**Załącznik nr 1** do zarządzenia
wewnętrznego w organizacji o nazwie:
Starostwo Powiatowe w Kutnie

# Zasady Bezpieczeństwa Informacji

*w organizacji o nazwie:*

**STAROSTWO POWIATOWE W KUTNIE**

**99-300 KUTNO, UL. KOŚCIUSZKI 16**

## Spis treści



## § 1

## Postanowienia ogólne

### 1. Deklaracja Kierownictwa

Zgodnie z treścią § 20 ust. 1 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, w Starostwie Powiatowym w Kutnie realizującym zadania publiczne ustanawia się, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

Kierownictwo Starostwa Powiatowego w Kutnie deklaruje, w szczególności:

1) Zapewnienie dostępności zasobów potrzebnych do utrzymania, rozwoju i ciągłego doskonalenia SZBI;
2) Zaangażowanie w odniesieniu do SZBI, w tym kompleksową ochronę informacji i aktywów wspierających ich przetwarzanie w Starostwie oraz promowanie ciągłego doskonalenia ustanowionego Systemu;
3) Kierowanie i aktywne wspieranie osób przyczyniających się do osiągnięcia skuteczności SZBI oraz stałe podnoszenie świadomości pracowników Starostwa w zakresie bezpieczeństwa informacji.

### 2. Wprowadzenie

1) Zasady bezpieczeństwa informacji opisane w niniejszym dokumencie zostały opracowane w celu zapewnienia poufności, integralności i dostępności przetwarzanych informacji w Starostwie Powiatowym w Kutnie (dalej: Starostwo). Znajomość tych zasad i ich stosowanie jest obowiązkowe dla personelu oraz jeżeli ma to zastosowanie stron zainteresowanych, współpracujących ze Starostwem (zwanych dalej użytkownikami).

2) Za zapewnienie bezpiecznego przetwarzania informacji odpowiedzialny jest każdy pracownik Starostwa. Niniejszy dokument określa zasady i procedury zapewniające bezpieczeństwo informacji. Oprócz zasad i procedur określonych w niniejszym dokumencie, należy kierować się również należytą starannością zawodową, posiadaną wiedzą profesjonalną, jak również dobrymi praktykami.

3) Sekretarz Powiatu wraz z Audytorem wewnętrznym, Administratorem Systemu Informatycznego oraz Inspektorem ochrony danych, zobowiązany jest do monitorowania adekwatności niniejszych zasad oraz dokonywania ich przeglądu, nie rzadziej niż raz w roku oraz aktualizowania ich, jeżeli zaistnieje taka potrzeba wywołana czynnikami wewnętrznymi, bądź zewnętrznymi.

4) Zasady określone w niniejszym dokumencie mają zastosowanie do wszystkich informacji przetwarzanych przez Starostwo z wyłączeniem jedynie informacji niejawnych w rozumieniu ustawy o ochronie informacji niejawnych, dla których obowiązują zasady i procedury ustanowione w odrębnych dokumentach.

## 3. Kontekst wewnętrzny i zewnętrzny organizacji

1) Organizacja określa kontekst wewnętrzny uwzględniając następujące czynniki:

   a) schemat organizacyjny będący odzwierciedleniem zależności pomiędzy komórkami funkcjonalnymi w kontekście przepływu informacji, w tym danych osobowych,

   b) ład organizacyjny w rozumieniu zindywidualizowanych zasad zarządzania organizacją znajdujących swoje źródło we wdrożonych procedurach i normach,

   c) ustanowione przez kierownictwo cele organizacji w rozumieniu celów strategicznych, ekonomicznych i pozaekonomicznych, taktycznych, operacyjnych (katalog otwarty),

   d) określoną przez kierownictwo misję organizacji w rozumieniu zespołu wartości podkreślających rolę organizacji na rzecz otoczenia, w którym organizacja działa,

   e) aktywa organizacji w postaci zasobu ludzkiego - jego wiedzy, kompetencji, umiejętności oraz postaw,

   f) procesy podejmowania decyzji uwzględniając strukturę organizacyjną,

   g) kulturę organizacji,

   h) relacje do wewnątrz organizacji.

