ZARZĄDZENIE NR 0152/61/2009
WÓJTA GMINY BOJSZOWY
z dnia 12.02.2009r.

w sprawie: polityki bezpieczeństwa ochrony danych osobowych i instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Gminy Bojszowy.

Na podstawie art. 30 ust. 1 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (tekst jednolity Dz. U. Nr 142, poz. 1591 z 2001 r. z późniejszymi zmianami) w związku z art. 36 ust. 1 i 2 ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 roku (tekst jednolity Dz. U. Nr 101, poz. 926 z 2002 r. z późniejszymi zmianami oraz § 3 i § 4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024)

postanawiam:

1. Przyjąć politykę bezpieczeństwa ochrony danych osobowych w brzmieniu stanowiącym załącznik nr 1 do niniejszego zarządzenia.
2. Przyjąć instrukcję zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Gminy Bojszowy, stanowiącą załącznik nr 2 do niniejszego zarządzenia.
3. Zobowiązać administratora danych do:
   - udzielania upoważnień dopuszczających pracowników Urzędu Gminy do przetwarzania danych osobowych i włączenia ich do dokumentacji personalnej osób przetwarzających dane osobowe, (wg załącznika nr 3) ,
   - prowadzenia ewidencji udzielonych upoważnień do przetwarzania danych osobowych zgodnie z załącznikiem nr 4,
   - prowadzenia ewidencji osób upoważnionych do systemów informatycznych przetwarzających dane osobowe zgodnie z załącznikiem nr 5,
   - realizacji innych zadań nałożonych na administratora przez ustawę o ochronie danych osobowych.
4. Utrzymać w mocy powierzenie ABI panu Andrzejowi Moisa.
5. Pozostawić upoważnienie do wykonywania niektórych czynności Administratora Danych Pani Patrycji Czarnynoga.
6. Traci moc Zarządzenie 0151/54/2004 Wójta Gminy Bojszowy z dnia 20.09.2004r. w sprawie *polityki bezpieczeństwa ochrony danych osobowych i instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Gminy Bojszowy*
7. Zarządzenie wchodzi w życie z dniem podpisania.

Zał. Nr 1
do Zarządzenia Nr 0152/61/2009
Z dnia 12.02.2009r.

Polityka bezpieczeństwa

SPIS TREŚCI

I. Wstęp

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

- sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu, jak np. pożar, zalanie pomieszczeń, katastrofa budowlana, napad, kradzież, włamanie, działania terrorystyczne, niepożądana ingerencja ekipy remontowej;
- niewłaściwe parametry środowiska, zakłócające pracę urządzeń komputerowych (nadmierna wilgotność lub bardzo wysoka temperatura, oddziaływanie pola elektromagnetycznego i inne);
- awarie sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne naruszenia ochrony danych, niewłaściwe działanie serwisantów, w tym pozostawienie serwisantów bez nadzoru, a także przyzwolenie na naprawę sprzętu zawierającego dane poza siedzibą administratora danych;
- podejmowanie pracy w systemie z przełamaniem lub zaniechaniem stosowania procedur ochrony danych, np. praca osoby, która nie jest upoważniona do przetwarzania, próby stosowania nie swojego hasła i identyfikatora przez osoby upoważnione;
- celowe lub przypadkowe rozproszenie danych w internecie z ominięciem zabezpieczeń systemu lub wykorzystaniem błędów systemu informatycznego administratora danych;
- ataki z internetu;
- naruszenia zasad i procedur określonych w dokumentacji z zakresu ochrony danych osobowych przez osoby upoważnione do przetwarzania danych osobowych, związane z nieprzestrzeganiem procedur ochrony danych, w tym zwłaszcza:
  - niezgodne z procedurami zakończenie pracy lub opuszczenie stanowiska pracy (nieprawidłowe wyłączenie komputera, niezablokowanie wyświetlenia treści pracy na ekranie komputera przed tymczasowym opuszczeniem stanowiska pracy, pozostawienie po zakończeniu pracy nieschowanych do zamykanych na klucz szaf dokumentów zawierających dane osobowe, niezamknięcie na klucz pokoju po jego opuszczeniu i odniesieniu klucza do gabloty lub przekazanie bezpośrednio osobie sprzątającej pomieszczenie),
  - naruszenie bezpieczeństwa danych przez nieautoryzowane ich przetwarzanie,
  - ujawnienie osobom nieupoważnionym procedur ochrony danych stosowanych u administratora danych,
  - ujawnienie osobom nieupoważnionym danych przetwarzanych przez administratora danych, w tym również nieumyślne ujawnienie danych osobom postronnym, przebywającym bez nadzoru lub niedostatecznie nadzorowanym w pomieszczeniach administratora danych,
  - niewykonywanie stosownych kopii zapasowych,
  - przetwarzanie danych osobowych w celach prywatnych,
  - wprowadzanie zmian do systemu informatycznego administratora danych i instalowanie programów bez zgody administratora systemu.

