

**ZARZĄDZENIE Nr 58 /2017**  
**WÓJTA GMINY BIELSK PODLASKI**  
**z dnia 11 grudnia 2017 r.**

**w sprawie „Polityki Bezpieczeństwa Informacji w Urzędzie Gminy Bielsk Podlaski” oraz  
„Instrukcji Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych  
Osobowych w Urzędzie Gminy Bielsk Podlaski”**

Na podstawie art. 31 oraz art. 33 ust.3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2017 r. poz. 1875) w związku z art.36 i art. 36a ust.1-8 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz 922) i § 3-5 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r. Nr. 100 poz.10240) zarządzam, co następuje:

**§1**

Ustala się Politykę Bezpieczeństwa Informacji w Urzędzie Gminy Bielsk Podlaski stanowiącą załącznik nr 1 do Zarządzenia oraz Instrukcję Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych w Urzędzie Gminy Bielsk Podlaski stanowiącą załącznik nr 2.

**§2**

Kierowników komórek organizacyjnych zobowiązuje się do zapoznania podległych pracowników z instrukcjami, o których mowa w §1, oraz do prowadzenia nadzoru i kontroli przestrzegania i stosowania zasad określonych w Polityce Bezpieczeństwa Informacji oraz Instrukcji Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych.

**§3**

1. Powołuję Pana Pawła Demianiuka pracownika Referatu Organizacyjnego i Spraw Obywatelskich do pełnienia funkcji Administratora Bezpieczeństwa Informacji w Urzędzie Gminy Bielsk Podlaski.
2. Upoważniam Panią Martę Grygoruk pracownika Referatu Organizacyjnego i Spraw Obywatelskich do realizacji zadań Administratora Bezpieczeństwa Informacji w przypadku nieobecności osoby wyznaczonej.

#### §4

Traci moc zarządzenie Nr 13/2013 Wójta Gminy Bielsk Podlaski z dnia 08.02.2013 r. w sprawie wdrożenia Polityki Bezpieczeństwa i Instrukcji zarządzania systemem informatycznym do przetwarzania danych osobowych oraz wyznaczenia Administratora Bezpieczeństwa Informacji w Urzędzie Gminy Bielsk Podlaski.


#### §5

Wykonanie zarządzenia powierza się wszystkim pracownikom Urzędu.

#### §6

Zarządzenie wchodzi w życie z dniem podpisania

**WÓJT**  
  
**mgr Raisa Rajeka**

  
Bartoszew

# POLITYKA BEZPIECZEŃSTWA INFORMACJI W URZĘDZIE GMINY BIELSK PODLASKI

## Rozdział I

### Postanowienia ogólne, definicje

#### §1

1. Polityka Bezpieczeństwa Informacji jest zbiorem zasad i procedur obowiązujących przy przetwarzaniu i wykorzystywaniu danych osobowych we wszystkich zbiorach danych osobowych administrowanych przez Urząd Gminy Bielsk Podlaski.
2. Podstawą do opracowania i wdrożenia dokumentu są:
  - 1) Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2016 r. poz 922, ze 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, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr. 100, poz. 1024).
  - 3) Przetwarzanie danych osobowych w Urzędzie Gminy Bielsk Podlaski jest dopuszczalne wyłącznie pod warunkiem przestrzegania wyżej wymienionych dokumentów i wydanych na jej podstawie przepisów wykonawczych w tym niniejszej polityki i instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych.

#### §2

Definicje stosowanych pojęć w Polityce Bezpieczeństwa Informacji oznaczają:

- 1) **dane osobowe** – wszelka informacja pozwalająca na jednoznaczną identyfikację konkretnej osoby w konkretnym środowisku,
- 2) **zbiór danych osobowych** – dane osobowe zgromadzone w usystematyzowany sposób, pozwalający na łatwe dotarcie do konkretnej informacji,
- 3) **komputerowy zbiór danych** – zbiór danych osobowych w formie elektronicznej,
- 4) **tradycyjny zbiór danych** – zbiór danych osobowych w formie papierowej (np. księgi, wykazy, ewidencje),

- 5) **przetwarzanie danych** – wszystkie czynności wykonywane na danych, tj. gromadzenie, utrwalanie, przechowywanie, modyfikowanie, przenoszenie, przekazywanie i usuwanie, niezależnie od formy w jakiej wykonywane są te czynności,
- 6) **Administrator Danych Osobowych (ADO)** – Wójt Gminy Bielsk Podlaski, osoba reprezentująca Urząd Gminy oraz odpowiedzialna za całokształt zagadnień związanych z przetwarzaniem danych osobowych w administrowanych przez nią zbiorach danych,
- 7) **Administrator Bezpieczeństwa Informacji (ABI)** – osoba nadzorująca przestrzeganie zasad i ochrony danych osobowych,
- 8) **Administrator Systemów Informatycznych (ASI)** – należy przez to rozumieć pracownika informatyki odpowiedzialnego za stosowanie technicznych i organizacyjnych środków ochrony danych osobowych. W przypadku gdy ASI nie jest powołany, jego zadania realizuje pracownik informatyki,
- 9) **osoba upoważniona lub użytkownik systemu** – osoba posiadająca upoważnienie do przetwarzania danych osobowych w określonym zakresie wydane przez ADO lub osoba uprawniona przez niego i dopuszczona jako użytkownik do przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej, w zakresie wskazanym w upoważnieniu, zwana dalej użytkownikiem,
- 10) **osoba uprawniona** – osoba posiadająca uprawnienie wydane przez ADO na mocy którego wykonuje w jego imieniu określone czynności,
- 11) **osoba trzecia** – każda osoba nieuprawniona do przetwarzania danych osobowych będących w posiadaniu Administratora Danych Osobowych, a także osoba posiadająca upoważnienie ale podejmująca czynności w zakresie przekraczającym zakres jej upoważnienia,
- 12) **sprawozdanie** – należy przez to rozumieć dokument, o którym mowa w art.36c ustawy, opracowany przez administratora bezpieczeństwa informacji po dokonaniu sprawdzenia
- 13) **system informatyczny** – zespół środków technicznych (urządzenia: komputerowe, drukujące, łączność, wraz z okablowaniem i oprogramowaniem), zespół zabezpieczeń środków technicznych, użytkownicy tych urządzeń i programów, a także sieć informatyczna i udostępnianie przez nią zasoby,
- 14) **sieć lokalna (LAN)** – należy przez to rozumieć połączenie systemów informatycznych urzędu wyłącznie dla własnych potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych,

- 15) **sieć rozległa (WAN)** – rozległa sieć teleinformatyczna,
- 16) **zabezpieczenie danych w systemie informatycznym** – wdrożenie i eksploatacja stosowanych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
- 17) **identyfikator użytkownika (LOGIN)** – ciąg znaków literowych i cyfrowych, lub innych, jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
- 18) **hasło (Password)** – ciąg znaków literowych cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym,
- 19) **zalogowanie** – uwierzytelnienie czyli działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

## **Rozdział II**

### **Zasady postępowania przy przetwarzaniu danych osobowych**

#### **§3**

1. Administrator Danych Osobowych, którym jest Wójt, zarządzeniem wyznacza Administratora Bezpieczeństwa Informacji dla danych zawartych w systemach informatycznych Urzędu Gminy, zwanego dalej Administratorem Bezpieczeństwa Informacji oraz osobę upoważnioną do zastępowania ABI.
2. Administrator Danych Osobowych jest zobowiązany do:
  - a) czuwania nad tym by przetwarzanie danych osobowych będących w jego posiadaniu było zgodne z prawem,
  - b) zastosowania niezbędnych środków technicznych i organizacyjnych w celu zapewnienia ochrony przetwarzanych danych osobowych,
  - c) sprawowanie kontroli nad bezpieczeństwem oraz sposobem przetwarzania danych,
  - d) prowadzenie ewidencji osób uprawnionych do przetwarzania danych osobowych, stanowiącej **załącznik Nr 1 do Polityki Bezpieczeństwa Informacji w Urzędzie Gminy Bielsk Podlaski.**
3. Administrator Bezpieczeństwa Informacji realizuje zadania w zakresie ochrony danych, a w szczególności:
  - a) kontroli komórek organizacyjnych Urzędu w zakresie właściwego zabezpieczenia systemów informatycznych oraz pomieszczeń, w których przetwarzane są dane osobowe,
  - b) ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych Urzędu Gminy,

