ZARZĄDZENIE NR 60/2015
WÓJTA GMINY JEDWABNO
z dnia 30 czerwca 2015

w sprawie wprowadzenia „Polityki Bezpieczeństwa Przetwarzania Danych Osobowych w Urzędzie Gminy Jedwabno".

Na podstawie art. 36 ust. 1, 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2014 r. poz. 1182) oraz § 3, 4 i 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) zarządza się, co następuje:

§ 1

Wprowadza się „Politykę Bezpieczeństwa Przetwarzania Danych Osobowych w Urzędzie Gminy Jedwabno" stanowiącą załącznik Nr 1 do niniejszego zarządzenia.

§ 2

Zobowiązuje się wszystkie osoby przetwarzające dane osobowe w Urzędzie Gminy Jedwabno do przestrzegania zasad i realizacji zadań określonych w załączniku, o których mowa w § 1.

§ 3

Zarządzenie wchodzi w życie z dniem podpisania.

§ 4

Traci moc zarządzenie Nr 81/2011 Wójta Gminy Jedwabno z dnia 31 sierpnia 2011 roku w sprawie ustalenia polityki bezpieczeństwa danych osobowych w Urzędzie Gminy w Jedwabnie

WÓJT

SŁAWOMIR AMBROZIAK

Załącznik do zarządzenia Nr 60/2015
Wójta Gminy Jedwabno
z dnia 30.06.2015 r.

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH W Urzędzie Gminy Jedwabno

(Jedwabno, 2015)

I. Wstęp

§ 1

Celem Polityki Bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Jedwabno, zwanej dalej Polityką Bezpieczeństwa, jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych, sposobu przetwarzania w Urzędzie Gminy Jedwabno informacji zawierających dane osobowe, a przede wszystkim zapewnienie ochrony danych osobowych przetwarzanych w Urzędzie Gminy Jedwabno przed wszelkiego rodzaju zagrożeniami, tak zewnętrznymi jak i wewnętrznymi.

§ 2

Polityka Bezpieczeństwa została utworzona w związku z wymaganiami zawartymi w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych oraz rozporządzeniu 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. Opracowany dokument jest zgodny również z dyrektywą 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. w sprawie przetwarzania danych osób oraz ochrony prywatności w sektorze komunikacji elektronicznej.

§ 3

Obszarem przetwarzania danych osobowych w Urzędzie Gminy Jedwabno są pomieszczenia biurowe w budynku, przy ul. Warmińska 2, 12-122 Jedwabno.

§ 4

Ochrona danych osobowych realizowana jest poprzez zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz użytkowników.

§ 5

1. Utrzymanie bezpieczeństwa przetwarzanych danych osobowych w Urzędzie Gminy Jedwabno rozumiane jest jako zapewnienie ich poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z ochroną danych osobowych.
2. Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:
   1) poufność danych - rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom;
   2) integralność danych - rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
   3) rozliczalność danych - rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie;
   4) integralność systemu - rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej;
   5) dostępność informacji - rozumianą jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne;
   6) zarządzanie ryzykiem - rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych służących do przetwarzania danych osobowych.

§ 6

Administratorem Danych Osobowych przetwarzanych w Urzędzie Gminy Jedwabno jest Wójt Gminy Jedwabno.

§ 7

Na Administratora Bezpieczeństwa Informacji w Urzędzie Gminy Jedwabno mianowany jest Karol Biernacki.

II. Definicje

§ 8

Przez użyte w Polityce Bezpieczeństwa określenia należy rozumieć:

1) **Polityka Bezpieczeństwa** - rozumie się przez to Politykę Bezpieczeństwa Ochrony Danych Osobowych w Urzędzie Gminy Jedwabno;

2) **Administrator Danych Osobowych** - dalej jako Administrator danych; rozumie się przez to Wójt Gminy Jedwabno;

3) **Administrator Bezpieczeństwa Informacji (także ABI)** - rozumie się przez to osobę wyznaczoną przez Administratora Danych Osobowych, nadzorującą przestrzeganie zasad ochrony danych osobowych, w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;

4) **Biuro** - Biuro Urzędu Gminy Jedwabno;

5) **Ustawa** - ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2014 r. poz.1182);

6) **Rozporządzenie** - 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. z 2004 r. Nr 100, poz. 1024);

7) **Dane osobowe** - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;

8) **Zbiór danych osobowych** - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych

kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;

9) **Baza danych osobowych** - zbiór uporządkowanych powiązanych ze sobą tematycznie zapisanych np. w pamięci wewnętrznej komputera. Baza danych jest złożona z elementów o określonej strukturze - rekordów lub obiektów, w których są zapisywane dane osobowe;

10) **Usuwanie danych** - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dotyczą.