II. Postanowienia ogólne

1. Definicje

Ilekroć w polityce bezpieczeństwa jest mowa o:

- **administratorze bezpieczeństwa informacji** – rozumie się przez to osobę, której administrator danych powierzył pełnienie obowiązków administratora bezpieczeństwa informacji – Andrzej Moisa,
- **administratorze danych** – Wójt Gminy Bojszowy,
- **osoba upoważniona prze Administratora Danych** – osoba upoważniona do wykonywania niektórych czynności w imieniu Administratora Danych
- **administratorze systemu** – informatyka,
- **haśle** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi,
- **identyfikatorze** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
- **integralności danych** – rozumie się przez to właściwość zapewniającą, że dane osobowe nie

zostały zmienione lub zniszczone w sposób nieautoryzowany,

- **odbiorcy danych** – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:
  - osoby, której dane dotyczą,
  - osoby upoważnionej do przetwarzania danych,
  - przedstawiciela, o którym mowa w art. 31a ustawy,
  - podmiotu, o którym mowa w art. 31 ustawy,
  - organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem,
- **osobie upoważnionej do przetwarzania danych osobowych** – rozumie się przez to osobę, która upoważniona została do przetwarzania danych osobowych przez Wójta Gminy na piśmie,
- **poufności danych** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom,
- **przetwarzającym** – rozumie się przez to podmiot, któremu zostało powierzone przetwarzanie danych osobowych na podstawie umowy zawieranej zgodnie z art. 31 ustawy,
- **raporcie** – rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych,
- **rozliczalności** – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,
- **rozporządzeniu** – rozumie się przez to rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (DzU nr 100, poz. 1024),
- **sieci publicznej** – rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 22 ustawy z dnia 21 lipca 2000 r. – Prawo telekomunikacyjne (DzU nr 73, poz. 852 ze zm.),
- **sieci telekomunikacyjnej** – rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 23 ustawy z dnia 21 lipca 2000 r. – Prawo telekomunikacyjne,
- **serwisancie** – rozumie się przez to firmę lub pracownika firmy zajmującej się sprzedażą, instalacją, naprawą i konserwacją sprzętu komputerowego,
- **systemie informatycznym administratora danych** – rozumie się przez to sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów procedur przetwarzania informacji i narzędzi programowych; w systemie tym pracuje co najmniej jeden komputer centralny i system ten tworzy sieć teleinformatyczną administratora danych,
- **teletransmisji** – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej,
- **ustawie** – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. DzU z 2002 r. nr 101, poz. 926 ze zm.),
- **uwierzytelnianiu** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu,
- **użytkowniku** – rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych, której nadano identyfikator i przyznano hasło.

2. Cel

Wdrożenie polityki bezpieczeństwa u administratora danych ma na celu zabezpieczenie przetwarzanych przez niego danych osobowych, w tym danych przetwarzanych w systemie informatycznym administratora danych i poza nim, poprzez wykonanie obowiązków wynikających z ustawy i rozporządzenia.

W związku z przetwarzaniem danych wrażliwych, oraz podłączeniem systemów do sieci publicznej za pomocą DSL dostarczonego przez TP SA niniejsza polityka bezpieczeństwa służy zapewnieniu wysokiego poziomu bezpieczeństwa danych w rozumieniu § 6 rozporządzenia. Niniejszy dokument opisuje niezbędny do uzyskania tego bezpieczeństwa zbiór procedur i zasad dotyczących przetwarzania danych osobowych oraz ich zabezpieczenia.

