszenia ochrony danych osobowych Pełnomocnik niezwłocznie informuje inspektora ochrony danych.

19.4.4 Kwalifikacja zdarzenia i decyzja o dalszym postępowaniu

1) Na podstawie wstępnej oceny zdarzenie kwalifikowane jest jako:
   a) zdarzenie niemające wpływu na system zarządzania bezpieczeństwem informacji, w tym niezgodność,
   b) incydent bezpieczeństwa informacji,
   c) naruszenie ochrony danych osobowych.
2) Decyzja o kwalifikacji oraz dalszym postępowaniu podejmowana jest bez zbędnej zwłoki, nie później niż w ciągu dwudziestu czterech godzin od zgłoszenia.
3) Dla zdarzeń zakwalifikowanych jako incydenty lub naruszenia wyznacza się osobę odpowiedzialną za ich obsługę oraz dokumentowanie.

19.4.5 Obsługa incydentu i ograniczanie skutków

1) Obsługa incydentu obejmuje działania mające na celu ograniczenie jego skutków oraz zapobieżenie dalszemu rozprzestrzenianiu się zagrożenia.
2) Administrator systemów informatycznych może podjąć działania techniczne ograniczające funkcjonowanie systemów, jeżeli jest to niezbędne dla ochrony informacji.
3) Decyzje wpływające na realizację zadań publicznych podejmowane są w porozumieniu z najwyższym kierownictwem JST.
4) Wszystkie działania są dokumentowane od momentu zgłoszenia do zakończenia obsługi incydentu.

19.4.6 Zabezpieczenie i archiwizacja materiału dowodowego

1) W toku obsługi incydentu JST zabezpiecza wszelkie materiały dowodowe związane ze zdarzeniem.
2) Materiał dowodowy jest gromadzony i przechowywany w sposób zapewniający jego integralność, poufność i możliwość późniejszego wykorzystania.
3) Dostęp do materiałów dowodowych jest ograniczony do osób upoważnionych.

19.4.7 Eskalacja do organów zewnętrznych

1) Incydenty spełniające kryteria ustawowe podlegają zgłoszeniu do właściwego Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego (CERT).
2) Zgłoszenie incydentu istotnego lub poważnego realizowane jest w ustawowych terminach, w szczególności poprzez przekazanie:
   a) informacji wstępnej nie później niż w ciągu dwudziestu czterech godzin,
   b) zgłoszenia szczegółowego nie później niż w ciągu siedemdziesięciu dwóch godzin,
   c) raportu końcowego po zakończeniu obsługi incydentu.
3) W przypadku naruszenia ochrony danych osobowych Administrator danych dokonuje zgłoszenia do Prezesa Urzędu Ochrony Danych Osobowych nie później niż w ciągu siedemdziesięciu dwóch godzin od stwierdzenia naruszenia.
4) Jeżeli naruszenie może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, JST dokonuje zawiadomienia osób, których dane dotyczą.

19.4.8 Usunięcie przyczyn incydentu i przywrócenie działania

1) Po opanowaniu incydentu JST podejmuje działania mające na celu trwałe usunięcie jego przyczyn.
2) Przywrócenie normalnego funkcjonowania systemów odbywa się w sposób kontrolowany, z zachowaniem zasad bezpieczeństwa informacji.
3) Skuteczność działań naprawczych podlega weryfikacji.

19.4.9 Analiza i wyciąganie wniosków

1) Po zakończeniu obsługi incydentu JST przeprowadza analizę przyczyn źródłowych oraz skutków zdarzenia.
2) Analiza służy identyfikacji słabości organizacyjnych, technicznych lub proceduralnych.
3) Wnioski z analizy stanowią podstawę do wdrożenia działań korygujących i zapobiegawczych.
4) Wszystkie incydenty, postepowanie oraz efektywność działań oceniana jest w ramach przeglądu zarządzania.

19.4.10 Archiwizacja materiału dowodowego

1) Całość postępowania podlega archiwizacji przez okres minimum trzech lat od zakończenia postępowania z incydentem.
2) Materiały dowodowe oraz postepowanie muszą być archiwizowane w sposób gwarantujący poufność i integralność materiału dowodowego.

19.5 Metryka

Lp.	Zakres zmiany	Data przyjęcia i podstawa stosowania
1.	Utworzenie dokumentu	00-00-2026 Zarządzenie …

19.6 Uwagi

Regulacja nie musi być rozszerzana, możliwe obszary doprecyzowania (przykładowe):

a) rejestr incydentów,
b) zgłoszenie incydentu przez pracownika (druk),
c) raport z incydentu.

19.7 Załączniki

1) Instrukcja zgłaszania incydentu *[do samodzielnego uzupełnienia przez JST]*
2) Rejestr incydentów *[do samodzielnego uzupełnienia przez JST]*

20. Kopie zapasowe

20.1 Cel

Celem niniejszej procedury jest ustanowienie jednolitych, systemowych i kompleksowych zasad wykonywania, przechowywania, ewidencjonowania, testowania oraz ochrony kopii zapasowych danych i systemów technologii informacyjno-komunikacyjnych wykorzystywanych w JST. Procedura ma na celu zapewnienie dostępności, integralności oraz możliwości odtworzenia danych i systemów JST w przypadku awarii, incydentów bezpieczeństwa informacji, błędów ludzkich, zdarzeń losowych lub innych zakłóceń mogących wpływać na realizację zadań publicznych. Podstawy prawne określone są w dokumencie Polityki Bezpieczeństwa.