11) **Przetwarzane 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;

12) **System informatyczny** - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;

13) **System tradycyjny** - rozumie się przez to zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji i wyposażenia i środków trwałych w celu przetwarzania danych osobowych na papierze;

14) **Zabezpieczenie danych w systemie informatycznym** - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;

15) **Administrator systemu informatycznego** - rozumie się przez to osobę lub osoby, upoważnione przez administratora danych osobowych do administrowania i zarządzania systemami informatycznymi w Urzędzie Gminy Jedwabno;

16) **Użytkownik** - rozumie się przez to upoważnionego przez Administratora danych lub Administratora Bezpieczeństwa Informacji, wyznaczonego do przetwarzania

danych osobowych pracownika Urzędu Gminy Jedwabno, który został poinformowany w zakresie ochrony tych danych.

III. Zakres stosowania

§ 9

1. W Urzędzie Gminy Jedwabno przetwarzane są przede wszystkim informacje służące do obsługi interesantów oraz mieszkańców gminy.
2. Informacje te są przetwarzane i składowane zarówno w postaci dokumentacji tradycyjnej jak i elektronicznej.
3. Polityka Bezpieczeństwa zawiera dokumenty dotyczące wprowadzonych zabezpieczeń technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych.

§ 10

Politykę Bezpieczeństwa stosuje się przede wszystkim do:

1) Danych osobowych przetwarzanych w systemie: PUMA, Płatnik, PB_USC.
2) Wszystkich informacji dotyczących danych pracowników Urzędzie Gminy Jedwabno, w tym danych osobowych pracowników i treści zawieranych umów o pracę.
3) Wszystkich danych kandydatów do pracy zbieranych na etapie rekrutacji.
4) Informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych.
5) Rejestru osób dopuszczonych do przetwarzania danych osobowych.
6) Innych dokumentów zawierających dane osobowe.

§ 11

1. Zakresy ochrony danych osobowych określone przez dokumenty Polityki Bezpieczeństwa mają zastosowanie do systemów informatycznych, w których są przetwarzane dane osobowe, a w szczególności do:

   a) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są dane osobowe podlegające ochronie;

   b) wszystkich lokalizacji - budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie;

   c) wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, stażystów i innych osób mających dostęp do informacji podlegających ochronie.

2. Do stosowania zasad określonych przez dokumenty Polityki Bezpieczeństwa zobowiązani są wszyscy pracownicy w rozumieniu Kodeksu Pracy, stażyści oraz inne osoby mające dostęp do informacji podlegających ochronie.

§ 12

Informacje niejawne nie są objęte zakresem niniejszej Polityki Bezpieczeństwa.

IV. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe oraz sposobów ich zabezpieczeń

§ 13

1. Polityka obowiązuje w Urzędzie Gminy Jedwabno, w pomieszczeniach lub częściach pomieszczeń, w których przetwarzane są dane osobowe, a których wykaz został zamieszczony poniżej.

2. Urzędzie Gminy Jedwabno mieści się pod adresem: Warmińska 2, 12-122 Jedwabno

3. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe w Urzędzie Gminy Jedwabno stanowi załącznik Nr 5 do polityki bezpieczeństwa.

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

§ 14

1. Dane osobowe są gromadzone, przechowywane i przetwarzane w kartotekach, skorowidzach, księgach, wykazach oraz w innych zbiorach ewidencyjnych poszczególnych komórek organizacyjnych jednostki organizacyjnej w postaci dokumentów papierowych i w systemie informatycznym, w którym stosowane są pakiety biurowe lub wyspecjalizowane aplikacje (programy).

2. Zestawienie zbiorów danych osobowych oraz programów do przetwarzania tych danych stanowi załącznik Nr 4 do polityki bezpieczeństwa.

VI. Struktura zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych

§ 15

Struktura zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych dla programów i systemów stosowanych w Urzędzie Gminy Jedwabno stanowi załącznik Nr 7 do polityki bezpieczeństwa.

VII. Sposób przepływu danych między poszczególnymi systemami, współpracy systemów informatycznych ze zbiorami danych

Sposób przepływu danych między poszczególnymi systemami, współpracy systemów informatycznych ze zbiorami danych w Urzędzie Gminy Jedwabno stanowi załącznik Nr 8 do polityki bezpieczeństwa.