- c) podejmowanie stosowanych działań zgodnie z niniejszą Polityką Bezpieczeństwa Informacji w przypadku nieuprawnionego dostępu bądź naruszenia zabezpieczenia danych znajdujących się w systemie informatycznym,
  - d) niezwłocznego informowania ADO lub osoby przez niego upoważnionej o przypadkach naruszenia przepisów ustawy o ochronie danych osobowych,
  - e) nadzoru i kontroli systemów informatycznych służących do przetwarzania danych osobowych i osób przy nim zatrudnionych,
  - f) opracowanie i wdrożenie programu szkolenia w zakresie zabezpieczenia systemu informatycznego.
4. Osoba zastępująca ABI powyższe zadania realizuje tylko w przypadku jego nieobecności po czym składa relacje z podejmowanych działań.
5. Kierownicy referatów są zobowiązani do:
- a) współdziałania z ABI w zakresie przestrzegania instrukcji,
  - b) sprawowania nadzoru nad pracą podległych pracowników w zakresie wykonywania czynności służbowych,
  - c) niezwłocznego zawiadomienia ADO o konieczności utworzenia nowego zbioru danych osobowych, wymagających rejestracji, wzór wniosku stanowi **załącznik nr 2 do Polityki Bezpieczeństwa Informacji w Urzędzie Gminy Bielsk Podlaski**.
6. Pracownik upoważniony przez ADO do przetwarzania danych osobowych, jest zobowiązany do:
- a) odbycia wewnętrznego szkolenia dotyczącego przetwarzania i ochrony danych osobowych,
  - b) zapoznania się z przepisami prawa w zakresie ochrony danych osobowych,
  - c) stosowania określonych procedur i środków mających na celu zabezpieczenie danych przed ich udostępnieniem osobom trzecim,
  - d) podporządkowania się poleceniom ABI oraz właściwego kierownika w zakresie ochrony danych.
7. Wszelkie czynności przeprowadzane na danych osobowych mogą dokonywać jedynie pracownicy upoważnieni przez ADO. Wzór upoważnienia stanowi **załącznik nr 3 do Polityki Bezpieczeństwa Informacji w Urzędzie Gminy Bielsk Podlaski**.
8. Bezpośredni nadzór nad przetwarzaniem danych osobowych w referatach Urzędu Gminy sprawują kierownicy referatów, a w przypadku pracowników na samodzielnych stanowiskach Wójt, Z-ca Wójta – każdy w swoim pionie.

9. Pracownicy którym udzielono upoważnienia są zobowiązani do podpisania oświadczenia – wzór oświadczenia stanowi **załącznik nr 4 do Polityki Bezpieczeństwa Informacji w Urzędzie Gminy Bielsk Podlaski.**
10. W przypadku zatrudnienia nowego pracownika, zmiany stanowiska, zmiany zakresu obowiązków pracowniczych, utworzenia nowego zbioru danych osobowych, zmiany sposobu przetwarzania danych lub w innych przypadkach wpływających bezpośrednio na rodzaj i zakres przetwarzania danych, kierownik zobowiązany jest bezzwłocznie skierować wniosek do Administratora Danych Osobowych o wydanie lub cofnięcie upoważnienia. W przypadku samodzielnych stanowisk pracy cofnięcie lub wydanie upoważnienia dokonuje administrator danych. Wzór pisma o cofnięciu upoważnienia stanowi **załącznik nr 5 do Polityki Bezpieczeństwa Informacji w Urzędzie Gminy Bielsk Podlaski.**
11. Obowiązek przestrzegania tajemnicy danych osobowych spoczywa na wszystkich pracownikach, którzy mają do nich dostęp, również po ustaniu stosunku pracy.

### **Rozdział III**

#### **Obszar przetwarzania danych osobowych**

##### **§4**

1. Obszar przetwarzania danych osobowych w Urzędzie obejmuje budynek, pomieszczenia i część pomieszczeń, w których przetwarzane są dane osobowe oraz miejsca, gdzie przechowuje się nośniki informacji zawierające dane osobowe (szafy z dokumentacją papierową, szafy zawierające elektroniczne nośniki informacji, pomieszczenia, w których składowane są uszkodzone nośniki danych).
2. Budynek zajmowany przez Urząd Gminy Bielsk Podlaski znajduje się w centrum miasta Bielsk Podlaski. Jest to budynek czteropiętrowy stanowiący współwłasność ze Starostwem Powiatowym, w którym Urząd Gminy użytkuje pomieszczenia na parterze, pierwszym piętrze, część podpiwniczenia oraz położoną na wschód od obiektu salę konferencyjną.
3. Za ochronę budynku odpowiada Biuro Ochrony Osób i Mienia „LIDER” będącą koncesjonowanym przedsiębiorcą prowadzącym działalność gospodarczą w zakresie ochrony osób i mienia, która ma podpisana umowę z Gminą Bielsk Podlaski. Pracownicy ochrony wykonują czynności związane z monitorowaniem sygnałów alarmowych z budynku biurowego Urzędu Gminy Bielsk Podlaski za pośrednictwem zainstalowanego systemu powiadamiania, 24 godziny na dobę. Pomieszczenie z usytuowanym systemem IT nie posiada okien, brak możliwości podglądu z zewnątrz. Wyposażone jest w drzwi drewniane z zamkiem 3 klasy.

## §5

Wykaz budynków oraz pomieszczeń stanowiących obszar przetwarzania danych osobowych.

Lp.	Adres	Nr pomieszczenia
	ul. Mickiewicza 46, 17-100 Bielsk Podlaski	<b>Parter:</b> Biuro Obsługi Klienta, 1,2,4,5, 6,7,8,11
		<b>I Piętro:</b> 101,103,105, 106,107,108, 109,110,111, 112,113, serwerownia

## Rozdział IV

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

## §6

1. Za zbiór danych osobowych przetwarzanych w Urzędzie Gminy Bielsk Podlaski uważa się:
  - a) dokumentację papierową (korespondencję wnioski, deklaracje, itp.),
  - b) systemy informatyczne przetwarzania danych oraz oprogramowanie komputerowe służące do przetwarzania informacji,
  - c) wydruki komputerowe.
2. Wykaz zbioru danych przetwarzanych w Urzędzie zawiera następujące informacje:
  - a) nazwę zbioru danych,
  - b) sposób gromadzenia danych osobowych (papierowy, elektroniczny),
  - c) stosowane przy przetwarzaniu danych osobowych oprogramowanie.
3. Wzór wykazu zbioru danych osobowych w Urzędzie stanowi **załącznik nr 6 do Polityki Bezpieczeństwa Informacji w Urzędzie Gminy Bielsk Podlaski.**
4. Opis struktury zbiorów danych osobowych stanowi **załącznik nr 7 do Polityki Bezpieczeństwa Informacji w Urzędzie Gminy Bielsk Podlaski..**
5. W Urzędzie Gminy Bielsk Podlaski nie istnieją żadne relacje pomiędzy różnymi systemami informatycznymi.

