[Nazwa jednostki / organizacji]

[Adres siedziby]

PBI Polityka Bezpieczeństwa Informacji

Kod dokumentu	SIT-F1-M05-D01
Moduł	M05 Podstawy KRI
Typ	Dokument
Wersja	v2.2.8
Data	2026-03-26
Właściciel dokumentu	[Właściciel dokumentu]
Zatwierdzający	[Zatwierdzający]
Przegląd okresowy	[Przegląd okresowy]
Klasyfikacja	Dokument wewnętrzny

Spis treści

Pojęcie	Definicja
Informacja	każdy komunikat, dane lub wiedza utrwalona w dowolnej postaci, posiadająca wartość dla jednostki.
Aktywo	wszelkie zasoby wspierające przetwarzanie informacji (np. sprzęt, oprogramowanie, dane, usługi, ludzie).
Incydent bezpieczeństwa	zdarzenie, które narusza lub może naruszyć poufność, integralność lub dostępność informacji albo usług.

Skrót	Znaczenie
KRI	Krajowe Ramy Interoperacyjności
SZBI	System Zarządzania Bezpieczeństwem Informacji
GABI	Główny Administrator Bezpieczeństwa Informacji
ASI	Administrator Systemu Informatycznego (lub rola IT odpowiedzialna za systemy)
MFA	Uwierzytelnianie wieloskładnikowe
RPO	Recovery Point Objective – maksymalna akceptowalna utrata danych
RTO	Recovery Time Objective – maksymalny akceptowalny czas odtworzenia usługi

Rola	Odpowiedzialności (minimum)	Dowody / artefakty
Kierownik jednostki	Zatwierdza PBI i zapewnia zasoby; wyznacza role (GABI/ASI); akceptuje wyjątki istotne dla ryzyka.	Zatwierdzenie PBI; akceptacje wyjątków; protokoły przeglądów.
GABI	Nadzoruje SZBI; prowadzi przeglądy; koordynuje reagowanie na incydenty; utrzymuje rejestry i wymagania.	Rejestr incydentów; rejestr szkoleń; raporty przeglądów.
ASI / IT	Wdraża zabezpieczenia techniczne; zarządza kontami i uprawnieniami; wykonuje backupy i testy odtwarzania.	Rejestr dostępów; rejestr backupów; logi; protokoły testów.
Użytkownicy	Stosują zasady; chronią hasła i urządzenia; zgłaszają incydenty; uczestniczą w szkoleniach.	Potwierdzenia szkoleń; oświadczenia; zgłoszenia incydentów.

Klasa	Opis	Przykłady
Publiczne	Informacje przeznaczone do publikacji lub udostępnienia bez ograniczeń.	BIP, ogłoszenia, komunikaty prasowe.
Wewnętrzne	Informacje do użytku wewnętrznego, nieprzeznaczone do publikacji.	Procedury, korespondencja wewnętrzna, plany pracy.
Poufne	Informacje wymagające zwiększonej ochrony ze względu na ryzyko dla osób lub organizacji.	Dane osobowe, dane kadrowe, dane finansowe, dane prawnie chronione.

1. Cel i zakres

Polityka Bezpieczeństwa Informacji ustanawia minimalne i nadrzędne zasady ochrony informacji w jednostce, niezależnie od tego, czy jest nią urząd, szkoła, uczelnia czy instytucja kultury.

Dokument obejmuje informacje papierowe i elektroniczne, systemy własne i usługi zewnętrzne, a także sytuacje, w których część IT utrzymywana jest przez podmiot zewnętrzny lub wspólną jednostkę obsługującą.

- Minimum regulacyjne: zgodność z KRI oraz obowiązkami kierownictwa jednostki w zakresie organizacji bezpieczeństwa.
- Minimum operacyjne: obowiązywanie zasad dla wszystkich pracowników, współpracowników, stażystów i dostawców mających dostęp do informacji jednostki.
- Rekomendacja rozszerzona: coroczne potwierdzenie zakresu polityki w przeglądzie zarządczym SZBI.

2. Definicje i skróty

- GABI - osoba koordynująca governance bezpieczeństwa, ryzyko, przeglądy i raportowanie.
- ASI / IT - rola odpowiedzialna za wykonanie techniczne, logowanie, aktualizacje, odtwarzanie i dostępy.
- IOD - rola wspierająca zgodność z RODO, ocenę skutków oraz obsługę naruszeń danych osobowych.
- Właściciel procesu - osoba odpowiedzialna za dany proces publiczny, np. obsługę mieszkańca, dydaktykę, sekretariat lub sprzedaż biletów.
- Właściciel usługi - osoba odpowiedzialna za dany system, usługę lub dostawcę wspierającego proces jednostki.

