


# POLITYKA BEZPIECZEŃSTWA INFORMACJI

## Starostwo Powiatowe w Żyrardowie

|                 |   |
|-----------------|---|
| Rozdzielnik:    | Dokument do użytku wewnętrznego   |
| Podmiot:        | Starostwo Powiatowe w Żyrardowie  |
| Wersja:         | Nr 2  |
| z dnia:         |   |
| Zatwierdził(a): | <div>WICESTAROSTA</div> <div><br/>.....Krzysztof Dąbrowski.....</div> |

## **SPIS TREŚCI**

|  |   |
|--|---|
| SPIS TREŚCI.....                                   | 2 |
| 1. CEL.....  | 3 |
| 2. ZAKRES STOSOWANIA.....                          | 3 |
| 3. DEFINICJE .....                                 | 4 |
| 4. OBOWIĄZKI OSÓB PRZETWARZAJĄCYCH INFORMACJE..... | 5 |
| 5. ORGANIZACJA SYSTEMU OCHRONY INFORMACJI .....    | 6 |
| 6. OBOWIĄZYWANIE DOKUMENTU .....                   | 7 |
| 7. WYKAZ ZAŁĄCZNIKÓW .....                         | 7 |
| 8. DOKUMENTY ZWIĄZANE.....                         | 7 |

## 1. CEL

- 1) Celem niniejszego dokumentu jest wprowadzenie spójnych zasad zachowania bezpieczeństwa informacji w Starostwie Powiatowym w Żyrardowie zwanym dalej Starostwem.
- 2) Polityka Bezpieczeństwa Informacji jest dokumentem nadrzędnym dla innych polityk, procedur oraz regulaminów z zakresu ochrony informacji przyjętych w Starostwie
- 3) Zarządzanie bezpieczeństwem informacji jest pojęciem obejmującym zasady zarządzania systemem chroniącym dane oraz sposoby reagowania na zagrożenia. Zapewnienie odpowiedniej wiedzy zarządzających Starostwem oraz siecią informatyczną w zakresie pojawiających się nowych zagrożeń oraz metod ochrony jest kolejnym elementem zapewnienia bezpieczeństwa. Osoby obsługujące systemy przetwarzające informacje są ogniwem zabezpieczeń, na którego skuteczność wpływa również zapewnienie rzetelnej informacji w zakresie sposobu bezpiecznego użytkowania oprogramowania i sprzętu.
- 4) Zastosowanie niniejszej Polityki Bezpieczeństwa Informacji powinny zapewnić zabezpieczenia adekwatne i proporcjonalne do ryzyka występującego dla przetwarzanych i przechowywanych informacji, zwłaszcza w systemach informatycznych Starostwa.
- 5) Polityka Bezpieczeństwa Informacji jest jednocześnie dokumentem określającym zadania osób funkcyjnych, pracowników oraz pracowników i współpracowników podmiotów trzecich, które na mocy zawartych umów mają dostęp do informacji chronionych. Ma ona pomóc w zapewnieniu: poufności, integralności, dostępności oraz rozliczalności przetwarzanych informacji i innych zidentyfikowanych aktywów informacyjnych.

## 2. ZAKRES STOSOWANIA

- 1) Politykę Bezpieczeństwa Informacji stosują osoby przetwarzające dane chronione, niezależnie od formy zatrudnienia w Starostwie lub formy prawnej wiążącej Starostwo z tą osobą. W szczególności mogą być to osoby zatrudnione na umowę o pracę, stażyści, praktykanci, wolontariusze oraz osoby realizujące zadania na podstawie podpisanej z Starostwem umowy cywilnoprawnej, a także pracownicy i współpracownicy podmiotów trzecich, z którymi została zawarta umowa, na mocy której ww. osoby mają dostęp do informacji chronionych, w tym danych osobowych.
- 2) Polityka Bezpieczeństwa Informacji obejmuje wszystkie informacje podlegające ochronie, przetwarzanych w pomieszczeniach Starostwa niezależnie od formy ich przetwarzania.
- 3) Do skutecznej realizacji Polityki Bezpieczeństwa Informacji, Starostwo zapewnia:
  - a) szkolenia w zakresie przetwarzania informacji i sposobów ich ochrony,
  - b) okresowe szacowanie ryzyka zagrożeń dla przetwarzanych danych,
  - c) kontrolę, monitoring i nadzór nad przetwarzaniem informacji,
  - d) monitorowanie zastosowanych środków ochrony,
  - e) wdrażanie odpowiednich środków technicznych i organizacyjnych, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku,
  - f) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,

