

**STAROSTWO POWIATOWE W KAMIENIU POMORSKIM**

---



**Instrukcja Zarządzania Systemem Informatycznym  
służącym do przetwarzania  
Danych Osobowych**

w Starostwie Powiatowym w Kamieniu Pomorskim  
ul. Wolińska 7b

**OPRACOWAŁ :** Andrzej ZIELIŃSKI  
Pełnomocnik  
ds. Ochrony Informacji Niejawnych

## SPIS TREŚCI

1. WSTĘP	3
2. DEFINICJE	3
3. POSTANOWIENIA OGÓLNE	3
4. OBOWIĄZKI W ZAKRESIE OCHRONY DANYCH OSOBOWYCH	4
5. POZIOM BEZPIECZEŃSTWA	4
6. BEZPIECZNA EKSPLOATACJA SPRZĘTU I OPROGRAMOWANIA	4
7. PROCEDURA KORZYSTANIA Z INTERNETU I POCZTY ELEKTRONICZNEJ	5
8. PROCEDURA NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH	7
9. METODY I ŚRODKI UWIERZYTELNIAJĄCE	7
10. WYMOGI DOTYCZĄCE ZMIANY HASEŁ	9
11. PROCEDURA ROZPOCZĘCIA , ZAWIESZENIA I ZAKOŃCZENIA PRACY	9
12. PROCEDURA TWORZENIA KOPI ZAPASOWYCH	9
13. SPOSÓB, MIEJSCE I OKRES PRZECHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI I WYDRUKÓW	10
14. PROCEDURA ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO , PRZED DZIAŁALNOŚCIĄ OPROGRAMOWANIA ZŁOŚLIWEGO	11
15. ZASADY I SPOSÓB ODNOTOWYWANIA W SYSTEMIE INFORMACJI O UDOSTĘPNIANIU DANYCH OSOBOWYCH	12
16. PROCEDURA WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI	12
17. ZAŁĄCZNIKI	13
Załącznik nr 1- Wzór - Oświadczenie	
Załącznik nr 2- Wzór - Upoważnienie do przetwarzania danych osobowych	
Załącznik nr 3- Rejestr użytkowników i ich uprawnień w systemie informatycznym.	
Załącznik nr 4 – Wzór- Zlecenia nadania/ zmiany/ anulowania zakresu uprawnień użytkownika	
. Załącznik nr 5 – Ewidencja udostępniania danych	
Załącznik nr 6 - Wzór- Protokół zniszczenia uszkodzonych nośników komputerowych	
Załącznik nr 7 – Wzór – Rejestr nośników komputerowych zawierających kopie zapasowe	

## 1. Wstęp

Podstawę prawną do opracowania i wdrożenia niniejszej instrukcji stanowią ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych ( t. j. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr. 100, poz. 1024 z późn. zm. ) Instrukcja stanowi zestaw procedur opisujących zasady zapewnienia bezpieczeństwa danych osobowych w systemach i aplikacjach informatycznych.

## 2. Definicje

2.1 Ilekoć w niniejszym dokumencie jest mowa o :

- 2.1.1 **Urządzie** – należy przez to rozumieć Starostwo Powiatowe w Kamieniu Pomorskim
- 2.1.2 **Administratorze Danych Osobowych (ADO)** – należy przez to rozumieć Starostę Kamieńskiego ( zwany dalej Starostą ) decydującego o celach i środkach przetwarzania danych osobowych.
- 2.1.3 **Administratorze Bezpieczeństwa Informacji (ABI)** – pracownik Starostwa, wyznaczony przez Starostę , odpowiedzialny za organizację ochrony danych osobowych
- 2.1.4 **Administrator Systemu Informatycznego (ASI)** - pracownik Starostwa, wyznaczony przez Starostę, odpowiedzialny za bezpieczeństwo danych osobowych przetwarzanych we wskazanych systemach informatycznych, nadzorujący pracę systemu informatycznego oraz wykonujący w nim czynności wymagające specjalnych uprawnień. ASI odpowiedzialny jest za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego do przetwarzania danych osobowych
- 2.1.5 **Użytkownika systemu** - należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym urzędu.

## 3. Postanowienia ogólne

- 3.1 Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w urzędzie zwana dalej „Instrukcją” określa zasady, tryb postępowania i zalecenia Administratora Danych Osobowych, które muszą być stosowane przez osoby przez niego upoważnione do przetwarzania danych osobowych w systemach informatycznych.
- 3.2 Instrukcja została opracowana zgodnie z wymogami § 5 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).
- 3.3 Podstawowymi celami zabezpieczeń systemów informatycznych służących do przetwarzania danych osobowych jest zapewnienie jak najwyższego poziomu bezpieczeństwa przetwarzanych danych osobowych w systemach informatycznych.

3.4 Za priorytet uznano zagwarantowanie zgromadzonemu danym osobowemu, przez cały okres ich przetwarzania w systemach, charakteru poufności wraz z zachowaniem ich integralności i rozliczalności.

3.5 Administrator Bezpieczeństwa Informacji powinien posiadać stosowne uprawnienia w nadzorowanych systemach informatycznych, gwarantujące skuteczne wykonywanie zadań z zakresu nadzoru wszędzie tam, gdzie jest to możliwe.