20.2 Zakres stosowania

1) Procedura ma zastosowanie do wszystkich systemów technologii informacyjno-komunikacyjnych, danych oraz zasobów informacyjnych wykorzystywanych przez JST.
2) Procedura obejmuje dane przetwarzane w systemach produkcyjnych, systemach pomocniczych oraz w środowiskach wspierających realizację zadań publicznych.
3) Procedura obowiązuje wszystkie komórki organizacyjne JST, kierownictwo, pracowników oraz osoby trzecie wykonujące zadania na rzecz JST w zakresie wynikającym z powierzonych im obowiązków.

20.3 Odpowiedzialności za procedurę

1) Kierownik JST odpowiada za zapewnienie warunków organizacyjnych i finansowych umożliwiających realizację procesu wykonywania kopii zapasowych.
2) Osoba odpowiedzialna za bezpieczeństwo informacji sprawuje nadzór nad zgodnością procesu wykonywania kopii zapasowych z systemem zarządzania bezpieczeństwem informacji oraz nad jego skutecznością.

3) Komórka organizacyjna odpowiedzialna za obsługę informatyczną odpowiada za planowanie, wykonywanie, przechowywanie oraz testowanie kopii zapasowych.
4) Właściciele systemów i danych odpowiadają za określenie wymagań dotyczących częstotliwości wykonywania kopii oraz krytyczności danych.
5) Pracownicy JST są zobowiązani do przestrzegania zasad niniejszej procedury w zakresie korzystania z danych i systemów.

20.4 Opis postępowania

20.4.1 Zasady ogólne wykonywania kopii zapasowych

1) JST zapewnia wykonywanie kopii zapasowych danych (dalej jako zbiorów danych) i systemów w sposób planowy, regularny i udokumentowany.
2) Zakres danych objętych kopiami zapasowymi jest określany na podstawie znaczenia danych dla realizacji zadań publicznych, wyników analizy ryzyk oraz zaleceń właścicieli systemów i danych (aktywów).
3) Kopie zapasowe są wykonywane w sposób zapewniający możliwość skutecznego odtworzenia danych i systemów.

20.4.2 Harmonogram i częstotliwość wykonywania kopii zapasowych

1) JST prowadzi ewidencję wszystkich wykonywanych kopii zapasowych.
2) Ewidencja obejmuje informacje umożliwiające identyfikację kopii, ich lokalizację oraz status przechowywania.
3) Dla każdego systemu i zbioru danych JST określa częstotliwość wykonywania kopii zapasowych.
4) Harmonogram wykonywania kopii uwzględnia wymagania dotyczące dostępności danych oraz dopuszczalny czas ich utraty.
5) Harmonogram jest dokumentowany i okresowo weryfikowany.
6) Harmonogram zawiera co najmniej informacje:
   a) nazwa systemu / zasobu / aktywa,
   b) częstotliwość kopiowania,

c) metodyka kopiowania (np. pełna / przyrostowa itd.),
d) okres przechowywania,
e) miejsce przechowywania,
f) uwagi (np. narzędzie niezbędne do wykonania / odtworzenia).

7) Harmonogram jest informacją chronioną i nie podlega upublicznieniu w ramach SZBI.
8) Rejestr kopii zapasowych (harmonogram) jest aktualizowany na bieżąco i wykorzystywany do celów audytowych oraz operacyjnych.

20.4.3 Oznaczanie kopii zapasowych

1) Każda kopia zapasowa jest jednoznacznie oznaczana w sposób umożliwiający jej identyfikację.
2) Oznaczenie kopii zawiera informacje pozwalające określić zakres danych, datę wykonania oraz system, którego dotyczy kopia oraz klasyfikację informacji.

20.4.4 Przechowywanie i kolokacja kopii zapasowych

1) Kopie zapasowe są przechowywane w sposób zapewniający ich ochronę przed utratą, zniszczeniem lub nieuprawnionym dostępem.
2) JST zapewnia przechowywanie części kopii zapasowych w lokalizacji odrębnej od miejsca przetwarzania danych produkcyjnych – co najmniej jedna pełna kopia jest oddzielona od systemów produkcyjnych.
3) Kolokacja kopii zapasowych jest realizowana w sposób ograniczający ryzyko jednoczesnej utraty danych produkcyjnych i kopii zapasowych.

20.4.5 Kopie zapasowe przechowywane w trybie odłączonym

1) JST zapewnia wykonywanie kopii zapasowych przechowywanych w trybie odłączonym od systemów produkcyjnych (tzw. „kopii offline”).
2) Kopie przechowywane w trybie odłączonym są zabezpieczone przed nieuprawnionym dostępem oraz modyfikacją.
3) Dostęp do kopii przechowywanych w trybie odłączonym jest ograniczony do osób upoważnionych.

20.4.6 Testowanie kopii zapasowych

1) JST prowadzi okresowe testy odtwarzania danych i systemów z kopii zapasowych.
2) Testy mają na celu potwierdzenie integralności kopii oraz skuteczności procesu odtworzeniowego.
3) Wyniki testów są dokumentowane.

20.4.7 Postępowanie w przypadku odtwarzania danych

1) Odtwarzanie danych z kopii zapasowych odbywa się w sposób kontrolowany i udokumentowany.
2) Decyzja o odtworzeniu danych jest podejmowana przez osoby upoważnione.
3) Po zakończeniu odtwarzania weryfikuje się poprawność i kompletność odtworzonych danych.

20.5 Załączniki

Załącznik nr 1 Rejestr kopii zapasowych *[do samodzielnego uzupełnienia przez JST]*.

20.6 Uwagi

Regulacja nie musi być rozszerzana, możliwe obszary doprecyzowania (przykładowe):

a) rejestr kopii zapasowych (w tym lokacja, okres, zasoby itd.),
b) protokół z testowania kopii.

20.7 Metryka

Lp.	Zakres zmiany	Data przyjęcia i podstawa stosowania
1.	Utworzenie dokumentu	00-00-2026 Zarządzenie …