## Rozdział V

### Opis zdarzeń naruszających ochronę danych osobowych

## §7

Podział zagrożeń:

1. Zagrożenia losowe zewnętrzne: np. klęski żywiołowe, przerwy w zasilaniu prądu – których występowanie może prowadzić do utraty integralności danych, ich uszkodzenia lub zniszczenia,



2. Zagrożenia losowe wewnętrzne: np. niezamierzone pomyłki operatorów, administratora systemu, awarie sprzętowe, błędy oprogramowania – przy których może dojść do zniszczenia danych, a ciągłość pracy systemu może zostać zakłócona oraz może nastąpić naruszenie poufności danych,
3. Zagrożenia zamierzone, świadome i celowe – w wyniku ich wystąpienia zazwyczaj nie występuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy. W ramach tej kategorii zagrożeń wystąpić mogą:
  - a) nieuprawniony dostęp do systemu z zewnątrz,
  - b) nieuprawniony dostęp do systemu z wewnątrz,
  - c) nieuprawnione przekazanie danych,
  - d) bezpośrednie zagrożenie materialnych składników np. kradzież, zniszczenie.

## §8

### **Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe to głównie:**

1. Sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: pożar, zalanie pomieszczenia, katastrofa budowlana itp.
2. Niewłaściwe parametry środowiska: nadmierna wilgotność, wysoka temperatura.
3. Awaria sprzętu lub oprogramowania, które wyraźnie wskazuje na umyślne działanie w kierunku naruszenia ochrony danych, a także niewłaściwe działanie serwisu.
4. Niedopuszczalna manipulacja danymi osobowymi w systemie.
5. Ujawnienie osobom nieupoważnionym danych osobowych lub objętych tajemnicą procedur ochrony przetwarzania albo innych strzeżonych elementów systemu.
6. Ujawnienie istnienia nieautoryzowanych kont dostępu do danych.
7. Naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie.
8. Rażąco naruszenie dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, prace na danych osobowych w celach prywatnych itp.).
9. Nieuprawniony dostęp lub próba dostępu do danych osobowych lub pomieszczeń, w których się one znajdują.

**Procedury postępowania w przypadku naruszenia ochrony danych osobowych**

1. Każdy pracownik Urzędu, który stwierdzi fakt naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane osobowe, bądź posiada informacje mogące mieć wpływ na bezpieczeństwo danych osobowych jest zobowiązany niezwłocznie zgłosić to Administratorowi Bezpieczeństwa Informacji, a w przypadku jego nieobecności należy zawiadomić bezpośrednio przełożonego.
2. Do czasu przybycia na miejsce Administratora Bezpieczeństwa Informacji należy:
  - a) podjąć czynności niezbędne do powstrzymania skutków naruszenia ochrony,
  - b) rozważyć wstrzymanie bieżącej pracy w celu zabezpieczenia zdarzenia,
  - c) ustalić przyczynę i sprawcę naruszenia ochrony.
3. Administrator Bezpieczeństwa Informacji po przybyciu na miejsce zdarzenia podejmuje następujące kroki:
  - a) zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości pracy urzędu,
  - b) dokonać fizycznego odłączenia urządzeń i segmentów sieci, które mogły umożliwić dostęp do bazy danych osobie nieuprawnionej,
  - c) zażądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
  - d) rozważa celowość i potrzebę powiadomienia o zaistniałym naruszeniu Administratora Danych Osobowych,
  - e) nawiązać bezpośredni kontakt, jeżeli zachodzi taka potrzeba ze specjalistami spoza Urzędu.
4. Administrator Bezpieczeństwa Informacji dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych osobowych sporządzając raport który przekazuje Administratorowi Danych Osobowych. Wzór raportu stanowi **załącznik nr 8 do Polityki Bezpieczeństwa Informacji w Urzędzie Gminy Bielsk Podlaski**.
5. Administrator Bezpieczeństwa Informacji zasięga potrzebnych mu opinii i proponuje działania naprawcze (w tym także ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń, oraz terminu wznowienia przetwarzania danych osobowych).
6. W sytuacjach wyjątkowych, wszystkie działania związane z usuwaniem skutków incydentu i wyjaśnieniem jego przyczyn mogą być realizowane przez osoby upoważnione przez Administratora Bezpieczeństwa Informacji.
7. ABI odpowiada za sporządzenie listy pracowników mających prawo do podejmowania kroków w razie incydentów w sytuacji, gdy nie mogą one być wykonywane osobiście przez niego.

8. Jeżeli incydent był spowodowany celowym działaniem, ABI jest zobowiązany do pisemnego powiadomienia Wójta Gminy – Administratora Danych Osobowych lub Zastępcę Wójta.
9. Wójt Gminy (ADO) lub Zastępca Wójta, biorąc pod uwagę charakter zdarzenia może poinformować organy uprawnione do ścigania przestępstw o fakcie celowego naruszenia bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym.

## **§10**

### **Środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności przy przetwarzaniu danych osobowych**

1. Administrator Danych Osobowych jest zobowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych w systemie informatycznym Urzędu Gminy, a w szczególności:
  - a) zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym,
  - b) zapobiegać przed zabraniem danych przez osoby trzecie,
  - c) zapobiegać przetwarzaniu danych z naruszeniem ustawy oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych,
2. Do zastosowania środków technicznych należy:
  - a) wejście do budynku zabezpieczone jest zamkami drzwiowymi oraz alarmem,
  - b) stosuje się niszcarki dokumentów,
  - c) odrębne zasilanie sprzętu komputerowego,
  - d) urządzenia wchodzące w skład infrastruktury sieciowej, serwera oraz komputery na których przetwarzane są dane osobowe podłączone są do lokalnych awaryjnych zasilaczy UPS, zabezpieczających przed skokami napięcia i zanikiem zasilania,
  - e) na komputerach użytkowników systemu działa program antywirusowy,
  - f) klucze zapasowe do pomieszczeń przechowywane są w specjalnej szafie i mogą być wydawane w sytuacjach awaryjnych,
3. Do zastosowania środków organizacyjnych należą przede wszystkim następujące zasady:
  - a) każdy nowo zatrudniony pracownik mający dostęp do danych osobowych podlega przeszkoleniu w zakresie przepisów o ochronie danych osobowych oraz wynikających z nich zadań oraz obowiązków,
  - b) wszyscy pracownicy podlegają okresowym szkoleniom, stosownie do potrzeb wynikających ze zmian w systemie informatycznym oraz w związku ze zmianą przepisów o ochronie danych osobowych lub zmian wewnętrznych regulacji,
  - c) szkolenia odbywają się na wniosek kierowników komórek organizacyjnych,
  - d) urządzenia służące do przetwarzania danych osobowych znajdują się w pomieszczeniach zabezpieczonych zamkami, które muszą być zamykane podczas nieobecności użytkownika,

- e) dostęp do pomieszczenia w którym znajdują się urządzenia serwerowe ma tylko Administrator Bezpieczeństwa Informacji oraz Administrator Systemu Informatycznego,
  - f) dostęp do baz danych osobowych zastrzeżony jest wyłącznie dla uprawnionych pracowników,
  - g) zastosowano identyfikator i hasło dostępu do danych na poziomie aplikacji,
  - h) dla każdego użytkownika systemu wyznaczony jest odrębny identyfikator,
  - i) użytkownicy mają dostęp do aplikacji umożliwiający dostęp tylko do tych danych osobowych, do których mają uprawnienia,
  - j) zastosowano wygaszanie ekranu w przypadku dłuższej nieaktywności użytkownika,
  - k) tymczasowe wydruki z danymi osobowymi są po ustaniu ich przydatności niszczone,
  - l) dane przetwarzane przy użyciu tradycyjnych środków pisarskich gromadzone i przechowywane są w zamkniętych szafach.
4. Administrator Bezpieczeństwa Informacji jest odpowiedzialny za organizację szkoleń, oraz prowadzi wykaz osób, które zostały zapoznane z polityką bezpieczeństwa informacji oraz instrukcją zarządzania systemem informatycznym – **załącznik Nr 9 do Polityki Bezpieczeństwa Informacji w Urzędzie Gminy Bielsk Podlaski.**

**EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA  
DANYCH OSOBOWYCH  
W URZĘDZIE GMINY BIELSK PODLASKI**

Lp	Imię i nazwisko osoby upoważnionej	Zakres upoważnienia	Nr zbiorów objętych zakresem upoważnieniem	Okres upoważnienia		Przyczyna ustania upoważnienia
				od	do	
1						
2						
3						
4						