## **4. Obowiązki w zakresie ochrony danych osobowych**

4.1 Do obowiązków osób zaangażowanych w przetwarzanie danych osobowych w systemach informatycznych należy:

4.1.1, Podejmowanie współpracy przy ustaleniu przyczyn naruszenia ochrony danych osobowych oraz usuwania skutków tych naruszeń, w tym zapobieganie ich ewentualnemu ponownemu wystąpieniu.

4.1.2. Przetwarzanie danych osobowych wyłącznie w celach określonych przez swoich przełożonych.

4.2 Do kompetencji osób zarządzających pracownikami należy w szczególności wystawianie dla bezpośrednio podległych pracowników wniosków o nadanie, zmianę lub cofnięcie uprawnień do systemów informatycznych, w których są przetwarzane dane osobowe.

4.3 Użytkownicy powinni podlegać okresowym szkoleniom, stosownie do potrzeb wynikających ze zmian w systemie informatycznym (wymiana sprzętu na nowszej generacji, zmiana oprogramowania) oraz w związku ze zmianą przepisów o ochronie danych osobowych lub zmianą wewnętrznych regulacji.

## **5. Poziom bezpieczeństwa**

W Starostwie Powiatowym w Kamieniu Pomorskim obowiązuje wysoki poziom bezpieczeństwa systemu informatycznego z uwagi na to, że jest on połączony z siecią publiczną (z Internetem).

## **6. Bezpieczna eksploatacja sprzętu i oprogramowania**

Celem procedury jest określenie wymagań bezpieczeństwa dla sprzętu i oprogramowania eksploatowanego w Starostwie Powiatowym w Kamieniu Pomorskim. Bezpieczna eksploatacja systemów informatycznych przetwarzających dane osobowe zostaje zapewniona poprzez przestrzeganie następujących zasad:

6.1 Użytkownikom zabrania się wprowadzania zmian do oprogramowania, sprzętu informatycznego poprzez jego samodzielne konfigurowanie i wyposażanie.

6.2 Użytkownikom zabrania się umożliwiania stronom trzecim uzyskiwania nieupoważnionego dostępu do systemów informatycznych.

6.3 Użytkownikom nie wolno instalować nowego lub aktualizować już zainstalowanego oprogramowania.

6.4 Użytkownikom nie wolno korzystać z systemów informatycznych dla celów innych niż związane z wykonywaniem obowiązków służbowych.

- 6.5 Użytkownikom nie wolno podejmować prób testowania, modyfikacji i naruszenia zabezpieczeń systemów informatycznych lub jakichkolwiek działań noszących takie znamiona.
- 6.6 Informacje przetwarzane przy użyciu współdzielonych aplikacji sieciowych na stacjach roboczych muszą być zapisywane na dyskach serwera.
- 6.7 Wszystkie aplikacje sieciowe, współdzielone zasoby użytkowe muszą być ulokowane na przeznaczonych do tego celu serwerach.
- 6.8 Nieautoryzowane podłączenie własnego lub strony trzeciej urządzenie teleinformatycznego do systemu informatycznego jest zabronione.
- 6.9 Urządzenia aktywne obsługujące sieć lokalną urzędu chronią ją na poziomie warstwy łącza danych na ewentualność podłączenia obcych urządzeń.
- 6.10 Ekrany monitorów są wyposażone w wygaszacie zabezpieczone hasłem , które aktywują się automatycznie po upływie określonego czasu od ostatniego użycia komputera.
- 6.11 Programy zainstalowane na komputerach obsługujących przetwarzanie danych osobowych są użytkowane z zachowaniem praw autorskich i posiadają licencje.
- 6.12 Instalacji oprogramowania może dokonywać jedynie pracownik Starostwa Powiatowego w Kamieniu Pomorskim - Administratora Systemu Informatycznego (ASI). W razie konieczności instalacji oprogramowania przez pracowników firm zewnętrznych czynność ta powinna być wykonywana za przyzwoleniem i w obecności pracownika komórki informatyzacji.
- 6.13 System Informatyczny wyposażony jest w mechanizmy oraz uwierzytelnienia użytkownika sprawujące kontrole dostępu do danych osobowych jedynie osób upoważnionych.
- 6.14 Użytkownikom nie wolno uruchamiać oprogramowania z innych źródeł ( nośniki wymienne , Internet ) bez zgody Administratora Systemu Informatycznego (ASI).
- 6.15 Komputer przenośny może być używany do przetwarzania danych osobowych po odpowiednim jego zabezpieczeniu.
- 6.16 Użytkownik korzystający z komputera przenośnego jest zobowiązany do zachowania szczególnej ostrożności podczas transportu komputera oraz nie może udostępniać komputera osobom nieupoważnionym.
- 6.17 Ekrany monitorów są ustawione w miarę możliwości w taki sposób , żeby uniemożliwić odczyt wyświetlanych informacji osobom nieupoważnionym.

## **7. Procedury korzystania z Internetu i poczty elektronicznej**

Celem procedury jest uregulowanie zasad korzystania z internetu i poczty elektronicznej, aby zagwarantować bezpieczeństwo danych osobowych przesyłanych przez media. Użytkownicy internetu zobowiązani są do przestrzegania następujących zasad:

- 7.1 Zakazuje się ściągania przez użytkowników plików lub przeglądania zasobów informacyjnych o treści prawnie zabronionej , obscenicznej bądź pornograficznej.
- 7.2 Zaleca się, aby do wymiany korespondencji w czasie korzystania z systemu informatycznego urzędu wykorzystywać jedynie służbową pocztą elektroniczną.
- 7.3 Szczególne rygory należy stosować wobec ściągania z Internetu plików wykonywalnych. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowania ściągnięte z Internetu i przez niego używane.
- 7.4 Do korzystania z internetu użytkownicy mogą wykorzystywać jedynie zaakceptowane przez Administratora Systemu Informatycznego (ASI) formy dostępu ( dotyczy prób obchodzenia poustawianych obostrzeń oraz podłączania dodatkowych urządzeń komunikacyjnych).