3. Zakres stosowania

a) Niniejsza polityka bezpieczeństwa dotyczy zarówno danych osobowych przetwarzanych w sposób tradycyjny w księgach, wykazach i innych zbiorach ewidencyjnych, jak i w systemach informatycznych.

b) Procedury i zasady określone w niniejszym dokumencie stosuje się do wszystkich osób upoważnionych do przetwarzania danych osobowych, zarówno zatrudnionych, jak i innych, np. wolontariuszy, stażystów, pracowników na zlecenie, praktykantów.

III. Organizacja przetwarzania danych osobowych

1. Administrator danych osobowych

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

1. podejmuje decyzje o celach i środkach przetwarzania danych osobowych z uwzględnieniem przede wszystkim zmian w obowiązującym prawie, organizacji administratora danych oraz technik zabezpieczenia danych osobowych;
2. upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym zakresowi jej obowiązków;
3. wyznacza administratora bezpieczeństwa informacji oraz określa zakres jego zadań i czynności;
4. wyznacza pracownika Referatu organizacyjnego – osoba upoważniona przez Wójta jako pracownika właściwego do prowadzenia ewidencji osób upoważnionych oraz prowadzenia procedur związanych z rejestracją zbiorów w GIODO pozostałej dokumentacji z zakresu ochrony danych,
5. zleca kierownikowi działu organizacyjnego, by we współpracy z administratorem systemu oraz administratorem bezpieczeństwa informacji zapewnił użytkownikom odpowiednie stanowiska pracy umożliwiające bezpieczne przetwarzanie danych;
6. podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur bezpiecznego przetwarzania danych osobowych.

2. Administrator bezpieczeństwa informacji

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

1. sprawuje nadzór nad wdrożeniem stosownych środków fizycznych, a także organizacyjnych i technicznych – w celu zapewnienia bezpieczeństwa danych,
2. sprawuje nadzór nad funkcjonowaniem systemu zabezpieczeń, w tym także nad prowadzeniem ewidencji z zakresu ochrony danych osobowych,
3. prowadzi w uzgodnieniu z osoba upoważnioną przez wójta aktualizuję dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych,
4. podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia systemu informatycznego,
5. przygotowuje materiały szkoleniowe z zakresu ochrony danych osobowych i prowadzi szkolenia osób upoważnianych do przetwarzania danych osobowych,
6. w porozumieniu z administratorem danych osobowych oraz Sekretarzem Gminy na czas nieobecności dłuższej niż 21 dni (np. choroba) wyznacza swojego zastępcę, którego należy powołać Zarządzeniem.

3. Osoba upoważniona przez administratora danych

a) nadzoruje udostępnianie danych osobowych odbiorcom danych i innym podmiotom,
b) przygotowuje wnioski zgłoszeń rejestracyjnych i aktualizacyjnych zbiorów danych oraz prowadzi inną korespondencję z Generalnym Inspektorem Ochrony Danych Osobowych,
c) uczestniczy w przygotowaniu wzorów dokumentów dotyczących udostępniania danych osobowych (podstawy prawne, odmowa udostępnienia) przygotowywanych przez komórki organizacyjne administratora danych,
d) Określa budynki, pomieszczenia lub części pomieszczeń, tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego.
e) Opracowuje instrukcję w uzgodnieniu z ABI, określającą sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji i przedkłada Administratorowi Danych do zatwierdzenia..
f) Prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych
g) Organizuje szkolenia mające na celu zaznajomienie każdej osoby przetwarzającej dane osobowe z przepisami dotyczącymi ich ochrony (Informuje o zmian w przepisach obowiązujących)
h) Odpowiada za to by zakres czynności osoby zatrudnionej przy przetwarzania danych osobowych określał odpowiedzialność tej osoby za:

a) ochronę danych przed niepowołanym dostępem,
b) nieuzasadnioną modyfikację lub zniszczenie danych,
c) nielegalne ujawnienie danych.