- g) zdolność do szybkiego przywrócenia dostępności danych i dostępu do nich w razie incydentu fizycznego lub technicznego,
- h) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

### 3. DEFINICJE

- 1) *Administrator danych (ADO)* - Starostwo Powiatowe w Żyrardowie;
- 2) *Administrator Systemu Informatycznego ASI* - pracownik lub podmiot zewnętrzny odpowiedzialny za prawidłową pracę systemów informatycznych;
- 3) *dane osobowe* - informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
- 4) *dostępność danych* - rozumie się przez to właściwość zapewniającą, że dane są udostępniane dla upoważnionego podmiotu wtedy, gdy ich potrzebuje do przetwarzania;
- 5) *integralność danych* - rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
- 6) *Inspektor Ochrony Danych (IOD)* - osoba powołana przez administratora danych oraz zarejestrowana w Urzędzie Ochrony Danych Osobowych w celu zapewnienia prawidłowości przetwarzanych danych w Starostwie;
- 7) *naruszenie bezpieczeństwa informacji* - wszelkie zdarzenia lub działania, w tym również niezamierzone, które mogą stanowić przyczynę utraty zasobów, obniżenia wymaganego poziomu poufności, integralności, dostępności informacji lub niezawodności systemów, a także odstępstwa od obowiązujących procedur postępowania, nawet jeżeli nie prowadzą do negatywnych skutków dla organizacji. Zdarzenia lub działania, które mogą prowadzić do naruszenia praw lub wolności osób fizycznych;
- 8) *naruszenie ochrony danych osobowych* - naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
- 9) *odbiorca danych* - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem powszechnie obowiązującym, nie są jednak uznawane za odbiorców - przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych, mającymi zastosowanie stosownie do celów przetwarzania. Przy czym przez sformułowanie „strona trzecia” rozumie się osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot

przetwarzający czy osoby, które z upoważnienia Administratora lub podmiotu przetwarzającego - mogą przetwarzać dane osobowe;

- 10) *osoba upoważniona do przetwarzania danych osobowych* - osoba, która złożyła ADO oświadczenie o zachowaniu w tajemnicy przetwarzanych danych i stosowanych sposobach zabezpieczenia tych danych, posiadająca imienne upoważnienie wydane przez ADO, określające imię i nazwisko osoby upoważnionej, datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych oraz identyfikator, jeżeli dane są przetwarzane w systemie informatycznym;
- 11) *podmiot przetwarzający* - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora;
- 12) *przetwarzanie* - operacje lub zestaw operacji wykonywanych na danych, w szczególności danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
- 13) *poufność danych* - rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
- 14) *rozliczalność danych* - rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
- 15) *RODO* - Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);
- 16) *usuwanie danych* - trwałe zniszczenie danych/ trwałe zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
- 17) *uwierzytelnianie* - rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
- 18) *użytkownik/pracownik (w tym podmiotu trzeciego)* - osoba przetwarzająca dane w systemie oraz poza nim (np. dokumentacji w formie tradycyjnej), niezależnie od formy zatrudnienia w Starostwie lub formy prawnej wiążącej z tą osobą. W szczególności mogą być to osoby zatrudnione na umowę o pracę, stażyści, praktykanci, osoby realizujące zadania na podstawie podpisanej umowy cywilnoprawnej;
- 19) *zbiór danych* - to uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
- 20) *zgoda na przetwarzanie danych osobowych* - oświadczenie woli osoby, której dane są przetwarzane przez administratora danych, w której wyraża swoją aprobatę dla tego procesu.

