Załącznik nr 1 do Zarządzenia Nr 106/2015
Wójta Gminy Zaleszany z dnia 22 czerwca 2015 r.
w sprawie polityki bezpieczeństwa informacji
oraz instrukcji zarządzania systemami informatycznymi
służącymi do przetwarzania danych osobowych

# Polityka bezpieczeństwa w sprawie danych osobowych gromadzonych w zbiorach Urzędu Gminy w Zaleszanach

Opracował: Sebastian Nabrzeski

## Rozdział 1
## Zastosowane pojęcia i definicje

Ilekroć w Polityce bezpieczeństwa w sprawie ochrony danych osobowych gromadzonych w zbiorach Urzędu Gminy w Zaleszanach jest mowa o:

1) Wójcie - należy przez to rozumieć Wójta Gminy Zaleszany,
2) Urzędzie - należy przez to rozumieć Urząd Gminy w Zaleszanach,
3) Ustawie - należy przez to rozumieć ustawę z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.),
4) Rozporządzeniu – należy przez to rozumieć rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024 z późn. zm.),
5) przetwarzaniu danych – należy przez to rozumieć jakiekolwiek operacje wykonywane na danych osobowych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
6) Regulaminie organizacyjnym – należy przez to rozumieć Regulamin organizacyjny Urzędu Gminy w Zaleszanach,
7) Polityce bezpieczeństwa - należy przez to rozumieć Politykę w sprawie ochrony danych osobowych gromadzonych w zbiorach Urzędu Gminy w Zaleszanach,
8) danych osobowych – należy przez to rozumieć wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, czyli takiej, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne,
9) danych osobowych sensytywnych – należy przez to rozumieć dane wskazane w art. 27 ust. 1 Ustawy, podlegające szczególnej ochronie,
10) ADO – należy przez to rozumieć Administratora Danych Osobowych, którym jest Urząd reprezentowany przez Wójta.
11) ABI - należy przez to rozumieć Administratora Bezpieczeństwa Informacji, pracownika Urzędu, który w imieniu ADO wykonuje czynności z zakresu ochrony danych osobowych.
12) ASI – należy przez to rozumieć Administratora Systemu Informatycznego, czyli:

a. upoważnionego przez ABI do administrowania Elektronicznym Systemem Obiegu Spraw i Dokumentów lub innym systemem informatycznym, w którym przetwarzane są dane osobowe pracownika Referatu Organizacyjnego odpowiedzialnego za wdrożenie i stosowanie zasad bezpieczeństwa danych osobowych w zakresie technicznych i logicznych zabezpieczeń systemu,
b. innego pracownika Urzędu, który otrzymał stosowne upoważnienie od ABI albo od podmiotu będącego administratorem systemu (oprogramowania), albo któremu podmiot będący administratorem systemu (oprogramowania) nadał takie upoważnienie w drodze zawartej umowy.

13) LABI – należy przez to rozumieć Lokalnego Administratora Bezpieczeństwa Informacji, czyli: Sekretarza, Skarbnika, kierownika referatu oraz samodzielne stanowisko kierownicze lub urzędnicze, wyszczególnione w schemacie organizacyjnym Urzędu stanowiącym załącznik do Regulaminu organizacyjnego, posiadającego powierzenie obowiązków udzielone przez ABI,
14) Kierowniku Referatu - należy przez to rozumieć Kierownika Referatu lub kierownika równorzędnej komórki organizacyjnej funkcjonującej w Urzędzie,
15) Referacie - należy przez to rozumieć Referat, inną równorzędną komórkę organizacyjną funkcjonującą w Urzędzie oraz samodzielne stanowisko wyszczególnione w schemacie organizacyjnym Urzędu, stanowiącym załącznik do Regulaminu organizacyjnego,
16) Osobie nieupoważnionej – należy przez to rozumieć osobę fizyczną lub prawną nieposiadającą aktualnego upoważnienia do przetwarzania danych osobowych, nadanego w trybie art. 37 Ustawy,
17) Użytkowniku – należy przez to rozumieć osobę posiadającą aktualne upoważnienie do przetwarzania danych osobowych w Urzędzie,
18) Użytkowniku systemu – należy przez to rozumieć osobę posiadającą aktualne upoważnienie do przetwarzania danych w systemie informatycznym w Urzędzie,
19) Pracowniku – należy przez to rozumieć pracownika Urzędu, bez względu na sposób nawiązania stosunku pracy,
20) Stażyście, wolontariuszu, praktykancie – należy przez to rozumieć stażystę, wolontariusza oraz osobę odbywającą praktykę uczniowską lub studencką w Urzędzie,
21) Radnym – należy przez to rozumieć radnego Rady Gminy w Zaleszanach,
22) identyfikatorze – należy przez to rozumieć ciąg znaków literowych, cyfrowych i innych specjalnych, jednoznacznie identyfikujących Użytkownika systemu,
23) GIODO – należy przez to rozumieć Generalnego Inspektora Ochrony Danych Osobowych,

24) Zasadzie czystego biurka – należy przez to rozumieć metodę podnoszącą poziom bezpieczeństwa, zapobiegającą ujawnieniu lub kradzieży informacji, polegającą na sprzątaniu ze stanowiska pracy, po jej zakończeniu, wszelkich dokumentów i nośników danych oraz zamknięciu ich na klucz w szafach, szufladach, itp.
25) Zasadzie czystego ekranu – należy przez to rozumieć metodę podnoszącą poziom bezpieczeństwa, zapobiegającą ujawnieniu lub kradzieży informacji, polegającą na wylogowaniu się z systemu przy opuszczaniu stanowiska komputerowego lub wygaszeniu ekranu w sposób, który przy ponownym jego włączeniu wymusza podanie hasła dostępu.

## Rozdział 2
## Postanowienia ogólne

1. Polityka bezpieczeństwa została opracowana w oparciu o:
   1) ustawę z dnia 29 sierpnia 1997r. 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 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).
2. Polityka bezpieczeństwa zawiera reguły dotyczące bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy w Zaleszanach, określające granice dopuszczalnego zachowania wszystkich pracowników Urzędu przetwarzających dane osobowe w:
   1) kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych,
   2) systemach informatycznych, także w przypadku przetwarzania danych poza zbiorem danych,

   oraz wskazuje konsekwencje, jakie mogą ponosić osoby przekraczające określone granice oraz procedury postępowania wprowadzone w celu zapobiegania i minimalizowania skutków zagrożeń.
3. Polityka bezpieczeństwa określa tryb postępowania w przypadku, gdy:
   1) stwierdzono naruszenie zabezpieczenia systemu informatycznego,
   2) stan urządzenia przetwarzającego dane osobowe, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji, w tym również w sieci informatycznej, mogą wskazywać na naruszenie zabezpieczeń danych,

3) stwierdzono zagrożenie ochrony danych osobowych lub naruszenie ochrony tych danych na skutek innych zdarzeń, nie mających związku z funkcjonowaniem systemu informatycznego,
4) wystąpiły inne sytuacje wskazujące na możliwości naruszenia bezpieczeństwa danych osobowych.

4. Polityka bezpieczeństwa obowiązuje wszystkich pracowników Urzędu Gminy w Zaleszanach, niezależnie od sposobu nawiązania stosunku pracy, a także inne osoby biorące udział w procesie przetwarzania danych osobowych, w szczególności stażystów, wolontariuszy oraz osoby odbywające praktykę uczniowską lub studencką.

