Polityka Bezpieczeństwa Informacji

w Starostwie Powiatowym w Gołdapi

STAROSTA
Marzanna Marianna
Wardziejewska

30. 12. 2022

Spis treści

Dokumenty powiązane:
Instrukcja zarządzania systemami informatycznymi.
Zasady bezpiecznej pracy.
Instrukcja zarządzania ryzykiem.
Instrukcja kancelaryjna.

Wstęp

Polityka bezpieczeństwa określa sposób prowadzenia i zakres dokumentacji opisującej sposób przetwarzania informacji oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych informacji odpowiednią do zagrożeń oraz kategorii danych objętych ochroną w Starostwie Powiatowym w Gołdapi.

Dokumentacja „Polityki bezpieczeństwa informacji" została opracowania na podstawie przepisów art. 20 ust. 1 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. Nr 2247.).

Jako załącznik do niniejszej polityki opracowano i wdrożono:

Instrukcję zarządzania systemem informatycznym służącym do przetwarzania informacji, zwaną dalej **„Instrukcją zarządzania systemem informatycznym"**. Określa ona sposób zarządzania systemem informatycznym, służącym do przetwarzania informacji, ze szczególnym uwzględnieniem zapewnienia bezpieczeństwa informacji.

Zasady bezpiecznej pracy w systemach informatycznych, zwanej dalej „Instrukcją użytkownika", określająca sposoby bezpiecznego wykorzystania systemów informatycznych obowiązująca wszystkich pracowników.

Instrukcja zarządzania ryzykiem, zwanej dalej „Analizą ryzyka", określająca zasady szacowania ryzyka i postępowania z zidentyfikowanymi ryzykami.

Ze względu na to, że urządzenia systemu informatycznego, służącego do przetwarzania informacji, połączone są z siecią publiczną, zgodnie z rozporządzeniem Starostwo Powiatowe w Gołdapi ma obowiązek zapewnić środki bezpieczeństwa tych danych na poziomie wysokim.

Kierownictwo mając na uwadze dobro stron pragnie dołożyć szczególnej staranności w ochronę interesów tych osób. Propaguje aktywne podejście do zarządzania bezpieczeństwem informacji. Kierownictwo deklaruje zaangażowanie w realizację postanowień polityki i aktywne propagowanie bezpieczeństwa wewnątrz instytucji.

Cele Polityki bezpieczeństwa

1. Celem Polityki Bezpieczeństwa jest ochrona systemu informacyjnego i jego poszczególnych elementów, a przede wszystkim zapewnienie technicznych i organizacyjnych zabezpieczeń mających wpływ na zarządzanie systemami informacyjnymi.
2. Celem polityki bezpieczeństwa jest:

1) zapewnienie ochrony informacji przed wszelkiego rodzaju zagrożeniami, tak wewnętrznymi, jak i zewnętrznymi, świadomymi lub nieświadomymi,
2) wskazanie działań, jakie należy wykonać oraz ustanowienie zasad i reguł postępowania, które należy stosować, aby właściwie wykonać obowiązki w zakresie bezpieczeństwa danych osobowych.

Przepisy ogólne

1. Niniejszy dokument został opracowany na podstawie zapisów Polskiej Normy PN-ISO/IEC-27000 określającej praktyczne zasady zarządzania bezpieczeństwem informacji w obszarze technik informatycznych.
2. Polityka bezpieczeństwa obowiązuje wszystkich pracowników.
3. Administrator Danych, którym jest Starosta Gołdapski, powołał Inspektora Ochrony Danych.
4. IOD podlega bezpośrednio nadzorującemu jednostkę.
5. Do zadań Inspektora Ochrony Danych należy :
   1) *zapewnienie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:*
      a) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowywanie w tym zakresie sprawozdania dla administratora danych,
      b) nadzorowanie opracowania i aktualizowania dokumentacji opisującej sposób przetwarzania danych,
      c) nadzorowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych osobowych,
      c) zapewnienie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz dokumentacją Polityki Bezpieczeństwa Informacji,
      d) wykonywanie sprawdzeń.
   2) prowadzenie rejestru czynności przetwarzania danych osobowych.

Definicje

Ilekroć w dokumencie jest mowa o:

1. **PBI (Polityce bezpieczeństwa informacji),**– należy przez to rozumieć „Politykę bezpieczeństwa informacji w Starostwie Powiatowym w Gołdapi";
2. **Danych osobowych** - należy przez to rozumieć wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;