\*Legenda:

<b>ZB-</b> zbieranie danych osobowych	<b>WD</b> – wgląd w dane osobowe	<b>PR</b> – przechowywanie danych osobowych	<b>OP</b> - opracowywanie danych osobowych	<b>UT</b> – utrwalanie danych osobowych	<b>ZM</b> – zmienianie danych osobowych	<b>US</b> – usuwanie danych osobowych	<b>PS</b> – prace serwisowe w systemach przetwarzania danych
--	-------------------------------------	--	---	--	--	---	---

### Wniosek o rejestrację zbioru danych osobowych

1. Nazwa zbioru:
2. Podstawa prawna upoważniająca do prowadzenia zbioru danych:
3. Cel przetwarzania danych w zbiorze:
4. Kategorie osób których dane są przetwarzane:
5. Zakres danych przetwarzanych w zbiorze:
6. Sposób zbierania danych do zbioru:
7. Sposób udostępniania danych ze zbioru
8. Odbiorcy lub kategorie odbiorców, którym dane mogą być przekazywane:
9. Informacja dotycząca ewentualnego przekazywania danych do państwa trzeciego:

.....  
(podpis pracownika z który będzie  
przetwarzał dane osobowe)

.....  
(podpis Kierownika Referatu)

Bielsk Podlaski, dnia .....

**UPOWAŻNIENIE Nr .....**  
**do przetwarzania danych osobowych**

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922)

**upoważniam**

.....  
(imię i nazwisko)

zatrudnionego/nej w Urzędzie Gminy Bielsk Podlaski

na stanowisku.....

do przetwarzania danych osobowych oraz obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych w Urzędzie Gminy Bielsk Podlaski w ramach zadań określonych zakresem obowiązków.

Upoważnienie obejmuje prawo zbierania, utrwalania, przechowywania, opracowywania, zmieniania, udostępniania i usuwania danych osobowych.

Zobowiązuję Pana/Panią do przestrzegania przepisów dotyczących ochrony danych osobowych oraz Polityki Bezpieczeństwa Informacji i Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Gminy Bielsk Podlaski.

Zgodnie z art.39 ust. 2 ustawy o ochronie danych osobowych, ma Pan/Pani obowiązek zachować w tajemnicy dane osobowe oraz sposoby ich zabezpieczenia.

Niniejsze upoważnienie :

- 1) zostało wydane na czas : .....
- 2) może być w każdym czasie cofnięte
- 3) wygasa z dniem rozwiązania lub wygaśnięcia stosunku pracy z nieupoważnionym pracownikiem

.....  
(podpis Administratora Danych Osobowych)

Otrzymują:

1. upoważniony
2. kadry
3. a/a

Bielsk Podlaski, dnia .....

.....  
(imię i nazwisko)

.....  
(stanowisko)

## OŚWIADCZENIE

Ja niżej podpisany(a) ..... zobowiązuje się do zachowania w tajemnicy danych osobowych, do których mam/będę miał(a) dostęp w związku z wykonywaniem przeze mnie zadań służbowych i obowiązków pracowniczych w Urzędzie Gminy Bielsk Podlaski, zarówno w trakcie obecnie wiążącego mnie stosunku pracy, stażu, praktyki jak i po ustaniu zatrudnienia.

Zobowiązuję się przestrzegać regulaminów, instrukcji i procedur obowiązujących w Urzędzie Gminy Bielsk Podlaski wiążących się z ochroną danych osobowych, a w szczególności nie będę bez upoważnienia służbowego wykorzystywał(a) danych osobowych ze zbiorów w .....

Stwierdzam, że zostałem(am) przeszkolony(a) i zrozumiałem(am) treść definicji danych osobowych w rozumieniu art. 6 Ustawy z dnia 29.08.1997 r., o ochronie danych osobowych (tekst jednolity Dz. U z roku 2002 nr 101, poz. 926) oraz aktów wykonawczych i instrukcji polityki bezpieczeństwa w Urzędzie Gminy Bielsk Podlaski.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane za naruszenie obowiązków pracowniczych w rozumieniu Kodeksu Pracy.

.....  
podpis składającego  
oświadczenie



## WYCOFANIE UPOWAŻNIENIA

Na podstawie art. 37 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych ( Dz. U. z 2016 r. poz. 922) w związku z: .....

.....  
.....  
.....

### cofam upoważnienie

Pan/Pani

.....

zatrudnionego/zatrudnionej w .....

na stanowisku .....

do przetwarzania danych osobowych, wynikającego z zakresu obowiązków pracowniczych.

.....

(data i podpis  
Administratora Danych Osobowych)

Otrzymałem(łam) dnia: .....

.....

(podpis pracownika)

**Wykaz zbiorów oraz programów służących do ich przetwarzania**

Lp.	Nazwa zbioru	Sposób gromadzenia		Nazwa programu
		papierowa	elektroniczna	
1	Rejestr mieszkańców	X	X	SEL-WIN ŹRÓDŁO
2	Rejestr zamieszkania cudzoziemców	X	X	SEL-WIN
3	Rejestr wydanych i unieważnionych dowodów osobistych	X	X	ŹRÓDŁO
4	Rejestr wyborców	X	X	SEL-WIN WOW
5	Oświadczenia majątkowe	X		
6	System Informacji Oświatowej		X	SIO
7	Ewidencja spełniania obowiązku nauki przez młodzież w wieku 16-18 lat	X		
8	Ewidencja osób ubiegających się o stypendia i zasiłki szkolne	X		
9	Ewidencja osób ubiegających się o dofinansowanie z ZFŚS	X		
10	Ewidencja radnych Rady Gminy Bielsk Podlaski	X		
11	Ewidencja sołtysów z terenu Gminy Bielsk Podlaski	X		
12	Ewidencja podmiotów ubiegających się o refundację kosztów przygotowania zawodowego młodocianych pracowników	X		
13	Ewidencja umów w sprawie zwrotu kosztów dowożenia dziecka (ucznia) niepełnosprawnego do szkoły (przedszkola)	X		
14	Akta osobowe	X	X	Kadry i Płace
15	Rejestr zwolnień lekarskich	X		
16	Ewidencja emerytów i rencistów urzędu	X		
17	Rejestr wypadków przy pracy	X		

18	Rejestr wypadków w drodze do pracy lub z pracy	X		
19	Rejestr korespondencji przychodzącej i wychodzącej	X	X	SmartDoc
20	Rejestr skarg i wniosków	X		
21	Rejestr delegacji służbowych	X		
22	Płace	X	X	Kadry i Płace GROSZEK
23	Ewidencja podatków rolnych	X	X	FISKUS
24	Ewidencja podatków od nieruchomości	X	X	FISKUS
25	Ewidencja podatków leśnych	X	X	FISKUS
26	Ewidencja środków transportowych	X	X	FISKUS
27	Opłata eksploatacyjna	X		
28	Rejestr wydanych zaświadczeń	X		
29	Ewidencja osób otrzymujących zwrot podatku akcyzowego	X		
30	Ewidencja tytułów i upomnień wykonawczych	X	X	
31	Rejestr kwitariuszy	X		
32	Ewidencja wniosków o wydanie zezwolenia na usunięcie drzew lub krzewów	X	X	P.Z.
33	Rejestr zezwoleń na sprzedaż napojów alkoholowych	X		
34	Rejestr wydanych decyzji o warunkach zabudowy i zagospodarowania terenu	X		
35	Rejestr rozdysponowania mienia komunalnego	X		
36	Rejestr numeracji porządkowej nieruchomości (ewidencja miejscowości, ulic i adresów)	X	X	e-mapa
37	Rejestr wpisów do ewidencji działalności gospodarczej	X	X	CEIDG
38	Rejestr decyzji o lokalizacji inwestycji celu publicznego	X		