## Rozdział 3
## Podstawowe obowiązki i uprawnienia osób biorących udział w procesie przetwarzania danych osobowych.

1. ADO w Urzędzie jest Wójt. ADO decyduje o celach i środkach przetwarzania danych osobowych w Urzędzie i posiada pełny dostęp do wszystkich danych przetwarzanych w Urzędzie.
2. ABI jest pracownik, który sprawuje merytoryczny nadzór nad przetwarzaniem danych osobowych w Urzędzie.
3. Do zadań ABI należy w szczególności:
   1) przygotowywanie, na wniosek LABI, wniosków zgłoszenia zbiorów danych osobowych do rejestracji GIODO, z wyłączeniem przypadków określonych w art. 43 ust. 1 Ustawy,
   2) prowadzenie rejestru zawierającego informacje o zbiorach danych osobowych, ich strukturze oraz programach zastosowanych do przetwarzania tych danych, zgłoszonych przez LABI,
   3) udostępnianie informacji na temat przetwarzanych w Urzędzie danych osobowych inspektorom GIODO,
   4) sprawowanie nadzoru nad przestrzeganiem przepisów o ochronie danych osobowych i przekazywanie wniosków ADO,
   5) prowadzenie nadzoru systemów informatycznych, w których przetwarzane są dane osobowe pod kątem możliwości nieuprawnionego dostępu oraz utraty danych i zgłaszanie wniosków ADO,
   6) prowadzenie nadzoru usunięcia danych osobowych z nośników informatycznych przewidzianych do kasacji lub przekazywanych innym podmiotom,
   7) przedstawianie okresowo ADO, nie rzadziej niż raz na kwartał, sprawozdań z zabezpieczenia danych osobowych przetwarzanych w Urzędzie,

8) podejmowanie natychmiastowych działań w celu usunięcia stwierdzonego naruszenia bezpieczeństwa danych osobowych,
9) udzielanie Użytkownikom upoważnień do przetwarzania danych osobowych, na wniosek LABI, oraz prowadzenie ewidencji upoważnień,
10) prowadzenie nadzoru nad udostępnianiem danych osobowych odbiorcom danych i innym podmiotom,
11) opracowywanie projektów Polityki bezpieczeństwa oraz Instrukcji zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych i ich aktualizacja,
12) nadzór nad przestrzeganiem Polityki bezpieczeństwa w Urzędzie oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
13) opracowywanie projektów wewnętrznych aktów prawnych w zakresie działania ABI,
14) opiniowanie Szczegółowej polityki bezpieczeństwa danych osobowych przygotowanej przez LABI,
15) prowadzenie ewidencji miejsc przetwarzania danych osobowych, zgłoszonych przez LABI,
16) zgłaszanie potrzeb szkoleniowych z zakresu przetwarzania i ochrony danych osobowych,
17) przeprowadzanie wstępnego przeszkolenia nowoprzyjętych Pracowników, stażystów, wolontariuszy i praktykantów w zakresie ochrony danych osobowych,

4. ABI posiada pełny dostęp do wszystkich danych osobowych przetwarzanych w Urzędzie w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych oraz w systemach informatycznych, także w przypadku przetwarzania danych poza zbiorem danych, a także pełny dostęp do pomieszczeń Urzędu, w których przetwarzane są dane osobowe. Dostęp do pomieszczeń odbywa się w obecności LABI lub osoby go zastępującej.
5. ABI podlega bezpośrednio ADO i w jego imieniu wykonuje czynności z zakresu ochrony danych osobowych. W przypadku nieobecności ABI jego zadania realizują we wskazanej kolejności: ASI w Referacie Organizacyjnym, ADO. Osoba zastępująca składa ABI relację z zaistniałych zdarzeń i działań podejmowanych w czasie pełnienia zastępstwa.
6. Z mocy niniejszego zarządzenia ABI jest upoważniony do powierzania Pracownikom, obowiązków ASI i LABI oraz udzielania Pracownikom, stażystom, wolontariuszom, praktykantom, radnym oraz innym osobom, które biorą udział w procesie przetwarzania

danych osobowych znajdujących się w zasobach Urzędu, upoważnień do przetwarzania danych osobowych.

7. ABI sprawuje nadzór merytoryczny nad ASI i LABI w zakresie przetwarzania danych osobowych.
8. ASI w Referacie Organizacyjnym posiada pełny dostęp do danych osobowych znajdujących się w systemach informatycznych, o których mowa w Rozdziale 1 pkt 12 lit. a oraz do instalacji informatycznej, systemów i urządzeń znajdujących się w Urzędzie, za pomocą których przetwarzane są dane osobowe. Posiada także pełny dostęp do wszystkich pomieszczeń Urzędu, w których ulokowany jest sprzęt informatyczny oraz okablowanie strukturalne.

   Wzór powierzenia obowiązków ASI stanowi załącznik nr 1 do Polityki bezpieczeństwa.
9. ASI nadaje Identyfikator do pracy w administrowanym przez niego systemie informatycznym.
10. LABI jest: Sekretarz, Skarbnik, kierownik referatu oraz osoba zatrudniona na samodzielnym stanowisku kierowniczym lub urzędniczym, wyszczególnionym w schemacie organizacyjnym stanowiącym załącznik do Regulaminu organizacyjnego, posiadający powierzenie obowiązków i upoważnienie do przetwarzania danych osobowych nadane przez ABI. W przypadku nieobecności LABI jego zadania realizuje osoba go zastępująca zgodnie z systemem zastępstw obowiązującym w Urzędzie.

    Wzór powierzenia obowiązków LABI stanowi załącznik nr 2 do Polityki bezpieczeństwa.
11. LABI jest odpowiedzialny za:
    1) opracowanie „Szczegółowej polityki bezpieczeństwa danych osobowych", która nie może być sprzeczna z Polityką bezpieczeństwa, o ile Polityka bezpieczeństwa jest niewystarczająca dla bezpiecznego przetwarzania danych osobowych w Referacie,
    2) wdrożenie Polityki bezpieczeństwa i Szczegółowej polityki bezpieczeństwa danych osobowych w Referacie,
    3) wnioskowanie do ABI o udzielenie upoważnień dla Pracowników oraz osób niebędących pracownikami Urzędu, biorących udział w procesie przetwarzania danych osobowych znajdujących się w zasobach Urzędu,
    4) dopuszczenie do przetwarzania danych osobowych wyłącznie tych Użytkowników, którzy posiadają upoważnienie do przetwarzania danych osobowych udzielone przez ABI,

5) nadzorowanie przygotowywania projektów umów z podmiotami zewnętrznymi w sposób opisany w Rozdziale 7 ust. 3 pkt 10,
6) wnioskowanie do ABI o zarejestrowanie zbioru danych osobowych w biurze GIODO, z wyłączeniem przypadków określonych w art. 43 ust. 1 Ustawy,
7) niezwłoczne informowanie ABI o założeniu bądź likwidacji każdego zbioru danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych,
8) niezwłoczne informowanie ABI o każdej zmianie struktury prowadzonego zbioru danych,
9) informowanie ABI o miejscach przetwarzania danych osobowych najpóźniej w dniu podjęcia pierwszej czynności związanej z przetwarzaniem danych osobowych w tych miejscach,
10) nadzorowanie właściwego zabezpieczenia danych osobowych po zakończeniu pracy przez podległych mu Pracowników, w tym przestrzegania zasady czystego biurka,
11) podejmowanie działań w sposób przewidziany w Rozdziale 11 w przypadku stwierdzenia naruszenia lub podejrzenia wystąpienia naruszenia opisanego w Rozdziale 6 Polityki bezpieczeństwa
12) analizę pracy pracowników upoważnionych do przetwarzania danych osobowych, w celu wykrycia potencjalnych zagrożeń,
13) nadzór nad prowadzeniem rejestru wniosków o udostępnienie danych osobowych oraz nad ich realizacją,
14) nadzór nad dostarczaniem dokumentów i innych nośników zawierających dane osobowe do likwidacji:
    a. dokumentów papierowych – do bezpiecznych pojemników,
    b. utrwalonych na nośnikach magnetycznych lub optycznych – poprzez gromadzenie w bezpiecznych miejscach w Referacie, a następnie umieszczanie w bezpiecznych pojemnikach zamawianych okresowo i wskazanych przez pracownika Referatu Organizacyjnego poprzez podanie tej informacji do wiadomości Pracowników.
15) spełnienie obowiązku informacyjnego wynikającego z art. 24 Ustawy, poprzez:
    a. zamieszczenie i bieżące aktualizowanie tej informacji w Biuletynie Informacji Publicznej,
    b. podanie jej na wnioskach przyjmowanych w formie papierowej oraz udostępnionych w wersji elektronicznej,
16) spełnienie obowiązku informacyjnego wynikającego z art. 25 Ustawy,
17) nadzór nad bieżącym archiwizowaniem dokumentów, zgodnie z odrębnymi przepisami obowiązującymi w tym zakresie,

18) bieżące informowanie ABI, które mogą pobierać i oddawać klucze do pomieszczeń, zgodnie z odrębnym zarządzeniem Wójta obowiązującym w tym zakresie.