Użytkownicy systemu poczty elektronicznej zobowiązani są do przestrzegania następujących zasad:

- 7.5 Przesyłanie informacji za pośrednictwem poczty elektronicznej winno odbywać się zgodnie z uprawnieniami adresatów do korzystania z określonego typu danych. W przypadku wątpliwości nadawca powinien sprawdzić, czy dana osoba ma uprawnienia do korzystania z dokumentów danego typu lub o określonej klauzuli poprzez skonsultowanie się z Administratorem Systemu Informatycznego (ASI).
- 7.6 Jeśli adresatem wiadomości zawierającej dane osobowe jest pracownik urzędu zaleca się doręczenia danych w formie elektronicznej w sposób wykorzystujący wewnętrzne mechanizmy przekazywania danych ( dyski sieciowe, udostępnienia folder użytkownika docelowego).
- 7.7 Przesyłanie informacji poza obręb urzędu może odbywać się tylko przez osoby do tego upoważnione do adresatów upoważnionych do przesyłanych danych.
- 7.8 W razie konieczności przesyłania danych osobowych dane te należy uprzednio odpowiednio zabezpieczyć wykorzystując mechanizmy kompresji z szyfrowaniem z tym zastrzeżeniem , że hasło musi zostać dostarczone do adresata drogą inną niż same dane ( np. przez telefon). Złożoność hasła: na poziomie minimum 10 znaków w tym duża, mała litera, znak specjalny oraz cyfra.
- 7.9 Użytkownicy powinni zwrócić szczególną uwagę na poprawność adresu odbiorcy dokumentu.
- 7.10 Jeżeli istotne jest potwierdzenie otrzymania przez adresata przesyłki, użytkownik winien skorzystać, o ile jest to technicznie możliwe, z opcji systemu poczty elektronicznej informującej o dostarczeniu i otwarciu dokumentu. Dodatkowo zaleca się, aby użytkownik zawarł w treści dokumentu prośbę o potwierdzenie otrzymania i zapoznania się z informacją. Adresat zobowiązany jest w takiej sytuacji przesłać nadawcy potwierdzenie.
- 7.11 Informacje przesyłane za pośrednictwem poczty elektronicznej muszą być zgodne z prawem i z zasadami zawartymi w Polityce Bezpieczeństwa Danych Osobowych obowiązującej w Starostwie Powiatowym w Kamieniu Pomorskim.
- 7.12 Użytkownicy nie powinni otwierać przesyłek od nieznanych sobie osób , których tytuł nie sugeruje związku z wypełnianymi przez nich obowiązkami służbowymi. W przypadku otrzymania takiej przesyłki , użytkownik powinien ją zniszczyć lub skontaktować się z Administratorem Systemu Informatycznego (ASI).
- 7.13 Użytkownicy nie powinni uruchamiać wykonywalnych załączników ( pliki. exe) dołączonych do wiadomości przesyłanych pocztą elektroniczną. W takim przypadku użytkownik powinien poinformować o zdarzeniu Administratora Bezpieczeństwa Informacji (ABI) , który winien sprawdzić, czy załącznik stanowi zagrożenie dla przetwarzanych w systemie informatycznym informacji.
- 7.14 Użytkownicy nie powinni rozsyłać za pośrednictwem poczty elektronicznej informacji o zagrożeniach dla systemu informatycznego, „łańcuszków szczęścia”
- 7.15 Użytkownicy nie powinni rozsyłać , wiadomości zawierających załączniki o dużym rozmiarze ( powyżej 10 MB) do większej liczby adresatów. W razie konieczności przesłania większych załączników winni skontaktować się z pracownikiem komórki informatyzacji.
- 7.16 Użytkownicy powinni okresowo kasować niepotrzebne wiadomości pocztowe.

## **8. Procedura nadawania uprawnień do przetwarzania danych osobowych**

Celem procedury jest zapewnienie użytkownikom odpowiednich uprawnień do przetwarzania danych osobowych, aby redukować zagrożenie nieuprawnionego dostępu do danych osobowych i utraty poufności.

8.1 Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się z :

- 1) Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych ( Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm);
- 2) Polityką Bezpieczeństwa danych osobowych w Starostwie Powiatowym w Kamieniu Pomorskim;
- 3) Niniejszym dokumentem.

8.2 Zapoznanie się z powyższymi informacjami pracownik potwierdza własnoręcznym podpisem na oświadczeniu , którego wzór stanowi załącznik nr 1.

8.3 Administrator Systemu Informatycznego przyznaje uprawnienia w zakresie dostępu do systemu informatycznego na podstawie pisemnego zlecenia złożonego przez bezpośredniego przełożonego pracownika, którego zlecenie dotyczy - wzór zlecenia stanowi załącznik nr 4.