2) **Organizacja określa kontekst zewnętrzny uwzględniając następujące czynniki:**

   a) relacje z zewnętrznymi podmiotami,

   b) środowisko zewnętrzne mające wpływ na cele organizacji:

      - prawne,
      - finansowe,
      - ekonomiczne,
      - technologiczne.

## 4. Podstawy prawne

1) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.U.UE.L.2016.127.2),
2) ustawa z dnia 17 lutego 2005r. o informatyzacji działalności podmiotów realizujących zadania publiczne (tekst jedn. Dz.U. z 2021r., poz. 2070 z późn.zm.),
3) ustawa z dnia 5 lipca 2018r. o krajowym systemie cyberbezpieczeństwa (tekst jedn. Dz.U. z 2022r., poz. 1863),
4) Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (tekst jedn. Dz.U. z 2017r., poz. 2247),
5) ustawa z dnia 10 maja 2018 o ochronie danych osobowych (tj. Dz.U. z 2019r., poz. 1781 z późn.zm.),
6) ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych (tj. Dz.U. z 2022r., poz. 1634 z późn.zm.)

5. **Definicje i skróty** użyte w dokumentacji Systemu Zarządzania bezpieczeństwem Informacji – zostały opisane w **załączniku do Zasad Bezpieczeństwa Informacji.**

## § 2
## Organizacja Bezpieczeństwa Informacji

1. W ramach ustanowionego SZBI, role i odpowiedzialności w zakresie bezpieczeństwa informacji zostały zidentyfikowane i przypisane.
2. Odpowiedzialność za bezpieczeństwo informacji ponoszą wszyscy pracownicy Starostwa, praktykanci, stażyści, wolontariusze oraz inne osoby i podmioty objęte zakresem ustanowionego SZBI.
3. Przedmiotowa odpowiedzialność polega na przestrzeganiu wymagań prawa powszechnie obowiązującego, zapisów niniejszego dokumentu oraz pozostałych wymogów wskazanych w dokumentacji bezpieczeństwa, w szczególności na:
   1) ochronie powierzonych informacji i zabezpieczeniu aktywów wspierających ich przetwarzanie,
   2) realizacji przypisanych zadań w obszarze bezpieczeństwa informacji,
   3) nieudostępnianiu informacji osobom lub podmiotom nieuprawnionym,
   4) zachowaniu w tajemnicy chronionych informacji oraz sposobów ich zabezpieczenia,
   5) informowaniu o podejrzeniu lub wszelkich zauważonych nieprawidłowościach, które mogą mieć wpływ na bezpieczeństwo informacji.
4. Celem realizacji w/w działań role i odpowiedzialności, w zakresie bezpieczeństwa informacji zostały przypisane do członków personelu w Starostwie, tj.:
   1) Administrator informacji (AI) – Starosta Kutnowski,
   2) Koordynator ds. bezpieczeństwa informacji (KBI) – Sekretarz Powiatu,
   3) Właściciele zasobów danych/ informacji (WŁ) – dyrektorzy, kierownicy nadzorujący pracę poszczególnych komórek organizacyjnych oraz osoby zatrudnione na samodzielnych stanowiskach pracy,
   4) Administrator Systemu Informatycznego (ASI) – informatyk odpowiedzialny za obsługę informatyczną Urzędu,
   5) Inspektor ochrony danych (IOD) – odpowiedzialny za nadzór, monitoring zasad przetwarzania danych osobowych w Urzędzie.
   6) Użytkownicy.
5. Szczegółowe zadania w/w osób zostały opisane w PBI ODO.