12. Do przetwarzania danych osobowych LABI dopuści Użytkownika i Użytkownika systemu pod warunkiem, że przed podjęciem pierwszej czynności związanej z przetwarzaniem danych osobowych, osoba ta będzie posiadała udzielone przez ABI aktualne upoważnienie, o którym mowa w ust. 6.
13. Stażysta, wolontariusz, praktykant, radny oraz inna osoba biorąca udział w procesie przetwarzania danych osobowych, w szczególności na podstawie zawartej umowy cywilnoprawnej, przed podjęciem pierwszej czynności związanej z przetwarzaniem danych osobowych składają oświadczenie o treści zgodnej z załącznikiem nr 8 do Polityki bezpieczeństwa i odbierają upoważnienie, o którym mowa w ust. 6. Upoważnienie do przetwarzania danych osobowych przez te osoby nie obejmuje danych osobowych przetwarzanych w systemie informatycznym.
14. Pracownik lub przedstawiciel firmy zewnętrznej wykonującej zlecenie na rzecz Gminy może brać udział w procesie przetwarzania danych pod warunkiem posiadania upoważnienia, o którym mowa w ust. 6.
15. Ewidencję osób upoważnionych do przetwarzania danych osobowych w Urzędzie prowadzi ABI.

## Rozdział 4
## Procedura nadawania, zmiany lub pozbawiania upoważnień do przetwarzania danych osobowych

1. Do przetwarzania danych osobowych w Urzędzie mogą być dopuszczone wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych udzielone przez ABI, a w razie jego nieobecności przez osobę go zastępującą.
2. Procedura nadawania, zmiany lub pozbawiania upoważnień do przetwarzania danych obejmuje:
   1) sporządzenie przez ASI lub LABI wniosku o nadanie (zmianę / pozbawienie) upoważnienia do przetwarzania danych osobowych dla Pracownika lub osoby niebędącej pracownikiem Urzędu, zgodnie z załącznikiem nr 3 do Polityki bezpieczeństwa i przekazanie go do ASI,
   2) nadanie (zablokowanie) przez ASI Identyfikatora do pracy w systemie informatycznym, zgodnie z załącznikiem nr 3 do Polityki bezpieczeństwa i przekazanie go do ABI – z zastrzeżeniem przepisu Rozdziału 3 ust. 14.
   3) weryfikację prawidłowości upoważnienia pod względem formalnym przez ABI,

4) nadanie (zmianę / pozbawienie) przez ABI upoważnienia do przetwarzania danych osobowych dla Pracownika lub osoby niebędącej Pracownikiem Urzędu, zgodnie z załącznikami nr 4 - 6 do Polityki bezpieczeństwa,
5) złożenie przez Pracownika lub osobę niebędącą Pracownikiem Urzędu oświadczenia, zgodnie z załącznikami nr 7 i nr 8 do Polityki bezpieczeństwa.
6) odebranie przez Użytkownika dokumentu upoważnienia (pozbawienia upoważnienia) do przetwarzania danych osobowych oraz przekazanie przez ABI informacji o tym fakcie osobom wskazanym w rozdzielniku dokumentu.

3. Upoważnienie wygasa w przypadku:
   1) upływu terminu, na jaki zostało wydane,
   2) przejścia Pracownika do innego Referatu
   3) zmiany nazwy Referatu,
   4) zmiany imienia lub nazwiska Użytkownika,
   5) rozwiązania stosunku pracy,
   6) zakończenia wykonywania stażu, praktyki lub wolontariatu,
   7) zaprzestania wykonywania mandatu radnego,
   8) wygaśnięcia lub rozwiązania umowy cywilnoprawnej zawartej z osobą fizyczną.
4. ABI pozbawia Użytkownika lub Użytkownika systemu udzielonego upoważnienia:
   1) na żądanie ADO,
   2) na uzasadniony wniosek ASI i LABI,
   3) z własnej inicjatywy z chwilą powzięcia informacji o wystąpieniu realnego zagrożenia danych osobowych przetwarzanych przez Użytkownika lub Użytkownika systemu.
5. W przypadku planowanej zmiany zakresu upoważnienia do przetwarzania danych, należy złożyć ponowny wniosek o udzielenie (zmianę, pozbawienie) upoważnienia i uzyskać upoważnienie przed podjęciem pierwszej czynności dotyczącej przetwarzania danych we wnioskowanym zakresie.

## Rozdział 5
## Zasady przetwarzania danych osobowych

1. Przetwarzanie danych osobowych w Urzędzie odbywa się:
   1) metodą klasyczną (papierową), w rozumieniu art. 2 ust. 2 pkt 1 Ustawy,
   2) w systemach informatycznych, w rozumieniu art. 2 ust. 2 pkt 2 Ustawy,
   3) w zbiorach i poza zbiorami danych.
2. Dane osobowe przetwarza się przy zachowaniu szczególnej staranności, w ochronie interesów osób, których dane dotyczą oraz przy przestrzeganiu zasad:

1) legalności – przetwarzania danych zgodnie z przepisami prawa,
2) celowości – przetwarzania danych dla zrealizowania zgodnych z prawem celów,
3) merytorycznej poprawności – przetwarzania danych prawdziwych, kompletnych i aktualnych,
4) adekwatności – przetwarzania wyłącznie tych danych, które są niezbędne do zrealizowania celu,
5) ograniczenia czasowego – przechowywania danych nie dłużej, niż to jest konieczne do osiągnięcia celu.

3. Osobie, której dane są przetwarzane w Urzędzie, przysługuje prawo kontroli tych danych w zakresie, o którym mowa w art. 32 ust. 1 Ustawy.
4. Na wniosek osoby, o której mowa w ust. 3 LABI jest obowiązany w terminie 30 dni udzielić informacji dotyczących jej danych osobowych, w szczególności informacji:
   1) czy istnieje zbiór, w którym przetwarzane są jej dane osobowe, kto jest ADO, jaki jest adres i siedziba ADO,
   2) o celu, zakresie, sposobie przetwarzania danych,
   3) od kiedy przetwarza się dane osobowe wnioskodawcy w zbiorze,
   4) o źródle, z którego dane pochodzą, chyba, że zobowiązany jest do zachowania w tym zakresie w tajemnicy informacji niejawnych lub tajemnicy zawodowej,
   5) o sposobie udostępniania danych, a zwłaszcza o odbiorcach lub kategoriach odbiorców, którym dane są udostępniane.
5. W przypadku przesyłania, udostępniania lub przekazywania dokumentów zawierających dane osobowe do podmiotów (osób) zewnętrznych, dostarczanie przesyłek do wskazanych adresatów może odbywać się z wykorzystaniem:
   1) listu poleconego,
   2) posłańca, gońca, kuriera lub wskazanej osoby posiadającej odpowiednie upoważnienie
      do przetwarzania danych osobowych,
   3) innego sposobu określonego wymogiem prawa lub zawartą umową, gwarantującego bezpieczeństwo danych osobowych.
6. Realizacja zadań służbowych z wykorzystaniem danych osobowych odbywa się z zastosowaniem środków bezpieczeństwa, w szczególności:
   1) nie pozostawia się dokumentów ani ich kopii zawierających dane osobowe w miejscach niezabezpieczonych, dostępnych dla Osób nieupoważnionych, w szczególności w pobliżu urządzeń drukujących, kopiujących, w koszach na śmieci itp.,
   2) zobowiązuje się Pracowników, stażystów, wolontariuszy i praktykantów do zachowania szczególnej ostrożności w trakcie prowadzenia rozmów

telefonicznych, w celu uniknięcia niekontrolowanego udostępnienia danych osobowych Osobom nieupoważnionym,