8.4 Zlecenie to podlega zatwierdzeniu przez ABI , na podstawie którego wydane zostaje upoważnienie do przetwarzania danych osobowych - wzór upoważnienia stanowi załącznik nr 2. Upoważnienia do przetwarzania danych osobowych wydaje ADO w stosunku do Wicestarosty i Sekretarza, natomiast ABI w stosunku naczelników i pracowników na stanowiskach samodzielnych, pozostałym osobom wydają bezpośredni przełożeni pracownika.

8.5 Przyznanie uprawnień w zakresie dostępu do systemu informatycznego polega na wprowadzeniu do systemu dla każdego użytkownika unikalnego identyfikatora , hasła oraz zakresu dostępnych danych i operacji.

8.6 Hasło ustanowione podczas przyznawania uprawnień przez Administratora Systemu Informatycznego (ASI) należy zmienić na indywidualne podczas pierwszego logowania się w systemie.

8.7 Pracownik ma prawo do wykonywania tylko tych czynności , do których został upoważniony.

8.8 Pracownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu.

8.9 Odbieranie uprawnień pracownikowi następuje na pisemny wniosek przełożonego, któremu pracownik podlega z podaniem daty oraz przyczyny odebrania uprawnień .

8.10 Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych należy bezzwłocznie wyrejestrować z systemu informatycznego, w którym są one przetwarzane oraz unieważnić jej hasło. Wzór „ Zlecenia nadania- zmiany- anulowania zakresu uprawnień użytkownika” przedstawia załącznik nr 4.

8.11 Administrator Systemu Informatycznego (ASI) zobowiązany jest do prowadzenia i ochrony rejestru użytkowników i ich uprawnień w systemie informatycznym - rejestr stanowi załącznik nr 3 .

## **9. Metody i środki uwierzytelniające.**

Celem procedury jest zapewnienie, że do systemów informatycznych przetwarzających dane osobowe mają dostęp jedynie osoby do tego upoważnione.

Identyfikatory i hasła są sposobem zagwarantowania rozliczalności, poufności i integralności danych osobowych przetwarzanych w systemach informatycznych.

Służą do weryfikowania tożsamości użytkownika, uzyskania dostępu do określonych zasobów, kont uprzywilejowanych lub uruchomienia określonej funkcjonalności.

- 9.1 Wszystkie konta dostępowe (identyfikatory) do systemów informatycznych powinny być chronione hasłem lub innym bezpiecznym, zaakceptowanym przez Administrator Systemu Informatycznego (ASI) sposobem uwierzytelniania.
- 9.2 Identyfikator oraz nadane uprawnienia powinny umożliwiać wykonywanie czynności wyłącznie zgodnych z zakresem powierzonych obowiązków.
- 9.3 Identyfikator użytkownika powinien być niepowtarzalny, a po wyrejestrowaniu się z systemu informatycznego nie powinien być przydzielany innej osobie.
- 9.4 Identyfikator, który utracił ważność nie może być ponownie przydzielony innemu użytkownikowi.
- 9.5 Hasło początkowe, które jest przydzielane przez Administratora Systemu Informatycznego (ASI), powinno umożliwiać użytkownikowi zarejestrowanie się w systemie tylko jeden raz i powinno być natychmiast zmienione przez użytkownika.

Mając na uwadze zagwarantowanie wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych oraz zagwarantowania użytkownikom pełnej rozliczalności wykonywanych przez nich operacji w systemach informatycznych, wszyscy użytkownicy przy uwierzytelnianiu do systemów informatycznych powinni stosować się do poniższych zasad:

- 9.5.1 Pierwsze hasło dla użytkownika ustala przydziela Administrator Systemu Informatycznego (ASI) przy wprowadzaniu identyfikator użytkownika do systemu.
- 9.5.2 Użytkownik systemu niezwłocznie ustala swoje, znane tylko jemu hasło, po nadaniu hasła przez Administrator Systemu Informatycznego (ASI).
- 9.5.3 Użytkownik systemu w trakcie pracy w aplikacji może zmienić swoje hasło dostępu.
- 9.5.4 Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów.
- 9.5.5 Hasło nie może być ujawnione nawet po utracie przez nie ważności.
- 9.5.6 Hasła mają charakter poufny - są znane tylko jego właścicielowi.
- 9.5.7 Zabronione jest zapisywanie haseł w sposób jawny oraz przekazywanie ich innym osobom.
- 9.5.8 Hasło winno składać się z co najmniej 8 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.
- 9.5.9 Hasła administratora do poszczególnych programów / systemów powinny być spisane oraz umieszczone w zamkniętej kopercie w miejscu uniemożliwiającym dostęp do nich osobom nieupoważnionym, chroniącym przed utratą lub zniszczeniem oraz gwarantującym ich odczytanie upoważnionemu użytkownikowi, a także kierownikowi urzędu.
- 9.5.10 Zarejestrowane hasła administratora, oprócz treści hasła winny posiadać adnotację o dacie ich wprowadzenia do systemu.
- 9.5.11 W przypadku utraty uprawnień przez osobę administrującą systemem należy niezwłocznie zmienić hasła, do których miała dostęp.

#### **Uwierzytelnienie na poziomie dostępu do aplikacji przetwarzającej dane osobowe.**

- 9.6 Hasło na poziomie dostępu do programu powinno składać się z co najmniej 8 znaków, zawierać małe i wielkie litery, cyfry i znaki specjalne.
- 9.7 O ile aplikacja nie umożliwia wymuszenia zasad zmiany haseł za systematyczna oraz terminowa zmianę hasła odpowiada użytkownik.

