SYSTEM ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

Polityka Bezpieczeństwa Informacji

- forma deklaratywna

w organizacji o nazwie:

Urząd Miasta Pszów

System Zarządzania Bezpieczeństwem Informacji opracowano uwzględniając:	
PRZEPISY PRAWA: UoKSC – Ustawa o krajowym systemie cyberbezpieczeństwa KRI - Rozporządzenie ws. krajowych ram interoperacyjności RODO - ogólne rozporządzenie unijne o ochronie danych osobowych	**STANDARDY ISO:** PN-EN ISO/IEC 27001:2023 PN-EN ISO 22301:2020

Oznaczenie dokumentu:	**SZBI-1-PBI – Forma deklaratywna**	Data zarządzenia wdrażającego SZBI:	**23 września 2025 r.**
Wydanie / wersja:	**1**	Nr zarządzenia wdrażającego SZBI:	**BM.0050.140.2025**

Sprawdził:

Inspektor Ochrony Danych
/-/
Aleksander Kloc

(pieczęć i podpis)

Zatwierdził:

Burmistrz Miasta
/-/
Piotr Kowol

(pieczęć i podpis)

§1

System Zarządzania Bezpieczeństwem Informacji (SZBI)

1. Mając świadomość wymogów formalnoprawnych oraz technicznych w procesie przetwarzania danych, w tym danych osobowych, najwyższe kierownictwo zdecydowało o konieczności wprowadzenia do podmiotu procedur, które składają się na System Zarządzania Bezpieczeństwem Informacji.

2. Najwyższe kierownictwo niniejszym określa jakie są główne założenia obowiązującego w podmiocie Systemu Zarządzania Bezpieczeństwem Informacji, a także jakie są cele w powyższym zakresie, a także jak rozkłada się odpowiedzialność. Najwyższe kierownictwo podmiotu ma świadomość, iż bezpieczeństwo informacji osiąga się poprzez wdrożenie odpowiednich polityk, zasad, procedur, procesów czy struktur odpowiedzialności. Aby osiągnąć założone cele w zakresie bezpieczeństwa informacji podmiot definiuje, wdraża, monitoruje, przegląda i doskonali wdrożone w ramach SZBI środki techniczne i organizacyjne, co deklaruje w ramach niniejszej polityki.

3. Na SZBI składają się następujące polityki:

1) Polityka Bezpieczeństwa Informacji - forma deklaratywna;

Celem ustanowienia „Polityki Bezpieczeństwa Informacji – forma deklaratywna" jest zakomunikowanie stronom zainteresowanym jakiego rodzaju standardy w zakresie bezpieczeństwa informacji i ochrony danych, w tym danych osobowych stosuje organizacja.

2) Polityka ochrony danych osobowych w fazie projektowania i domyślnej ochrony danych;

3) Polityka Bezpieczeństwa Organizacyjnego;

4) Polityka Bezpieczeństwa Osobowego;

5) Polityka Bezpieczeństwa Fizycznego;

6) Polityka Bezpieczeństwa Technologicznego;

7) Polityka szacowania ryzyka bezpieczeństwa informacji.

§2

Definicje legalne

1. Ilekroć w niniejszej polityce mówi się o:

1) **Organizacji** – rozumie się przez to osobę prawną, organ publiczny, jednostkę lub inny podmiot. Do celów niniejszej polityki wprowadza się nazwę własną organizacji: **Urząd Miasta Pszów**;

2) **Administratorze danych (Administratorze)** – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych tj. **Burmistrz Miasta Pszów; Miasto Pszów.**

3) **Najwyższym kierownictwie (kierownictwie organizacji)** – rozumie się przez to osoby, które reprezentują organizację, ustanawiają System Zarządzania Bezpieczeństwem Informacji oraz inne procedury, a także określają role, odpowiedzialność i uprawnienia.

4) **Systemie Zarządzania Bezpieczeństwem Informacji (SZBI)** - rozumie się przez to zbiór polityk, procedur, wytycznych oraz przydzielonych aktywów, zarządzanych wspólnie przez organizację w celu ochrony swoich zasobów informacyjnych.

§3

Podstawy legalności SZBI

2. Z racji tego, iż najwyższe kierownictwo w ramach realizacji praw podstawowych w zakresie ochrony danych osobowych, kieruje się zasadą legalności przetwarzania zgodnego z prawem, opiera System Zarządzania Bezpieczeństwem Informacji określony w niniejszej polityce na następujących podstawach prawnych oraz normach ISO:

1) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);

2) Ustawa z dnia 10 maja 2018 o ochronie danych osobowych;

3) Wytyczne Grupy Roboczej art. 29 / EROD;

4) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 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 (Dyrektywa NIS-2);

5) Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;

6) Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne;

7) Rozporządzenie 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;

8) Narodowe Standardy Cyberbezpieczeństwa (NSC);

9) Licencjonowane wobec organizacji normy:

a) PN-EN ISO/IEC 27001:2023 (Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji - Wymagania);

b) PN-EN ISO 22301:2020 (Bezpieczeństwo i odporność – System Zarządzania Ciągłością Działania – Wymagania).