4. Administrator systemu

Administrator systemu realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym administratora danych, w tym zwłaszcza:

1. zarządza systemem informatycznym, w którym przetwarzane są dane osobowe, posługując się hasłem dostępu do wszystkich stacji roboczych z pozycji administratora,
2. przeciwdziała dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe,
3. na wniosek kierownika odpowiedniego referatu przydziela każdemu użytkownikowi identyfikator oraz hasło do systemu informatycznego oraz dokonuje ewentualnych modyfikacji uprawnień, a także usuwa konta użytkowników zgodnie z zasadami określonymi w instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
4. nadzoruje działanie mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych,
5. podejmuje działania w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego,
6. wyrejestrowuje użytkowników na polecenie administratora danych lub kierownika odpowiedniego referatu,
7. zmienia w poszczególnych stacjach roboczych hasła dostępu, ujawniając je wyłącznie danemu użytkownikowi oraz, w razie potrzeby, administratorowi bezpieczeństwa informacji lub administratorowi danych,
8. w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informuje ABI o naruszeniu i współdziała z nim przy usuwaniu skutków naruszenia,
9. prowadzi dokumentację naruszeń bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym,
10. sprawuje nadzór nad wykonywaniem napraw, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe, nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego,
11. podejmuje działania służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji.

5. Osoba upoważniona do przetwarzania danych osobowych

Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana przestrzegać następujących zasad:

1. może przetwarzać dane osobowe wyłącznie w zakresie ustalonym indywidualnie przez administratora danych w upoważnieniu oraz w powierzonym zakresie czynności lub czynności wynikających z zawartej umowy i tylko w celu wykonywania nałożonych na nią obowiązków. Dostępu do danych zgromadzonych osobowych w systemach możliwy jest po przydzieleniu niepowtarzalnego identyfikatora użytkownika, niezbędnego do rozpoczęcia pracy w systemie. Rozwiązanie stosunku pracy, odwołanie z pełnionej funkcji powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych chyba że upoważnienie takie zostało przedłużone. Upoważnienie do przetwarzania danych automatycznie przedłuża ważność nadanego identyfikatora w systemie.;
2. musi zachować tajemnicę danych osobowych oraz przestrzegać procedur ich bezpiecznego przetwarzania. Przestrzeganie tajemnicy danych osobowych obowiązuje przez cały okres zatrudnienia u administratora danych, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji;
3. zapoznaje się z przepisami prawa w zakresie ochrony danych osobowych oraz postanowieniami niniejszej polityki i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych;
4. stosuje określone przez administratora danych oraz administratora bezpieczeństwa informacji procedury oraz wytyczne mające na celu zgodne z prawem, w tym zwłaszcza adekwatne, przetwarzanie danych;
5. korzysta z systemu informatycznego administratora danych w sposób zgodny ze

wskazówkami zawartymi w instrukcjach obsługi urządzeń wchodzących w skład systemu informatycznego, oprogramowania i nośników;

6. zabezpiecza dane przed ich udostępnianiem osobom nieupoważnionym.

IV. Infrastruktura przetwarzania danych osobowych

1. Obszar przetwarzania danych osobowych

Tabela 1. Wykazu budynków i pomieszczeń wchodzących w skład obszaru przetwarzania danych osobowych

Wykaz budynków i pomieszczeń wchodzących w skład obszaru przetwarzania danych osobowych	
Adres: Urząd Gminy Bojszowy ul. Gaikowa 35, 43-220 Bojszowy	Pomieszczenia: – piwnica – parter, numery pokojów: 1, 3, 4 (serwerownia) – I piętro, numery pokojów: 5, 6, 7, 8, 9, 15, 20 – II piętro, numery pokojów: 16, Archiwum, 10, 11, 12

2. Zbiory danych

Tabela 2. Wykaz zbiorów danych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych w jednostce

