**ZARZĄDZENIE NR 15/2011**
**WÓJTA GMINY SIEMIATYCZE**

z dnia 26 kwietnia 2011 r.

**w sprawie wdrożenia dokumentacji przetwarzania i ochrony danych osobowych w Urzędzie Gminy Siemiatycze.**

Na podstawie art. 31 i 33 ust.3 ustawy z dnia 8 marca 1990 roku o samorządzie gminnym ( Dz.U. z 2001r. Nr 142, poz. 1591 z późniejszymi zmianami) w związku z art. 36 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych ( Dz.U.z 2002 r. Nr 101, poz.926 z późniejszymi zmianami) oraz § 3 rozporządzenia 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), zarządzam, co następuje:

**§ 1.** Wprowadzam do użytku służbowego:

1) "Politykę bezpieczeństwa" w brzmieniu ustalonym w załączniku nr 1 do zarządzenia,
2) "Instrukcję zarządzania systemami informatycznymi służącymi do przetwarzania danych" w brzmieniu stanowiącym załącznik nr 2 do zarządzenia,
3) "Regulamin organizacji i przetwarzania danych osobowych" w brzmieniu ustalonym w załączniku nr 3 do zarządzenia.

**§ 2.** Wykonanie zarządzenia zleca się Administratorowi Bezpieczeństwa Informacji.

**§ 3.** Zarządzenie wchodzi w życie z dniem podpisania.

Wójt
**Edward Zaremba**

Załącznik Nr 1 do Zarządzenia Nr 15/2011

Wójta Gminy Siemiatycze

z dnia 26 kwietnia 2011 r.

# Polityka bezpieczeństwa

## Rozdział 1.
## Postanowienia ogólne.

**§ 1.** Niniejsza „Polityka bezpieczeństwa", zwana dalej Polityką, została opracowana zgodnie z wymogami § 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).

**§ 2.** Określenia i skróty użyte w Polityce oznaczają:

1) Administrator Danych Osobowych – Wójt Gminy Siemiatycze, zwany dalej Administratorem.
2) Administrator Bezpieczeństwa Informacji, zwany dalej ABI – osoba wyznaczona przez Administratora, w rozumieniu art. 36 ust. 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. Nr 101 poz. 926 z późn. zm.), dalej jako Ustawa.
3) Administrator Systemu Informatycznego, zwany dalej ASI – osoba wyznaczona przez Administratora, pracownik odpowiedzialny za wdrażanie i stosowanie zasad bezpieczeństwa danych osobowych w zakresie technicznych zabezpieczeń systemu informatycznego Urzędu Gminy Siemiatycze.
4) Osoba upoważniona, zwana dalej użytkownikiem – osoba posiadająca upoważnienie nadane przez Administratora lub osobę wyznaczoną przez niego i uprawniona do przetwarzania danych osobowych, w zakresie wskazanym w upoważnieniu.
5) Przełożony użytkownika, zwany dalej przełożonym – kierownik referatu, osba odpowiedzialna za przestrzeganie zasad przetwarzania i ochrony danych osobowych przez podległych mu pracowników
6) System informatyczny, zwany dalej systemem, w rozumieniu art. 7 pkt 2a) Ustawy.
7) Zabezpieczenie danych w systemie, zwane dalej zabezpieczeniem – czynności wykonywane w rozumieniu art. 7 pkt 2b) Ustawy.
8) Wewnętrzna sieć teleinformatyczna – sieć Administratora, łącząca co najmniej dwa indywidualne stanowiska komputerowe, umożliwiająca użytkownikom określony dostęp do danych.
9) Dane sensytywne – dane w rozumieniu art. 27 Ustawy, podlegające szczególnej ochronie.
10) Urząd Gminy Siemiatycze, zwany dalej Urzędem..
11) Zarządzenie Wójta Gminy Siemiatycze w sprawie wdrożenia dokumentacji przetwarzania i ochrony danych osobowych w Urzędzie Gminy Siemiatycze, zwane dalej Zarządzeniem.

## Rozdział 2.
## Cele i zakres polityki bezpieczeństwa.

**§ 3.** 1. Polityka określa podstawowe zasady bezpieczeństwa i zarządzania bezpieczeństwem systemów.

2. Polityka dotyczy wszystkich danych osobowych, przetwarzanych w Urzędzie niezależnie od formy ich przetwarzania (zbiory ewidencyjne, systemy informatyczne) oraz od tego czy dane są lub mogą być przetwarzane w zbiorach danych.

**§ 4.** Celem Polityki jest ochrona danych osobowych, przetwarzanych w Urzędzie przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów określających zasady postępowania przy przetwarzaniu danych osobowych oraz przed zmianą, uszkodzeniem lub zniszczeniem.

**§ 5.** 1. Cele Polityki realizowane są poprzez zapewnienie danym osobowym następujących cech:

a) poufności — właściwości zapewniającej, że dane nie są udostępniane nieupoważnionym podmiotom;

b) integralności — właściwości zapewniającej, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

c) rozliczalności — właściwości zapewniającej, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

2. Za pomiot nieupoważniony uważa się podmiot, który nie otrzymał zgody Administratora na udostępnienie mu danych osobowych w trybie i na zasadach określonych w art. 29 Ustawy oraz osobę nieposiadającą upoważnienia do przetwarzania danych osobowych, nadanego przez Administratora w trybie art. 37 Ustawy.

**§ 6.** Dla skutecznej realizacji Polityki Administrator zapewnia:

1) odpowiednie do zagrożeń i kategorii danych objętych ochroną, środki techniczne i rozwiązania organizacyjne;

2) szkolenia w zakresie przetwarzania danych osobowych i sposobów ich ochrony;

3) okresowe szacowanie ryzyka zagrożeń dla zbiorów danych;

4) kontrolę i nadzór nad przetwarzaniem danych osobowych;

5) monitorowanie zastosowanych środków ochrony.

**§ 7.** Administrator zapewnia zgodność niniejszej Polityki z przepisami określającymi zasady przetwarzania danych osobowych, tj.:

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) rozporządzeniem 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);

## Rozdział 3.
## Obowiązki i odpowiedzialność w zakresie zarządzania bezpieczeństwem.

**§ 8.** 1. Zarządzanie bezpieczeństwem systemów jest procesem ciągłym, realizowanym przy współdziałaniu użytkowników z ABI i ASI.

2. Wszystkie osoby przetwarzające dane osobowe zobowiązane są do:

1) przetwarzania danych osobowych zgodnie z obowiązującymi przepisami;

2) postępowania zgodnie z ustaloną przez Administratora Polityką oraz z:

a) „Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych";

b) Regulaminem organizacji i przetwarzania danych osobowych".

3. W przypadku naruszenia przepisów lub zasad postępowania użytkownik podlega odpowiedzialności służbowej i karnej.

**§ 9.** 1. Do obowiązków ABI należy kontrola i nadzór przestrzegania zasad bezpieczeństwa i ochrony danych osobowych określonych w dokumentacji, o której mowa w § 8 ust. 2.

2. Użytkownicy zobowiązani są do:

a) ścisłego przestrzegania zakresu nadanego upoważnienia;

b) przetwarzania i ochrony danych osobowych zgodnie z przepisami;

c) zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia;

d) zgłaszania ASI incydentów związanych z naruszeniem bezpieczeństwa danych oraz niewłaściwym funkcjonowaniem systemu, a także informowania ABI o przypadkach naruszenia zasad ochrony danych.