3. Bezpieczeństwo informacji podmiot rozumie jako zestaw narzędzi i procedur oraz zabezpieczeń, które szeroko chronią poufne informacje podmiotu przed nieautoryzowanym dostępem, zakłóceniami, incydentami oraz naruszeniami. Bezpieczeństwo informacji obejmuje aspekt fizyczny i środowiskowy, kontrolę dostępu oraz cyberbezpieczeństwo.

§4

Cele wprowadzenia SZBI

1. Celem wprowadzenia Systemu Zarządzania Bezpieczeństwem Informacji jest zharmonizowanie systemu ochrony danych osobowych w taki sposób, by zapewnić realizacje podstawowych praw i wolności osób fizycznych, których dane osobowe podmiot przetwarza w związku z realizacją swoich zadań. Celem jest także ciągłe edukowanie osób zaangażowanych w proces przetwarzania danych osobowych. System Zarządzania Bezpieczeństwem Informacji ma również na celu zapewnienie poufności oraz integralności danych osobowych, względem których zachodzi proces przetwarzania poprzez przypisanie odpowiedzialności i uprawnień względem osób upoważnionych do przetwarzania tych danych oraz użytkowników systemów teleinformatycznych.

2. Najwyższe kierownictwo zobowiązuje się do spełnienia obowiązujących wymagań związanych z bezpieczeństwem informacji, a także do ciągłego doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji.

3. Poprzez to, iż najwyższe kierownictwo wykazuje przywództwo i zaangażowanie w stosunku do zarządzania bezpieczeństwem informacji i ma świadomość, iż odpowiedzialność za bezpieczeństwo informacji powinna być określona i przypisana, ustanawia strukturę zarządzania tak, aby można było nadzorować wdrażanie oraz eksploatację bezpieczeństwa informacji w podmiocie. Najwyższe kierownictwo dba o to, by odpowiedzialność za bezpieczeństwo informacji była z góry przypisana konkretnym właścicielom poszczególnych ryzyk, a role w procesie przetwarzania danych osobowych były zdefiniowane.

4. Najwyższe kierownictwo zatwierdza wszelkie zmiany w Systemie Zarządzania Bezpieczeństwem Informacji.

§5

Zarządzanie SZBI

1. Zarządzanie bezpieczeństwem informacji opiera się na następujących procesach:

1) **Zarządzania ryzykiem** - strategicznym elementem zarządzania aktywami i bezpieczeństwem informacji jest przeprowadzanie okresowej analizy ryzyka oraz opracowania planów postępowania z ryzykiem. Analiza jej wyników stanowi podstawę podejmowania wszelkich działań w zakresie utrzymania i doskonalenia ochrony zasobów podmiotu. Szacowanie ryzyka bazuje na wytycznych normy PN-ISO/IEC 27005 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji).

2) **Monitorowania i przeglądów Systemu Zarządzania Bezpieczeństwem Informacji** – przeprowadzanie audytów z zakresu bezpieczeństwa informacji oraz cyklicznych przeglądów formalnych w zakresie dokumentacyjnym względem zmieniającego się otoczenia prawnego, faktycznego oraz organizacyjnego.

3) **Utrzymania i doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji** - przeprowadzanie działań korygujących oraz ocena ich skuteczności; przeprowadzanie działań zapobiegawczych oraz ocena ich skuteczności; informowanie zainteresowanych stron o działaniach i udoskonaleniach.

4) **Nadzoru nad dokumentacją** - prowadzenie i nadzorowanie dokumentacji systemowej; prowadzenie i nadzorowanie zapisów systemowych.

5) **Zarządzania dostępem do zasobów** - zarządzanie dostępem do zasobów odbywa się w ramach procesu opartego na systemie obiegu karty uprawnień.

6) **Zarządzania naruszeniem -** prowadzone jest w ramach procedury zarządzania incydentami.

2. W podmiocie stosuje się kodeks dobrych praktyk w zakresie przetwarzania danych, w tym danych osobowych, a są to zasady kierujące wszystkimi przedsięwzięciami w aspekcie bezpieczeństwa informacji. Wszelkiego rodzaju odstępstwa od ustalonych w podmiocie zasad

bezpieczeństwa informacji mogą mieć swoje źródło jedynie w przepisach prawa, którymi podmiot jest związany (w myśl zasady „Lex specialis derogat legi generali").

Podstawa prawna:

- Zgodnie z art. 24 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r.
- Zgodnie z § 19 ust. 1 Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych

W oparciu o:

- Norma PN-EN ISO/IEC 27001:2023 zał. A 5.1