WÓJT GMINY PIĄTEK

Zarządzenie Nr 2 /2014
Wójta Gminy Piątek
z dnia 20 stycznia 2014r.

w sprawie: ustalenia Polityki Bezpieczeństwa Informacji oraz Instrukcji Zarządzania Systemem Informatycznym w Urzędzie Gminy Piątek.

Na podstawie art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, Dz. U. z 2002 r. Nr 153, poz.1271, Dz. U. z 2004 r. Nr 25, poz. 219, Dz. U. z 2004 r. Nr 33, poz. 285, Dz. U. z 2006 r. Nr 104, poz. 708, Dz. U. z 2006 r. Nr 104 poz. 711, Dz. U. z 2007 r. Nr 165, poz. 1170, Dz. U. z 2007 r. Nr 176, poz. 1238, Dz. U. z 2010 r. Nr 41, poz. 233, Dz. U. z 2010 r. Nr 182, poz. 1228, Dz. U. z 2010 r. Nr 229, poz. 1497) oraz § 3 ust. 3, § 4 i 5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 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. z 2004 r. Nr 100, poz.1024)

zarządzam, co następuje:

§ 1. Ustalam „Politykę Bezpieczeństwa Informacji" w Urzędzie Gminy Piątek, stanowiącą załącznik Nr 1 do zarządzenia,

§ 2. Ustalam „Instrukcję określającą sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych" w Urzędzie Gminy Piątek, stanowiącą załącznik Nr 2 do zarządzenia.

§ 3. Zobowiązuję pracowników Urzędu Gminy Piątek, do stosowania zasad określonych w „Polityce Bezpieczeństwa Informacji" oraz „Instrukcji określającej sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych".

§ 4. Wykonanie zarządzenia powierzam Administratorowi Bezpieczeństwa Informacji

§ 5. Traci moc Zarządzenie Nr 19/2008 Kierownika Urzędu Wójta Gminy Piątek z dnia 01 grudnia 2008r.w sprawie ustalenia „Polityki bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Gminy Piątek"

§ 5. Zarządzenie podlega ogłoszeniu i wchodzi w życie z dniem podjęcia.

WÓJT GMINY PIĄTEK

WÓJT
mgr Krzysztof Ltsiecki

WÓJT GMINY PIĄTEK

Załącznik Nr 1
Do Zarządzenia Nr 2 /2014
Wójta Gminy Piątek
z dnia 20 stycznia 2014r.

Polityka Bezpieczeństwa Informacji

Urząd Gminy Piątek

Wersja nr 1		Pieczęć:	
Opracował:	**Data:**	**Zatwierdził:**	**Data:**
Administrator Bezpieczeństwa Informacji Anna Tybura		Administrator Danych Osobowych Krzysztof Lisiecki	

Spis treści

1. Wstęp

Celem Polityki Bezpieczeństwa Informacji jest zapewnienie ochrony danych osobowych przetwarzanych przez Urząd Gminy Piątek.

Polityka Bezpieczeństwa Informacji określa obowiązki Administratora Danych Osobowych w zakresie zabezpieczenia danych osobowych o których mowa w § 36 Ustawy o Ochronie Danych Osobowych.

Polityka Bezpieczeństwa Informacji określa reguły dotyczące procedur zapewnienia bezpieczeństwa danych osobowych podczas ich przetwarzania w postaci tradycyjnej (papierowej) oraz z wykorzystaniem systemów informatycznych.

Integralną częścią niniejszego dokumentu jest Instrukcja określająca sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwana dalej „Instrukcją Zarządzania Systemem Informatycznym" oraz załączniki wskazane w **rozdziale 14 niniejszej Polityki**.
Polityka Bezpieczeństwa Informacji została opracowana zgodnie z wymogami określonymi w § 4 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). Niniejszy dokument został opracowany z uwzględnieniem wytycznych Generalnego Inspektora Ochrony Danych Osobowych oraz dobrymi praktykami.

Polityka Bezpieczeństwa Informacji obowiązuje wszystkich pracowników Urzędu Gminy Piątek oraz procesorów, dostawców usług, podmiotów współpracujących na zasadzie umów i innych mających jakikolwiek kontakt z danymi osobowymi objętymi ochroną.

Ochrona danych osobowych jest realizowana poprzez zastosowanie środków bezpieczeństwa fizycznego, informatycznego i procedury organizacyjne. System ochrony danych osobowych jest nadzorowany przez Administratora Bezpieczeństwa Informacji, który podlega oraz ściśle współpracuje w tym zakresie z Administratorem Danych Osobowych.

Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:

- poufność danych – rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom,
- integralność danych – rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
- rozliczalność danych – rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie,
- integralność systemu – rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej.

2. Deklaracja ochrony

Administrator Danych Osobowych świadomy wagi zagrożeń prywatności, w tym zwłaszcza zagrożeń danych osobowych przetwarzanych w związku z wykonywaniem zadań, deklaruje podejmowanie wszelkich możliwych działań koniecznych do zapobiegania m. in. takim zagrożeniom, jak:

1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu, jak np. pożar, zalanie pomieszczeń, katastrofa budowlana, napad, kradzież, włamanie, działania terrorystyczne;
2) niewłaściwe parametry środowiska, zakłócające pracę urządzeń komputerowych (nadmierna wilgotność lub bardzo wysoka temperatura, oddziaływanie pola elektromagnetycznego i inne);
3) awarie sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne naruszenia ochrony danych, niewłaściwe działanie procedur serwisowych w tym przyzwolenie na naprawę sprzętu zawierającego dane osobowe poza siedzibą administratora danych osobowych;
4) naruszenie bezpieczeństwa danych przez nieautoryzowane ich przetwarzanie; ujawnienie osobom nieupoważnionym procedur ochrony danych stosownych przez administratora danych osobowych,
5) celowe lub przypadkowe rozproszenie danych w Internecie z ominięciem zabezpieczeń systemu lub wykorzystaniem błędów systemu informatycznego administratora danych osobowych;
6) ataki z Internetu;
7) naruszenia zasad i procedur określonych w dokumentacji z zakresu ochrony danych osobowych przez osoby upoważnione do przetwarzania danych osobowych, związane z nieprzestrzeganiem procedur ochrony danych, w tym zwłaszcza:
   - niezgodne z procedurami zakończenie pracy lub opuszczenie stanowiska pracy,
   - naruszenie bezpieczeństwa danych przez nieautoryzowane ich przetwarzanie,
   - ujawnienie osobom nieupoważnionym procedur ochrony danych stosowanych u administratora danych osobowych,
   - ujawnienie osobom nieupoważnionym danych przetwarzanych przez administratora danych osobowych, w tym również nieumyślne ujawnienie danych osobom postronnym, przebywającym bez nadzoru lub niedostatecznie nadzorowanym w pomieszczeniach administratora danych osobowych,
   - niewykonywanie stosownych kopii zapasowych,
   - przetwarzanie danych osobowych w celach prywatnych,
   - wprowadzanie zmian do systemu informatycznego administratora danych i instalowanie programów bez zgody administratora systemu informatycznego.

3. Postanowienia ogólne

3.1. Definicje

Ilekroć w niniejszej polityce bezpieczeństwa informacji jest mowa o:

1) polityce – rozumie się przez to Politykę Bezpieczeństwa Informacji, która została przyjęta jako obowiązujący dokument w Urzędzie Gminy Piątek,
2) ustawie – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. Dz. U. z 2002 r. Nr 101, poz.926 ze zm.),
3) rozporządzeniu – rozumie się przez to rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku 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),
4) administratorze danych osobowych – rozumie się przez to Urząd Gminy Piątek reprezentowany przez Wójta, zwanego w dalszej części dokumentu ADO,
5) administratorze bezpieczeństwa informacji – rozumie się przez to osobę, którą administrator danych osobowych powołał w drodze pisemnej, w celu nadzorowania systemu ochrony danych osobowych funkcjonującego w Urzędzie Gminy Piątek, zwanego w dalszej części dokumentu ABI,
6) administratorze systemu informatycznego – rozumie się przez to osobę nadzorującą pracę systemu informatycznego administratora danych osobowych oraz wykonującą w nim czynności wymagające specjalnych uprawnień administracyjnych, zwanego w dalszej części dokumentu ASI,
7) danych osobowych – rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
8) zbiorze danych – rozumie się przez to uporządkowany zestaw (także rozproszony oraz podzielony funkcjonalnie) zawierający dane osobowe, posiadający cechy pozwalające na odnalezienie informacji, w którym dostęp do danych będzie możliwy poprzez określone kryteria,
9) osobie upoważnionej do przetwarzania danych osobowych - rozumie się przez to osobę, która została upoważniona na piśmie przez Administratora Danych Osobowych do przetwarzania danych osobowych w Urzędzie Gminy Piątek,
10) użytkowniku – rozumie się przez to osobę upoważnioną na piśmie do przetwarzania danych osobowych, której Administrator Systemu Informatycznego nadał identyfikator i przyznał hasło,
11) przetwarzającym – rozumie się przez to osobę fizyczną lub podmiot, któremu zostało powierzone przetwarzanie danych osobowych na podstawie umowy zawieranej zgodnie z art. 31 ustawy,
12) odbiorcy danych – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:
    - osoby, której dane dotyczą,
    - osoby upoważnionej do przetwarzania danych,

- przedstawiciela, o którym mowa w art. 31a ustawy,
- podmiotu, o którym mowa w art. 31 ustawy,
- organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem,

13) identyfikatorze – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
14) haśle – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi,
15) sieci telekomunikacyjnej – rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 35 ustawy z 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800 ze zm.);
16) sieci publicznej – rozumie się przez to publiczną sieć telekomunikacyjną w rozumieniu art. 2 pkt 29 ustawy z 16 lipca 2004 r. – Prawo telekomunikacyjne;
17) teletransmisji – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej,
18) usuwaniu danych (anonimizacji) – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację , która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
19) uwierzytelnianiu – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości osoby fizycznej lub podmiotu,
20) zgodzie osoby, której dane dotyczą – rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści,
21) przetwarzaniu danych – rozumie się przez to 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,
22) rozliczalności – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,
23) integralności danych – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
24) poufności danych – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom,
25) systemie informatycznym administratora danych osobowych – rozumie się przez to sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów procedur przetwarzania informacji i narzędzi programowych; w systemie tym pracuje co najmniej jeden komputer centralny i system ten tworzy sieć teleinformatyczną administratora danych osobowych,
26) zabezpieczeniu systemu informatycznego – rozumie się przez to wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą.

3.2. Cel

1. Wdrożenie polityki bezpieczeństwa u ADO ma na celu zabezpieczenie przetwarzanych przez niego danych osobowych, w tym danych przetwarzanych w systemie informatycznym i poza nim, poprzez wykonanie obowiązków wynikających z ustawy i rozporządzenia.
2. W związku z tym, że w zbiorach ADO przetwarzane są między innymi dane wrażliwe, a system informatyczny posiada szerokopasmowe połączenie z Internetem, niniejszy dokument służy zapewnieniu wysokiego poziomu bezpieczeństwa danych w rozumieniu § 6 rozporządzenia.
3. Dokument ten opisuje niezbędny do uzyskania wymaganego poziomu bezpieczeństwa zbiór procedur i zasad dotyczących przetwarzania danych osobowych oraz ich zabezpieczenia.