3) dokumenty lub wydruki zawierające dane osobowe, nośniki magnetyczne, optyczne, taśmy zbędne w realizacji zadań umieszcza się w bezpiecznych pojemnikach,
4) danych osobowych nie przetwarza się za pomocą poczty elektronicznej,
5) pobierania kluczy do pomieszczeń służbowych następuje po odnotowaniu tego faktu w zeszycie w sekretariacie,
6) po zakończeniu pracy na swoim stanowisku pracy stosuje się zasadę czystego biurka,
7) stanowisko komputerowe powinno być tak usytuowane, aby Osoba nieupoważniona nie miała wglądu w treść przetwarzanych na nim danych osobowych.
8) w czasie pracy przy komputerze stosuje się zasadę czystego ekranu – każde stanowisko komputerowe musi mieć ustawiona opcję wygaszacza ekranu, która zostaje uruchomiona po upływie co najwyżej 10 minut, a dla komputerów zlokalizowanych w sekretariacie po upływie co najwyżej 3 minut, z obowiązkowym użyciem hasła dostępu przy wznowieniu pracy komputera,
9) po zakończeniu pracy szafy, w których przechowywane są dane osobowe zamyka się na klucz, który przechowuje się w sposób bezpieczny, ustalony w Referacie przez LABI,
10) pomieszczenia służbowe, w których przetwarzane są dane osobowe zamyka się na klucz, który zostaje oddany do sekretariatu
11) archiwizowanie dokumentów odbywa się zgodnie z przepisami prawa obowiązującymi w tym zakresie,
12) nie wynosi się poza obszar przetwarzania danych komputerów, ani nośników, na których zapisane są dane osobowe, z zastrzeżeniem przepisów Rozdziału 9 ust. 1 i Rozdziału 7 ust. 3 pkt 9.

## Rozdział 6
## Opis zdarzeń naruszających ochronę danych osobowych

1. Podział zagrożeń:

   1) zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu) – ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu - ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych.

   2) zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki Administratora, Użytkowników, awarie sprzętowe, błędy oprogramowania, pogorszenie jakości

sprzętu i oprogramowania) - może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych.

3) zagrożenia zamierzone, czyli świadome i celowe działania powodujące naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te dzielimy na:

a. nieuprawniony dostęp do danych pochodzący z zewnątrz, np. włamanie do systemu informatycznego lub pomieszczeń, w których przetwarzane są dane osobowe,
b. nieuprawniony dostęp do danych z jego wnętrza (np. zamierzony i nieuprawniony dostęp do danych przez Użytkownika w celu pozyskania danych),
c. nieuprawnione przekazanie danych,
d. bezpośrednie zagrożenie elementów materialnych, np. kradzież lub zgubienie sprzętu, nośników lub dokumentów.

2. Naruszenie lub podejrzenie naruszenia integralności systemu informatycznego lub poufności danych w systemie informatycznym, w którym przetwarzane są dane osobowe następuje w sytuacji:

1) losowego lub nieprzewidzianego oddziaływania czynników zewnętrznych na zasoby systemu, np. wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, itp.,
2) niewłaściwych parametrów środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,
3) awarii sprzętu lub oprogramowania, które mogą wskazywać na umyślne działanie w kierunku naruszenia ochrony danych,
4) podejrzenia nieuprawnionej modyfikacji danych w systemie lub innego odstępstwa od stanu oczekiwanego,
5) naruszenia lub próby naruszenia integralności systemu lub bazy danych w tym systemie,
6) pracy w systemie wykazującej odstępstwa uzasadniające podejrzenie przełamania lub zaniechania ochrony danych osobowych, np. praca osoby, która nie jest formalnie dopuszczona do obsługi systemu,
7) ujawnienia nieautoryzowanych kont dostępu do systemu,
8) naruszenia dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji, np. niewylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, itp.
9) wystąpienia innych, niewymienionych wyżej sytuacji, wskazujących na możliwość naruszenia bezpieczeństwa danych osobowych.

3. Za naruszenie lub próbę naruszenia bezpieczeństwa i ochrony danych osobowych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia fizycznego miejsc przechowywania i przetwarzania danych osobowych, w szczególności.
   1) niezabezpieczone pomieszczenia,
   2) nienadzorowane, otwarte szafy, biurka, regały,
   3) pozostawianie dokumentów zawierających dane osobowe w nieodpowiednich miejscach, np. w koszach na śmieci, korytarzach, okolicach kserokopiarki itp.
4. Za naruszenie lub próbę naruszenia bezpieczeństwa i ochrony danych osobowych uznaje się także brak należytej organizacji w zakresie przetwarzania danych osobowych, w szczególności:
   1) przetwarzanie danych bez aktualnego upoważnienia,
   2) niedopełnienie obowiązku zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia,
   3) przetwarzanie danych osobowych niezgodnie z zasadami opisanymi w Rozdziale 5 ust. 2.
   4) spowodowanie incydentu naruszającego prawa osób, których dane osobowe są przetwarzane,
   5) przetwarzanie danych osobowych sensytywnych, gdy ich przetwarzanie nie jest dopuszczalne.

## Rozdział 7
## Środki techniczne i organizacyjne niezbędne dla zapewnienia ochrony danych osobowych

1. ADO jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych, w szczególności:
   4) zabezpiecza dane przed ich udostępnieniem osobom nieupoważnionym,
   5) zabezpiecza dane przed ich zabraniem przez osobę nieuprawnioną,
   6) zapobiega zmianie, utracie, uszkodzeniu lub zniszczeniu danych,
   7) zapewnia przetwarzanie danych zgodnie z obowiązującymi przepisami Ustawy.
2. W imieniu ADO zadania określone w ust. 1 wykonuje ABI.
3. Użytkownicy mają obowiązek realizować techniczną ochronę danych osobowych:
   1) Przetwarzanie danych osobowych odbywa się wyłącznie:
      a. w pomieszczeniach lub częściach pomieszczeń położonych w budynkach będących siedzibami Urzędu,
      b. w innych miejscach, jeżeli Statut, Regulamin organizacyjny, zakres obowiązków służbowych, uprawnień i odpowiedzialności pracownika, a także

posiadanie pełnomocnictwo lub pełnione zastępstwo wskazują na taką konieczność,

c. dopuszcza się zdalne logowanie do systemu i przetwarzanie danych przez ADO i ASI z dowolnego miejsca na terenie Rzeczpospolitej Polskiej,

d. w szczególnie uzasadnionych przypadkach dopuszcza się możliwość zdalnego logowania do systemu i przetwarzanie danych, przez innego pracownika, niż wskazany w lit. c za każdorazową zgodą ABI udzieloną na umotywowany wniosek LABI, wyłącznie na czas określony niezbędny do zrealizowania danego zadania, o ile technicznie jest to możliwe i nie zagraża bezpieczeństwu danych.