3. **Przetwarzaniu danych** – należy przez to rozumieć jakiekolwiek operacje wykonywane na danych osobowych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;
4. **Systemie informacyjnym** – należy przez to rozumieć posiadającą wiele poziomów strukturę pozwalającą użytkownikowi na przetwarzanie, za pomocą procedur i modeli, informacji wejściowych w wyjściowe;
5. **Systemie informatycznym** – należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
6. **Zabezpieczeniu danych w systemie informatycznym** – należy przez to rozumieć wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
7. **Usuwaniu danych** – należy przez to rozumieć zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
8. **Odbiorcy danych** – należy przez to rozumieć każdego, komu udostępnia się dane osobowe;
6. **Administratorze Danych Osobowych (ADO)** – należy przez to rozumieć Starostę Gołdapskiego.
7. **Osobie upoważnionej lub użytkowniku systemu** – należy przez to rozumieć osobę posiadającą upoważnienie wydane przez ADO (lub osobę uprawnioną przez niego) i dopuszczoną jako użytkownik do przetwarzania danych osobowych w systemie informatycznym, w zakresie wskazanym w upoważnieniu;
8. **Sieci Lokalnej (LAN** Local Area Network**)** – sieć w siedzibie Urzędu pozwalająca na połączenie stacji roboczych z serwerami.
9. **Sieci rozległej (WAN)** – należy przez to rozumieć sieć Internet;
10. **Identyfikatorze użytkownika** – należy przez to rozumieć ciąg znaków literowych, cyfrowych i specjalnych umożliwiający jednoznaczną identyfikację osoby upoważnionej do przetwarzania danych osobowych w systemie informatycznym;
11. **Haśle** - należy przez to rozumieć ciąg znaków literowych, cyfrowych i specjalnych znany jedynie osobie uprawnionej (użytkownikowi) umożliwiający wejście (zalogowanie się) i pracę w systemie informatycznym;
12. **Zalogowaniu** –należy przez to rozumieć uwierzytelnienie czyli działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

Nadzorowanie PBI

1.Nadawanie upoważnień.

1) Do przetwarzania danych osobowych dopuszczone są wyłącznie osoby posiadające upoważnienie nadane przez Administratora Danych Osobowych,
2) Upoważnienie do przetwarzania danych osobowych uzyskuje osoba, której stanowisko pracy wymaga takiego zezwolenia.
3) Upoważnienie do przetwarzania danych osobowych otrzymują również osoby pracujące na terenie jednostki nie będące etatowymi pracownikami, np. stażyści oraz praktykanci.
4) Upoważnienia do przetwarzania danych osobowych nadaje Administrator Danych Osobowych.
5) Każdy pracownik, który otrzyma upoważnienie do przetwarzania danych osobowych, zobowiązuje się pisemnie do zachowania w tajemnicy tych danych oraz sposobów ich zabezpieczania.

2. Odebranie uprawnień.

1) Wyrejestrowanie użytkownika z systemu informatycznego może mieć charakter czasowy lub trwały.
2) ASI wyrejestrowuje na stałe użytkownika z systemu na podstawie kserokopii karty obiegowej (przedłożonej mu przez użytkownika, kierownika komórki organizacyjnej lub pracownika ds. kadr), która pozostaje w posiadaniu ADO.
3) Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy lub innego stosunku prawnego, w ramach którego użytkownik wykonywał zadania.
4) Na pisemny wniosek kierownika danej komórki organizacyjnej wyrejestrowanie może mieć charakter czasowy.
5) Czasowe wyrejestrowanie użytkownika z systemu informatycznego występuje w razie:
    1) zawieszenia w pełnieniu obowiązków służbowych,
    2) wszczęcia postępowania dyscyplinarnego względem osoby upoważnionej do przetwarzania danych osobowych.
6) Czasowe wyrejestrowanie użytkownika z systemu informatycznego następuje na wniosek kierownika komórki organizacyjnej, poprzez zablokowanie konta użytkownika do czasu ustania przyczyn uzasadniających blokadę, tj. do czasu złożenia przez kierownika danej komórki organizacyjnej pisemnego wniosku o odblokowanie konta użytkownika.
7) Czasowe wyrejestrowanie następuje poprzez zablokowanie konta użytkownika do czasu ustania przyczyn uzasadniających blokadę.

Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

Część ta zawiera opis środków technicznych, organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych. Szczególny opis zawarto w **Instrukcji zarządzania systemem informatycznym**.

Polityka obejmuje następujące zasady:

- ochrony fizycznej
- pracy z danymi osobowymi,
- autoryzacji w systemach informatycznych,
- zarządzania majątkiem,
- zarządzania hasłami,
- dotyczące polityki czystego biurka i czystego ekranu,
- postępowania z nośnikami wymiennymi,
- korzystania z usług w sieci Internet,
- zarządzania oprogramowaniem,
- zarządzania ryzykami,
- monitorowania bezpieczeństwa,
- udostępniania informacji,
- zarządzania zmianą w systemach informatycznych,
- zarządzania incydentami,
- zarządzania kopiami zapasowymi.

Postanowienia końcowe

1. Polityka Bezpieczeństwa jest dokumentem wewnętrznym i nie może być udostępniana osobom postronnym w żadnej formie.
2. Pracownicy są zobligowani do zapoznania się z dokumentem polityki bezpieczeństwa oraz z zasadami bezpiecznej pracy i bezwzględnego przestrzegania zasad w nim zawartych.
3. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych.
4. Wobec osoby, która w przypadku powzięcia informacji o naruszeniu zabezpieczeń systemu informacyjnego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.
5. Kara dyscyplinarna orzeczona wobec osoby uchylającej się od powiadomienia, nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z 24 maja 2018 r. o ochronie danych

osobowych oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

6. Polityka bezpieczeństwa wchodzi w życie z dniem podpisania.
7. Jakiekolwiek zmiany wprowadzone w załącznikach do niniejszego dokumentu nie wymagają zmiany zarządzenia, które wprowadziło niniejszą instrukcję w życie.