VIII. Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzania danych

§ 16

1. Zabezpieczenia organizacyjne

   a) sporządzono i wdrożono Politykę Bezpieczeństwa;

   b) sporządzono i wdrożono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Jedwabno;

   c) wyznaczono ABI;

   d) do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez Administratora danych bądź osobę przez niego upoważnioną;

   e) stworzono procedurę postępowania w sytuacji naruszenia ochrony danych osobowych;

   f) osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego;

   g) osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy;

h) przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych;

i) przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych;

j) dokumenty i nośniki informacji zawierające dane osobowe, które podlegają zniszczeniu, neutralizuje się za pomocą urządzeń do tego przeznaczonych lub dokonując takiej ich modyfikacji, która nie pozwoli na odtworzenie ich treści, aby po dokonaniu usunięcia danych niemożliwa była identyfikacja osób.

2. Zabezpieczenia techniczne

a) wewnętrzną sieć komputerową zabezpieczono poprzez odseparowanie od sieci publicznej za pomocą UTM FortiGate 60D

b) stanowiska komputerowe wyposażono w indywidualną ochronę antywirusową,

c) komputery zabezpieczono przed możliwością użytkowania przez osoby nieuprawnione do przetwarzania danych osobowych, za pomocą indywidualnego identyfikatora użytkowania i cykliczne wymuszanie zmiany hasła,

3. Środki ochrony fizycznej:

a) obszar, na którym przetwarzane są dane osobowe, poza godzinami pracy, chroniony jest alarmem,

b) urządzenia służące do przetwarzania danych osobowych umieszcza się w zamykanych pomieszczeniach.

IX. Instrukcja postępowania w przypadku zagrożeń i incydentów zagrażających bezpieczeństwu danych osobowych

§ 17

1. Instrukcja definiuje katalog zagrożeń i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Celem instrukcji jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa, ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

2. Każdy pracownik Urzędu Gminy Jedwabno w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest poinformować Administratora danych lub ABI.

3. Do typowych zagrożeń bezpieczeństwa danych osobowych należą:

   a) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,

   b) niewłaściwe zabezpieczenie sprzętu, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,

   c) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników.

4. Do typowych incydentów bezpieczeństwa danych osobowych należą:

   a) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),

   b) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/ zagubienie danych),

   c) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).

5. W przypadku stwierdzenia wystąpienia zagrożenia, Administrator danych lub ABI prowadzi postępowanie wyjaśniające w toku, którego:

   a) ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki,

   b) inicjuje ewentualne działania dyscyplinarne,

   c) rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości,

   d) dokumentuje prowadzone postępowania.

6. W przypadku stwierdzenia incydentu (naruszenia), Administrator danych lub ABI prowadzi postępowanie wyjaśniające w toku, którego:

   a) ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały,

   b) zabezpiecza ewentualne dowody,

   c) ustala osoby odpowiedzialne za naruszenie,

   d) podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody),

   e) inicjuje działania dyscyplinarne,

   f) wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości,

   g) dokumentuje prowadzone postępowania.

X. Zadania Administratora Bezpieczeństwa Informacji

§ 18

Do najważniejszych obowiązków Administratora Danych lub Administratora Bezpieczeństwa Informacji należy:

1. organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami ustawy o ochronie danych osobowych,

2. zapewnienie przetwarzania danych zgodnie z uregulowaniami Polityki,

3. wydawanie i anulowanie upoważnień do przetwarzania danych osobowych,

4. prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,

5. prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych, prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych,

6. nadzór nad bezpieczeństwem danych osobowych,

7. kontrola działań komórek organizacyjnych pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych,

8. inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych

§ 19

Administrator Bezpieczeństwa Informacji ma prawo:

1) wyznaczania, rekomendowania i egzekwowania wykonania zadań związanych z ochroną danych osobowych w Urzędzie Gminy Jedwabno;

2) wstępu do pomieszczeń w których zlokalizowane są zbiory danych i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z ustawą;

3) żądania złożenia pisemnych lub ustnych wyjaśnień w zakresie niezbędnym do ustalenia stanu faktycznego;

4) żądania okazania dokumentów i wszelkich danych mających bezpośredni związek z problematyką kontroli;

5) żądania udostępnienia do kontroli urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych.