## Rozdział 4.
## Obszary przetwarzania danych.

**§ 10.** 1. Wykaz pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe w Urzędzie jest prowadzony przez ABI.

2. Pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane na czas nieobecności w nich osób zatrudnionych, w sposób uniemożliwiający dostęp osób trzecich. Osoby postronne mogą przebywać wewnątrz wyżej wymienionego obszaru jedynie w obecności osoby upoważnionej do przetwarzania danych osobowych.

3. Za obszar przetwarzania danych uznaje się obszar, w którym wykonywana jest choćby jedna z czynności wymienionych w art. 7 pkt. 2 Ustawy.

**§ 11.** 1. Kierownicy referatów zobowiązani są do niezwłocznego przekazywania ABI informacji o lokalizacji miejsc przetwarzania danych osobowych.

2. ABI przekazują Administratorowi oceny i wnioski wynikające z zagrożeń bezpieczeństwa i analizy stanu ochrony obszarów przetwarzania danych osobowych w Urzędzie.

## Rozdział 5.
## Wykaz zbiorów danych oraz programów zastosowanych do przetwarzania danych

**§ 12.** Wykaz zbiorów danych oraz programów zastosowanych do przetwarzania danych jest prowadzony przez ABI.

## Rozdział 6.
## Struktury zbiorów danych oraz przepływ danych pomiędzy systemami.

**§ 13.** 1. Dane osobowe są przetwarzane przy zastosowaniu systemów informatycznych, w zbiorach ewidencyjnych oraz poza zbiorami.

2. Zbiory danych osobowych zlokalizowane są w przedmiotowych bazach danych umieszczonych na serwerach bazodanowych bądź stacjach roboczych.

3. Dane osobowe w zbiorach są przetwarzane tylko w aplikacjach (programach) dostosowanych do merytorycznych potrzeb komórek organizacyjnych Urzędu.

**§ 14.** 1. Zawartość pól informacyjnych, występujących w aplikacjach (programach) systemów zastosowanych do przetwarzania danych, musi być zgodna z przepisami prawa, które uprawniają lub zobowiązują Administratora do przetwarzania danych osobowych.

2. Na żądanie Administratora lub osoby przez niego upoważnionej osoby, o których mowa w § 11 ust. 1, zobowiązane są wskazać podstawy prawne określające zakres przetwarzanych danych.

**§ 15.** 1. Opisy struktur zbiorów danych wskazujące zawartość poszczególnych pól informacyjnych i powiązania pomiędzy nimi, wykonuje ASI na podstawie aplikacji zastosowanych do przetwarzania tych danych.

2. Opisy wykonywane są w postaci wydruków zrzutów ekranowych lub struktur tablic bazy prezentujących zawartość pól informacyjnych i powiązań pomiędzy nimi. W przypadku braku możliwości uzyskania wydruku zrzutu ekranowego ASI sporządza inne dostępne opisy struktury zbioru.

3. ASI zobowiązany jest do przekazywania opisów ABI oraz natychmiastowego informowania go o wszelkich zmianach tych opisów.

**§ 16.** 1. Schematy przepływu danych pomiędzy systemami informatycznymi, zastosowanymi w celu przetwarzania danych osobowych, wykonuje ASI, zgodnie z relacjami występującymi w programach służących do przetwarzania danych osobowych.

2. ASI zobowiązany jest do przekazywania schematów ABI oraz natychmiastowego informowania go o wszelkich w nich zmianach.

**§ 17.** 1. Przepływ danych pomiędzy systemami zastosowanymi w celu przetwarzania danych osobowych może odbywać się w postaci przepływu jednokierunkowego lub przepływu dwukierunkowego.

2. Przesyłanie danych pomiędzy systemami może odbywać się w sposób manualny, przy wykorzystaniu nośników zewnętrznych (np. dyskietka, CD, DVD, taśma streamera, dysk wymienny, PenDrive itp.) lub w sposób półautomatyczny, przy wykorzystaniu funkcji eksportu (importu) danych za pomocą teletransmisji (np. poprzez wewnętrzną sieć teleinformatyczną).Należy zapewnić ochrone kryptograficzna oraz zachować szczególną ostrożność podczas ich transportu i przetwarzania.

## Rozdział 7.
## Środki ochrony.

**§ 18.** 1. Administrator zapewnia zastosowanie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

2. Osoby, o których mowa w § 12 ust. 1 przeprowadzają okresową analizę ryzyka dla poszczególnych systemów i na tej podstawie przedstawiają Administratorowi propozycje dotyczące zastosowania środków technicznych i organizacyjnych (środków ochrony), celem zapewnienia właściwej ochrony przetwarzanym danym.

3. Analiza ryzyka obejmuje:

a) identyfikację występujących zagrożeń dla systemów, zbiorów i baz danych;

b) ocenę dotychczas stosowanej ochrony obszarów przetwarzania danych osobowych;

c) określenie wielkości ryzyka, tj. prawdopodobieństwa, że określone zagrożenie wykorzysta podatność (słabość) zasobu;

d) identyfikację obszarów wymagających szczególnych zabezpieczeń.

4. Zastosowane środki ochrony (techniczne i organizacyjne) powinny być adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych osobowych.

**§ 19.** 1. Środki ochrony, zastosowane przez Administratora dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych, obejmują:

a) środki fizyczne;

b) środki osobowe;

c) środki techniczne.

2. Środki ochrony fizycznej obejmują:

a) lokalizację miejsc przetwarzania danych osobowych w pomieszczeniach o ograniczonym dostępie;

b) ustalenie zasad gospodarki kluczami do pomieszczeń i szaf;

c) wyposażenie pomieszczeń, w których przetwarzane są dane osobowe, w odpowiednio zabezpieczone okna, meble, zamknięcia i niezbędne zabezpieczenia alarmowe;

d) składowanie danych sensytywnych oraz nośników wymiennych i nośników kopii zapasowych, w odpowiednio zabezpieczonych szafach;

e) odpowiednie wyposażenie i zabezpieczenie pomieszczeń serwerowni.

3. Środki ochrony osobowej obejmują:

a) dopuszczenie do przetwarzania danych osobowych wyłącznie osób posiadających upoważnienie nadane przez Administratora lub osobę upoważnioną przez niego;

b) zapoznanie tych osób z zasadami przetwarzania danych osobowych oraz obsługą systemu służącego do ich przetwarzania;

c) odebranie stosownych zobowiązań i oświadczeń; tj. zobowiązania do zachowania w tajemnicy danych i sposobów ich zabezpieczenia oraz oświadczenia o zapoznaniu z treścią przepisów określających zasady postępowania przy przetwarzaniu danych osobowych, a także z dokumentacją przetwarzania i ochrony danych osobowych.

4. Środki ochrony technicznej obejmują:

a) mechanizmy kontroli dostępu do systemów i zasobów;

b) zastosowanie odpowiednich i regularnie aktualizowanych narzędzi ochronnych (programy antywirusowe, firewalle, itp.);

c) zastosowanie ochrony zasilania.

**§ 20.** 1. Uwzględniając kategorie przetwarzanych danych oraz zagrożenia zidentyfikowane w wyniku przeprowadzonej analizy ryzyka dla poszczególnych systemów, stosuje się następujące poziomy bezpieczeństwa:

a) podstawowy;

b) podwyższony;

c) wysoki.

2. Określenia poziomu bezpieczeństwa systemu informatycznego dokonuje ABI na wniosek osób o których mowa § 11 ust. 1.

3. Poziomy bezpieczeństwa odnotowuje się w dokumentacji prowadzonej przez ABI.

**§ 21.** Systemy informatyczne, którym przypisano poziomy bezpieczeństwa wymienione w § 20 muszą spełniać wymagania wymienione w załączniku do 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).