## § 3
## Klasyfikacja przetwarzanych informacji

1. Informacje przetwarzane w Starostwie Powiatowym w Kutnie objęte zakresem ustanowionego SZBI klasyfikowane są w następujących grupach:
   1) dane osobowe (w rozumieniu przepisów dot. ochrony danych osobowych),
   2) tajemnice prawnie chronione (tajemnice powołane na mocy ustaw, których obowiązek ochrony wynika z tychże ustaw),
   3) tajemnice Urzędu (informacje, których ujawnienie mogłoby narazić Starostwo na szkodę oraz informacje wewnętrzne udostępniane na zasadzie „wiedzy uzasadnionej"),
   4) informacje jawne (w tym informacje udostępniane w trybie informacji publicznej),
   5) informacje niejawne, z tym że szczegółowe zasady i tryb ochrony informacji niejawnych w Starostwie Powiatowym w Kutnie określone zostały w treści odrębnych uregulowań wewnętrznych.
2. Szczegółowe zasady dot. bezpieczeństwa i ochrony poszczególnych grup informacji, w tym ich zakres, tryb udostępniania i dystrybucji oraz archiwizacji i niszczenia zostały określone w **Polityce Bezpieczeństwa Informacji, w tym danych osobowych** (PBI ODO) stanowiącej **załącznik nr 2** do **SZBI.**

## § 4
## Zarządzanie ryzykiem w bezpieczeństwie informacji

1. W celu skutecznego zarządzania bezpieczeństwem informacji podejmuje się okresowe działania w obszarze zarządzania ryzykiem, w szczególności w zakresie szacowania tj. identyfikowania, analizy i oceny ryzyka w bezpieczeństwie informacji, zmierzających do ograniczenia oraz eliminacji przedmiotowego ryzyka.
2. Działania związane z zarządzaniem ryzykiem mającym wpływ na bezpieczeństwo informacji obejmują w szczególności:
   1) przygotowanie oraz okresową aktualizację dokumentów dot. zarządzania ryzykiem,
   2) prowadzenie okresowego szacowania ryzyka,
   3) postępowanie z ryzykiem,
   4) podejmowanie działań korygujących.
3. Szczegółowe zasady dot. zarządzania ryzykiem w bezpieczeństwie informacji zostały uregulowane w **Procedurze Analiza ryzyka ogólnego i Ocena skutków dla przetwarzania danych (DPIA)** stanowiącej **załącznik nr 4 SZBI.**
4. Procedura kontroli zarządczej oraz procedura zarządzania ryzykiem w Powiecie Kutnowskim zostały wdrożone do stosowania *Zarządzeniem Nr 11/2018 Starosty Kutnowskiego z dnia 31 stycznia 2018r. w sprawie ustalenia procedury kontroli zarządczej oraz procedury zarządzania ryzykiem w Powiecie Kutnowskim* (ze zmianami).

## § 5
## Kontrola dostępu do informacji

1. W celu zapewnienia ograniczonego dostępu do aktywów informacyjnych Starostwa, w tym do budynków i pomieszczeń, sprzętu i urządzeń oraz systemów informatycznych tylko dla osób i podmiotów uprawnionych, prowadzona jest kontrola dostępu fizycznego.
2. Szczegółowe zasady zarządzania dostępem do aktywów informacyjnych Starostwa zostały uregulowane w **PBI ODO** Starostwa Powiatowego w Kutnie, stanowiącej **załącznik nr 2** do **SZBI.**

## § 6
## Bezpieczeństwo fizyczne i środowiskowe

1. W celu zapobieżenia nieuprawnionemu fizycznemu dostępowi, szkodom i zakłóceniom w przetwarzaniu informacji i środkach przetwarzania informacji oraz utracie, zniszczeniu, uszkodzeniu, kradzieży aktywów informacyjnych Starostwa stosowane są mechanizmy ochrony w obszarze bezpieczeństwa fizycznego i środowiskowego.
2. Szczegółowe zasady dot. zarządzania bezpieczeństwem fizycznym i środowiskowym zostały uregulowane w **PBI ODO** Starostwa.