39	Ewidencja dodatków mieszkaniowych	X		
40	Rejestr decyzji na zajęcie pasa drogowego i uzgodnień drogowych	X		
41	Rejestr użytkowników sieci wodno - kanalizacyjnej	X	X	WODA
42	Ewidencja użytkowników wieczystych gruntów	X		
43	Ewidencja gospodarowania odpadami	X	X	FISKUS
44	Ewidencja decyzji o podział nieruchomości	X		
45	Ewidencja umów najmu lokali użytkowych	X		
46	Ewidencja osób ubiegających się o dofinansowanie na usuwanie azbestu	X		
47	Rejestr wydanych decyzji środowiskowych	X		
48	Ewidencja przydomowych oczyszczalni ścieków i zbiorników szczelnych	X		
49	Ewidencja zbiorników bezodpływowych	X		
50	Ewidencja osób podlegających stawiennictwu do kwalifikacji wojskowej	X		
51	Ochotnicze Straże Pożarne	X		
52	Obrona RZECZYPOSPOLITEJ POLSKIEJ oraz obrona cywilna	X		
53	Wnioski Gminnej Komisji Rozwiązywania Problemów Alkoholowych	X		

### Opis struktury zbiorów danych osobowych

Lp.	Nazwa zbioru	Opis zbioru
1	Rejestr mieszkańców	Nazwisko, imiona, nazwisko rodowe, imiona i nazwiska rodowe rodziców, data urodzenia, miejsce urodzenia, kraj urodzenia, stan cywilny, oznaczenie aktu urodzenia i urzędu stanu cywilnego, w którym został on sporządzony, płeć, numer PESEL, obywatelstwo albo status bezpaństwowca, imię i nazwisko rodowe oraz numer PESEL małżonka, jeżeli został mu nadany, data zawarcia związku małżeńskiego, oznaczenie aktu małżeństwa i urzędu stanu cywilnego, data rozwiązania związku małżeńskiego, sygnatura akt i oznaczenie sądu, który rozwiązał małżeństwo, sygnatura akt i oznaczenie sądu, który ustalił nieistnienie małżeństwa, sygnatura akt i oznaczenie sądu, który unieważnił małżeństwo, data zgonu małżonka albo data znalezienia jego zwłok, oznaczenie jego aktu zgonu i urzędu stanu cywilnego, w którym ten akt został sporządzony, adres i data zameldowania na pobyt stały, kraj i miejsce zamieszkania, kraj poprzedniego miejsca zamieszkania, data wymeldowania z pobytu stałego, adres i data zameldowania na pobyt czasowy oraz data upływu deklarowanego terminu pobytu, data wymeldowania z miejsca pobytu czasowego, data wyjazdu poza granice RP trwającego dłużej niż 6 miesięcy i wskazanie kraju wyjazdu, data powrotu z wyjazdu poza granice RP trwającego dłużej niż 6 miesięcy, seria, numer i data ważności ostatniego wydanego dowodu osobistego obywatela polskiego oraz oznaczenie organu wydającego dokument, seria, numer i data ważności ostatniego wydanego paszportu obywatela polskiego, data zgonu albo data znalezienia zwłok, numer aktu zgonu i oznaczenie urzędu stanu cywilnego, w którym ten akt został sporządzony.
2	Rejestr zamieszkania cudzoziemców	Nazwisko i imię, data urodzenia, kraj urodzenia, płeć, numer PESEL, obywatelstwo albo status bezpaństwowca, data i adres zameldowania na pobyt stały, kraj miejsca zamieszkania, kraj poprzedniego miejsca zamieszkania, data wymeldowania z miejsca pobytu stałego, seria, numer i data ważności dokumentu podróży cudzoziemca.
3	Rejestr wydanych i unieważnionych dowodów osobistych	Nazwisko i imiona, nazwisko rodowe, imiona i nazwiska rodowe rodziców, data i miejsce urodzenia, PESEL, płeć, obywatelstwo; adres zameldowania, wizerunek twarzy, data wystawienia dowodu osobistego, data wydania, data unieważnienia,

		przyczyna unieważnienia dowodu osobistego; seria i numer poprzedniego dowodu osobistego, oznaczenie organu wydającego dowód osobisty.
4	Rejestr wyborców	Nazwisko, imiona, imię ojca, data urodzenia, numer PESEL, adres zameldowania wyborcy, adres zamieszkania wyborcy.
5	Oświadczenia majątkowe	Nazwisko i imiona, nazwisko rodowe, data i miejsce urodzenia; adres zamieszkania, dane o stanie majątkowym Stanowisko lub funkcja osoby składającej oświadczenie dobra majątkowe, zobowiązania pieniężne; informacje dotyczące prowadzenia działalności gospodarczej, informacje zawarte w zeznaniu o wysokości osiągniętego dochodu (PIT).
6	System Informacji Oświatowej	Zakres gromadzonych danych na podst. art. 7 ustawy z dnia 5 kwietnia 2011 r. o systemie informacji oświatowej (Dz. U. z 2016 r. poz. 1927 z późn. zm.) stopień awansu zawodowego), Imię i nazwisko ucznia, PESEL (pomoc materialna), Imię i nazwisko nauczyciela, PESEL (stopień awansu zawodowego).
7	Ewidencja spełniania obowiązku nauki przez młodzież w wieku 16-18 lat	Imię i nazwisko, PESEL, adres zamieszkania, miejsce realizacji obowiązku szkolnego (nazwa szkoły); rok ukończenia szkoły, miejsce realizacji obowiązku nauki (nazwa szkoły).
8	Ewidencja osób ubiegających się o stypendia i zasiłki szkolne	Nazwisko i imiona ucznia, data i miejsce urodzenia, imiona rodziców, numer PESEL, adres zamieszkania, seria i numer dowodu osobistego, numer telefonu, miejsce nauki, informacje o szkole do której uczęszcza uczeń, nazwiska i imiona pozostałych członków rodziny, stopień pokrewieństwa, dochody członków rodziny, źródło dochodu, formy udzielania pomocy.
9	Ewidencja osób ubiegających się o dofinansowanie z ZFŚS	Nazwiska i imiona wnioskodawcy (emeryta, rencisty), adres zamieszkania lub pobytu, numer telefonu, informacje zawarte w zeznaniu składającego oświadczenie (małżonka) o wysokości osiągniętego dochodu (poniesionej straty) w roku podatkowym.
10	Ewidencja radnych Rady Gminy Bielsk Podlaski	Imię i nazwisko, data urodzenia, miejsce urodzenia; adres zamieszkania lub pobytu, numer PESEL, miejsce pracy, zawód, wykształcenie, seria i numer dowodu osobistego, numer telefonu, nr rachunku bankowego, adres poczty elektronicznej, wysokość diet radnych.
11	Ewidencja sołtysów z terenu Gminy Bielsk Podlaski	Imię i nazwisko; numer telefonu; adres zameldowania lub pobytu, nazwa sołectwa.
12	Ewidencja podmiotów ubiegających się o refundację kosztów przygotowania zawodowego młodocianych pracowników	Nazwa pracodawcy, nazwisko i imiona młodocianego, adres zamieszkania, okres przygotowania zawodowego, kwota refundacji i rok wypłaty.
13	Ewidencja umów w sprawie zwrotu kosztów dowożenia dziecka (ucznia) niepełnosprawnego do	Imię i nazwisko dziecka (ucznia), numer PESEL, imię i nazwisko rodziców (opiekunów), nr i seria dowodu osobistego, informacje dotyczące samochodu, którym jest dowożone dziecko (uczeń), miejsce uczęszczania do przedszkola (szkoły), nr telefonu, nr rachunku bankowego rodziców (opiekunów),