3.3. Zakres stosowania

1. Niniejsza polityka bezpieczeństwa informacji dotyczy zarówno danych osobowych przetwarzanych w sposób tradycyjny w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych, jak i w systemach informatycznych także w przypadku przetwarzania danych poza zbiorami ADO.
2. Procedury i zasady określone w niniejszym dokumencie stosuje się do wszystkich osób upoważnionych do przetwarzania danych osobowych, zarówno zatrudnionych, jak i innych, np. stażystów, praktykantów, wolontariuszy oraz do podmiotów i procesorów, którym ADO powierzył lub dał dostęp do przetwarzania danych osobowych.

4. Organizacja przetwarzania danych osobowych

4.1. Administrator danych osobowych

Administrator danych osobowych (ADO) realizuje zadania w zakresie ochrony danych osobowych, w tym zwłaszcza:

1) podejmuje decyzje o celach i środkach przetwarzania danych osobowych z uwzględnieniem przede wszystkim zmian w obowiązującym prawie, organizacji zasad pracy ADO oraz technik zabezpieczenia danych osobowych;
2) upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym zakresowi jej obowiązków;
3) wyznacza administratora bezpieczeństwa informacji (ABI) oraz określa zakres jego zadań i czynności jako właściwego do prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych oraz pozostałej dokumentacji z zakresu ochrony danych, o ile jako właściwy do jej prowadzenia nie zostanie wskazany w niniejszym dokumencie inny podmiot;
4) zapewnia użytkownikom odpowiednie stanowiska pracy w tym sprzęt informatyczny, umożliwiające bezpieczne i zgodne z obowiązującym prawem przetwarzanie danych osobowych;
5) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur bezpiecznego przetwarzania danych osobowych.

4.2. Administrator bezpieczeństwa informacji

Administrator bezpieczeństwa informacji (ABI) realizuje zadania w zakresie nadzoru nad przestrzeganiem zasad ochrony danych osobowych, w tym zwłaszcza:

1) sprawuje nadzór nad wdrożeniem i funkcjonowaniem adekwatnych środków fizycznych, a także organizacyjnych i technicznych – w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych,
2) sprawuje nadzór nad prowadzeniem ewidencji osób upoważnionych do przetwarzania danych osobowych,
3) koordynuje wewnętrzne audyty przestrzegania przepisów ustawy o ochronie danych osobowych,
4) nadzoruje udostępnianie danych osobowych odbiorcom danych i innym podmiotom,
5) nadzoruje spełnianie wymagań ustawy o ochronie danych osobowych u podmiotów, którym powierzył przetwarzanie danych osobowych,
6) przygotowuje wnioski zgłoszeń rejestracyjnych i aktualizacyjnych zbiorów danych osobowych oraz prowadzi korespondencję z Generalnym Inspektorem Ochrony Danych Osobowych,
7) przygotowuje wzory dokumentów dotyczące ochrony danych osobowych,
8) prowadzi oraz aktualizuje dokumentację opisującą sposób przetwarzania danych

osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych,

9) wspólnie z ADO podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia bezpieczeństwa przetwarzania danych osobowych ze szczególnym uwzględnieniem systemu informatycznego,
10) przygotowuje wyciągi z polityki bezpieczeństwa informacji, dostosowane do zakresów obowiązków osób upoważnianych do przetwarzania danych osobowych,
11) przygotowuje materiały szkoleniowe z zakresu ochrony danych osobowych i prowadzi szkolenia osób upoważnianych do przetwarzania danych osobowych lub współpracuje w tym zakresie z wyspecjalizowanym podmiotem zewnętrznym,
12) w porozumieniu z ADO na czas swojej nieobecności wyznacza w formie pisemnej swojego zastępcę,
13) inicjuje i podejmuje przedsięwzięcia w zakresie doskonalenia ochrony danych osobowych u ADO.

Administrator bezpieczeństwa informacji ma prawo:

1) wstępu do pomieszczeń, w których zlokalizowane są zbiory danych osobowych i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z ustawą,
2) żądać od pracowników i podmiotów współpracujących złożenia pisemnych lub ustnych wyjaśnień w zakresie niezbędnym do ustalenia stanu faktycznego,
3) żądać okazania dokumentów i wszelkich danych mających bezpośredni związek z problematyką kontroli,
4) żądać udostępnienia do kontroli dokumentacji, urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych u ADO oraz u procesorów .

4.3. Administrator systemu informatycznego

Administrator systemu informatycznego (ASI) realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym administratora danych osobowych, w tym zwłaszcza:

1) zarządza systemem informatycznym, w którym przetwarzane są dane osobowe, posługując się hasłem administracyjnym dostępu do wszystkich stacji roboczych i serwerów z pozycji administratora,
2) przeciwdziała dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe,
3) na wniosek ABI przydziela każdemu użytkownikowi identyfikator oraz hasło do systemu informatycznego oraz dokonuje ewentualnych modyfikacji uprawnień, a także usuwa konta użytkowników zgodnie z zasadami określonymi w instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
4) nadzoruje prawidłowe działanie mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych,
5) podejmuje działania w zakresie ustalania i kontroli identyfikatorów dostępu do

systemu informatycznego,

6) wyrejestrowuje użytkowników na polecenie ADO lub ABI,
7) w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informuje ADO i ABI o naruszeniu oraz współdziała z nimi przy usuwaniu skutków naruszenia,
8) prowadzi szczegółową dokumentację naruszeń bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym,
9) wykonuje oraz sprawuje nadzór nad wykonywaniem napraw, konserwacją oraz likwidacją urządzeń komputerowych, na których przetwarzane są dane osobowe,
10) wykonuje oraz sprawuje nadzór nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego,
11) podejmuje działania służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji.