9.8 Zmiana hasła do systemu operującego następuje nie rzadziej , niż co 30 dni oraz niezwłocznie w przypadku podejrzenia , że hasło mogło zostać ujawnione.

## **10. Wymogi dotyczące zmiany haseł.**

10.1 Użytkownik jest zobowiązany zmieniać hasło, w którego posiadaniu się znajduje:

10.1.1 Okresowo, zgodnie z wymaganiami dla danego systemu informatycznego (przed upływem terminu ważności hasła).

10.1.2 W przypadku ujawnienia lub podejrzenia ujawnienia hasła.

10.2 W przypadku braku dostępu do konta chronionego hasłem, w którego posiadaniu się znajduje, użytkownik zobowiązany jest wystąpić o zmianę hasła do Administratora Systemu Informatycznego (ASI), w sytuacji:

1) Zapomnienia/zgubienia hasła.

2) Wygaśnięcia ważności hasła.

3) Zablokowania konta spowodowanego nieprawidłowym wprowadzeniem hasła.

4) Braku uprawnień/interfejsu umożliwiających samodzielną zmianę hasła.

10.3 Zmiana haseł użytkowników powinna być wymuszana przez system co 30 dni, w przypadku braku wymuszenia przez system, użytkownik sam jest zobowiązany do zmiany hasła co 30 dni.

## **11. Procedura rozpoczęcia, zawieszenia i zakończenia pracy**

Celem procedury jest zabezpieczenie danych osobowych przed nieuprawnionym dostępem i utratą poufności w sytuacji , gdy użytkownik rozpoczyna, przerywa lub kończy pracę w systemie informatycznym przetwarzającym dane osobowe.

11.1 Rozpoczynając pracę na komputerze użytkownik loguje się do systemu informatycznego.

11.2 Dostęp do danych osobowych możliwy jest jedynie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia użytkownika.

11.3 Jeśli system to umożliwia , po przekroczeniu 5 prób logowania system blokuje dostęp do systemu informatycznego na poziomie danego użytkownika.

11.4 ASI ustala przyczyny zablokowania systemu oraz w zależności od zaistniałej sytuacji podejmuje odpowiednie działania. O zaistniałym incydencie powiadamia Administratora Bezpieczeństwa Informacji (ABI).

11.5 Przed opuszczeniem stanowiska pracy, użytkownik obowiązany jest:

11.5.1 wylogować się z systemu informatycznego, lub

11.5.2 wywołać blokowany hasłem wygaszacz ekranu.

11.6 Kończąc pracę należy:

11.6.1 wylogować się z systemu informatycznego , a następnie wyłączyć sprzęt komputerowy,

11.6.2 zabezpieczyć stanowisko pracy , w szczególności wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się dane osobowe.

## **12. Procedura tworzenia kopii zapasowych.**

Tworzenie kopii bezpieczeństwa danych osobowych z programów.

12.1 . Kopie zapasowe danych z programów przetwarzających dane osobowe wykonywane są na koniec każdego dnia roboczego z wykorzystaniem odpowiednio skonfigurowanych zasobów sieciowych urzędu.

- 12.2 Kopie zapasowe na macierz dyskową wykonuje się w cyklu dziennym oraz miesięcznym
- 12.3 Zapis kopii zapasowych na macierzy dyskowej dokonuje się w sposób rotacyjny, zapewniający zachowanie kopii miesięcznych z okresu minimum 3 miesięcy, po tym okresie kopia jest usuwana .
- 12.4 W wypadku użycia nośnika zewnętrznego kopie zapasowe są odpowiednio oznakowane- Załącznik nr 7
- 12.5 Poza macierzą dyskową miesięczne kopie bezpieczeństwa przechowywane są na serwerach plików odpowiednio do tego celu zabezpieczonych.
- 12.6 ASI sprawuje nadzór nad wykonywaniem kopii zapasowych oraz weryfikuje ich poprawność.
- 12.7 W przypadku wystąpienia problemów z archiwizacją , konieczny jest kontakt z Administratorem Systemu Informatycznego (ASI).

### **13. Sposób , miejsce i okres przechowywania elektronicznych nośników informacji i wydruków.**

Procedura określa sposób postępowania z nośnikami , na których znajdują się dane osobowe, celem zabezpieczenia ich przed niszczeniem , kradzieżą , dostępem osób nieupoważnionych.

#### **13.1 Dane osobowe mogą być przechowywane:**

- 13.1.1 Na serwerach zlokalizowanych w obszarach wyznaczonych do przetwarzania danych osobowych.

- 13.1.2 Na wymiennych nośnikach elektronicznych.

13.2 Po wykorzystaniu dane osobowe w postaci elektronicznej należy niezwłocznie usunąć z nośnika elektronicznego w sposób uniemożliwiający ich ponowne odtworzenie.

13.3 Wykorzystanie wymiennych nośników elektronicznych (CD/DVD, pamięć USB, wymienna karta pamięci, dyskietka) powinno być ściśle kontrolowane i dozwolone wyłącznie dla upoważnionych użytkowników.

13.4 Wymienne nośniki elektroniczne, o ile nie są użytkowane, powinny być przechowywane w zamkniętych szafkach.

13.5 Nośniki zawierające kopie zapasowe powinny być przechowywane w innym pomieszczeniu niż to, w którym umieszczony jest serwer przetwarzający dane osobowe.