	szkoły (przedszkola)	informacje o niepełnosprawności dziecka (ucznia), kwota zwrotu kosztów przejazdu do przedszkola (szkoły).
14	Akta osobowe	Imię i nazwisko, numer PESEL, data urodzenia, miejsce urodzenia, adres zamieszkania, nr telefonu.
15	Rejestr zwolnień lekarskich	Imię i nazwisko, numer PESEL, okres zwolnienia.
16	Ewidencja emerytów i rencistów urzędu	Imię i nazwisko, data urodzenia, adres zamieszkania, nr telefonu, data rozwiązania umowy o pracę.
17	Rejestr wypadków przy pracy	Imię nazwisko, numer PESEL, adres zamieszkania, stanowisko pracy, miejsce i data wypadku, informacje dot. skutków wypadku dla poszkodowanego, liczba dni niezdolności do pracy.
18	Rejestr wypadków w drodze do pracy lub z pracy	Imię nazwisko, numer PESEL, adres zamieszkania, stanowisko pracy, miejsce i data wypadku, informacje dot. skutków wypadku dla poszkodowanego, liczba dni niezdolności do pracy.
19	Rejestr korespondencji przychodzącej i wychodzącej	Imię i nazwisko lub nazwa nadawcy, data urodzenia, PESEL, NIP, adres zameldowania, adres do korespondencji, numer działki, seria i numer dowodu osobistego, nr telefonu, adres e-mail data wysłania, data wpływu, znak pisma, informacja o sprawie, komu zlecono załatwienie.
20	Rejestr skarg i wniosków	Data wpływu, imię i nazwisko petenta, nazwa instytucji, redakcji, adres, przedmiot skargi, zażalenie i odwołania, data zlecenia załatwienia, komu zlecono załatwienie, data wysłania, sposób załatwienia, kogo zawiadomiono, uwagi.
21	Rejestr delegacji służbowych	Imię i nazwisko, data, miejsce i cel wyjazdu, środek lokomocji.
22	Płace	Nazwiska i imiona, nazwisko rodowe, data i miejsce urodzenia, imiona rodziców, adres zamieszkania lub pobytu, numer PESEL, NIP, seria i numer dowodu osobistego, numer telefonu, Nr rachunku bankowego.
23	Ewidencja podatków rolnych	Imię i nazwisko, imiona i nazwiska rodziców, data urodzenia, adres zameldowania lub pobytu, numer PESEL, NIP położenia i powierzchnia użytkowa nieruchomości, numery geodezyjne działek, numer telefonu.
24	Ewidencja podatków od nieruchomości	Imię i nazwisko, imiona i nazwiska rodziców, data urodzenia, adres zameldowania lub pobytu, numer PESEL, NIP, położenia i powierzchnia użytkowa nieruchomości, numery geodezyjne działek, powierzchnia domu, powierzchnia budynków gospodarczych, numer telefonu.
25	Ewidencja podatków leśnych	Imię i nazwisko, imiona i nazwiska rodziców, data urodzenia, adres zameldowania lub pobytu, numer PESEL, NIP, numery geodezyjne działek, powierzchnia domu, powierzchnia lasu, numer telefonu.
26	Ewidencja środków transportowych	Imię i nazwisko, data urodzenia, adres zameldowania lub pobytu, numer PESEL, NIP, nr rejestracyjny pojazdu, numer VIN.
27	Opłata eksploatacyjna	Imię i nazwisko, NIP, adres zameldowania, nr telefonu, nr działki z której wydobywana jest kopalina.
28	Rejestr wydanych zaświadczeń	Imię i nazwisko, numer PESEL, adres zameldowania, powierzchnia użytków rolnych, powierzchnia hektarów przeliczeniowych.
29	Ewidencja osób otrzymujących zwrot podatku akcyzowego	Imię i nazwisko, adres, numer PESEL, seria i numer dokumentu stwierdzającego tożsamość, użytki rolne, ilość zakupionego oleju, nr konta, nr telefonu.

30	Ewidencja tytułów i upomnień wykonawczych	Nazwiska i imiona, imiona rodziców, data urodzenia, numer PESEL, adres zameldowania lub pobytu, REGON, NIP.
31	Rejestr kwitariuszy	Imię i nazwisko, adres zameldowania lub pobytu,
32	Ewidencja wniosków o wydanie zezwolenia na usunięcie drzew lub krzewów	Imię, nazwisko, nr działki, adres zameldowania, adres do korespondencji, nr telefonu, nr księgi wieczystej, nr ewidencyjny działki.
33	Rejestr zezwoleń na sprzedaż napojów alkoholowych	Nazwiska i imiona, nazwa firmy, adres, tytuł prawny do lokalu stanowiącego punkt sprzedaży, nr telefonu, NIP.
34	Rejestr wydanych decyzji o warunkach zabudowy i zagospodarowania terenu	Imię i nazwisko, adres zamieszkania, adres do korespondencji; nr ewidencyjny działki, nr telefonu.
35	Rejestr rozdysponowania mienia komunalnego	Imię i nazwisko, adres zamieszkania, numer PESEL, nr działki ewidencyjnej, obręb ewidencyjny, powierzchnia użytków, okres dzierżawy, seria i numer dowodu osobistego.
36	Rejestr numeracji porządkowej nieruchomości (ewidencja miejscowości, ulic i adresów)	Imię i nazwisko, imiona rodziców, adres zamieszkania, nr geodezyjny nieruchomości, nr telefonu.
37	Rejestr wpisów do ewidencji działalności gospodarczej	Nazwisko i imiona, data i miejsce urodzenia, numer PESEL, NIP, REGON, adres zamieszkania lub pobytu, seria i numer dowodu osobistego, nr telefonu, adres e-mail, miejsce pracy, nr rachunku bankowego, dane o ubezpieczeniu, informacje o wspólności małżeńskiej, informacje o uczestnictwie w spółkach, nazwa firmy.
38	Rejestr decyzji o lokalizacji inwestycji celu publicznego	Nazwiska i imiona, adres zamieszkania lub pobytu, nr ewidencyjny działki, nr telefonu.
39	Ewidencja dodatków mieszkaniowych	Imiona i nazwiska, adres zamieszkania, nazwa i siedziba zarządcy domu, tytuł prawny do zajmowanego lokalu, seria i numer dowodu osobistego, nr telefonu, imiona i nazwiska oraz stopień pokrewieństwa osób zamieszkujących w gospodarstwie domowym.
40	Rejestr decyzji na zajęcie pasa drogowego i uzgodnień drogowych	Imię i nazwisko wnioskodawcy robot, adres zamieszkania lub pobytu, nr telefonu, nr drogi, imię i nazwisko kierownika z ramienia wykonawcy, imię i nazwisko oraz nr telefonu kierownika budowy, seria i numer dowodu osobistego.
41	Rejestr użytkowników sieci wodno - kanalizacyjnej	Pełna nazwa firmy, adres siedziby, imię i nazwisko, adres zameldowania lub pobytu, numer PESEL, nr telefonu, lokalizacja nieruchomości (gmina, numer budynku, miejscowość, numer działki).
42	Ewidencja użytkowników wieczystych gruntów	Imię i nazwisko, adres zameldowania lub pobytu, nr działki ewidencyjnej, numer PESEL, seria i numer dowodu osobistego.
43	Ewidencja gospodarowania odpadami	Nazwiska i imiona, imiona rodziców; adres zameldowania, adres do korespondencji, numer PESEL, nr telefonu, numer ewidencyjny działki, adres e-mail; adres nieruchomości na której