Załącznik Nr 2 do Zarządzenia Nr 15/2011

Wójta Gminy Siemiatycze

z dnia 26 kwietnia 2011 r.

**Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.**

## Rozdział 1.
## Postanowienia ogólne.

**§ 1.** 1. Niniejsza „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych", zwana dalej Instrukcją, obejmuje swoim zakresem wszystkie osoby biorące udział w procesie przetwarzania danych osobowych w Urzędzie Gminy Siemiatycze, a w szczególności zaś osoby pełniące funkcje:

1) administratora bezpieczeństwa informacji w Urzędzie;

2) administratora systemu informatycznych w Urzędzie;

3) bezpośrednich przełożonych osób przetwarzających dane osobowe;

4) inne osoby wskazane przez Administratora.

2. Instrukcja ma zastosowanie także do podmiotów zewnętrznych i osób fizycznych, które współpracują z Urzędem i na podstawie przepisów współuczestniczą w procesie przetwarzania danych osobowych, a w szczególności:

1) podmioty, którym na podstawie przepisów udostępniono dane osobowe;

2) podmioty, którym na podstawie umowy przekazano lub udostępniono dane osobowe do przetwarzania;

3) przedsiębiorcy świadczący usługi związane z konserwacją systemu informatycznego;

4) inne osoby, niebędące pracownikami Urzędu, wykonujące prace na podstawie stosunków cywilnoprawnych.

**§ 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.** Określenia i skróty użyte w Instrukcji oznaczają:

1) Administrator Danych Osobowych – Wójta Gminy Siemiatycze, zwany dalej Administratorem.

2) Administrator Bezpieczeństwa Informacji, zwany dalej ABI – osoba wyznaczona przez Administratora, w rozumieniu art. 36 ust. 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. Nr 101, poz. 926 z późn. zm.), dalej zwana Ustawą.

3) Administrator Systemu Informatycznego, zwany dalej ASI – osoba wyznaczona przez Administratora, pracownik odpowiedzialny za wdrażanie i stosowanie zasad bezpieczeństwa danych osobowych w zakresie technicznych zabezpieczeń systemu informatycznego Urzędu Gminy Siemiatycze.

4) Osoba upoważniona, zwana dalej użytkownikiem – osoba posiadająca upoważnienie nadane przez Administratora lub osobę wyznaczoną przez niego i uprawniona do przetwarzania danych osobowych, w zakresie wskazanym w upoważnieniu.

5) Przełożony użytkownika, zwany dalej przełożonym – kierownik referatu, osoba odpowiedzialna za przestrzeganie zasad przetwarzania i ochrony danych osobowych przez podległych mu pracowników.

6) System informatyczny, zwany dalej systemem, w rozumieniu art. 7 pkt 2a) Ustawy.

7) Zabezpieczenie danych w systemie informatycznym, zwane dalej zabezpieczeniem – czynności wykonywane w rozumieniu art. 7 pkt 2b) Ustawy.

8) Wewnętrzna sieć teleinformatyczna – sieć Administratora, łącząca co najmniej dwa indywidualne stanowiska komputerowe, umożliwiająca użytkownikom określony dostęp do danych osobowych.

9) Indywidualne stanowisko komputerowe – komputer stacjonarny, w którym przetwarzane są dane osobowe, bez podłączenia do sieci teleinformatycznej.

10) Urządzenie zabezpieczające system przed awarią zasilania lub zakłóceniami w sieci zasilającej, zwane dalej UPS.

11) Urząd Gminy Siemiatycze, zwany dalej Urzędem.

12) Dane sensytywne – dane w rozumieniu art. 27 Ustawy, podlegające szczególnej ochronie.

13) Zarządzenie Wójta w sprawie wdrożenia dokumentacji przetwarzania i ochrony danych osobowych w Urzędzie Gminy Siemiatycze, zwane dalej Zarządzeniem.

## Rozdział 2.
## Procedury nadawania uprawnień do przetwarzania danych osobowych i rejestrowania tych uprawnień w systemach informatycznych.

**§ 4.** 1. Do przetwarzania danych osobowych w systemach informatycznych mogą mieć dostęp wyłącznie osoby posiadające upoważnienie nadane przez Administratora lub osobę przez niego upoważnioną.

2. Procedury nadawania upoważnień i zgłaszania zmian w tym zakresie zawarte zostały w § 6 „Regulaminu organizacji przetwarzania danych osobowych", stanowiącego załącznik nr 3 do Zarządzenia.

**§ 5.** 1. Użytkownika w systemie rejestruje ASI na wniosek przełożonego po nadaniu użytkownikowi upoważnienia do przetwarzania danych.

2. Uprawnienia użytkownika do pracy w systemie informatycznym, w którym przetwarzane są dane osobowe, mogą obejmować w swym zakresie dostęp do baz danych w swojej komórce organizacyjnej oraz:

1) odczyt danych;

2) wprowadzanie nowych danych;

3) modyfikację istniejących danych;

4) wydruk danych;

5) przekazywanie danych wewnątrz Urzędu.

3. Uprawnienia użytkownika uprzywilejowanego do pracy w systemie informatycznym, zastosowanym do przetwarzania danych osobowych, mogą obejmować uprawnienia, o których mowa w ust. 2 oraz:

1) dostęp do baz danych innych komórek organizacyjnych;

2) udostępnianie danych podmiotom i osobom, o których mowa w § 1 ust. 2;

3) usuwanie danych ze zbiorów swojej komórki organizacyjnej;

4. ASI obok uprawnień wymienionych w ust. 2 i ust. 3, uprawniony jest do:

1) zakładania, modyfikacji lub usuwania baz danych;

2) migracji danych pomiędzy bazami;

3) usuwania lub anonimizacji danych w bazach danych na podstawie pisemnego polecenia osób, o których mowa w § 1 ust. 1 lit e);

4) archiwizowania danych ze zbiorów.

5. Administrator lub osoba przez niego wskazana na wniosek ABI może cofnąć, ograniczyć lub nie wyrazić zgody na przyznanie określonych uprawnień użytkownikom, którzy powodują incydenty mające negatywny wpływ na bezpieczeństwo przetwarzania danych w systemach.

6. ABI posiada uprawnienia administratora systemu, które umożliwiają realizację zadań, o których mowa w art. 38 Ustawy.

**§ 7.** ASI wyrejestrowuje lub ogranicza uprawnienia użytkownika w przypadkach, o których mowa w § 5 ust. 5 oraz na wniosek przełożonego użytkownika po zmianie lub utracie upoważnienia dostępu do danych.

## Rozdział 3.
## Metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem.

**§ 7.** 1. System, w którym przetwarza się dane osobowe wyposażony jest w mechanizmy uwierzytelnienia użytkownika oraz kontroli dostępu osób. Jednym z elementów umożliwiającym dostęp do systemu jest hasło, które pełni rolę weryfikowania tożsamości użytkownika.

2. Hasło dostępu składa się z ciągu literowo – cyfrowego i nie może kojarzyć się bezpośrednio z użytkownikiem. Hasła dostępu nie mogą powtarzać się w danym roku.

3. Hasło dostępu zapisywane jest na ekranie monitora w formie niejawnej i znane jest tylko użytkownikowi.

4. W przypadku gdy hasła dostępu używa się do uwierzytelnienia użytkowników w systemie, powinno ono składać się z:

1) co najmniej z 6 znaków - przy podstawowym poziomie bezpieczeństwa;

2) co najmniej z 8 znaków - przy podwyższonym i wysokim poziomie bezpieczeństwa.