XI. Zadania Administratora Systemu Informatycznego

§ 20

1. Administrator Systemu Informatycznego odpowiedzialny jest za:

   a) Bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych.

   b) Optymalizację wydajności systemu informatycznego, baz danych, instalacje i konfiguracje sprzętu sieciowego i serwerowego.

   c) Instalacje i konfiguracje oprogramowania systemowego, sieciowego, oprogramowania bazodanowego.

   d) Konfigurację i administrowanie oprogramowaniem systemowym, sieciowym oraz bazodanowym zabezpieczającym dane chronione przed nieupoważnionym dostępem.

   e) Nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych.

f) Współpracę z dostawcami usług oraz sprzętu sieciowego i serwerowego oraz zapewnienie zapisów dotyczących ochrony danych osobowych.

g) Zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego, sieciowego.

h) Zarządzanie kopiami awaryjnymi danych osobowych oraz zasobów umożliwiających ich przetwarzanie.

i) Przeciwdziałanie próbom naruszenia bezpieczeństwa informacji.

j) Przyznawanie na wniosek Administratora danych lub Administratora Bezpieczeństwa Informacji ściśle określonych praw dostępu do informacji w danym systemie.

k) Wnioskowanie do Administratora danych lub Administratora Bezpieczeństwa Informacji w sprawie zmian lub usprawnienia procedur bezpieczeństwa i standardów zabezpieczeń.

l) Zarządzanie licencjami, procedurami ich dotyczącymi.

m) Prowadzenie profilaktyki antywirusowej.

2. Praca Administratora Systemu Informatycznego jest nadzorowana pod względem przestrzegania ustawy o ochronie danych osobowych, 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 oraz Polityki Bezpieczeństwa przez Administratora danych lub Administratora Bezpieczeństwa Informacji.

XII. Sprawozdanie roczne stanu systemu ochrony danych osobowych

§ 21

1. Corocznie do dnia 15 marca, ABI lub wyznaczony przez Administratora danych pracownik przygotowuje sprawozdanie roczne stanu funkcjonowania systemu ochrony danych osobowych,
2. W spotkaniu sprawozdawczym uczestniczą: Administrator danych oraz ABI. Na wniosek co najmniej jednego z uczestników w spotkaniu mogą wziąć udział: informatyk, kierownicy działów/jednostek.
3. Sprawozdanie przygotowywane jest w formie pisemnej.

XIII. Szkolenia użytkowników

§ 22

1. Każdy użytkownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej winien być poinformowany w zakresie ochrony danych osobowych w zbiorach elektronicznych i papierowych.
2. Za przeprowadzenie szkolenia odpowiada Administrator danych lub ABI.
3. Zakres szkolenia powinien obejmować zaznajomienie użytkownika z przepisami ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz instrukcjami obowiązującymi u Administratora danych, a także o zobowiązaniu się do ich przestrzegania.

4. Szkolenie zostaje zakończone podpisaniem przez słuchacza oświadczenia o wzięciu udziału w szkoleniu i jego zrozumieniu oraz zobowiązaniu się do przestrzegania przedstawionych w trakcie szkolenia zasad ochrony danych osobowych.

5. Dokument ten jest przechowywany w aktach osobowych użytkowników i stanowi podstawę do podejmowania działań w celu nadania im uprawnień do korzystania z systemu informatycznego przetwarzającego dane osobowe.

XIV. Postanowienia końcowe

§ 23

1. Polityka jest dokumentem wewnętrznym i nie może być udostępniania osobom postronnym w żadnej formie.

2. Administrator danych lub Administrator Bezpieczeństwa Informacji ma obowiązek zapoznać z treścią Polityki każdego użytkownika.

3. Wszystkie regulacje dotyczące systemów informatycznych, określone w Polityce dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiejkolwiek innej formie.

4. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w Polityce.

5. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.

6. Kara dyscyplinarna orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby, zgodnie z ustawą oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

7. W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy ustawy oraz rozporządzenia.

Wójt

Sławomir Ambroziak

Załącznik Nr 1 do Polityki Bezpieczeństwa Informacji w Urzędzie Gminy Jedwabno

WZÓR

O Ś W I A D C Z E N I E

Imię i nazwisko	
Stanowisko służbowe	
Nazwa komórki organizacyjnej	

Stwierdzam własnoręcznym podpisem, że zapoznałem/am/ się z „Polityką Bezpieczeństwa Informacji w Urzędzie Gminy Jedwabno" oraz Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Jedwabno.

Jednocześnie, zgodnie z przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. , poz. 1182) zobowiązuję się do ochrony przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem, danych osobowych przetwarzanych w Urzędzie Gminy Jedwabno oraz do zachowania ich w tajemnicy w czasie trwania jak i po ustaniu zatrudnienia.