## § 7
## Bezpieczeństwo Teleinformatyczne

1. W ramach zarządzania bezpieczeństwem teleinformatycznym podejmowane są działania w zakresie szacowania i kontroli ryzyka utraty poufności, integralności, dostępności informacji w związku z korzystaniem systemu informatycznego Starostwa Powiatowego w Kutnie oraz aplikacji, komputerów i urządzeń mobilnych, sieci komputerowych i transmisji danych.
2. Działania powyższe podejmowane są w szczególności w zakresie rozwoju, monitorowania i doskonalenia infrastruktury teleinformatycznej.
3. Szczegółowe uregulowania została opisane w **Polityce Bezpieczeństwa Teleinformatycznego** – stanowiącej **załącznik nr 3** do **SZBI**.
4. Odrębne procedury określające sposób zarządzania systemem informatycznym służącym do przetwarzania danych w programach POJAZD i KIEROWCA wdrożone zostały na podstawie *Zarządzenia Nr 31/2009 Starosty Kutnowskiego z dnia 22 czerwca 2009r. w sprawie wprowadzenia instrukcji określającej sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych „Pojazd" i „Kierowca" w Starostwie Powiatowym w Kutnie.*

## § 8
## Bezpieczeństwo zasobów ludzkich

1. W celu ograniczenia ryzyka błędu ludzkiego, kradzieży, nadużycia, niewłaściwego korzystania z urządzeń oraz zapewnienia, że pracownicy Starostwa, praktykanci, stażyści, wolontariusze, zleceniobiorcy oraz inne osoby i podmioty wykonujące czynności w imieniu i na rzecz Administratora posiadające dostęp do aktywów informacyjnych Urzędu są świadomi odpowiedzialności i swoich obowiązków dotyczących bezpieczeństwa informacji oraz wypełniają je w odpowiedni sposób, podejmowane są poniższe działania:
   1) szkolenie w/w personelu i podmiotów – w zakresie bezpieczeństwa informacji oraz regularne informowanie o aktualizacji polityk i procedur związanych z ich stanowiskiem pracy,
   2) zapewnienie wykwalifikowanej kadry i/lub innych osób oraz podmiotów zewnętrznych do realizacji zadań,
   3) uwzględnienie odpowiednich zapisów dot. odpowiedzialności w zakresie bezpieczeństwa informacji w umowach zawieranych z w/w osobami i podmiotami.
2. Kierownictwo Starostwa zapewnia aby w/w personel (pracownicy, wykonawcy, użytkownicy) był informowany o swoich obowiązkach związanych z bezpieczeństwem informacji przed przyznaniem im dostępu do systemów informacyjnych.
3. W przypadku naruszenia procedur/ polityk bezpieczeństwa informacji opisanych w SZBI - prowadzi się postępowanie wyjaśniające oraz/ lub dyscyplinarne wobec członka personelu.

## § 9
## Zapewnienie ciągłości działania

1. W Starostwie podejmowane są działania w zakresie planowania, weryfikowania, przeglądu i oceny ciągłości działania i postępowania w przypadku wystąpienia sytuacji kryzysowych.

2. Szczegółowe zasady dot. zarządzania ciągłością działania zostały uregulowane w dokumencie o nazwie **Procedura stosowania planów awaryjnych w zakresie ciągłości działania w obszarze odtwarzania techniki informatycznej po katastrofie,** stanowiącym **załącznik nr 6** do **SZBI PBI.**

## § 10
## Relacje z podmiotami zewnętrznymi

1. W celu zapewnienia ochrony aktywów informacyjnych/ zasobów danych udostępnianych usługodawcom i innym osobom lub podmiotom zewnętrznym wykonującym czynności w imieniu i na rzecz Administratora, którzy posiadają dostęp do aktywów informacyjnych Starostwa, wprowadza się zasady postępowania - w przypadku współpracy związanej z dostępem do w/w zasobów.
2. W przypadku wykonywania zadań na rzecz i w imieniu Administratora przez osoby lub podmioty zewnętrzne, w drodze stosownej umowy lub porozumienia, wprowadza się zasady i wymogi współpracy uregulowane w **Polityce bezpieczeństwa w relacjach z podmiotami zewnętrznymi oraz Powierzanie przetwarzania danych osobowych** - stanowiącej **załącznik nr 7** do **SZBI.**