		powstają odpady, liczba osób zamieszkałych pod danym adresem; wysokość miesięcznej opłaty za gospodarowanie odpadami komunalnymi.
44	Ewidencja decyzji o podział nieruchomości	Imiona i nazwiska, adres zameldowania lub pobytu, nr telefonu, nr ewidencyjny działki.
45	Ewidencja umów najmu lokali użytkowych	Imiona i nazwiska, adres zameldowania lub pobytu, nr telefonu, nr ewidencyjny działki.
46	Ewidencja osób ubiegających się o dofinansowanie na usuwanie azbestu	Adres zameldowania lub pobytu, NIP, numer PESEL, nr telefonu, informacje o tytule prawnym do nieruchomości, nr geodezyjny działki.
47	Rejestr wydanych decyzji środowiskowych	Nazwiska i imiona, adres zameldowania lub pobytu, nr telefonu, numer PESEL, NIP.
48	Ewidencja przydomowych oczyszczalni ścieków i zbiorników szczelnych	Nazwiska i imiona, adres zameldowania, adres do korespondencji, numer PESEL, nr telefonu, nr ewidencyjny działki.
49	Ewidencja zbiorników bezodpływowych	Imię i nazwisko, adres posesji na której powstają nieczystości, nr telefonu, liczba osób zamieszkujących pod wskazanym adresem, dane firmy odbierającej nieczystości.
50	Ewidencja osób podlegających stawiennictwu do kwalifikacji wojskowej	Nazwiska i imiona, płeć, data i miejsce urodzenia, adres zamieszkania lub pobytu, numer PESEL, seria i numer dowodu osobistego, nr z pozycji książki orzeczeń lekarskich.
51	Ochotnicze Straże Pożarne	Imię i nazwisko, adres zamieszkania, nr telefonu.
52	Obrona RZECZYPOSPOLITEJ POLSKIEJ oraz obrona cywilna	Imię i nazwisko, imiona i nazwiska rodziców, data urodzenia, miejsce urodzenia, adres zameldowania lub pobytu, PESEL, nr telefonu, zawód, wykształcenie, seria i numer dowodu osobistego.
53	Wnioski Gminnej Komisji Rozwiązywania Problemów Alkoholowych	Nazwiska i imiona, adres zameldowania lub pobytu, numer telefonu komórkowego, numer PESEL, Informacje o pobycie w Izbie Wytrzeźwień, Informacje o interwencji Policji, stan rodziny, źródło utrzymania, opinie biegłych.

W Urzędzie Gminy Bielsk Podlaski nie istnieją relacje pomiędzy różnymi systemami informatycznymi

**Raport**  
**z naruszenia bezpieczeństwa danych osobowych**  
**w Urzędzie Gminy Bielsk Podlaski**

1. Data: ..... Godzina .....  
(dd mm rrrr) (gg: mm)

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. Przyczyny wystąpienia zdarzenia:

.....  
.....  
.....

6. Podjęte działania

.....  
.....  
.....

7. Postępowania wyjaśniające:

.....  
.....  
.....

.....

(data, podpis Administratora Bezpieczeństwa Informacji)

Załącznik Nr 9  
do Polityki Bezpieczeństwa Informacji  
w Urzędzie Gminy Bielsk Podlaski

**Wykaz osób, które zostały zapoznane z „Polityką Bezpieczeństwa  
Informacji w Urzędzie Gminy Bielsk Podlaski” oraz „Instrukcją  
zarządzania systemem informatycznym służącym do przetwarzania  
danych osobowych w Urzędzie Gminy Bielsk Podlaski”**

<b>Lp.</b>	<b>Imię i nazwisko</b>	<b>Stanowisko</b>	<b>Data</b>	<b>Podpis</b>
1				
2				
3				
4				

## **Instrukcja zarządzania systemami informatycznymi służącym do przetwarzania danych osobowych w Urzędzie Gminy Bielsk Podlaski**

### **§1**

#### **Wprowadzenie**

1. Niniejsza instrukcja określa zasady eksploatacji i zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Gminy Bielsk Podlaski.
2. Zasady opisane w niniejszym dokumencie są zgodne z obowiązującymi wymogami prawnymi, w szczególności:
  - a) Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2016 r. poz 922, ze zm.),
  - b) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr. 100, poz. 1024).

### **§2**

#### **Definicje**

Definicje stosowanych pojęć w Instrukcja zarządzania systemami informatycznymi oznaczają:

- 1) zbiór danych osobowych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
- 2) Miejsce Przetwarzania Danych (MPD)** – pomieszczenia Urzędu Gminy Bielsk Podlaski, ul. Mickiewicza 46, 17-100 Bielsk Podlaski, w których są przetwarzane dane osobowe.
- 3) Administrator Danych Osobowych** – zadania Administratora Danych Osobowych wykonuje Wójt Gminy Bielsk Podlaski.

- 4) **Administrator Bezpieczeństwa Informacji** – osoba wyznaczona przez Administratora Danych Osobowych, odpowiedzialna za bezpieczeństwo danych osobowych przetwarzanych we wskazanych systemach informatycznych.
- 5) **Administrator Systemu Informatycznego** – osoba odpowiedzialna za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego do przetwarzania danych osobowych w MPD (może to być administrator sieci lokalnej, systemu operacyjnego, bazy danych itp.).
- 6) **system informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
- 7) **stacja robocza** – stacjonarny lub przenośny komputer wchodzący w skład systemu informatycznego umożliwiający użytkownikom systemu dostęp do danych osobowych znajdujących się w systemie.
- 8) **Bezpieczeństwo Systemu Informatycznego** – wdrożenie przez Administratora Danych Osobowych lub osobę przez niego uprawnioną środków organizacyjnych i technicznych w celu zabezpieczenia oraz ochrony danych przed dostępem, modyfikacją, ujawnieniem, pozyskaniem lub zniszczeniem.
- 9) **przetwarzanie danych osobowych** - wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie.
- 10) **osoba upoważniona** – osoba posiadająca upoważnienie wydane przez ADO (lub osobę uprawnioną przez niego) i dopuszczona, jako użytkownik przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej w zakresie wskazanym w upoważnieniu.
- 11) **użytkownik systemu** – osoba posiadająca uprawnienia do przetwarzania danych osobowych w systemie informatycznym.
- 12) **osoba uprawniona** – osoba posiadająca upoważnienie wydane przez ADO do wykonywania w jego imieniu określonych czynności.

### §3

#### **Procedury nadawania i zmiany upoważnień do przetwarzania danych**

1. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych jest zobowiązany do zapoznania się:
  - a) Ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych,
  - b) Polityką Bezpieczeństwa Informacji w Urzędzie Gminy,

b) Instrukcją zarządzania systemami informatycznymi w Urzędzie Gminy.

2. Podstawą do nadawania uprawnień do przetwarzania danych osobowych w systemie informatycznym Urzędu jest upoważnienie do przetwarzania danych osobowych. Upoważnienie wydawane jest przez Administratora Danych Osobowych.
3. Upoważnienie wydawane jest na wniosek przełożonego danego pracownika, a w przypadku osoby nie będącej pracownikiem Urzędu na wniosek pracownika Urzędu koordynującego działania osoby, dla której upoważnienie jest wydawane.
4. Oryginał upoważnienia zostaje przekazany pracownikowi za potwierdzeniem odbioru, kopia zaś zostaje dołączona do akt osobowych pracownika oraz przekazana do wiadomości przełożonego pracownika.
5. Przyznanie uprawnienia w zakresie dostępu do systemu informatycznego polega na wprowadzeniu do systemu dla każdego użytkownika unikalnego identyfikatora oraz hasła. Za przydzielenie i wygenerowanie identyfikatora i hasła użytkownikowi, który pierwszy raz będzie korzystał z systemu informatycznego, odpowiada administrator odpowiedniego systemu informatycznego (czynności te wykonuje na pisemny lub przesłany drogą elektroniczną wniosek ABI).
6. Pracownik ma prawo do wykonywania tylko tych czynności do których został upoważniony.
7. Pracownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu.
8. Wszelkie przekroczenia lub próby przekroczenia przyznaných upoważnień traktowane będą jako naruszenie podstawowych obowiązków pracowniczych.
9. Identyfikator osoby która utraciła uprawnienia dostępu do danych osobowych należy niezwłocznie wyrejestrować z systemu informatycznego oraz unieważnić jej hasło. Wyrejestrowanie użytkownika z systemu informatycznego może nastąpić na wniosek administratora danych osobowych, przełożonego użytkownika lub koordynatora zadania, na rzecz którego były wykonywane czynności związane z przetwarzaniem danych osobowych. Pisemny wniosek o wyrejestrowanie użytkownika z systemu należy złożyć do ABI.
10. Administrator Bezpieczeństwa Informacji prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych. Każda zmiana w zakresie informacji zawartych w ewidencji podlega niezwłocznemu odnotowaniu w ewidencji.