4.4. Obowiązki pracownika Urzędu Gminy Piątek

Pracownik może przetwarzać dane osobowe wyłącznie w zakresie ustalonym indywidualnie przez ADO i tylko w celu wykonywania nałożonych na niego obowiązków. Zakres uprawnień do zbiorów danych osobowych przetwarzanych z wykorzystaniem systemu informatycznego przypisany jest do indywidualnego i niepowtarzalnego identyfikatora użytkownika, niezbędnego do pracy w systemie. Rozwiązanie stosunku pracy lub odwołanie z pełnionej funkcji wymaga od ABI wycofania upoważnienia do przetwarzania danych osobowych.

Pracownicy upoważnieni do przetwarzania danych osobowych, pisemnie oświadczają, że zobowiązują się do zachowania w tajemnicy danych osobowych oraz przestrzegania procedur ich bezpiecznego przetwarzania a także zachowania w tajemnicy zastosowanych u ADO środków bezpieczeństwa. Przestrzeganie tajemnicy danych osobowych obowiązuje przez cały okres zatrudnienia u ADO, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji.

Naruszenie przez pracowników upoważnionych do przetwarzania danych osobowych, procedur bezpiecznego przetwarzania, w szczególności świadome udostępnienie danych osobie niepowołanej, jest ciężkim naruszeniem obowiązków pracowniczych i może uzasadnić rozwiązanie umowy o pracę w trybie art. 52 Kodeksu Pracy.

Wszyscy pracownicy są zobowiązani do:

1) zapoznania się z przepisami prawa w zakresie ochrony danych osobowych, w tym przepisami niniejszej polityki bezpieczeństwa informacji i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
2) stosowania określonych przez ADO oraz ABI procedur oraz wytycznych mających na celu zgodne z prawem, w tym zwłaszcza adekwatne przetwarzanie danych osobowych,
3) odpowiedniego zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym.

5. Analiza ryzyka związanego z przetwarzaniem danych osobowych

Punktem wyjścia dla skutecznego zabezpieczenia danych osobowych jest analiza ryzyka wystąpienia zagrożeń dla ich bezpieczeństwa. Są to m.in.:

a) błędy i pominięcia w obsłudze,
b) nieuprawnione użycie nośników danych,
c) oszustwo, kradzież, sabotaż,
d) awarie sprzętu, oprogramowania, usług sieciowych i łączności oraz zasilania,
e) wahania prądu, ładunki elektrostatyczne, promieniowane elektromagnetyczne,
f) ekstremalne temperatury, wilgoć, kurz,
g) błędy w konserwacji urządzeń, błędy w transmisji danych,
h) nieuprawniony dostęp do sieci, instalowanie lub użycie nieautoryzowanego oprogramowania,
i) niedobór personelu, niewłaściwe wykorzystanie zasobów.

W odniesieniu do poufności, bezpieczeństwa, integralności i rozliczalności danych osobowych w Urzędzie zidentyfikowano zagrożenia zestawione w poniższej tabeli.

Zagrożenia dla poufności danych	Zagrożenia dla autentyczności danych
1. Pokonywanie zabezpieczeń fizycznych lub programowych 2. Niekontrolowana obecność osób nieuprawnionych w obszarze przetwarzania 3. Niedyskrecja osób upoważnionych 4. Udostępnianie danych osobowych przez osobę nieupoważnioną 5. Zabranie danych osobowych przez osobę nieupoważnioną 6. Niekontrolowane wytwarzanie i wypływ poza obszar przetwarzania nośników informacji oraz komputerów przenośnych zawierających dane osobowe 7. Naprawy i konserwacje systemu lub sieci teleinformatycznej wykonywane przez osoby nieuprawnione 8. Podsłuchy i podglądy	1. Przypadkowe lub celowe modyfikowanie systemów i aplikacji informatycznych lub urządzeń sieciowych 2. Przypadkowe lub celowe wprowadzanie zmian do chronionych danych osobowych 3. Brak rejestrowania zdarzeń tworzenia lub modyfikowania danych osobowych 4. Kradziez tożsamości
Zagrożenia dla integralności danych	**Zagrożenia dla rozliczalności danych**
1. Przypadkowe lub celowe uszkodzenie systemów i aplikacji informatycznych lub urządzeń sieciowych 2. Przypadkowe lub celowe uszkodzenie, utrata, zniszczenie lub nieuprawniona modyfikacja danych 3. Infekcje wirusowe	1. Nieprzydzielenie użytkownikom identyfikatorów 2. Niewłaściwa administracja systemem informatycznym 3. Niewłaściwa konfiguracja systemu informatycznego 4. Zniszczenie lub zafałszowanie logów

4. Klęski żywiołowe 5. Ataki terrorystyczne	systemowych 5. Brak rejestrowania zdarzeń udostępniania danych 6. Podszywanie się pod innego pracownika

6. Infrastruktura przetwarzania danych osobowych

6.1. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe.

Szczegółowe informacje na temat obszarów, w których są przechowywane zbiory danych osobowych prowadzonych w formie papierowej i elektronicznej, zawierającej dane osobowe, opisane zostały w załączniku nr 1.3 pt. „Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe".

6.2. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.

Wykaz zbiorów danych osobowych prowadzonych w postaci dokumentacji papierowej oraz w formie elektronicznej wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, opisany został w załączniku nr 1.4 pt. „Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych".

6.3. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi.

Opis struktury zbiorów danych osobowych prowadzonych w postaci dokumentacji papierowej oraz w formie elektronicznej wraz ze wskazaniem pól informacyjnych, opisany został w załączniku nr 1.5 pt. „Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi".