L.p.	Nazwa zbioru	Numer księgi rejestrowej	Data rejestracji	Aktualizacje zbioru	Aktualnie zastosowany program do przetwarzania danych	Miejsce przechowywania
1.	Urząd Stanu Cywilnego	012900	12.06.2000r. Sygn.akt. DRZDO/ZR/000686/00	1. 09.05.2000r. - Sygn.akt. DRZDO/ZR/000686/00 2. 28.08.2007 Sygn.akt. DRZDO/402/001759/07	PB_USC-baza danych SQL	Pokój nr 3 SERWEROWNIA
2.	Ewidencja Numeracji Nieruchomości	012890	12.02.2001r. Sygn.akt. DRZDO/402/000209/01			Pokój nr 6
3.	PODATKI I OPŁATY	012895	12.02.2001r. Sygn.akt. DRZDO/402/000209/01	1. 28.08.2007 Sygn.akt. DRZDO/402/001760/07	ZINTEGROWANY SYSTEM ZARZĄDZANIA KSAT 2000 – - BAZA DANYCH ORACLE	Pokój nr 1 SERWEROWNIA
4.	Decyzje o ustaleniu warunków zabudowy, pozwolenia na budowę i w zakresie podziału gruntów	012892	12.02.2001r. Sygn.akt. DRZDO/402/000209/01			Pokój nr 6
5.	Rejestr wieczystych użytkowników i dzierżawców gruntów rolnych	012898	12.02.2001r. Sygn.akt. DRZDO/402/000209/01			Pokój nr 5
6.	Rejestr wycinek drzew	013419	12.02.2001r. Sygn.akt. DRZDO/402/000209/01			Pokój nr 20
7.	Świadectwa miejsca pochodzenia zwierząt	013426	12.02.2001r. Sygn.akt. DRZDO/402/000209/01	W trakcie wyrejestrowywania		-
8.	Ewidencja ludności i dowody osobiste	016261	12.02.2001r. Sygn.akt. DRZDO/402/000209/01	1. 23.05.2001 Sygn.akt. DRZDO/401/R/014722/99-7435/02 2. 13.11.2007 Sygn.akt. DRZDO/402/001761/07	INTEGROWANY SYSTEM ZARZĄDZANIA KSAT 2000 – - BAZA DANYCH ORACLE IDL System dowody Osobiste	Pokój nr 3 SERWEROWNIA
9.	ŁAWNICY	055732	12.02.2001r. Sygn.akt. DRZDO/402/000209/01			Pokój nr 5
10.	Korespondencja – pisma przychodzące i wychodzące	028578	12.02.2001r. Sygn.akt. DRZDO/402/000209/01	1. 28.08.2007 Sygn.akt. DRZDO/402/001762/0	System Elektronicznego obiegu Dokumentów MDOK – baza danych ORACLE	Baza - SERWEROWNIA Pokój nr:1, 3, 5, 6, 7, 8, 9, 10, 11, 12, 15, 16, 20, 20a, 20 b
11.	Psy agresywne	031768	12.02.2001r. Sygn.akt.			Pokój nr 10

			DRZDO/402/000209/01			
12.	Rejestr skarg i wniosków	033057	12.02.2001r. Sygn.akt. DRZDO/402/000209/01			Pokój nr 9
13.	Rejestr przedpoborowych	040132	12.02.2001r. Sygn.akt. DRZDO/402/000209/01			Pokój nr 16
14.	Komitet przeciwpowodziowy	040139	12.02.2001r. Sygn.akt. DRZDO/402/000209/01	W trakcie wyrejestrowywania		-
15.	Członkowie Ochotniczych Straży Pożarnych	040140	12.02.2001r. Sygn.akt. DRZDO/402/000209/01			Pokój nr 16
16.	Członkowie Komisji spoza Rady Gminy	040723	12.02.2001r. Sygn.akt. DRZDO/402/000209/01	W trakcie wyrejestrowywania		-
17.	Właściciele psów zaszczepionych przeciw wściekliźnie	040794	12.02.2001r. Sygn.akt. DRZDO/402/000209/01			Pokój nr 10
18.	Rejestr wydanych decyzji o zajęciu pasa drogowego	062194	04.06.2004r. Sygn.akt. DRZDO/402/001538/04			Pokój nr 11
19.	Rejestr wniosków o informacje publiczną	062826	04.06.2004r. Sygn.akt. DRZDO/402/001537/04			Pokój nr 9
20.	Wykaz osób przewidzianych do wykonania świadczeń rzeczowych i o sobistych na rzecz obrony /Akcja Kurierska/	062177	04.06.2004r. Sygn.akt. DRZDO/402/001539/04			Pokój nr 16
21.	ZEZNANIA PIT	063767	23.11.2004r. Sygn.akt. DRZDO/402/002738/04			Pokój nr 15
22.	Oświadczenia majątkowe	063766	23.11.2004r. Sygn.akt. DRZDO/402/002737/04			Pokój nr 15, 5
23.	Gminna Komisja Rozwiązywania Problemów Alkoholowych	066441	15.11.2005 Sygn.akt. DRZDO/402/001756/05			Pokój nr 10
24.	System Informacji Oświatowej SIO	065527	22.11.2005 Sygn.akt. DRZDO/402/002438/05		SIO	Pokój nr 10 SERWEROWNIA
25.	Pomoc materialna dla uczniów STYPENDIA	065528	22.11.2005 Sygn.akt. DRZDO/402/002439/05			Pokój nr 10