Równocześnie oświadczam, że zostałem(am) poinformowany(a) o odpowiedzialności służbowej i karnej w przypadku naruszenia przepisów.

.....	.....
(imię, nazwisko i podpis osoby przyjmującej oświadczenie)	(data i podpis składającego oświadczenie)

Załącznik Nr 2 do Polityki Bezpieczeństwa Informacji w Urzędzie Gminy Jedwabno

WZÓR

UPOWAŻNIENIE NR

Zgodnie z art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U.z 2014 r. , poz. 1182), zgodnie z zakresem czynności i złożonego oświadczenia w sprawie znajomości przepisów dotyczących ochrony danych osobowych

U p o w a ż n i a m

Pana/Panią:

.....

...
imię i nazwisko

do przetwarzania danych osobowych gromadzonych w systemie informatycznym/ nie informatycznym w Urzędzie Gminy Jedwabno w zakresie realizowanych obowiązków służbowych
Powyższe upoważnienie wydaje się na okres do
.....
(wpisać na jaki okres lub bezterminowo)

....

... ...
Administrator Danych Osobowych /miejscowość/ /data/

Załącznik Nr 3 do Polityki Bezpieczeństwa Informacji w Urzędzie Gminy Jedwabno

WZÓR

Ewidencja osób upoważnionych do przetwarzania danych osobowych /art.39/

L.p.	Imię i nazwisko	Stanowisko	Komórka organizacyjna	Nr upoważnienia imiennego	Identyfikator	Data nadania upoważnienia	Data ustania upoważnienia	Zakres upoważnienia

Załącznik Nr 4 do Polityki Bezpieczeństwa Informacji w Urzędzie Gminy Jedwabno
WZÓR

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

Nazwa zbioru	Administrator Danych Osobowych	Przedsta wiciel ADO (art. 31a uodo)	Podmiot któremu powierzono przetwarzanie danych (art. 31 uodo)	Podstawa prawna upoważniająca do prowadzenia zbioru	Cel przetwarzania danych w zbiorze	Kategorie osób, których dane są przetwarzane	Zakres danych przetwarzanych w zbiorze	Sposób zbierania danych do zbioru	Sposób udostępniania danych ze zbioru	Oznaczenie odbiorcy/kategorii odbiorców, którym dane mogą być przekazywane	Przekaz. danych do państwa trzeciego (art. 7 pkt 7)
1	2	3	4	5	6	7	8	9	10	11	12
	Gmina Jedwabno, ul. Warmińska 2, 12-122 Jedwabno, NIP 745-18-11-359										
	Gmina Jedwabno, ul. Warmińska 2, 12-122 Jedwabno, NIP 745-18-11-359										
	Gmina Jedwabno, ul. Warmińska 2, 12-122 Jedwabno, NIP 745-18-11-359										

Załącznik Nr 5 do Polityki Bezpieczeństwa Informacji w Urzędzie Gminy Jedwabno

WZÓR

WYKAZ POMIESZCZEŃ STANOWIĄCYCH OBSZAR PRZETWARZANIA DANYCH OSOBOWYCH

Budynek		
Lp.	Nazwa pomieszczenia	Miejsce ,położenie
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		

Załącznik Nr 6 do Polityki Bezpieczeństwa Informacji w Urzędzie Gminy Jedwabno

WZÓR

RAPORT

z naruszenia ochrony danych osobowych

w Urzędzie Gminy Jedwabno

1. Data: ..... Godzina: .....
(dzień, miesiąc, rok) *(00:00)*

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

.....
(Imię, nazwisko, stanowisko służbowe, nazwa użytkownika (jeśli występuje))

3. Lokalizacja zdarzenia:

.....
(np. nr pokoju, nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

.....
.....

5. Podjęte działania:

.....
.....

6. Przyczyny wystąpienia zdarzenia:

.....
.....

7. Postępowanie wyjaśniające:
.....
.....

.....
/data, podpis Administratora Bezpieczeństwa Informacji/

WZÓR

STRUKTURY ZBIORÓW

L.P.	NAZWA ZBIORU	ZAKRES DANYCH W ZBIORZE

Załącznik Nr 8 do Polityki Bezpieczeństwa Informacji w Urzędzie Gminy Jedwabno

WZÓR

SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY POSZCZEGÓLNYMI SYSTEMAMI

Lp.	Rodzaj zbioru	System informatyczny	Kierunek przepływu danych	System informatyczny	Sposób transmisji
1					Manualny/sieć/internet
2					
3					
4					
5					
6					