13.6 Kopie zapasowe powinny być przechowywane w odpowiednio zabezpieczonej, ognioodpornej szafie, do której dostęp mogą mieć wyłącznie osoby upoważnione.

13.7 Nośniki magnetyczne i optyczne z danymi osobowymi powinny być:

- 13.7.1 Oznaczane i przechowywane w zamkniętych szafach lub sejfach.

- 13.7.2 Przechowywane maksymalnie przez okres wskazany dla danego rodzaju danych osobowych przez Administratora Bezpieczeństwa Informacji (ABI).

13.8 Pracownicy nie mogą wносить na zewnątrz urzędu wymiennych elektronicznych nośników informacji z zapisanymi danymi osobowymi bez zgody Administratora Danych Osobowych (ADO).

13.9 Dane osobowe w postaci elektronicznej należy usuwać z nośnika informacji w sposób uniemożliwiający ich ponowne odtworzenie , nie później niż po upływie tygodnia , po wykorzystaniu tych danych, chyba, że z odrębnych przepisów wynika obowiązek ich przechowywania.

- 13.10 Uszkodzone nośniki komputerowe , zawierające dane osobowe , są fizycznie niszczone przy udziale komisji powołanej przez Administratora Danych Osobowych (ADO), który sporządza protokół z wykonywanych czynności. Załącznik nr 6.
- 13.11 Nośniki danych są przechowywane w sposób uniemożliwiający dostęp do nich osób nieupoważnionych, jak również zabezpieczający je przed zagrożeniami środowiskowymi (zalanie, pożar, wpływ pól elektromagnetycznych )
- 13.12 Zaleca się, aby informacje wewnętrzne znajdujące się na nośnikach przenośnych, wynoszonych poza teren placówki , były szyfrowane.
- 13.13 Kopie zapasowe
  - 13.13.1 Kopie zapasowe zbioru danych osobowych oraz oprogramowania i narzędzi programowych zastosowanych do przetwarzania danych są przechowywane w metalowej szafie w budynku B pok. nr 10 B
  - 13.13.2 Dostęp do kopii zapasowych mają tylko upoważnieni pracownicy, tj. ABI oraz ASI.
  - 13.13.3 Cotygodniowe kopie bezpieczeństwa przechowywane są do momentu kolejnego nagrania wynikającego z cyklu rotacyjnego zapisu nośników.
- 13.14 Kopie archiwalne miesięczne przechowywane są przez okres ok. 3 miesięcy, po czym nośnik poddawany jest kolejnemu procesowi zapisania danych archiwalnych.
- 13.15 Nośniki, na których znajdują się kopie zawierające dane osobowe , są oznaczone w sposób trwały, jednoznacznie i czytelny i zaewidencjonowany w „Rejestrze nośników komputerowych zawierających ważne dane” stanowiącym Załącznik nr 7 do niniejszej instrukcji.
- 13.16 Kopie archiwalne należy:
  - 1) Okresowo sprawdzać pod kątem ich dalszej przydatności do odtwarzania.
  - 2) Bezzwłocznie usuwać po ustaniu użyteczności.
- 13.17 Wydruki
  - 13.17.1 Wydruki/ dokumenty np.: umowy , faktury, zawierające dane osobowe, przechowuje się w pokojach stanowiących obszar przetwarzania danych osobowych , określony w Polityce Bezpieczeństwa.
  - 13.17.2 Wydruki / dokumenty, zawierające dane osobowe , należy niszczyć przez pocięcie w niszczarce lub spalać w miejscu do tego wyznaczonym.
- 13.18 Za bezpieczeństwo danych osobowych zapisanych w formie tradycyjnej odpowiedzialności są osoby je przetwarzające.

#### **14. Procedura zabezpieczenia systemu informatycznego , przed działalnością oprogramowania złośliwego**

- Za ochronę antywirusową odpowiada Administrator Systemu Informatycznego (ASI). Na każdej stacji roboczej w sieci oraz serwerze przetwarzającym dane osobowe powinno być zainstalowane oprogramowanie antywirusowe skanujące na bieżąco system informatyczny.
- 14.1 Każdy komputer z dostępem do danych osobowych wyposażony jest w skaner antywirusowy.
  - 14.2 Programy antywirusowe, o których mowa poprzednio , winny być uaktywnione cały czas podczas pracy danego systemu.
  - 14.3 Wszystkie pliki otrzymywane z zewnątrz , jak również wysyłane na zewnątrz, podlegają sprawdzeniu pod kątem występowania wirusów najnowszą dostępną wersją programu antywirusowego.
  - 14.4 W przypadku stwierdzenia pojawienia się wirusy, każdy użytkownik winien powiadomić Administrator Systemu Informatycznego (ASI).