5. Użytkownik sam ustala hasło dostępu i w wypadku podejrzenia lub stwierdzenia jego ujawnienia niezwłocznie je zmienia. Jeżeli system nie wymusza zmiany hasła użytkownik ma obowiązek zmieniać je co najmniej raz w miesiącu.

6. Hasła dostępu do baz danych są różne od haseł uwierzytelniających użytkowników w systemie.

**§ 8.** 1. Identyfikator przyznaje się użytkownikom w przypadku dostępu do stanowiska komputerowego więcej niż jednej osoby.

2. Identyfikator użytkownika składa się z ciągu znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujących w systemie osobę upoważnioną do przetwarzania danych osobowych.

3. Identyfikator użytkownikowi przyznaje ASI, o czym informuje ABI.

4. Identyfikator podlega wpisowi do „Ewidencji osób upoważnionych do przetwarzania danych osobowych" i po jego wyrejestrowaniu nie może być przydzielony innej osobie.

5. Podczas przetwarzania danych osobowych w systemie posługiwanie się identyfikatorem innej osoby jest zabronione.

**§ 9.** 1. Użytkownik ponosi odpowiedzialność za czynności wykonywane w systemie przy użyciu identyfikatora i hasła. Nie dopuszcza się, aby hasła były przechowywane przez użytkownika w formie jakiegokolwiek zapisu.

2. Administrator dopuszcza możliwość stosowania do weryfikacji tożsamości użytkowników w systemie innych sposobów np.: karty mikroprocesorowe lub metody biometryczne.

3. Osobami odpowiedzialnymi za prawidłowe funkcjonowanie w systemie mechanizmów uwierzytelniających są ASI.

## Rozdział 4.
## Procedury rozpoczęcia, zawieszenia i zakończenia pracy przez użytkowników systemów.

**§ 10.** 1. Użytkownicy rozpoczynający pracę zobowiązani są do przestrzegania procedur mających na celu sprawdzenie działania systemu, a w szczególności:

1) sprawdzenie ogólnego stanu sprzętu i miejsca przechowywania nośników zawierających dane osobowe;

2) po włączeniu urządzeń - ocenienie jakości ich pracy.

2. Użytkownik przystępując do przetwarzania danych powinien zalogować się w systemie zgodnie z poleceniami wyświetlanymi na ekranie monitora, posługując się swoim identyfikatorem i hasłem - wiedząc, że:

1) maksymalna ilość prób wprowadzenia hasła do systemu wynosi 3;

2) po przekroczeniu liczby prób logowania zablokowany zostaje dostęp do systemu na poziomie użytkownika;

3) użytkownik zobowiązany jest poinformować o zdarzeniu ASI, który podejmuje stosowne w tym zakresie działania.

3. Przetwarzając dane osobowe w systemie użytkownik zobowiązany jest do wykonywania czynności mających na celu zapewnienie im bezpieczeństwa:

1) ustawiać monitory w sposób uniemożliwiający osobom nieupoważnionym podgląd ekranów;

2) stosować urządzenia zabezpieczające przed utratą danych, spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej;

3) wylogować się z systemu w przypadku, kiedy przerwa pracy w systemie trwa dłużej niż 30 minut.

4. Po zakończeniu pracy w systemie użytkownik zobowiązany jest:

1) zamknąć system i zaczekać na jego wyłączenie;

2) sprawdzić, czy elektroniczne nośniki informacji zawierające dane osobowe nie zostały pozostawione bez nadzoru.

5. Do czynności, o których mowa w ust. 4 lit. a), zalicza się:

1) zapisanie wszelkich zmian w opracowywanych dokumentach;

2) zamknięcie wszystkich używanych programów;

3) zamknięcie systemu poprzez użycie polecenia „Zamknij system".

**§ 11.** 1. Codzienną kontrolę bezpieczeństwa systemu przetwarzania danych osobowych na stanowiskach pracy sprawują użytkownicy oraz ich przełożeni.

2. Za naruszenie lub próbę naruszenia bezpieczeństwa danych osobowych uważa się w szczególności:

1) brak możliwości zalogowania się do systemu;

2) zmiany w wyglądzie aplikacji lub katalogów zawierających dane osobowe;

3) brak urządzeń systemu, nośników informacji lub kopii zapasowych;

4) pojawienie się niestandardowych komunikatów generowanych przez system;

5) ślady włamania do pomieszczeń lub obszaru przetwarzania danych;

6) ślady włamania lub prób włamania do mebli, w których przechowuje się elektroniczne lub papierowe nośniki danych osobowych;

7) informacja o zainfekowaniu systemu wirusami;

8) stwierdzenie prób włamania do systemu lub nieautoryzowanej modyfikacji danych;

9) fizyczne zniszczenie lub podejrzenie zniszczenia urządzeń systemu na skutek przypadkowych lub celowych działań;

10) celowe lub nieświadome spowodowanie przez użytkownika incydentu naruszającego prawa osób, których dane są przetwarzane w systemie;

11) uruchamianie stron internetowych umożliwiających przedostanie się do systemu szkodliwego oprogramowania.

**§ 12.** 1. W przypadku stwierdzenia okoliczności, o których mowa w § 11 ust. 2, użytkownik zobowiązany jest do bezzwłocznego powiadomienia swojego przełożonego oraz ASI.

2. ASI po otrzymaniu informacji o naruszeniu bezpieczeństwa blokują określonemu użytkownikowi dostęp do systemu i informują o incydencie ABI.

3. ABI podejmuje działania mające na celu wyjaśnienie przyczyn powstania zagrożenia. Po wyjaśnieniu zdarzenia polecają ASI przywrócenie funkcjonalności systemu.

4. ABI i ASI z przebiegu zdarzenia sporządzają notatkę służbową, którą przekazują Administratorowi lub osobie przez niego upoważnionej.

## Rozdział 5.
## Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi służących do ich przetwarzania.

**§ 13.** 1. W celu zapewnienia bezpieczeństwa przetwarzania danych osobowych istnieje obowiązek tworzenia kopii zapasowych. Proces tworzenia kopii zapasowych w Urzędzie nadzoruje ABI.

2. Kopie zapasowe tworzy się według potrzeb określonych przez przełożonych, na odpowiedniej jakości nośnikach informacji, wykorzystując następujące metody:

1) w kopii tygodniowej- metodę całościową.

3. Kopie zapasowe tworzy się wykorzystując narzędzia programowe i urządzenia systemu do tego przystosowane. Kopie zapasowe wykonuje ASI.

## Rozdział 6.
## Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych.

**§ 14.** 1. Elektroniczne nośniki informacji zawierające dane oraz wydruki przechowuje się wewnątrz obszaru przetwarzania danych, w meblach posiadających sprawne zamknięcia. Nośniki i wydruki nie powinny być wynoszone poza obszar przetwarzania danych bez zgody przełożonego.

2. Kopie zapasowe przechowuje się w szafach metalowych w pomieszczeniach, które nie są stałym miejscem ich przetwarzania i zapewniają właściwą ochronę przed nieuprawnionym dostępem, modyfikacją, uszkodzeniem lub zniszczeniem.