#### **4. OBOWIĄZKI OSÓB PRZETWARZAJĄCYCH INFORMACJE**

- 1) Każda osoba przetwarzająca informacje na potrzeby Starostwa jest obowiązana zapoznać się z treścią Polityki Bezpieczeństwa Informacji oraz bezwzględnie stosować się do jej zapisów.
- 2) Pracownicy/użytkownicy są zobowiązani do przestrzegania przepisów prawa powszechnie obowiązującego i regulacji wewnętrznych dotyczących ochrony danych, w tym danych osobowych tj. Polityki ochrony danych osobowych Starostwa Powiatowego w Żyrardowie.
- 3) Pracownicy/użytkownicy przetwarzający dane obowiązani są dołożyć należytej staranności w celu ich ochrony.
- 4) Naruszenie postanowień Polityki Bezpieczeństwa Informacji może skutkować zablokowaniem dostępu pracownika/użytkownika do informacji chronionych i systemów. W przypadku ciężkich naruszeń, takie działanie może prowadzić do wszczęcia postępowania dyscyplinarnego oraz do rozwiązania bądź wypowiedzenia umowy. W przypadku poniesienia strat w wyniku naruszenia, może dochodzić roszczeń odszkodowawczych na drodze sądowej.
- 5) Każde naruszenie bezpieczeństwa informacji powinno być niezwłocznie zgłaszane Administratorowi oraz w przypadku naruszeń ochrony danych osobowych Inspektorowi Ochrony Danych lub, w przypadku naruszeń bezpieczeństwa dotyczących systemów informatycznych, Administratorowi Systemu Informatycznego.
- 6) W razie wykrycia naruszenia ochrony informacji chronionych każdy pracownik ma obowiązek postępować zgodnie z procedurami określonymi w Starostwie.
- 7) Osoby odpowiedzialne za zarządzanie kadrami w Starostwie informują niezwłocznie ADO oraz ASI o każdej zmianie w zakresie czynności pracowników, która wiąże się ze zmianą zakresu uprawnień do przetwarzania informacji chronionych.
- 8) Cofnięcie upoważnień do przetwarzania informacji chronionych powinno nastąpić niezwłocznie po zakończeniu wykonywania obowiązków pracownika/ użytkownika.
- 9) Rozliczenie pracownika z aktywów związanych z przetwarzaniem informacji chronionych powinno odbywać się na podstawie stosowanej karty obiegu lub innych procedur określonych w Starostwie.

## **5. ORGANIZACJA SYSTEMU OCHRONY INFORMACJI**

- 1) Administrator danych odpowiada za zakres i bezpieczeństwo przetwarzania danych w Starostwie, w tym danych osobowych.
- 2) Administrator danych zapewnia i stosuje odpowiednie środki informatyczne, techniczne i organizacyjne, zapewniając ochronę przetwarzanych informacji, a w szczególności:
  - a) podejmuje decyzje o celach i środkach przetwarzania danych,
  - b) podejmuje decyzje o technicznych i organizacyjnych zabezpieczeniach oraz wdraża zasady i procedury postępowania mające na celu zapewnienie adekwatnego poziomu bezpieczeństwa przetwarzanych danych,
  - c) upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnym zakresie, odpowiadającym zakresowi jej obowiązków,

- d) wyznacza Administratora Systemów Informatycznych oraz określa zakres jego zadań i czynności w zakresie ochrony danych w systemach (wzór powołania ASI stanowi załącznik nr 1 do niniejszej Polityki),
- e) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia bezpieczeństwa informacji,
- f) prowadzi kontrolę przestrzegania procedur ochrony informacji,
- g) zapewnia środki techniczne oraz organizacyjne w celu zapewnienia działań wymaganych przez przepisy prawa dotyczące ochrony informacji,
- h) reprezentuje Starostwo w postępowaniach przed organami publicznymi oraz w kontaktach z podmiotami trzecimi w sprawach związanych z pozyskiwaniem, przetwarzaniem, ochroną informacji,
- i) analizuje sprawozdania Inspektora Ochrony Danych, weryfikuje ocenę ryzyka i ocenę skutków związane z przetwarzaniem danych osobowych, a także decyduje o formach przeciwdziałania ewentualnym zagrożeniom,
- j) zapewnia udział osób o odpowiednich kompetencjach i wiedzy (pracowników Administratora i podmiotów zewnętrznych) przy realizacji audytów i weryfikacji systemu ochrony informacji,
- k) zapewnia bezpieczne brakowanie danych, zwłaszcza w przypadku uzasadnionego żądania niezwłocznego usunięcia danych osobowych, bez zbędnej zwłoki,
- l) powołuje Inspektora Ochrony Danych (wzór powołania IOD stanowi załącznik nr 2 do niniejszej Polityki).

## **6. OBOWIĄZYWANIE DOKUMENTU**

Polityka Bezpieczeństwa Informacji wchodzi w życie z dniem przyjęcia i obowiązuje na wszystkich stanowiskach oraz obszarach gdzie dochodzi do przetwarzania informacji podlegających ochronie.

## **7. WYKAZ ZAŁĄCZNIKÓW**

Załącznik nr 1 – Wzór powołania Administratora Systemów Informatycznych

Załącznik nr 2 – Wzór powołania Inspektora Ochrony Danych

## **8. DOKUMENTY ZWIĄZANE**

Polityka ochrony danych osobowych w Starostwie Powiatowym w Żyrardowie

Instrukcja zarządzania systemem informatycznym w Starostwie Powiatowym w Żyrardowie

WICESTAROSTA

Krzysztof Dziwisz