## **15. Zasady i sposób odnotowywania w systemie informacji o udostępnieniu danych osobowych.**

- 15.1 Odbiorcą danych jest każdy, komu udostępnia się dane osobowe, z wyłączeniem:
  - 15.1.1 osoby, której dane dotyczą ,
  - 15.1.2 osoby użytkownika systemu lub innej osoby upoważnionej do przetwarzania danych osobowych w urzędzie.
  - 15.1.3 podmiotu, któremu powierzono przetwarzanie danych,
  - 15.1.4 organów państwowych lub organów samorządu terytorialnego, którym danym są udostępniane w związku z prowadzonym postępowaniem.
  - 15.1.5 Dane osobowe administrowane przez Starostwo Powiatowe w Kamieniu Pomorskim mogą być udostępnione osobom lub podmiotom uprawnionym do ich otrzymania na mocy Ustawy o Ochronie Danych Osobowych oraz innych przepisów powszechnie obowiązujących.
- 15.2 Dane osobowe udostępnia się na pisemny , umotywowany wniosek , chyba, że przepis innej ustawy stanowi inaczej.
- 15.3. Dane udostępniane urzędowi przez inny podmiot można wykorzystać wyłącznie zgodnie z przeznaczeniem , dla którego zostały udostępnione.
- 15.4 ABI prowadzi ewidencje udostępniania danych, o których mowa w pkt. 2. „ Ewidencję udostępniania danych” przedstawia załącznik 5.
- 15.5 . Odnotowanie obejmuje informację o :
  - 15.5.1 nazwie jednostki organizacyjnej lub imieniu i nazwisku osoby, której udostępniono dane.
  - 15.5.2 zakresie udostępnianych danych,
  - 15.5.3 dacie udostępnienia,
- 15.6 Odnotowanie informacji powinno nastąpić niezwłocznie po udostępnieniu danych.
- 15.7 Na żądanie osoby , której dane zostały udostępnione, informacje o udostępnieniu danych są zamieszczane w pisemnym raporcie.
- 15.8 Realizacja wymogów, o których mowa w § 7 ust. I pkt 4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r spełniona jest poprzez prowadzenie „ Ewidencji udostępniania danych”.

## **16. Procedury wykonywania przeglądów i konserwacji**

- 16.1 Aktualizacja oprogramowania powinna być przeprowadzana zgodnie z zaleceniami producentów oraz opinią rynkową co do bezpieczeństwa i stabilności nowych wersji.
- 16.2 Za terminowość przeprowadzenia przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada Administrator Systemu Informatycznego (ASI).
- 16.3 Zauważone nieprawidłowości w działaniach systemu informatycznego oraz oprogramowanie powinny być niezwłocznie usunięte, a ich przyczyny przeanalizowane.
- 16.4 Wszelkie prace konserwacyjne i naprawcze sprzętu komputerowego oraz uaktualnianie systemu informatyczny, wykonywane przez podmiot zewnętrzny, powinny odbywać się na zasadach określonych w szczegółowej umowie z uwzględnieniem klauzuli dotyczącej ochrony danych.
- 16.5 W przypadku naprawy sprzętu komputerowego dane osobowe należy zabezpieczyć, natomiast w przypadku naprawy sprzętu poza terenem danej jednostki , po zabezpieczeniu-usunąć z dysku. Gdy nie ma możliwości usunięcia danych, naprawa powinna być nadzorowana przez osobę upoważnioną przez administratora systemu

## 17. Załączniki

Załącznik nr 1- Wzór- Oświadczenie

Załącznik nr 2- Wzór- Upoważnienie do przetwarzania danych osobowych

Załącznik nr 3- Rejestr użytkowników i ich uprawnień w systemie informatycznym.

Załącznik nr 4- Wzór- Zlecenia nadania/ zmiany/ anulowania zakresu uprawnień  
użytkownika

Załącznik nr 5 – Ewidencja udostępniania danych

Załącznik nr 6 - Wzór- Protokół zniszczenia uszkodzonych nośników komputerowych

Załącznik nr 7 – Wzór – Rejestr nośników komputerowych zawierających ważne dane.

**ZAŁĄCZNIK NR 1  
do Instrukcji ZSI**

.....  
Imię i nazwisko

Kamień Pomorski , dnia .....2013 r

**OŚWIADCZENIE**

Oświadczam , iż zostałam/em zapoznana/ny z przepisami dotyczącymi ochrony danych osobowych, w szczególności z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz. U. z 2002r. Nr 101 , poz. 926 ze zm.), wydanych na jej podstawie aktów wykonawczych oraz wprowadzonych i wdrożonych do stosowania przez Administratora Danych Osobowych „Polityki Bezpieczeństwa Danych Osobowych,, oraz „Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania Danych Osobowych”.

Zobowiązuje się do :

- nie ujawniania danych osobowych nieuprawnionym osobom lub instytucjom w jakiegokolwiek formie bez zgody pracodawcy;
- przestrzegania zapisów zawartych w wyżej wymienionych dokumentach;
- korzystania z oprogramowania wyłącznie w związku z wykonywaniem obowiązków pracowniczych;
- wykorzystywania jedynie legalnego oprogramowania pochodzącego z innych źródeł;
- wnoszenia, wynoszenia i użytkowania komputerów przenośnych bądź innych nośników danych wyłącznie za wiedzą i zgodą Pracodawcy;
- należytej dbałości o powierzony sprzęt i oprogramowanie;
- korzystanie z produktów w wersjach ewaluacyjnych, testowych lub w jakikolwiek inny sposób ograniczony umowami licencyjnymi może być użytkowane zgodnie z ich przeznaczeniem , wyłącznie za zgodą pracodawcy.

Naruszenie przez Pracownika jego podstawowych obowiązków pracowniczych w zakresie wskazanym powyżej, będzie stanowić podstawę do podjęcia przez Pracodawcę przysługujących mu środków prawnych, a w szczególności , może stanowić przyczynę uzasadniającą wypowiedzenie przez pracodawcę umowy o pracę lub rozwiązanie przez Pracodawcę tejże umowy z dnia 26 czerwca 1974 r. Kodeks Pracy ( tekst jedn. : Dz. U. z 1998 r ., Nr 21 , poz. 94, ze zm. )

.....