3. Czas przechowywania kopii zapasowych zależy od aktualności zapisanych danych oraz potrzeby tworzenia kolejnych kopii. Jeżeli przepisy nie stanowią inaczej to czas przechowywania kopii zapasowych należy ograniczyć do:

1) tygodniowych – 1 miesiąc;

**§ 15.** 1. Kopie zapasowe i elektroniczne nośniki informacji, które zostały uszkodzone lub przeznaczone do likwidacji należy niszczyć mechanicznie pod nadzorem ASI, w sposób uniemożliwiający ich ponowne użycie.

2. Niepotrzebne wydruki z systemu, które zawierają dane osobowe należy niszczyć w niszczarkach w sposób uniemożliwiający ich odtworzenie.

**§ 16.** Przekazanie i niszczenie elektronicznych nośników informacji zawierających dane osobowe, odbywa się na podstawie protokółu podpisanego przez ASI oraz wskazanych użytkowników. Kopię protokołu zatwierdzonego przez przełożonego należy przesłać do ABI.

## Rozdział 7.
## Sposób zabezpieczenia systemu informatycznego przed działalnością wirusów komputerowych, nieuprawnionym dostępem oraz awarią zasilania.

**§ 17.** 1. System, w którym przetwarzane są dane osobowe jest wyposażony w mechanizmy ochrony antywirusowej.

2. Obszarami systemu narażonymi na ingerencję wirusów oraz innego szkodliwego oprogramowania są dyski twarde urządzeń i pamięć RAM oraz elektroniczne nośniki informacji.

3. Drogą przedostania się wirusów lub szkodliwego oprogramowania może być sieć publiczna, wewnętrzna sieć teleinformatyczna lub elektroniczne nośniki informacji.

4. Kontrola antywirusowa obejmuje urządzenia oraz wszelkiego rodzaju nośniki służące do przetwarzania danych.

5. Obowiązkiem ASI jest zarządzanie bazą antywirusową, w tym określanie warunków działania oprogramowania przy zachowaniu maksymalnej efektywności i minimalizacji jej negatywnego wpływu na korzystanie przez użytkowników z systemu, a w szczególności:

1) instalowanie i konfigurowanie modułów bazy antywirusowej;

2) uaktualnianie sygnatur w bazie antywirusowej;

3) dostosowywanie czasu pracy urządzeń systemu do określonego przez Administratora czasu pracy użytkowników.

**§ 18.** 1. System posiada zabezpieczenia przed działaniem oprogramowania mającego na celu uzyskanie nieuprawnionego dostępu do danych.

2. ASI ma obowiązek realizacji przedsięwzięć mających na celu wdrażanie technicznych i logicznych zabezpieczeń chroniących system przed nieuprawnionym dostępem do danych.

3. Nadzór nad czynnościami, o których mowa w ust. 2, sprawuje ABI

**§ 19.** 1. System, w którym przetwarzane są dane osobowe posiada mechanizmy pozwalające zabezpieczyć je przed utratą lub nieautoryzowaną zmianą spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

2. Dane osobowe przetwarzane w systemie chroni się stosując filtry zabezpieczające przed skutkami spadku napięcia oraz urządzenia podtrzymujące zasilanie do momentu poprawnego zapisania danych i wylogowania się użytkownika z systemu.

3. Dane osobowe przetwarzane w bazach umieszczonych na serwerach zabezpiecza się przed zanikiem napięcia wykorzystując UPS.

**§ 20.** Administrator może wprowadzić alternatywne metody ochrony przed szkodliwym działaniem programów mających na celu uzyskanie nieuprawnionego dostępu do danych. Do takich metod zalicza się:

1) odłączenie systemu od sieci publicznej oraz urządzeń umożliwiających odczyt danych z elektronicznych nośników informacji na określonych stanowiskach komputerowych;

2) tworzenie indywidualnych stanowisk komputerowych, które spełniają wymogi bezpieczeństwa przetwarzania danych osobowych na poziomie wysokim;

3) zastosowanie w urządzeniach kart PCI (RecoveryCard) lub kluczy szyfrujących USB, itp.

## Rozdział 8.
## Sposoby realizacji w systemie wymogów dotyczących przetwarzania danych.

**§ 21.** 1. Osobom, których dane są przetwarzane w systemie, Administrator zapewnia odnotowanie:

1) daty pierwszego wprowadzenia danych do systemu;

2) identyfikatora użytkownika wprowadzającego dane osobowe do systemu chyba, że dostęp do systemu posiada tylko jedna osoba;

3) źródła danych, w przypadku zbierania danych nie od osoby, której one dotyczą;

4) informacji o odbiorcach, którym dane osobowe zostały udostępnione (data i zakres udostępnienia) chyba, że system używany jest do przetwarzania danych w zbiorach jawnych;

5) sprzeciwu odnośnie przetwarzania danych, o których mowa w art. 32 ust. 1 pkt. 8 Ustawy.

2. Odnotowywanie w systemie informacji, o których mowa w ust. 1 lit. a) i b) następuje automatycznie, po zatwierdzeniu przez użytkownika operacji wprowadzania danych.

3. System zapewnia każdej osobie, której dane są przetwarzane, wydrukowanie raportu zawierającego w zrozumiałej formie informacje, o których mowa w ust. 1.

**§ 22.** 1. W przypadku przetwarzania danych, w co najmniej dwóch systemach - wymagania, o których mowa w § 21 ust. 1, są realizowane w jednym z nich lub w odrębnym systemie przeznaczonym do tego celu.

2. W sytuacjach przetwarzania danych w systemie służącym tylko do edycji tekstu nie obowiązują wymagania, o których mowa w § 21 ust. 1.

3. Oceny zgodności systemu i aplikacji z wymogami określonymi w § 21, dokonuje ABI na wniosek ASI.

**§ 23.** 1. Na czas trwania transportu nośniki, kopie i wydruki, o których mowa w § 14 ust. 1 i 2, umieszcza się w trwałych opakowaniach i chroni przed utratą, zniszczeniem lub uszkodzeniem. Przenosić lub przewozić mogą je tylko osoby do tego upoważnione.

2. Urządzenia, elektroniczne nośniki informacji i wydruki z systemu zawierające dane sensytywne, przekazywane poza obszar ich przetwarzania zabezpiecza się w sposób zapewniający poufność, integralność i rozliczalności tych danych.

3. Osoby użytkujące komputery przenośne, które są wykorzystywane do przetwarzania danych osobowych, zobowiązane są do stosowania właściwych zabezpieczeń technicznych i ochrony kryptograficznej oraz zachowania szczególnej ostrożności podczas ich transportu i przechowywania.

## Rozdział 9.
## Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych

**§ 24.** 1. Wykonywanie przeglądów i konserwacja systemu ma na celu:

1) sprawdzenie działania technicznych zabezpieczeń;

2) sprawdzenie funkcjonalności i jakości pracy;

3) sprawdzenie i określenie przydatność elektronicznych nośników informacji

4) zakwalifikowanie urządzeń do naprawy.

2. Przeglądy i konserwacja urządzeń wchodzących w skład platformy sprzętowej dla danego systemu lub aplikacji powinny być wykonywane w terminach określonych przez producenta, jeśli producent nie przewidział dla potrzeby dokonywania przeglądów eksploatacyjnych, lub też nie określił ich częstotliwości, to o dokonaniu przeglądu oraz sposobie jego przeprowadzenia decyduje ASI.

3. Czynności, o których mowa w ust. 1, wykonuje ASI co najmniej jeden raz na kwartał.

4. Nieprawidłowości ujawnione w trakcie przeglądów bądź konserwacji, powinny być niezwłocznie usunięte, a ich przyczyny przeanalizowane. O fakcie ujawnienia nieprawidłowości ASI informuje ABI.