6.4. Sposób przepływu danych pomiędzy poszczególnymi systemami.

Sposób przepływu danych pomiędzy poszczególnymi systemami, opisany został w załączniku nr 1.6 pt. „Sposób przepływu danych pomiędzy poszczególnymi systemami ".

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

7.1. Środki ochrony fizycznej

1. Przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych.
2. Przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej u ADO z ważnym upoważnieniem do przetwarzania danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych osobowych.
3. Zbiory danych osobowych są przechowywane w pomieszczeniach zabezpieczonych drzwiami zwykłymi (niewzmacnianymi, nieprzeciwpożarowymi).
4. Pomieszczenie, w którym znajduje się serwer jest zabezpieczone drzwiami przeciwwłamaniowymi o podwyższonej odporności ogniowej.
5. Pomieszczeniach na parterze są wyposażone w czujki przeciwwłamaniowe. Budynek jest objęty systemem alarmowym przeciwwłamaniowym.
6. Do pomieszczenia, w którym znajdują się serwery, infrastruktura informatyczna oraz system monitoringu, zastosowano system kontroli dostępu. Do ww. pomieszczenia dostęp posiada ADO, ABI oraz ASI i pisemni upoważnieni pracownicy.
7. Kopie zapasowe/archiwalne zbiorów danych osobowych przechowywane są w zamkniętej metalowej szafie w pomieszczeniu oddalonym od serwerowni o co najmniej jedno pomieszczenie.
8. Dostęp do pomieszczeń, w których przetwarza się dane osobowe jest możliwy po uprzednim po pobraniu klucza i wpisaniu się w rejestr pobranych/zdanych kluczy. Po zakończeniu pracy każdy pracownik ma obowiązek zdania klucza i odnotowania wyjścia w rejestrze pobranych/zdanych kluczy.
9. Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.
10. Dokumenty podlegające przepisom o archiwach są przechowywane w archiwum zakładowym.

7.2. Środki sprzętowe, informatyczne i telekomunikacyjne

1. Co najmniej jedno urządzenie systemu informatycznego służącego do przetwarzania danych osobowych połączone jest z siecią publiczną.
2. Lokalizacja urządzeń komputerowych (komputerów typu PC, terminali, drukarek) uniemożliwia osobom niepowołanym dostęp do nich oraz wgląd do danych wyświetlanych na monitorach komputerowych.
3. Komputery przenośne, wykorzystywane do przetwarzania danych osobowych, po zakończonej pracy są przechowywane w warunkach zapewniających ich bezpieczeństwo.

4. Zastosowano środki adekwatne do możliwości technicznych i organizacyjnych ADO, uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych.
5. Zastosowano lokalne urządzenia podtrzymujące zasilanie typu UPS, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania.
6. Okablowanie sieciowe zostało zaprojektowane w ten sposób, że dostęp do linii teletransmisyjnych jest możliwy tylko z pomieszczeń zamykanych na klucz.
7. Dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelniania.
8. Bieżąca konserwacja sprzętu wykorzystywanego przez ADO do ich przetwarzania jest prowadzona tylko przez jego pracowników, przede wszystkim zatrudnionych w dziale teleinformatycznym.
9. Poważne naprawy wykonywane przez personel zewnętrzny są realizowane w siedzibie ADO po zawarciu z podmiotem wykonującym naprawę umowy o powierzenie przetwarzania danych osobowych, określającej kary umowne za naruszenie bezpieczeństwa danych.
10. ASI dopuszcza konserwowanie i naprawę sprzętu poza siedzibą ADO jedynie po trwałym usunięciu danych osobowych lub pozostawieniu w siedzibie ADO nośników zawierających dane osobowe.
11. Zużyty sprzęt służący do przetwarzania danych osobowych może być zbywany dopiero po trwałym usunięciu danych osobowych lub pozostawieniu w siedzibie ADO nośników zawierających dane osobowe, a urządzenia uszkodzone powinny być przekazywane właściwym podmiotom w celu utylizacji.

7.2.1. Środki ochrony w ramach systemu operacyjnego

1. Dostęp do systemów operacyjnych komputerów, w których są przetwarzane dane osobowe zabezpieczone są za pomocą procesu uwierzytelniania z wykorzystaniem indywidualnego identyfikatora użytkownika (loginu) oraz hasła.
2. Rodzaj systemu operacyjnego i sposób jego konfiguracji zapewnia odpowiednie restrykcje w zakresie dostępu do danych i aplikacji.
3. W systemach operacyjnych zastosowano mechanizm wymuszający okresową zmianę haseł.
4. Użytkownicy systemu informatycznego nie posiadają praw do wykonywania kopii zapasowych zbiorów danych osobowych.
5. Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.
6. Zastosowano zabezpieczone hasłem wygaszanie ekranu w przypadku nieaktywności użytkownika dłuższej niż 15 minut.
7. Zastosowano działający w tle program antywirusowy na komputerach użytkowników.
8. Skonfigurowano i zapewniono automatyczne pobieranie aktualizacji do systemów operacyjnych.

7.2.2. Środki ochrony w ramach narzędzi baz danych i innych narzędzi programowych

1. Dostęp do zbiorów danych osobowych zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika (loginu) oraz hasła.
2. Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych.
3. Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych.