Podpis pracownika

Otrzymują :

1. Pracownik
2. Komórka ds. kadr, (do akt osobowych )

**ZAŁĄCZNIK NR 2  
do Instrukcji ZSI**

Kamień Pomorski , dnia.....2013r.

**Pani / Pan**

.....  
.....  
Wydział / Stanowisko służbowe

**UPOWAŻNIENIE  
do przetwarzania danych osobowych**

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych ( Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm. ), w związku z wykonywaniem zadań na stanowisku ..... upoważniam Panią/Pana do przetwarzania danych osobowych zawartych w zbiorach związanych z realizacją zadań zgodnych z zakresem obowiązków na zajmowanym stanowisku.

Niniejsze upoważnienie obejmuje przetwarzanie danych osobowych w formie tradycyjnej oraz elektronicznej.

Zgodnie z art. 39 ust. 2 upoważniona do przetwarzania danych osoba zobowiązana jest do zachowania w tajemnicy dane osobowe zawarte w wyżej wymienionych zbiorach również po ustaniu zatrudnienia oraz zachowania w tajemnicy informacji o ich zabezpieczeniu.

Otrzymują:

1. Osoba upoważniona
2. ABI

**ZAŁĄCZNIK NR 3**  
**do Instrukcji ZSI**

**REJESTR UŻYTKOWNIKÓW I ICH UPRAWNIENI W SYSTEMIE INFORMATYCZNYM**

Lp.	Nazwa zbioru danych (1)	Nazwa i imię użytkownika	Nazwa aplikacji	Nazwa identyfikatora	Rodzaj uprawnień (2)	Data zarejestrowania	Data wyrejestrowania	Uwagi

(1) nazwa zbioru danych

(2) Skróty stosowane do określenia uprawnień :

P- prawo do przeglądania danych na ekranie i drukowania danych

Z- prawo do zmiany danych

D- prawo do dopisywania danych

U- prawo do usuwania danych

N- prawo do zakładania nowych kont/ aktualizacji Planu Kont

O/ Z- prawo do otwierania / zamykania miesiąca / roku

A/W – prawo do akceptacji / wysyłania

A- prawo do wykonywania kopii archiwalnych

Dane aktualne na dzień : ...../...../.....

Data i podpis ABI : ...../...../.....

**ZAŁĄCZNIK NR 4**  
**do Instrukcji ZSI**

**Zlecenie**  
**Nadania/ zmiany/ anulowania zakresu uprawnień użytkownika**

▪ Nowy użytkownik	▪ Modyfikacja uprawnień	▪ Odebranie uprawnień w systemie informatycznym
-------------------	-------------------------	---

Imię i nazwisko użytkownika :	
Miejsce przetwarzania/ pokój :	Stanowisko :
<u>Opis zakresu uprawnień użytkownika w systemie informatycznym :</u>	
P - przeglądanie/ drukowanie;	N – zakładanie nowych kont/ aktualizacji Planu Kont;
Z - zmiana;	O/Z – otwarcie / zamknięcie miesiąca/ roku;
D – dopisanie;	A – archiwizowanie :
U – usuwanie;	
*) <i>zakreślić odpowiednio krzyżykiem</i>	

Uprawnienia		P	Z	D	U	N	O/Z	A
-------------	--	---	---	---	---	---	-----	---

**Programy**


Uwagi :.....

.....  
Data i podpis bezpośredniego przełożonego

.....  
Data i podpis ABI

.....  
Data nadania uprawnień i podpis ASI

**ZALĄCZNIK NR 5**  
**do Instrukcji ZSI**

**EWIDENCJA UDOSTĘPNIANIA DANYCH**

Lp.	Data udostępniania danych	Podmiot, któremu dane udostępniono ( nazwa, adres)	Podstawa prawna udostępniania danych	Zakres udostępniania danych	Podpis pracownika

**ZAŁĄCZNIK NR 6**  
**do Instrukcji ZSI**

Kamień Pomorski , dnia .....2013r

.....  
( akceptacja powołującego komisję )

**Protokół nr.....**

**Zniszczenie uszkodzonych nośników komputerowych w Starostwie Powiatowym  
w Kamieniu Pomorskim**

Dnia.....komisja powołana przez.....  
(data) ( imię, nazwisko i stanowisko osoby powołującej komisję)

w składzie:

1. Przewodniczący:.....

2. Członkowie: .....

.....

Dokonała trwałego zniszczenia nośników komputerowych :

Lp.	Nazwa	Nr ewidencyjny	Sposób zniszczenia	Uwagi

Dokonanie w/w czynności zostaje potwierdzone własnoręcznymi podpisami komisji:

.....

.....

.....

ZAŁĄCZNIK NR 7  
do Instrukcji ZSI

REJESTR NOŚNIKÓW KOMPUTEROWYCH  
ZAWIERAJĄCYCH KOPIE ZAPASOWE

Oznaczenie nośnika	Data wpisania w rejestr	Opis nośnika	Miejsce przechowywania nośnika	Podpis użytkownika	Uwagi

Oznaczenie nośnika :

*Kolejny nr nośnika / symbol nośnika/ symbol placówki*

Przykładowe symbole nośników:

DDS – taśma

D – dyskietka

CD – płyta CD

DVD – płyta DVD

P – pendrive

HDD - dysk twardy

RDX – kasetki o zwiększonej odporności na przeciążenia