5. Za terminowość przeprowadzenia przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada ASI.

## Rozdział 10.
## Postanowienia końcowe.

**§ 25.** Osoby upoważnione przez Administratora do wdrażania oprogramowania, aplikacji, urządzeń lub systemów służących do przetwarzania danych osobowych, zobowiązani są do uwzględniania zapisów umownych, o których mowa w § 21 „Regulaminu organizacji i przetwarzania danych osobowych", stanowiącego załącznik nr 3 do Zarządzenia.

**§ 26.** W sprawach nie uregulowanych niniejszą Instrukcją zastosowanie znajdują:

1) Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. Nr 101 poz. 926 z późn. zm.);

2) Rozporządzenie 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).

Załącznik Nr 3 do Zarządzenia Nr 15/2011

Wójta Gminy Siemiatycze

z dnia 26 kwietnia 2011 r.

# Regulamin organizacji i przetwarzania danych osobowych.

## Rozdział 1.
## Postanowienia ogólne.

**§ 1.** 1. Regulamin organizacji i przetwarzania danych osobowych" zwany dalej Regulaminem, określa ogólne zasady, cele przetwarzania danych i wskazuje działania podejmowane przez Administratora oraz osoby przez niego upoważnione, w zakresie organizacji przetwarzania i ochrony danych osobowych w Urzędzie Gminy Siemiatycze.

2. Regulamin został opracowany w wykonaniu dyspozycji art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. Nr 101, poz. 926 z późn. zm.), dalej jako „Ustawa", w celu określenia zadań organizacyjnych i technicznych, realizowanych w zakresie ochrony danych przez użytkowników, ich przełożonych oraz inne osoby wskazane przez Administratora.

**§ 2.** Określenia i skróty użyte w Regulaminie oznaczają:

1) Administrator Danych Osobowych – Wójt Gminy Siemiatycze, zwany dalej Administratorem.

2) Administrator Bezpieczeństwa Informacji, zwany dalej ABI – osoba wyznaczona przez Administratora, w rozumieniu art. 36 ust. 3 Ustawy.

3) Administrator Systemu Informatycznego, zwany dalej ASI – osoba wyznaczona przez Administratora, pracownik odpowiedzialny za wdrożenie i stosowanie zasad bezpieczeństwa danych osobowych w zakresie technicznych zabezpieczeń systemu informatycznego w Urzędzie Gminy Siemiatycze..

4) Osoba upoważniona, zwana dalej użytkownikiem – osoba posiadająca upoważnienie nadane przez Administratora lub osobę wskazaną przez niego i uprawniona do przetwarzania danych osobowych w zakresie wskazanym w upoważnieniu.

5) Przełożony użytkownika, zwany dalej przełożonym – kierownik referatu, osoba odpowiedzialna za przestrzeganie zasad przetwarzania i ochrony danych osobowych przez podległych mu pracowników.Urzędu Gminy Siemiatycze.

6) GIODO – Biuro Generalnego Inspektora Ochrony Danych Osobowych.

7) Dane sensytywne – dane w rozumieniu art. 27 Ustawy, podlegające szczególnej ochronie.

8) Urząd Gminy Siemiatycze, zwany dalej Urzędem.

9) Zarządzenie Wójta w sprawie wdrożenia dokumentacji przetwarzania i ochrony danych osobowych w Urzędzie Gminy Siemiatycze, zwane dalej Zarządzeniem.

**§ 3.** 1. Administrator może upoważnić osoby zatrudnione w Urzędzie do wykonywania określonych czynności, znajdujących się w zakresie zadań Administratora.

2. Kontrola prawidłowości wykonywania czynności, o których mowa w ust. 1, należy do Administratora.

## Rozdział 2.
## Ogólne zasady przetwarzania danych osobowych.

**§ 4.** 1. Dane osobowe są przetwarzane w Urzędzie w celu realizacji zadań określonych przepisami prawa.

2. Cel, o którym mowa w ust. 1, należy osiągać przy zachowaniu szczególnej staranności w realizacji przedsięwzięć dotyczących ochrony interesów osób, których dane dotyczą.

**§ 5.** 1. Zasadą obowiązującą w Urzędzie jest zachowanie przez użytkowników w tajemnicy wszelkich informacji dotyczących danych osobowych oraz sposobów ich zabezpieczania.

2. Możliwość wystąpienia zagrożeń bezpieczeństwa danych przetwarzanych w systemach lub kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych nakłada na użytkowników i ich przełożonych obowiązek zapewnienia danym skutecznej ochrony.

3. Przesyłanie danych osobowych za pomocą urządzeń telekomunikacyjnych lub transmisji danych w sieci publicznej wymaga wykorzystania odpowiednich urządzeń i przedsięwzięć zapewniających poufność i integralność ich przekazu.

4. Kopiowanie danych osobowych oraz wykonywanie wydruków jest zabronione, chyba że konieczność ich sporządzania wynika z nałożonych na użytkownika obowiązków i dozwolona jest przepisami prawa.

**§ 6.** 1. Przetwarzanie danych osobowych może być wykonywane wyłącznie przez osoby, które spełniają wymagania zawarte w art. 37 Ustawy.

2. Procedury nadawania (wycofywania) w Urzędzie upoważnień do przetwarzania danych osobowych obejmują:

1) złożenie przez przełożonego wniosku o nadanie (wycofanie) upoważnienia do przetwarzania danych osobowych;

2) podpisanie przez osobę ubiegającą się o nadanie upoważnienia, oświadczenia o zachowaniu w tajemnicy zasad przetwarzania danych oraz sposobów ich zabezpieczania, obejmującej także okres po ustaniu stosunku pracy;

3) nadanie przez Administratora lub osobę przez niego wskazaną, upoważnienia do przetwarzania danych osobowych.

3. Regulamin zawiera także załączniki, które stanowią:

1) załącznik nr 1 – wzór wniosku przełożonego o nadanie (pozbawienie) lub zmianę upoważnienia do przetwarzania danych osobowych;

2) załącznik nr 2 – wzór oświadczenia osoby ubiegającej się o nadanie upoważnienia do przetwarzania danych osobowych;

3) załącznik nr 3 – wzór upoważnienia do przetwarzania danych osobowych.

4. Kopie upoważnień oraz inne dokumenty, o których mowa w ust. 2, przechowuje ABI.

5. ABI prowadzi kontrolę realizacji obowiązku, o którym mowa w ust. 1.

**§ 7.** 1. Pomieszczenia lub ich część, w których przetwarzane są dane osobowe tworzą obszary przetwarzania danych osobowych w Urzędzie. Przebywanie osób nieuprawnionych w tych obszarach jest ograniczone i odbywać się może tylko w obecności użytkowników i za zgodą przełożonych.

2. Administrator zapewnia ochronę obszarów przetwarzania danych osobowych w Urzędzie, według zasad określonych w „Polityce bezpieczeństwa", stanowiącej załącznik nr 1 do Zarządzenia.

3. Do obszarów podlegających szczególnej ochronie Administrator zalicza serwerownię oraz pomieszczenia, w których przetwarzane są dane sensytywne.

## Rozdział 3.
## Procedury tworzenia, rejestrowania i dokonywania zmian w przetwarzaniu danych osobowych w zbiorach.

**§ 8.** 1. Tworzy się zbiory danych osobowych przez nadanie danym osobowym odpowiedniej struktury, dostępnej według określonych kryteriów, niezależnie od tego, czy zestaw danych jest rozproszony lub podzielony funkcjonalnie.