7.3. Środki organizacyjne

1. Powołano Administratora Bezpieczeństwa Informacji.
2. Opracowano i wdrożono Politykę bezpieczeństwa informacji oraz Instrukcję Zarządzania Systemem Informatycznym.
3. Wdrożono odpowiedni podział obowiązków i kontroli dostępu dla pracowników oraz administratorów.
4. Do danych osobowych mają dostęp jedynie osoby posiadające pisemne upoważnienie nadane przez ADO.
5. Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych.
6. Osoby upoważnione do przetwarzania danych osobowych przed dopuszczeniem do tych danych są szkolone przez ABI w zakresie obwiązujących przepisów o ochronie danych osobowych, procedur przetwarzania danych oraz informowane o podstawowych

zagrożeniach związanych z przetwarzaniem danych osobowych. Osoby te są zobowiązane do podpisania stosownego oświadczenia o odbyciu szkolenia.

7. Osoby zatrudnione przy przetwarzaniu danych osobowych zobowiązane są do zachowania ich oraz sposobów ich zabezpieczenia w tajemnicy.
8. Zapewniono klauzule poufności z wszystkimi podmiotami zewnętrznymi mającymi dostęp do danych osobowych w Urzędzie Gminy Piątek.

Ponadto każdy pracownik lub użytkownik upoważniony do przetwarzania danych osobowych ma obowiązek:

1) nieużywania powtórnego jednostronnie zadrukowanych dokumentów zawierających dane osobowe;
2) niepodawania w rozdzielniku decyzji do wiadomości stronom informacji o adresach innych;
3) zachowania tajemnicy danych przetwarzanych w siedzibie ADO, w tym także wobec najbliższych;
4) pilnego strzeżenia akt, dyskietek, płyt, pamięci przenośnych i komputerów przenośnych;
5) niepozostawiania bez kontroli dokumentów, nośników danych i sprzętu w hotelach i innych miejscach publicznych ani też w samochodach;
6) ustawiania ekranów komputerowych tak, aby osoby niepowołane nie mogły oglądać ich zawartości, a zwłaszcza nie naprzeciwko wejścia do pomieszczenia;
7) niezapisywania hasła wymaganego do uwierzytelniania się w systemie na papierze lub innym nośniku;
8) niepodłączania do listew podtrzymujących napięcie, przeznaczonych dla sprzętu komputerowego, innych urządzeń, szczególnie tych łatwo powodujących spięcia;
9) dbania o prawidłową wentylację komputerów;
10) przestrzegania swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosowania się do zaleceń ABI;
11) niepozostawiania osób postronnych w pomieszczeniu, w którym przetwarza się dane osobowe, bez osoby upoważnionej do przetwarzania danych osobowych;
12) opuszczania stanowiska pracy dopiero po aktywizowaniu wygaszacza ekranu lub po zablokowaniu stacji roboczej w inny sposób;
13) udostępniania danych osobowych pocztą elektroniczną tylko w postaci zaszyfrowanej;
14) nie wynoszenia na jakichkolwiek nośnikach całych zbiorów danych oraz wypisów z nich, nawet w postaci zaszyfrowanej;
15) wykonywania kopii roboczych danych, na których się właśnie pracuje, tak często, aby zapobiec ich utracie;
16) kończenia pracy na stacji roboczej po zapisaniu wszystkich zmian i prawidłowym wylogowaniu się użytkownika i wyłączeniu komputera;
17) niszczenia w niszczarce lub chowania do szaf zamykanych na klucz wszelkich wydruków zawierających dane osobowe, przed opuszczeniem miejsca pracy po zakończeniu dnia pracy;
18) chowania do zamykanych na klucz szaf wszelkich akt zawierających dane osobowe, przed opuszczeniem miejsca pracy po zakończeniu dnia pracy;
19) umieszczaniu kluczy do szaf w ustalonym, przeznaczonym do tego miejscu po zakończeniu dnia pracy;

20) zamykania okien w razie różnych zjawisk atmosferycznych, które mogą zagrozić bezpieczeństwu danych osobowych;
21) zamykania okien w razie opuszczenia pomieszczenia, w tym zwłaszcza po zakończeniu dnia pracy;
22) zamykania drzwi na klucz i zabierania ze sobą w przypadku czasowego opuszczenia pomieszczenia, które pozostaje bez dozoru;
23) niepozostawiana kluczy w drzwiach od strony zewnętrznej pomieszczeń, w których przetwarza się dane osobowe;
24) zamykania drzwi na klucz po zakończeniu pracy w danym dniu i składania klucza w punkcie informacyjnym.

8. Udostępnianie danych osobowych

1. Udostępnianie danych osobowych może nastąpić tylko po przedłożeniu wniosku o przekazanie lub udostępnienie informacji. Wniosek ten powinien mieć formę pisemną i zawierać:
    - oznaczenie wnioskodawcy,
    - wskazanie przepisów uprawniających do dostępu do informacji,
    - określenie rodzaju i zakresu potrzebnych informacji oraz formy ich przekazania lub udostępnienia,
    - wskazanie imienia, nazwiska osoby upoważnionej do pobrania informacji lub zapoznania się z ich treścią.
2. Udostępnianie danych osobowych na podstawie ustnego wniosku zawierającego wszystkie powyższe cztery elementy wniosku pisemnego może nastąpić tylko wtedy, gdy zachodzi konieczność niezwłocznego działania.
3. Osoba udostępniająca dane osobowe jest obowiązana zażądać od osoby upoważnionej pokwitowania pobrania dokumentów zawierających informacje przekazane na podstawie pisemnego wniosku albo potwierdzenia faktu uzyskania wglądu w treść informacji. Osoba upoważniona jest obowiązana do pokwitowania lub potwierdzenia.
4. Jeśli informacje są przekazywane na podstawie ustnego wniosku, należy stosownie do okoliczności zwrócić się z prośbą o pokwitowanie albo potwierdzenie. Jeśli pokwitowanie albo potwierdzenie ze względu na okoliczności udostępniania nie są możliwe, osoba udostępniająca informacje sporządza na tę okoliczność notatkę służbową.
5. Jeśli osoba upoważniona pouczyła osobę udostępniającą informacje o konieczności zachowania w tajemnicy faktu i okoliczności przekazania informacji, to okoliczność ta jest odnotowywana w rejestrze udostępnień niezależnie od odnotowania faktu udostępnienia informacji.
6. Osoby udostępniające dane osobowe do innych podmiotów na wniosek prowadzą rejestr udostępnień w swojej komórce organizacyjnej.