3. Role i odpowiedzialności

- Kierownik jednostki zatwierdza politykę, akceptuje ryzyka wysokie i zapewnia zasoby.
- GABI utrzymuje spójność zasad, rejestrów i przeglądów oraz przygotowuje materiał do raportu rocznego.
- ASI / IT wdraża środki techniczne, prowadzi dowody i wspiera właścicieli usług.

- IOD uczestniczy w analizie naruszeń, ocen skutków i ustalaniu wymagań wobec przetwarzania danych osobowych.
- Właściciele procesów i usług potwierdzają wymagania biznesowe, ciągłość działania i dopuszczalne odstępstwa.

4. Klasyfikacja informacji

- Jednostka klasyfikuje informacje co najmniej według wpływu na poufność, integralność i dostępność oraz skutku dla realizacji usług publicznych.
- Przy klasyfikacji należy uwzględnić dane osobowe, informacje prawnie chronione, dokumentację procesów publicznych, materiały dydaktyczne i dane odbiorców usług.
- Wariant szkoły, uczelni i instytucji kultury powinien obejmować także dane uczniów, studentów, uczestników wydarzeń i współpracowników sezonowych.

5. Zasady dostępu i kont

- Dostęp przyznaje się zgodnie z rolą i potrzebą biznesową, a nie z wygodą organizacyjną.
- Każdy dostęp do systemów i danych powinien mieć właściciela, termin przeglądu oraz ślad dowodowy w rejestrze.
- Dostępy do systemów krytycznych, systemów z danymi osobowymi i usług zewnętrznych muszą być okresowo przeglądane.

6. Hasła i MFA

- MFA jest obowiązkowe dla poczty, dostępu zdalnego, kont uprzywilejowanych i dostępu administracyjnego do usług zewnętrznych.
- W małej jednostce, w której nie ma centralnego IAM, minimalny standard MFA nadal obowiązuje dla usług najwyższego ryzyka.
- Wyjątki od MFA muszą być opisane, ocenione pod kątem ryzyka i zatwierdzone przez kierownictwo.

7. Backup i odtwarzanie

- Backup i odtwarzanie muszą być powiązane z ważnością usługi publicznej, a nie tylko z technicznym opisem systemu.
- Jednostka utrzymuje minimalne czasy odtworzenia i dopuszczalnej utraty danych dla usług krytycznych.
- Dowodem wykonania są rejestry, testy i wnioski z testów odtworzeniowych.

8. Praca zdalna/mobilna

- Zasady pracy zdalnej i mobilnej muszą obejmować urządzenia służbowe, prywatne urządzenia dopuszczone wyjątkowo oraz pracę terenową.
- W szkołach, uczelniach i instytucjach kultury należy uwzględnić pracę sezonową, wydarzenia oraz pracę poza stałą siedzibą.

- Dostęp zdalny powinien być ograniczany do niezbędnego minimum, rejestrowany i objęty MFA.

9. Incydenty

- Każdy pracownik musi znać kanał zgłaszania incydentu oraz minimalne pierwsze kroki po wykryciu zdarzenia.
- Naruszenia danych osobowych wymagają niezwłocznej współpracy z IOD i udokumentowania decyzji oraz osi czasu.
- Incydenty wpływające na usługi publiczne wymagają jednoczesnego spojrzenia technicznego, organizacyjnego i prawnego.

10. Rejestry i dowody

- Polityka jest wykonywana przez rejestry, checklisty, protokoły i raporty wskazane w modułach M01-M14.
- Każda jednostka powinna utrzymywać dowody adekwatne do swojej skali, ale zawsze rozliczalne i aktualne.
- Przegląd kompletności dowodów wykonuje się co najmniej kwartalnie oraz po istotnym incydencie lub zmianie organizacyjnej.

Podpisy

Opracował	**Zweryfikował**	**Zatwierdził**
Imię i nazwisko: _____	**Imię i nazwisko:** _____	**Imię i nazwisko:** _____
Stanowisko: _____	**Stanowisko:** _____	**Stanowisko:** _____
Data: _____	**Data:** _____	**Data:** _____
Podpis: _____	**Podpis:** _____	**Podpis:** _____