2. Przetwarzanie danych osobowych może odbywać się metodą:

1) papierową, w rozumieniu art. 2 ust. 2 pkt 1) Ustawy;

2) informatyczną, w rozumieniu art. 2 ust. 2 pkt 2) Ustawy;

3. Zgodnie z potrzebami realizacji zadań służbowych, przełożeni użytkowników tworzą zbiory lub wnioskują o ich wycofanie (zmianę), według następujących reguł:

1) nazwa zbioru powinna odzwierciedlać cel przetwarzania danych i być zgodna z nazewnictwem stosowanym w przepisach prawa;

2) należy wskazać podstawy prawne do przetwarzania danych;

3) należy określić sposób i miejsca przetwarzania danych oraz użytkowników;

4) należy przekazać informację ABI w celu określenia poziomu bezpieczeństwa systemu, w którym przetwarzane są dane;

5) należy zapewnić ochronę danym osobowym.

**§ 9.** Przełożeni użytkowników mają obowiązek zgłaszania ABI aktualnych wykazów zbiorów danych osobowych przetwarzanych przez podległych im pracowników.

**§ 10.** 1. Administrator ma obowiązek zgłosić zbiór danych do rejestracji w GIODO, z wyjątkiem przypadków określonych w art. 43 ust. 1 Ustawy.

2. Przełożeni mają obowiązek wypełnienia wniosku zgłoszenia zbioru do rejestracji i przekazania go ABI.

3. Wzór wniosku, o którym mowa w ust. 2, stanowi załącznik do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz.U. Nr 100, poz. 1025).

4. Dane osobowe w zbiorze można przetwarzać od momentu zgłoszenia go do GIODO pod warunkiem, że zbiór nie zawiera danych sensytywnych. Zbiór zawierający dane sensytywne można przetwarzać po potwierdzeniu przez GIODO jego zarejestrowania.

## Rozdział 4.
## Szkolenie oraz prowadzenie dokumentacji z zakresu przetwarzania danych osobowych.

**§ 11.** 1. Każda osoba przed rozpoczęciem przetwarzania danych ma obowiązek zapoznania się z przepisami dotyczącymi bezpieczeństwa przetwarzania i ochrony danych osobowych. Przełożony zobowiązany jest umożliwiać podwładnym zapoznanie się z tymi przepisami.

2. W przypadku wdrażania w Urzędzie nowych procedur przetwarzania i ochrony danych osobowych, Administrator na wniosek osób, o których mowa w § 15 ust 3, może polecić zorganizowanie dodatkowych szkoleń dla wskazanych przez przełożonych grup użytkowników.

3. Szkolenia, o których mowa w ust. 2 organizuje ABI.

**§ 12.** Dokumentacja przetwarzania i ochrony danych osobowych w Urzędzie obejmuje:

1) Politykę bezpieczeństwa przetwarzania danych osobowych",

2) Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych";

3) Regulamin organizacji i przetwarzania danych osobowych".

**§ 13.** 1. W procesie przetwarzania i ochrony danych osobowych prowadzi się następujące ewidencje i wykazy:

a) Ewidencja osób upoważnionych do przetwarzania danych osobowych"

b) Wykaz zbiorów danych osobowych oraz programów zastosowanych do ich przetwarzania";

c) Wykaz pomieszczeń tworzących obszary przetwarzania danych osobowych".

2. Ewidencję i wykazy, o których mowa w ust. 1, prowadzi ABI w formie elektronicznej lub papierowej.

3. Ewidencja, o której mowa w ust. 1 lit. a), zawiera:

a) imię i nazwisko użytkownika;

b) datę nadania i ustania oraz zakres upoważnienia;

c) nazwę komórki organizacyjnej;

d) identyfikator użytkownika.

4. Wykaz, o którym mowa w ust. 1 lit. b), zawiera:

a) nazwę zbioru danych;

b) nr rejestru GIODO;

c) sposób przetwarzania;

d) nazwę programu użytego do przetwarzania w systemie;

e) nadany poziom bezpieczeństwa;

f) nazwę komórki organizacyjnej, w której przetwarzane są dane.

5. Wykaz, o którym mowa w ust. 1 lit. c), zawiera:

a) nazwę komórki organizacyjnej;

b) nazwę zbioru danych

c) numer pomieszczenia.

## Rozdział 5.
## Obowiązki osób upoważnionych przez Administratora.

**§ 14.** 1. Administrator wykonuje zadania z zakresu przetwarzania i ochrony danych osobowych zgodnie z przepisami Ustawy.

2. Administrator stosuje środki techniczne i przedsięwzięcia organizacyjne zapewniające skuteczną realizację zadań w zakresie bezpieczeństwa i ochrony danych przetwarzanych w Urzędzie.

**§ 15.** 1. Zadania organizacji, koordynacji, kontroli i nadzoru przestrzegania przepisów o ochronie danych osobowych w Urzędzie wykonuje ABI na podstawie upoważnień nadanych przez Administratora lub osobę przez niego wskazaną.

2. Do zadań ABI należy:

1) koordynowanie przedsięwzięć kierowników komórek organizacyjnych, o których mowa w ust. 1, w zakresie przetwarzania i ochrony danych osobowych;

2) nadzorowanie sposobu wykonywania zadań przez osoby, o których mowa w ust. 3, oraz osobę pełniącą funkcje ABI;

3) cofanie, ograniczanie lub niewyrażanie zgody na przyznanie uprawnień do przetwarzania danych osobowych osobom niespełniającym warunków, o których mowa w § 6 oraz sprawcom zdarzeń, o których mowa w § 5 ust. 5 „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych ", będącej załącznikiem nr 2 do Zarządzenia;

4) przygotowywanie projektów zarządzeń, instrukcji i wytycznych Administratora;

5) opiniowanie umów dotyczących udostępniania lub powierzenia przetwarzania danych podmiotom zewnętrznym lub osobom, które nie są pracownikami Urzędu;

6) organizowanie szkolenia w zakresie ochrony danych osobowych dla osób, o których mowa w § 15 ust. 3.

**§ 16.** 1. Administrator realizuje czynności techniczne związane z zapewnieniem skutecznej ochrony danym osobowym przetwarzanym w Urzędzie.

2. Do Administratora należy:

1) wydawanie (wycofywanie) lub zmiana upoważnień do przetwarzania danych osobowych, zgodnie z art. 37 Ustawy;

2) prowadzenie ewidencji i wykazów, o których mowa w § 13;

3) zgłaszanie lub aktualizowanie zbiorów danych osobowych do rejestracji w GIODO zgodnie z art. 40 i art. 41 Ustawy;

4) decydowanie o przekazywaniu danych osobowych do państwa trzeciego, zgodnie z art. 47 Ustawy;

5) koordynowanie i nadzorowanie wykonywania zadań w Urzędzie w zakresie zgodności z prawem, celowości, poprawności i adekwatności przetwarzania danych osobowych, zgodnie z art. 26 Ustawy;

6) nadzorowanie i kontrolowanie wykonywania w Urzędzie zadań określonych w dokumentacji przetwarzania i ochrony danych osobowych poprzez inspirowanie działań ABI;

7) prowadzenie korespondencji z GIODO w imieniu Administratora

8) zapewnienie technicznego zabezpieczenia i wyposażenia pomieszczeń i obiektów, które tworzą obszary przetwarzania danych ze szczególnym uwzględnieniem zadań określonych w § 20 ust. 2 lit. c) – e) „Polityki bezpieczeństwa" stanowiącej załącznik nr 1 do Zarządzenia.