9. Odpowiedzialność osób upoważnionych do przetwarzania danych osobowych

1. Niezastosowanie się do prowadzonej przez ADO polityki bezpieczeństwa informacji, której założenia określa niniejszy dokument i naruszenie procedur ochrony danych przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez zachowania okresu wypowiedzenia na podstawie art. 52 Kodeksu pracy.
2. Niezależnie od rozwiązania stosunku pracy osoby popełniające przestępstwo będą pociągane do odpowiedzialności karnej zwłaszcza na podstawie art. 51.1-52 ustawy o ochronie danych osobowych oraz art. 266 Kodeksu karnego. Przykładowo przestępstwo można popełnić wskutek:

- stworzenia możliwości dostępu do danych osobowych osobom nieupoważnionym albo osobie nieupoważnionej,
- niezabezpieczenia nośnika lub komputera przenośnego,
- zapoznania się z hasłem innego pracownika wskutek wykonania nieuprawnionych operacji w systemie informatycznym administratora danych.

10. Szkolenia osób upoważnionych do przetwarzania danych

1. ABI prowadzi szkolenia dla pracowników upoważnionych do przetwarzania danych osobowych w przypadku:
   a) zmiany przepisów prawa odnoszących się do przetwarzania danych osobowych,
   b) zmiany obowiązującej dokumentacji u ADO (Polityka Bezpieczeństwa, Instrukcja Zarządzania Systemem Informatycznym itp.)
   c) każdorazowo w związku z zatrudnieniem nowego pracownika, stażysty, praktykanta, wolontariusza itp.
   d) na indywidualne polecenie ADO.

2. Tematyka szkoleń obejmuje:

   1) przepisy i instrukcje dotyczące ochrony danych osobowych, sporządzania i przechowywania ich kopii, niszczenia wydruków i zapisów na nośnikach,
   2) sposoby ochrony danych przed osobami postronnymi i procedury udostępniania danych osobom, które one dotyczą,
   3) obowiązki osób upoważnionych do przetwarzania danych osobowych,
   4) zasady i procedury określone w polityce bezpieczeństwa informacji,
   5) zmiany w przepisach o ochronie danych osobowych.

3. ABI może skorzystać z pomocy zewnętrznego wyspecjalizowanego podmiotu w zakresie przeprowadzenia szkolenia z zakresu ochrony danych osobowych.

11. Procedura postępowania w przypadku naruszenia bezpieczeństwa danych osobowych

1. Naruszeniem bezpieczeństwa danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawniania danych osobowych, udostępniania lub umożliwiania dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego, a w szczególności:
   a) nieautoryzowanego dostępu do danych,
   b) nieautoryzowane modyfikacje lub zniszczenie danych,
   c) udostępnianie danych nieautoryzowanym podmiotom,
   d) nielegalne ujawnianie danych,
   e) pozyskiwanie danych z nielegalnych źródeł.
2. W przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego lub zaistnienia sytuacji, które mogą wskazywać na naruszenie zabezpieczenia danych osobowych, każdy pracownik zobowiązany przerwać przetwarzanie danych osobowych i niezwłocznie powiadomić o tym fakcie ABI oraz bezpośredniego przełożonego, a następnie stosować się do podjętych przez nich decyzji.
3. Zgłoszenie naruszenia ochrony danych osobowych powinno zawierać:
   a) opis symptomów naruszenia ochrony danych osobowych,
   b) określenie sytuacji i czasu, w jakim stwierdzono naruszenie ochrony danych osobowych,
   c) określenie wszelkich istotnych informacji mogących wskazywać na przyczynę tego naruszenia,
   d) określenie znanych danej osobie sposobów zabezpieczenia systemu oraz wszelkich kroków podjętych po ujawnieniu zdarzenia.
4. ABI lub inna upoważniona przez niego osoba podejmuje wszelkie działania mające na celu:
   a) minimalizację negatywnych skutków zdarzenia,
   b) wyjaśnienie okoliczności zdarzenia,
   c) zabezpieczenie dowodów zdarzenia,
   d) umożliwienie dalszego bezpiecznego przetwarzania danych.
5. W celu realizacji procedury postępowania w przypadku naruszenia bezpieczeństwa danych osobowych ABI lub inna upoważniona przez niego osoba ma prawo do podejmowania wszelkich działań dopuszczonych przez prawo, a w szczególności:
   a) żądania wyjaśnień od pracowników,
   b) Korzystania z pomocy konsultantów (w tym zewnętrznych podmiotów),
   c) nakazanie przerwania pracy, zwłaszcza w zakresie przetwarzania danych osobowych.
6. Polecenia ABI wydawane w czasie realizacji zadań wynikających z Polityki bezpieczeństwa informacji są priorytetowe i powinny być wykonywane w pierwszej kolejności, zapewniając ochronę danych osobowych.