2) Należy zabezpieczać pomieszczenia, o których mowa w pkt 1 lit. a przed nieuprawnionym dostępem - sposób pobierania i oddawania kluczy do pomieszczeń znajdujących się w siedzibach Urzędu określa odrębne zarządzenie Wójta.

3) Dostęp do pomieszczeń serwerowni jest ograniczony:

a. prawo wstępu do serwerowni znajdującej się w głównym budynku Urzędu posiadają: ADO, ABI, ASI i LABI w Referacie Organizacyjnym, a w przypadku ich nieobecności, osoby je zastępujące.

b. do serwerowni posiadają wstęp pracownicy Urzędu przeprowadzający inwentaryzację (spis z natury) tylko na czas niezbędny do jej przeprowadzenia oraz pod trwającym cały czas nadzorem ASI lub osoby go zastępującej,

c. do serwerowni posiadają wstęp osoby z podmiotów zewnętrznych realizujących usługi zlecone przez Urząd, wyłącznie pod stałym nadzorem właściwego pracownika Referatu Organizacyjnego lub osoby go zastępującej,

4) Wyposażenie pomieszczeń musi dawać gwarancję bezpieczeństwa dokumentacji zawierającej dane osobowe. Dokumenty zawierające dane osobowe po godzinach pracy muszą znajdować się w szafach zamkniętych na klucz w zamkniętych pomieszczeniach. Osoba posiadająca klucze do szafy jest zobowiązana do ich właściwego zabezpieczenia.

5) Dokumenty zawierające dane osobowe, zbędne w realizacji zadań, należy umieścić w bezpiecznych pojemnikach. Niszczeniu podlegają zarówno dokumenty papierowe, jak również utrwalone na nośnikach magnetycznych i optycznych, w szczególności dyski magnetyczne i optyczne, karty pamięci, taśmy barwiące do faksu, pamięci USB.

6) W przypadku utylizacji lub przekazania sprzętu komputerowego innej jednostce, dysk twardy zostaje wymontowany przez pracowników Referatu Organizacyjnego i pozostaje w Referacie Organizacyjnym. Jeżeli dysk można wykorzystać

do dalszej pracy w Urzędzie, zostaje on sformatowany i przekazany na stanowisko pracy. W przeciwnym wypadku zostaje w sposób mechaniczny trwale zniszczony.

7) Zabrania się Użytkownikom przetwarzania danych osobowych na urządzeniach informatycznych w sposób, który mógłby doprowadzić do ich ujawnienia osobom nieuprawnionym. W razie powzięcia wątpliwości co do bezpiecznego przetwarzania danych osobowych za pomocą tych urządzeń, pracownik ma obowiązek zwrócić się z zapytaniem do właściwych służb, tj. informatyka zatrudnionego w Referacie Organizacyjnym.
8) Zabrania się przetwarzania danych osobowych przy pomocy poczty elektronicznej.
9) Zabrania się Użytkownikom wynoszenia dokumentów, nośników informatycznych oraz sprzętu komputerowego, na których znajdują się dane osobowe poza obszar, w którym przetwarzane są dane osobowe, z uwzględnieniem przepisu Rozdziału 9 ust. 1. Nie uznaje się za naruszenie niniejszego przepisu przenoszenia dokumentów, nośników informatycznych oraz sprzętu komputerowego pomiędzy obszarami, w których przetwarzane są dane osobowe, w godzinach pracy Użytkownika. W takim przypadku Użytkownik ma obowiązek zachować szczególny nadzór nad danymi osobowymi i wykazać szczególną ostrożność.
10) Użytkownicy, którzy przygotowują projekty umów i porozumień oraz posiadają upoważnienia do podpisywania z podmiotami zewnętrznymi umów, w myśl których podmiotom tym zostają powierzone dane osobowe, zobowiązani są do umieszczania postanowień umownych gwarantujących ADO zapewnienie bezpieczeństwa i ochrony danych przetwarzanych w wyniku podpisania tych umów. W przypadku, gdy autorem umowy jest podmiot zewnętrzny, należy do umowy dołączyć dokument zawierający postanowienia gwarantujące ADO zapewnienie bezpieczeństwa i ochrony danych przetwarzanych w wyniku podpisania tych umów.
11) W przypadku pojawienia się na ekranie komputera komunikatu alarmowego należy zaprzestać pracy na komputerze i poinformować o tym fakcie informatyka.

4. Organizacyjną ochronę danych i ich przetwarzania realizuje się poprzez:
   1) wyznaczenie ABI, ASI i LABI,
   2) udzielanie i cofanie upoważnień do przetwarzania danych osobowych oraz odbieranie od Pracowników oświadczeń zgodnie z procedurą opisaną w Rozdziale 4,

3) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,
4) prowadzenie dokumentacji, o której mowa w §4 Rozporządzenia,
5) wstępne zapoznanie przez ABI każdego nowoprzyjętego Pracownika z przepisami dotyczącymi ochrony danych osobowych przed dopuszczeniem go do pracy przy ich przetwarzaniu. Fakt wstępnego zapoznania pracownika w tym zakresie stwierdza ABI własnoręcznym podpisem złożonym na karcie obiegowej,
6) szkolenie pracowników w zakresie ochrony danych osobowych w miarę posiadanych środków finansowych,
7) wstępne zapoznanie przez ASI w Referacie Organizacyjnym każdego nowoprzyjętego Pracownika w zakresie bezpiecznej obsługi urządzeń i programów informatycznych, w tym antywirusowych, związanych z przetwarzaniem i ochroną danych osobowych. Fakt wstępnego zapoznania pracownika w tym zakresie stwierdza ASI własnoręcznym podpisem złożonym na karcie obiegowej,
8) wstępne zapoznanie przez LABI każdego nowoprzyjętego Pracownika w zakresie zabezpieczenia pomieszczeń, w których przetwarzane są dane osobowe w Referacie, oraz w zakresie Szczegółowej polityki bezpieczeństwa danych osobowych obowiązującej w Referacie. Fakt wstępnego zapoznania pracownika w tym zakresie stwierdza LABI własnoręcznym podpisem złożonym na karcie obiegowej,
9) dokonywanie kontroli i czynności operacyjnych, o których mowa w Rozdziale 10. Polityki bezpieczeństwa.

## Rozdział 8
## Wykaz zbiorów i programów stosowanych do przetwarzania danych osobowych

1. W Urzędzie tworzy się zbiory danych osobowych, które są przetwarzane w aplikacjach dostosowanych do merytorycznych potrzeb Referatów.
2. Dane osobowe można przetwarzać od momentu zgłoszenia zbioru danych do GIODO, z zastrzeżeniem art. 43 Ustawy. Dane osobowe sensytywne można przetwarzać w zbiorze dopiero po zarejestrowaniu zbioru przez GIODO.

3. Wniosek do ABI o zgłoszenie zbioru danych osobowych do rejestracji GIODO składa LABI.
4. O każdorazowym założeniu w Referacie nowego zbioru danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, o każdorazowej zmianie w opisie struktury zbiorów danych, o powiązaniach między nimi oraz o zmianie sposobu przepływu danych między poszczególnymi systemami LABI niezwłocznie informuje ABI.
5. Ewidencję zbiorów danych osobowych oraz programów zastosowanych do przetwarzania tych danych prowadzi ABI.