## §4

### **Zasady posługiwania się hasłami**

1. Bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym może nastąpić wyłącznie po wprowadzeniu identyfikatora i hasła.
2. Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi. Użytkownik odpowiedzialny jest za wszystkie czynności wykonane przy użyciu identyfikatora, którym się posługuje lub posługiwał.
3. Identyfikator wpisuje się do ewidencji (**Załącznik nr do Instrukcji zarządzania systemami informatycznymi**), prowadzonej przez administratora bezpieczeństwa informacji, wraz z imieniem i nazwiskiem użytkownika oraz nazwami systemów informatycznych, do których użytkownik uzyskał dostęp i wprowadzony jest przez ASI do właściwych systemów.
4. Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego nie może być przydzielony innej osobie.
5. Hasło nie powinno zawierać mniej niż 8 znaków, oraz nie może być takie samo jak identyfikator.
6. Użytkownikowi nie wolno zapisywać haseł na papierze.
7. Pracownicy są odpowiedzialni za zachowanie poufności swoich haseł, i takie wprowadzanie do komputera by uniemożliwić innym osobom jego poznanie.
8. W sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony należy natychmiast je zmienić.
9. System informatyczny wyposażony jest w mechanizm wymuszający zmianę hasła po upływie 30 dni od dnia ostatniej zmiany hasła

## §5

### **Procedura odbierania uprawnień do przetwarzania danych w systemie informatycznym**

1. W przypadku konieczności odebrania lub zmiany zakresu upoważnienia – w związku ze zmianą zakresu obowiązków służbowych pracownika lub zakończeniem pracy – jego przełożony wnioskuję do ADO o wykonanie powyższej czynności. ADO dokonuje odebrania lub zamiany zakresu upoważnienia, pracownik informatyki zaś dokonuje odebrania lub zamiany zakresu uprawnień w systemie informatycznym.

## §6

### **Procedury rozpoczęcia, zawieszenia i zakończenia pracy**

1. Przed rozpoczęciem pracy każdy pracownik obowiązany jest do zwrócenia bacznej uwagi, czy nie wystąpiły symptomy mogące świadczyć o naruszeniu ochrony danych osobowych.
2. Przed rozpoczęciem pracy w systemie komputerowym należy zalogować się do systemu przy użyciu indywidualnego identyfikatora i hasła.
3. Zmianę użytkownika stacji roboczej każdorazowo musi poprzedzać wylogowanie się poprzedniego użytkownika. Niedopuszczalne jest, aby dwóch lub większa ilość użytkowników wykorzystywała wspólnie jedno konto użytkownika. W przypadku, gdy przerwa w pracy na stacji roboczej trwa dłużej niż 60 minut użytkownik zobowiązany jest wylogować się z aplikacji systemu stacji roboczej, na której pracuje oraz sprawdzić czy nie zostały pozostawione bez zamknięcia nośniki informacji zawierające dane osobowe.
4. Po opuszczeniu stanowiska pracy na odległość uniemożliwiającą jego obserwację należy wylogować się z systemu (jeżeli istnieje taka konieczność wyjść z programu) lub uruchomić wygaszacz ekranu zabezpieczony hasłem.
5. Przed wyłączeniem komputera należy zakończyć pracę wszystkich uruchomionych programów.

## **§7**

### **Zasady instalacji oprogramowania**

1. Instalacji oprogramowania lub aktualizacji dokonuje Administrator Bezpieczeństwa Informacji.
2. Na wszystkich komputerach Urzędu Gminy Bielsk Podlaski dopuszcza się instalację tylko legalnego licencjowanego oprogramowania.
3. Zabrania się instalowania oprogramowania bez zgody Administratora Bezpieczeństwa Informacji.

## **§8**

### **Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania**

Dane osobowe przetwarzane w systemie informatycznym podlegają zabezpieczeniu poprzez tworzenie kopii zapasowych. Za proces tworzenia kopii zapasowych odpowiada ASI lub osoba specjalnie do tego celu wyznaczona. Kopie zapasowe przechowywane w systemie informatycznym przetwarzającym dane osobowe tworzone są w :

1. Sposób automatyczny poprzez specjalnie wydzielony do tego serwer z oprogramowaniem, tworzący samodzielne kopie zapasowe danych aplikacji oraz dokumentów użytkowników systemu informatycznego.



2. Sposób nieautomatyczny poprzez tworzenie kopii zapasowych danych aplikacji na nośnikach wymienionych w cyklach co tygodniowych i miesięcznych, kopia przechowywana jest w zamkniętej szafie.
3. Nośniki kopii zapasowych, które zostały wycofane z użycia, jeżeli jest to możliwe, należy pozbawić zapisanych danych za pomocą specjalnego oprogramowania do bezpiecznego usuwania zapisanych danych. W przeciwnym wypadku podlegają fizycznemu zniszczeniu z wykorzystaniem metod adekwatnych do typu nośnika, w sposób uniemożliwiający odczytanie zapisanych na nich danych.

## **§9**

### **Zasady dokonywania napraw**

1. Dokonywanie napraw, przeglądów i konserwacji systemu przez pracowników serwisu mogą odbywać się jedynie w obecności Administratora Bezpieczeństwa Informacji lub osoby przez niego upoważnionej.
2. Przeglądów należy dokonywać nie rzadziej niż raz na kwartał.
3. Uszkodzone nośniki magnetyczne lub inne zawierające dane osobowe nie mogą być użytkowane. Muszą być odpowiednio zabezpieczone przed nieuprawnionym udostępnieniem, a następnie zniszczone lub naprawione pod nadzorem osoby upoważnionej przez Administratora Danych.
4. Zabronione jest dokonywanie napraw sprzętu komputerowego samodzielnie przez pracowników urzędu.

## **§10**

### **Sposób i miejsce przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz wydruków**

1. W przypadku potrzeby przechowywania wydruków zawierających dane osobowe należy je przechowywać w miejscu uniemożliwiającym bezpośredni dostęp osobom niepowołanym.
2. Dane osobowe mogą być zapisywane na nośnikach przenośnych w przypadku tworzenia kopii zapasowych lub gdy istnieje konieczność przeniesienia tych danych w postaci elektronicznej, a wykorzystanie do tego celu sieci informatycznej jest nieuzasadnione, niemożliwe lub zbyt niebezpieczne
3. Pomieszczenia, w którym przechowywane są wydruki muszą być należycie zabezpieczone.
4. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

## **§11**

### **Profilaktyka antywirusowa**

1. Za ochronę antywirusową odpowiedzialny jest Administrator Bezpieczeństwa Informacji.
2. Każdy użytkownik komputera w urzędzie zobowiązany jest do używania w pracy dyskietek i płyt CD zakupionych przez urząd (nie prywatnych).
3. Informacje i dane przechowywane na dyskietkach i płytach CD mogą mieć wyłącznie charakter związany z pracą.
4. Każdy komputer minimum raz w tygodniu powinien zostać sprawdzony aktualną wersją programu antywirusowego.
5. W przypadku wykrycia wirusa choćby na jednym komputerze, należy sprawdzić wszystkie stacje robocze w Urzędzie.

Załącznik Nr 1  
do Instrukcji zarządzania systemami informatycznymi  
służącym do przetwarzania danych osobowych  
w Urzędzie Gminy Bielsk Podlaski

## WYKAZ SYSTEMÓW INFORMATYCZNYCH WRAZ Z LOGINAMI

<b>Numer pokoju</b>	<b>Imię i nazwisko użytkownika</b>	<b>Nazwa systemu informatycznego (nazwa programu)</b>	<b>Login</b>