7. Odmowa udzielenia wyjaśnień lub współpracy z ABI traktowana będzie jako naruszenie obowiązków pracowniczych.
8. ABI po zagrożeniu sytuacji nadzwyczajnej opracowuje raport końcowy na podstawie wzoru wg. załącznika nr 1.11, w którym przedstawia przyczyny i skutki zdarzenia oraz wnioski, w tym kadrowe, ograniczające możliwość wystąpienia zdarzenia w przyszłości.
9. Nieprzestrzeganie zasad określonych niniejsza Polityką bezpieczeństwa informacji stanowi naruszenie obowiązków pracowniczych i może być przyczyną odpowiedzialności dyscyplinarnej określonej w Kodeksie Pracy.
10. Jeżeli skutkiem działania określonego w ustępie 9 jest ujawnienie informacji osobie nieupoważnionej, sprawca może zostać pociągnięty do odpowiedzialności karnej wynikającej z przepisów Kodeksu Karnego.
11. Jeżeli skutkiem działania określonego w ustępie 9 jest szkoda, sprawca ponosi odpowiedzialność materialną na warunkach określonych w Kodeksie Pracy oraz Prawa Cywilnego.

12. Przeglądy polityki bezpieczeństwa i audyty systemu

1. Polityka bezpieczeństwa informacji powinna być poddawana przeglądowi (audytowi) przynajmniej raz na rok. W razie istotnych zmian dotyczących przetwarzania danych osobowych ABI może zarządzić przegląd polityki bezpieczeństwa informacji stosownie do potrzeb.
2. Do kontroli stanu ochrony danych osobowych w Urzędzie Gminy Piątek upoważnieni są:
   a) Administratora Danych Osobowych;
   b) Administrator Bezpieczeństwa Informacji;
   c) Administrator Systemu Informatycznego.
3. ABI analizuje, czy polityka bezpieczeństwa informacji i pozostała dokumentacja z zakresu ochrony danych osobowych jest adekwatna do:
   a) zmian w budowie systemu informatycznego,
   b) zmian organizacyjnych ADO, w tym również zmian statusu osób upoważnionych do przetwarzania danych osobowych,
   c) zmian w obowiązującym prawie.
4. Raz do roku kontroli podlegają wszystkie Systemy informatyczne przetwarzające dane osobowe oraz zabezpieczenia fizyczne i bezpieczeństwo osobowe.
5. ABI przygotowuje plan kontroli uwzględniając zakres oraz potrzeby fizyczne, czasowe i osobowe.
6. Kontroli podlega sprzęt, system teleinformatyczny, realizacja zabezpieczeń przez pracowników oraz przestrzeganie polityki bezpieczeństwa informacji.
7. ABI po uzgodnieniu z ADO może, stosownie do potrzeb, przeprowadzić wewnętrzny audyt zgodności przetwarzania danych z przepisami o ochronie danych osobowych.
8. Przeprowadzenie audytu wymaga uzgodnienia jego zakresu z ADO i ASI. Zakres, przebieg i rezultaty audytu dokumentowane są na piśmie w protokole podpisywanym przez ABI i ASI i przedstawiane w formie pisemnej do wiadomości ADO.
9. ADO biorąc pod uwagę wnioski administratorów, może zlecić przeprowadzenie audytu zewnętrznego przez wyspecjalizowany podmiot.
10. Za wyniki przeprowadzonych audytów odpowiedzialność ponosi ADO.

13. Postanowienia końcowe

1. Niniejsza Polityka Bezpieczeństwa Informacji jest dokumentem wewnętrznym i nie może być udostępniania osobom nieupoważnionym w żadnej formie.
2. Użytkownik zobowiązany jest złożyć oświadczenie o tym, iż został zaznajomiony z przepisami ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz instrukcjami obowiązującymi u administratora danych osobowych, a także o zobowiązaniu się do ich przestrzegania.
3. Oświadczenie potwierdzające zaznajomienie użytkownika z przepisami ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz instrukcjami obowiązującymi u Administratora danych osobowych, a także o zobowiązaniu się do ich przestrzegania, przechowywane jest w aktach osobowych pracownika.
4. Wszystkie regulacje dotyczące systemów informatycznych określone w Polityce Bezpieczeństwa Informacji dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiejkolwiek innej formie.
5. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce Bezpieczeństwa Informacji.
6. Niezastosowanie się do prowadzonej przez administratora danych osobowych, której założenia określa niniejszy dokument i naruszenie procedur ochrony danych przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, podlegające sankcjom dyscyplinarnym oraz sankcjom karnym, w szczególności wynikającym z art. 51-52 ustawy oraz art. 266 Kodeksu karnego.
7. Kara dyscyplinarna, orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jedn. Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.) oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
8. W sprawach nieuregulowanych w niniejszej Polityce Bezpieczeństwa Informacji mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r., o ochronie danych osobowych (tekst jedn. Dz. U. z 2002 r., Nr 101, poz. 926 ze zm.) oraz wydanych na jej podstawie aktów wykonawczych.

WÓJT
mgr Krzysztof Listecki

14. Spis załączników

14.1. Załącznik nr 1.1 – Wzór upoważnienia do przetwarzania danych osobowych

14.2. Załącznik nr 1.2 – Wzór powołania Administratora Bezpieczeństwa Informacji

14.3. Załącznik nr 1.3 – Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe

14.4. Załącznik nr 1.4 – Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

14.5. Załącznik nr 1.5 - Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi

14.6. Załącznik nr 1.6 – Sposób przepływu danych pomiędzy poszczególnymi systemami

14.7. Załącznik nr 1.7 – Wzór umowy powierzenia przetwarzania danych osobowych

14.8. Załącznik nr 1.8 – Ewidencja podmiotów, którym powierzono przetwarzanie danych osobowych

14.9. Załącznik nr 1.9 – Ewidencja osób upoważnionych do przetwarzania danych osobowych

14.10. Załącznik nr 1.10 – Rejestr udostępnień danych osobowych

14.11. Załącznik 1.11 – Wzór raportu z naruszenia bezpieczeństwa danych osobowych