## Rozdział 9
## Obszar przetwarzania danych osobowych

1. Za obszar przetwarzania danych uznaje się budynek, pomieszczenie lub część pomieszczenia, w których wykonywana jest jakakolwiek operacja na danych osobowych, w szczególności zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, usuwanie, a zwłaszcza ta, którą wykonuje się w systemach informatycznych. Obszarem przetwarzania danych osobowych są w szczególności pomieszczenia biurowe, serwerownie, archiwa, miejsca, w których zlokalizowane są urządzenia kopiujące oraz składowane są zużyte nośniki zawierające dane osobowe. W przypadku, gdy dane osobowe przetwarzane są w systemie informatycznym, do którego dostęp za pośrednictwem sieci telekomunikacyjnej posiada także inny podmiot, za obszar przetwarzania danych uznaje się dane tego podmiotu (nazwa i adres siedziby podmiotu oraz pomieszczenie, w którym dane osobowe są przetwarzane na serwerze). Jeśli Pracownik wykonuje czynności służbowe wynikające z Regulaminu organizacyjnego poza siedzibami Urzędu, w szczególności w siedzibach podmiotów nadzorowanych lub kontrolowanych, za obszar przetwarzania danych uznaje się dane tego podmiotu (nazwa i siedziba podmiotu).
2. Wyznacza się budynki, pomieszczenia, części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego lub w formie tradycyjnej:
   1) budynek główny (A) Urzędu przy ul. Tadeusza Kościuszki 16
   2) budynek (B) Urzędu przy pl. Kościuszki 5

3. LABI sporządza wykaz pomieszczeń, w których przetwarzane są dane osobowe, uaktualnia go i przekazuje do ABI najpóźniej w dniu podjęcia pierwszej czynności związanej z przetwarzaniem danych osobowych w tym pomieszczeniu.
4. W obszarze przetwarzania danych obowiązują następujące zasady:
   1) Prawo wstępu do serwerowni posiadają wyłącznie osoby upoważnione, a w szczególności ASI oraz ABI.
   2) Dostęp do pomieszczeń serwerowni zabezpieczony jest kluczem znajdującym się w sekretariacie.
   3) Jeżeli warunki techniczne na to pozwalają, strony przyjmuje się pojedynczo. W odmiennym wypadku należy zastosować takie środki, które gwarantują największą z możliwych ochronę przetwarzanych danych osobowych.
   4) Pobieranie i oddawanie kluczy do pomieszczeń, w których przetwarzane są dane osobowe następuje za pisemnym odnotowaniem tego faktu w zeszycie znajdującym się w sekretariacie głównej siedziby Urzędu.
   5) LABI zobowiązany jest do niezwłocznego powiadomienia ABI i Referatu Organizacyjnego o każdej zmianie osoby, która ma prawo pobierać i oddawać klucze do pomieszczeń, w których przetwarzane są dane osobowe.
   6) Zabrania się pozostawiania niezabezpieczonych pomieszczeń, w których przetwarzane są dane osobowe bez uprzedniego ich zamknięcia przed dostępem osób nieuprawnionych.
   7) Po godzinach pracy dokumenty zawierające dane osobowe przechowuje się w zamkniętych na klucz szafach w zamkniętych pomieszczeniach. Dane sensytywne przechowuje się w zamkniętych na klucz metalowych szafach w zamkniętych pomieszczeniach, a także w archiwum.
   8) LABI na bieżąco przekazuje materiały archiwalne zawierające dane osobowe do archiwum zakładowego zgodnie z odrębnymi przepisami obowiązującymi w tym zakresie.

## Rozdział 10
## Kontrola przestrzegania zasad bezpieczeństwa danych osobowych

1. ABI sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych wynikający z Ustawy oraz z Polityki bezpieczeństwa.
2. ABI dokonuje kontroli ochrony danych osobowych w Urzędzie na podstawie planu kontroli zatwierdzonego przez Wójta lub zleconych przez Wójta kontroli doraźnych. Do przeprowadzenia kontroli niezbędne jest posiadanie upoważnienia Wójta.

3. Niezależnie od uprawnień określonych w ust. 2, ABI ma prawo dokonywania na bieżąco czynności monitorujących w celu zapobiegnięcia incydentom zagrażającym bezpieczeństwu danych osobowych. Czynności monitorujące przeprowadza się bez upoważnienia. O wynikach tych czynności informuje się na bieżąco ADO.
4. Kontrolę oraz czynności monitorujące przeprowadza się w obecności LABI lub osoby go zastępującej.
5. Na podstawie informacji uzyskanych w wyniku przeprowadzenia czynności monitorujących oraz w oparciu o wyniki przeprowadzonej kontroli ABI sporządza sprawozdanie i przedstawia je ADO.

## Rozdział 11
## Postępowanie w przypadku naruszenia ochrony danych osobowych

1. W przypadku stwierdzenia:
   1) naruszenia zabezpieczenia systemu informatycznego,
   2) naruszenia technicznego stanu urządzeń,
   3) naruszenia zawartości zbioru danych osobowych,
   4) jakiegokolwiek odstępstwa pracy systemu odbiegającego od dotychczasowej pracy,
   5) wystąpienia innych zdarzeń mogących wskazywać na naruszenie ochrony danych osobowych lub mieć wpływ na naruszenie danych osobowych, w szczególności włamanie, zalanie, pożar, kradzież, niewłaściwe oddawanie, pobieranie i przechowywanie kluczy do pomieszczeń, itp.

   każdy Pracownik jest zobowiązany do niezwłocznego powiadomienia o tym fakcie LABI, a LABI ma obowiązek poinformować ABI.
2. Po wykonaniu czynności określonych w ust. 1 należy:
   1) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, w szczególności:
      a. zmienić hasło/hasła dostępu do systemu,
      b. fizycznie odłączyć system od sieci lokalnej, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców,
      c. zastosować inne możliwe działania.
   2) rozważyć wstrzymanie bieżącej pracy biurowej lub pracy na komputerze w celu zabezpieczenia miejsca zdarzenia,
   3) zaniechać - o ile to możliwe - dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę zdarzenia,

4) podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego lub aplikacji użytkowej,
5) zastosować się do innych zarządzeń Wójta, jeżeli odnoszą się one do zaistniałego przypadku,
6) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia ABI lub osoby go zastępującej.

3. W przypadku uzyskania przez ABI informacji o naruszeniu bezpieczeństwa sieci informatycznej lub elektronicznego zbioru danych, ABI niezwłocznie informuje o tym ASI.
4. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych ABI: zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy Urzędu :
   1) może żądać złożenia dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
   2) powiadamia o zaistniałym naruszeniu ADO,
   3) zleca usunięcie występujących naruszeń oraz, jeżeli zachodzi taka potrzeba, powiadamia odpowiednie instytucje lub organy.
5. ABI dokumentuje zaistniały przypadek naruszenia oraz sporządza raport według wzoru stanowiącego załącznik nr 9 do Polityki bezpieczeństwa oraz niezwłocznie przekazuje go ADO.
6. Zaistniałe naruszenie może stać się przedmiotem szczegółowej analizy prowadzonej przez zespół powołany przez Wójta. W skład zespołu wchodzą: ABI i ASI w Referacie Organizacyjnym (jeżeli stwierdzono naruszenie bezpieczeństwa systemu informatycznego), LABI w Referacie, w którym stwierdzono naruszenie, ewentualnie inne osoby wskazane przez Wójta.
7. Analiza, o której mowa w ust. 6, powinna zawierać wszechstronną ocenę zaistniałego naruszenia, wskazanie osób odpowiedzialnych, wnioski co do ewentualnych przedsięwzięć proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

## Rozdział 12
## Postanowienia końcowe

1. W zakresie nieunormowanym w Polityce bezpieczeństwa mają zastosowanie przepisy Ustawy.

2. Niezależnie od Polityki bezpieczeństwa, Pracownicy mają obowiązek przestrzegania innych przepisów obejmujących ochronę danych osobowych, w szczególności dotyczących archiwizacji dokumentów, bezpieczeństwa i higieny pracy oraz przepisów przeciwpożarowych.
3. Jeżeli przepisy odrębnych ustaw, które odnoszą się do przetwarzania danych osobowych, przewidują dalej idącą ich ochronę, niż to wynika z Ustawy, stosuje się przepisy tych ustaw.
4. Wszyscy Pracownicy przetwarzający dane osobowe mają obowiązek zachowania w tajemnicy przetwarzane dane osobowe oraz informacje o sposobach ich zabezpieczenia, zarówno w trakcie trwania zatrudnienia, jak również po jego ustaniu.
5. Wobec osoby, która w przypadku stwierdzenia naruszenia ochrony danych osobowych lub uzasadnionego domniemania wystąpienia takiego naruszenia nie podjęła działania określonego w Polityce bezpieczeństwa, wszczyna się postępowanie wyjaśniające.
6. Kierownik Referatu Organizacyjnego przekazuje każdemu nowoprzyjętemu Pracownikowi kartę obiegową i odbiera ją w chwili podpisania przez wskazane w niej osoby. Przejście pracownika do pracy w innym Referacie lub zakończenie stosunku pracy również wymagają zastosowania tej procedury.
7. Polityka bezpieczeństwa nie dotyczy danych osobowych przetwarzanych w zakresie informacji podlegających przepisom ustawy o ochronie informacji niejawnych.