## § 11
## Struktura dokumentacji SZBI

1. W ramach ustanowionego SZBI wprowadza się dokumentację bezpieczeństwa określającą zasady i tryb zarządzania bezpieczeństwem informacji w Starostwie Powiatowym w Kutnie, w skład której wchodzą:
   1) **Zasady bezpieczeństwa Informacji (ZBI) – załącznik nr 1**
   2) **Polityka Bezpieczeństwa Informacji, w tym danych osobowych (PBI ODO) – załącznik nr 2** ,
   3) **Polityka Bezpieczeństwa Teleinformatycznego (PBT) – załącznik nr 3**,
   4) Procedur**a Analiza ryzyka ogólnego i Ocena skutków dla przetwarzania danych (DPIA) – załącznik nr 4,**
   5) **Polityka zarządzania incydentami związanymi z bezpieczeństwem informacji (PZI) – załącznik nr 5,**
   6) **Procedura stosowania planów awaryjnych w zakresie ciągłości działania w obszarze odtwarzania techniki informatycznej po katastrofie (SZCD) – załącznik nr 6,**
   7) **Polityka bezpieczeństwa w relacjach z podmiotami zewnętrznymi oraz Powierzanie przetwarzania danych osobowych (PBZ) – załącznik nr 7,**
   8) **Oświadczenie o zapoznaniu z SZBI – załącznik nr 8.**

## § 12
## Naruszenie bezpieczeństwa informacji i odpowiedzialność z tytułu przedmiotowego naruszenia

1. Każdy, kto posiada dostęp do informacji/ zasobów danych przetwarzanych w Starostwie Powiatowym w Kutnie ma obowiązek informowania osób odpowiedzialnych za bezpieczeństwo informacji w organizacji o podejrzeniu lub zidentyfikowanym przypadku naruszenia bezpieczeństwa.
2. Nieprzestrzeganie zasad zwartych w dokumentacji bezpieczeństwa stanowi naruszenie obowiązków pracowniczych i może skutkować sankcjami natury dyscyplinarnej.
3. Naruszenie postanowień SZBI przez kontrahenta/ podmiot zewnętrzny lub jego pracowników może stanowić podstawę do odstąpienia od umowy i żądania pokrycia powstałej szkody lub zapłaty kary umownej, jeżeli taki obowiązek wynika z zawartej umowy.
4. Z tytułu działań personelu lub podmiotów zewnętrznych współpracujących z Urzędem, grożą odrębne kary określone, w szczególności w:
   1) Kodeksie pracy,
   2) Kodeksie cywilnym,
   3) Kodeksie karnym,

4) RODO.

5. Szczegółowe zasady dot. identyfikowania, zgłaszania, reagowania i obsługi zdarzeń i incydentów związanych z bezpieczeństwem informacji zostały uregulowane w **Polityce zarządzania incydentami związanymi z bezpieczeństwem informacji** stanowiącej **załącznik nr 5** do **SZBI.**
6. W przypadku naruszenia ochrony danych osobowych postępowanie wyjaśniające prowadzi IOD, w pozostałych przypadkach nadzór nad postępowaniem sprawuje Sekretarz Powiatu – Koordynator ds. bezpieczeństwa informacji.

podpis Administratora lub osoby uprawnionej do reprezentowania

Daniel Kowalik
Elektronicznie podpisany przez Daniel Kowalik
Data: 2022.11.22 10:43:50 +01'00'

Signature Not Verified

Dokument podpisany przez Wiesława Sobczyk.
Data: 2022.11.18 16:58:49 CET