3. Czynności, o których mowa w ust. 2, wykonuje się na wniosek ABI lub właściwego Kierownika komórki organizacyjnej Urzędu.

**§ 17.** 1. ASI realizuje czynności techniczne związane z zapewnieniem bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych.

2. Do zadań ASI w szczególności należy:

1) dostosowywanie systemów do wymogów prawa, o których mowa w § 22 ust 2;

2) w porozumieniu z ABI, planowanie i wdrażanie rozwiązań systemowych i technicznych elementów bezpieczeństwa danych przetwarzanych w systemach;

3) zapewnienie sprzętu i oprogramowania systemów, odpowiadających normom przewidzianym dla poziomów bezpieczeństwa przetwarzania danych w systemach;

4) nadzorowanie technicznego zabezpieczania i odpowiedniego wyposażenia pomieszczeń, w których znajdują się serwery.

3. 5) administrowanie systemami, w których przetwarzane są dane osobowe;

6) przyznawanie użytkownikom identyfikatorów i przyznawanie im uprawnień, które wynikają z nadanego upoważnienia do przetwarzania danych osobowych;

7) instalowanie, aktualizowanie i konfigurowanie oprogramowania systemowego i aplikacyjnego oraz urządzeń, o ile czynności te nie są wykonywane przez upoważnionych przedstawicieli dostawcy systemu na podstawie zawartej umowy;

8) instalowanie i aktualizowanie oprogramowania antywirusowego;

9) reagowanie w przypadku naruszenia bądź powstania zagrożenia bezpieczeństwa danych przetwarzanych w systemie;

10) tworzenie, rejestrowanie, przechowywanie i archiwizowanie kopii zapasowych baz danych osobowych;

11) przygotowywanie urządzeń, dysków i innych elektronicznych nośników informacji, zawierających dane osobowe, do likwidacji, przekazania innemu podmiotowi, konserwacji lub naprawy;

12) przekazywania do ABI opisów struktur zbiorów danych, schematów przepływu danych pomiędzy systemami, zawartości poszczególnych pól informacyjnych w aplikacjach oraz wszelkich zmian w tym zakresie;

13) zakładanie, modyfikacja lub usuwanie baz danych w systemie oraz realizowanie migracji danych pomiędzy nimi;

14) natychmiastowe informowanie ABI o zdarzeniach, o których mowa w pkt 9;

15) wykonywanie bieżącej konserwacji i przeglądu systemu;

16) uaktualnianie kont i uprawnień użytkowników systemu w porozumieniu z ABI.

**§ 18.** 1. Kierownicy referatów są odpowiedzialni za przestrzeganie przepisów dotyczących przetwarzania i ochrony danych osobowych w podległych im komórkach organizacyjnych w zakresie upoważnień nadanych przez Administratora.

2. Do zadań osób, o których mowa w ust. 1, należy:

1) decydowanie o udostępnianiu danych osobowych, zgodnie z art. 29 Ustawy;

2) wnioskowanie o rejestrację (aktualizację) zbiorów w GIODO - wypełnianie wniosków zgłoszenia;

3) przedkładanie ABI wniosków o nadanie (wycofanie) lub zmianę upoważnień do przetwarzania danych osobowych dla pracowników i innych osób;

4) zachowanie szczególnej staranności przy przetwarzaniu danych osobowych, zgodnie art. 26 Ustawy oraz zapewnienie kontroli wprowadzania i przekazywania danych, zgodnie z art. 38 Ustawy;

5) zabezpieczanie danych osobowych zgodnie z przepisami zawartymi w dokumentacji przetwarzania i ochrony danych osobowych;

6) udzielanie informacji, o której mowa w art. 24, art. 25 oraz art. 32 ust. 1 pkt. 1–5 a Ustawy oraz uzupełnianie, uaktualnianie lub prostowanie danych osobowych w przypadkach, o których mowa w art. 32 ust. 1 pkt 6 Ustawy;

7) zawieranie umów dotyczących udostępniania lub powierzenia przetwarzania danych osobom i podmiotom zewnętrznym, zgodnie z art. 31 Ustawy;

8) wskazywanie osoby wykonującej w komórce organizacyjnej czynności administracyjne związane z przetwarzaniem i ochroną danych osobowych;

9) przekazywanie ABI wykazu zbiorów danych i programów zastosowanych do ich przetwarzania oraz lokalizacji obszarów ich przetwarzania;

10) w porozumieniu z ABI rozpatrywanie skarg i wniosków dotyczących przetwarzania i ochrony danych osobowych;

11) na żądanie Administratora lub osoby przez niego upoważnionej przeprowadzenie okresowych analiz ryzyka dla poszczególnych systemów i na tej podstawie przedstawianie Administratorowi propozycji w zakresie stosowania środków technicznych i przedsięwzięć organizacyjnych w celu zapewnienia skutecznej ochrony przetwarzania danych.

3. Osoby, o których mowa w ust. 1, realizując zadania w imieniu Administratora współpracują z ABI, ASI oraz innymi osobami upoważnionymi przez Administratora.

**§ 19.** Kierownik Kadr zobowiązany jest do przekazywania ABI informacji dotyczących osób biorących udział w procesie przetwarzania i ochrony danych osobowych w Urzędzie. Informacje te zawierać powinny:

1) zmiany w nawiązaniu i rozwiązaniu stosunku pracy;

2) zmiany miejsc świadczenia pracy;

3) oddelegowanie lub przeniesienie pracownika do innej jednostki organizacyjnej;

4) przebywania na urlopie macierzyńskim lub urlopie bezpłatnym powyżej miesiąca;

5) przebywanie na zwolnieniu lekarskim powyżej miesiąca;

**§ 20.** 1. Osoby upoważnione przez Administratora do podpisywania umów z osobami lub podmiotami, o których mowa w § 1 ust. 2 „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych" stanowiącej załącznik nr 2 do Zarządzenia, zobowiązane są do umieszczania postanowień umownych, gwarantujących bezpieczeństwo i ochronę danych osobowych przetwarzanych w Urzędzie.

2. Postanowienia, o których mowa w ust. 1, dotyczą udostępniania lub powierzenia danych do przetwarzania i zawierają:

1) określenie przedmiotu i celu umowy;

2) zobowiązanie zleceniobiorcy do zapewnienia bezpieczeństwa i właściwej ochrony przetwarzanych danych osobowych;

3) zobowiązanie zleceniobiorcy do przestrzegania procedur, o których mowa w § 6;

4) oświadczenie zleceniobiorcy dotyczące dostosowania systemów informatycznych wykorzystywanych w procesie przetwarzania danych osobowych do wymogów rozporządzenia, o którym mowa w § 22 ust. 2;

5) zapewnienie zleceniodawcy nadzoru i kontroli nad przetwarzaniem i ochroną danych osobowych;

6) określenie kar umownych za nieprzestrzeganie zapisów umownych;

7) możliwość rozwiązania umowy w trybie natychmiastowym w przypadku stwierdzenia omijania przez zleceniobiorcę przepisów dotyczących bezpieczeństwa i ochrony przetwarzanych danych osobowych.

## Rozdział 6.
## Postanowienia końcowe.

**§ 21.** W sprawach nie uregulowanych niniejszym Regulaminem zastosowanie znajdują:

1) Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. Nr 101, poz. 926 z późn. zm.);

2) Rozporządzenie 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) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie wzoru zgłoszenia zbioru danych osobowych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz.U. Nr 100, poz. 1025).

4) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 22 kwietnia 2004 r. w sprawie imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz.U. Nr 94, poz. 923).