Załącznik nr 1
do Polityki bezpieczeństwa w sprawie danych osobowych
gromadzonych w zbiorach Urzędu Gminy w Zaleszanach

**Powierzenie obowiązków Administratora Systemu Informatycznego Nr ABI -.....**

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997r. o ochronie danych (Dz. U. z 2014 r., poz. 1182 ze zm.) oraz Zarządzenia Nr 106/2015 Wójta Gminy Zaleszany z dnia 22 czerwca 2015 r. w sprawie polityki bezpieczeństwa informacji oraz instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych

**p o w i e r z a m**

**Pani/Panu** .....

zatrudnionemu na stanowisku .....w .....

**obowiązki Administratora Systemu Informatycznego**

oraz **u p o w a ż n i a m**

- do pełnego dostępu do danych osobowych znajdujących się w administrowanym systemie informatycznym (oraz do instalacji technicznej, systemów i urządzeń znajdujących się w Urzędzie, za pomocą których przetwarzane są dane osobowe, a także pełnego dostępu do pomieszczeń Urzędu, w których ulokowany jest sprzęt informatyczny oraz okablowanie strukturalne),
- do przetwarzania danych osobowych w zakresie zgodnym z realizowanymi przez Urząd zadaniami wynikającymi z Regulaminu Organizacyjnego Urzędu Gminy w Zaleszanach, zakresem obowiązków służbowych, uprawnień i odpowiedzialności pracownika oraz zakresem udzielonych pełnomocnictw i upoważnień oraz pełnionych zastępstw.

Upoważnienie ważne jest ..... .

Rozwiązanie stosunku pracy, zmiana nazwy Referatu, przejście do pracy w innym Referacie, zmiana imienia lub nazwiska upoważnionego powoduje wygaśnięcie upoważnienia.

Upoważnienie nie może być przenoszone na inne osoby.

Identyfikator w systemie..... - .....

Identyfikator w systemie..... - .....

Identyfikator w systemie..... - .....

.....
data (Administrator Bezpieczeństwa Informacji)

Otrzymują:
- Administrator Systemu Informatycznego,
- Inspektor ds. kadr celem dołączenia do akt osobowych pracownika,
- Administrator Bezpieczeństwa Informacji.

Załącznik nr 2
do Polityki bezpieczeństwa w sprawie danych osobowych
gromadzonych w zbiorach Urzędu Gminy w Zaleszanach

**Powierzenie obowiązków Lokalnego Administratora Bezpieczeństwa Informacji Nr ABI - .....**

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997r. o ochronie danych (Dz. U. z 2014 r., poz. 1182 ze zm.) oraz Zarządzenia Nr 106/2015 Wójta Gminy Zaleszany z dnia 22 czerwca 2015 r. w sprawie polityki bezpieczeństwa informacji oraz instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych

**p o w i e r z a m**

**Pani/Panu** .....

zatrudnionej /-emu na stanowisku .....

**obowiązki Lokalnego Administratora Bezpieczeństwa Informacji**

oraz **u p o w a ż n i a m**

do przetwarzania danych osobowych w zakresie zgodnym z realizowanymi przez Referat zadaniami wynikającymi z Regulaminu Organizacyjnego Urzędu Gminy w Zaleszanach, zakresem obowiązków służbowych, uprawnień i odpowiedzialności pracownika oraz zakresem udzielonych pełnomocnictw, upoważnień i pełnionych zastępstw.

Upoważnienie ważne jest ..... .

Rozwiązanie stosunku pracy, zmiana nazwy Referatu, zmiana imienia lub nazwiska upoważnionego powoduje wygaśnięcie upoważnienia.

Upoważnienie nie może być przenoszone na inne osoby.

Identyfikator w systemie..... - .....

Identyfikator w systemie..... - .....

Identyfikator w systemie..... - .....

.....

data (Administrator Bezpieczeństwa Informacji)

Otrzymują :
- Lokalny Administrator Bezpieczeństwa Informacji,
- Inspektor ds. kadr, celem dołączenia do akt osobowych pracownika,
- Administrator Systemu Informatycznego,
- Administrator Bezpieczeństwa Informacji.

Załącznik nr 3
do Polityki bezpieczeństwa w sprawie danych osobowych
gromadzonych w zbiorach Urzędu Gminy w Zaleszanach

.....
nazwa Referatu / komórki organizacyjnej

**W n i o s e k do Administratora Bezpieczeństwa Informacji**

**Część I – wypełnia LABI**

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997r. o ochronie danych (Dz. U. z 2014 r., poz. 1182 ze zm.) oraz Zarządzenia Nr 106/2015 Wójta Gminy Zaleszany z dnia 22 czerwca 2015 r. w sprawie polityki bezpieczeństwa informacji oraz instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych, wnioskuję o:[1]

☐ powierzenie obowiązków ASI dla systemu informatycznego.....

☐ powierzenie obowiązków LABI

☐ nadanie upoważnienia

☐ zmianę upoważnienia

☐ pozbawienie upoważnienia

**Pani/Panu** .....

zatrudnionej/-emu na stanowisku/pełniącej/-emu funkcję.....

w .....
(nazwa Referatu / komórki organizacyjnej / organu)

do przetwarzania danych osobowych w zakresie:[2]

☐ zgodnym z zakresem realizowanych zadań wynikających z Regulaminu Organizacyjnego Urzędu Gminy w Zaleszanach, zakresem obowiązków służbowych, uprawnień i odpowiedzialności pracownika oraz zakresem udzielonych pełnomocnictw, upoważnień i pełnionych zastępstw

☐ innym zakresie: .....

na czas od..... do.....

☐ nadanie

☐ zablokowanie

uprawnienia do pracy w systemie informatycznym: [3].....
(nazwa systemu / systemów)

na czas od..... do.....

.....
data

.....
imię, nazwisko i podpis wnioskodawcy

**Część II – wypełnia ASI**

☐ nadano

☐ zablokowano[4] Identyfikator: ..... w systemie:.....

Identyfikator: ..... w systemie:.....

Identyfikator: ..... w systemie:.....

.....
data

.....
imię, nazwisko i podpis ASI

[1] właściwe zaznaczyć
[2] właściwe zaznaczyć
[3] w przypadku radnego, stażysty, praktykanta, wolontariusza, osoby zatrudnionej na podstawie umowy cywilnoprawnej – nie wypełniać
[4] właściwe zaznaczyć

Załącznik nr 4
do Polityki bezpieczeństwa w sprawie danych osobowych
gromadzonych w zbiorach Urzędu Gminy w Zaleszanach

**(dla Pracownika Urzędu)**

**Upoważnienie Nr ABI- .....**

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997r. o ochronie danych (Dz. U. z 2014 r., poz. 1182 ze zm.) oraz Zarządzenia Nr 106/2015 Wójta Gminy Zaleszany z dnia 22 czerwca 2015 r. w sprawie polityki bezpieczeństwa informacji oraz instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych

**u p o w a ż n i a m**

**Panią/Pana** .....

zatrudnioną / -ego na stanowisku .....

w .....

(nazwa Referatu / komórki organizacyjnej)

do przetwarzania danych osobowych w zakresie zgodnym realizowanymi zadaniami wynikającymi z Regulaminu Organizacyjnego Urzędu Gminy w Zaleszanach, zakresem obowiązków służbowych, uprawnień i odpowiedzialności pracownika oraz zakresem udzielonych pełnomocnictw, upoważnień i pełnionych zastępstw

Upoważnienie ważne jest .....
Przesłanki wymienione w Rozdziale 4 ust. 4 Polityki bezpieczeństwa w sprawie danych osobowych gromadzonych w zbiorach Urzędu Gminy w Zaleszanach powodują wygaśnięcie upoważnienia.
Upoważnienie nie może być przenoszone na inne osoby.
Traci moc upoważnienie nr ABI - .....

Identyfikator w systemie..... - .....

Identyfikator w systemie..... - .....

Identyfikator w systemie..... - .....

.....
data (Administrator Bezpieczeństwa Informacji)

Otrzymują:
- Użytkownik,
- Inspektor ds. kadr, celem dołączenia do akt osobowych pracownika,
- Administrator Systemu Informatycznego,
- Lokalny Administrator Bezpieczeństwa Informacji,
- Administrator Bezpieczeństwa Informacji.

Załącznik nr 5
do Polityki bezpieczeństwa w sprawie danych osobowych
gromadzonych w zbiorach Urzędu Gminy w Zaleszanach

**(dla osoby niebędącej pracownikiem Urzędu)**

**Upoważnienie Nr ABI- .....**

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997r. o ochronie danych (Dz. U. z 2014 r., poz. 1182 ze zm.) oraz Zarządzenia Nr 106/2015 Wójta Gminy Zaleszany z dnia 22 czerwca 2015 r. w sprawie polityki bezpieczeństwa informacji oraz instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych

**u p o w a ż n i a m**

**Panią/Pana** .....

zatrudnioną /-ego, pełniącą/-ego funkcję.....

w .....

(nazwa Referatu / organu)

do przetwarzania danych osobowych w zakresie: .....

.....

Upoważnienie ważne jest .....

.....powoduje wygaśnięcie upoważnienia.

Upoważnienie nie może być przenoszone na inne osoby.

Traci moc upoważnienie nr ABI - .....

Identyfikator w systemie..... - .....

.....

data (Administrator Bezpieczeństwa Informacji)

Otrzymują:
- Użytkownik,
- Lokalny Administrator Bezpieczeństwa Informacji,
- Administrator Systemu Informatycznego (o ile nadano uprawnienie do pracy w systemie informatycznym),
- Administrator Bezpieczeństwa Informacji.

Załącznik nr 6
do Polityki bezpieczeństwa w sprawie danych osobowych
gromadzonych w zbiorach Urzędu Gminy w Zaleszanach

**Pozbawienie upoważnienia Nr ABI - .....**

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997r. o ochronie danych (Dz. U. z 2014 r., poz. 1182 ze zm.) oraz Zarządzenia Nr 106/2015 Wójta Gminy Zaleszany z dnia 22 czerwca 2015 r. w sprawie polityki bezpieczeństwa informacji oraz instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych

**pozbawiam u p o w a ż n i e n i a**

nr ..... ..... nadanego w dniu .....

**Panią/Pana** .....

.....
data (Administrator Bezpieczeństwa Informacji)

Otrzymują:
- Użytkownik,
- Inspektor ds. kadr, celem dołączenia do akt osobowych pracownika,
- Administrator Systemu Informatycznego,
- Lokalny Administrator Bezpieczeństwa Informacji,
- Administrator Bezpieczeństwa Informacji.

Załącznik nr 7
do Polityki bezpieczeństwa w sprawie danych osobowych
gromadzonych w zbiorach Urzędu Gminy w Zaleszanach

**(dla Pracownika Urzędu)**

.....
(imię i nazwisko)

.....
(nazwa Referatu)

**Oświadczenie**

Ja, niżej podpisana/-y, oświadczam, że jest mi znana treść:

1) przepisów ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2014 r., poz. 1182 ze zm.),
2) Zarządzenia Nr 106/2015 Wójta Gminy Zaleszany z dnia 22 czerwca 2015 r. w sprawie polityki bezpieczeństwa informacji oraz instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych,

i zobowiązuję się do ich przestrzegania.

Stosownie do treści przepisów rozdziału 8 Ustawy, o której mowa w pkt 1. jestem świadoma/-y odpowiedzialności karnej grożącej mi z tytułu nieprzestrzegania przepisów ustawy.

Niezależnie od odpowiedzialności przewidzianej w w/w przepisach jestem świadoma/-y, że naruszenie ochrony danych osobowych w Urzędzie Gminy w Zaleszanach może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i może skutkować odpowiedzialnością dyscyplinarną.

Ponadto, zgodnie z art. 39 ust. 2 ustawy, zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia zarówno w czasie trwania zatrudnienia, jak również po jego ustaniu.

.....
data, podpis osoby składającej oświadczenie

Otrzymują:
- Użytkownik,
- Inspektor ds. kadr, celem dołączenia do akt osobowych pracownika,
- Administrator Bezpieczeństwa Informacji.

Załącznik nr 8
do Polityki bezpieczeństwa w sprawie danych osobowych
gromadzonych w zbiorach Urzędu Gminy w Zaleszanach

**(dla osoby niebędącej pracownikiem Urzędu)**

.....
(imię i nazwisko)

.....
(funkcja w organie / wykonywane zadania / numer umowy cywilnoprawnej)

**Oświadczenie**

Ja, niżej podpisana/-y, oświadczam, że jest mi znana treść przepisów ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2014 r., poz. 1182 ze zm.) i zobowiązuję się do ich przestrzegania.

Stosownie do treści przepisów rozdziału 8 ustawy jestem świadoma/-y odpowiedzialności karnej grożącej mi z tytułu nieprzestrzegania przepisów ustawy.

Zobowiązuję się do zapewnienia bezpieczeństwa i ochrony udostępnionych mi danych osobowych, w szczególności do zabezpieczenia ich przed dostępem osób nieupoważnionych,

Ponadto, zgodnie z art. 39 ust. 2 ustawy, zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia zarówno w czasie ich przetwarzania na podstawie udzielonego mi upoważnienia, jak również po ustaniu jego ważności.

.....
data, podpis osoby składającej oświadczenie

Otrzymują:
- Użytkownik,
- Administrator Bezpieczeństwa Informacji.

Załącznik nr 9
do Polityki bezpieczeństwa w sprawie danych osobowych
gromadzonych w zbiorach Urzędu Gminy w Zaleszanach

**Raport z naruszenia bezpieczeństwa danych osobowych w Urzędzie Gminy w Zaleszanach**

1. Data:.....godzina:.....powzięcia informacji przez powiadamiającego.
2. Data: .....godzina: .....powiadomienia.
3. Osoba powiadamiająca o zaistniałym zdarzeniu:

.....

(imię, nazwisko, stanowisko służbowe)

4. Lokalizacja zdarzenia:

.....

(np. adres, nr pokoju, nazwa pomieszczenia)

5. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

.....

.....

6. Podjęte działania:

.....

.....

7. Prawdopodobna przyczyna wystąpienia zdarzenia:

.....

.....

8. Postępowanie wyjaśniające:

.....

.....

.....

data, Administrator Bezpieczeństwa Informacji