26.	Ewidencja tytułów wykonawczych	069537	03.10.2007r. Sygn.akt DRZDO/402/001603/07			Pokój nr 1
27.	Wnioski o zmianę planu zagospodarowania przestrzennego	069535	03.10.2007r. Sygn.akt DRZDO/402/001604/07			Pokój nr 6
28.	Decyzje o środowiskowych uwarunkowaniach	068791	03.10.2007r. Sygn.akt DRZDO/402/001605/07			Pokój nr 6
29.	*Realizacja obowiązku szkolnego i nauki*	069529	03.10.2007r. Sygn.akt DRZDO/402/001606/07			Pokój nr 10
30.	R*ejestr aktów i zaświadczeń - awans zawodowy nauczycieli*	069528	03.10.2007r. Sygn.akt DRZDO/402/001607/07			Pokój nr 10
31.	Służba zastępcza	069523	03.10.2007r. Sygn.akt DRZDO/402/001608/07			Archiwum UG
32.	Listy poborowych	069522	03.10.2007r. Sygn.akt DRZDO/402/001609/07			Pokój nr 16
33.	*WN- Wykaz o nieuregulowanym stosunku do służby wojskowej*	068790	03.10.2007r. Sygn.akt DRZDO/402/001610/07			Pokój nr 16
34.	*Zbywanie nieruchomości stanowiących własność gminy*	069519	03.10.2007r. Sygn.akt DRZDO/402/001611/07			Pokój nr 5
35.	*KADRY I PŁACE*	Nie wymaga rejestracji	-	-	ZINTEGROWANY SYSTEM ZARZĄDZANIA KSAT 2000 – BAZA DANYCH ORACLE	Pokój nr 1,3 SERWEROWNIA
36.	*Akta postępowań sprawdzających*	Nie wymaga rejestracji	-	-	-	Pokój nr 16 (TK)
37.	*Rozliczenia z ZUS*	-		-	PŁATNIK	Pokój nr 3

3. System informatyczny[1]

Systemy informatyczny administratora danych obsługiwane są przez dwa serwery zlokalizowany w pok. nr 4 (SERWEROWNIA). System ten ma połączenie z internetem za pomocą łącza DSL 8 MB - środki ochrony stosowane przez dostawce usługi TP S.A. dodatkowo teletransmisja zabezpieczona jest identyfikatorem i hasłem, a dane przesyłane są w formie zaszyfrowanej z wykorzystaniem poufnych protokołów. Dane osobowe nie są przesyłane za pomocą środków komunikacji elektronicznej.

SERWER nr 1 – KSAT 2000 obsługujący całość aplikacji w ramach Zintegrowanego Systemu Zarządzania KSAT 2000,
Ewidencja Ludności, Podatki i Opłaty, Kadry i Płace, MDOK - Zintegrowany Systemem Zarządzania KSAT 2000 - baza danych: ORACLE 9.2.0.6 SE One (Ewidencja Ludności, Podatki i opłaty, Kadry i płace, MDOK) zabezpieczenie konta w celu kontroli działania użytkowników (indywidualne identyfikatory i hasła, ograniczenia i kontrola dostępu do zbiorów danych, rejestracja zdarzeń w bazie); wykorzystuje się zabezpieczenia baz danych ORACLE, bieżąca aktualizacja zabezpieczeń.

SERWER nr 2 – Linuxowy serwer sieciowy - system zapory ogniowej dla systemu operacyjnego LINUX i WINDOWS – firewall.
Dane zbiorów SIO, USC zapisywane są na stacja roboczych, kopie zapasowe danych tworzy się raz w tygodniu – USC SIO – w przypadku wprowadzania zmian nie rzadziej niż raz na kwartał.

SIO – wykorzystuje się zabezpieczenia bazy SIO zabezpieczenie konta w celu kontroli działania użytkowników (indywidualne identyfikatory i hasła, ograniczenia i kontrola dostępu do zbiorów danych, rejestracja zdarzeń w bazie.

Urząd Stanu Cywilnego - baza danych: SQL

- zabezpieczenie konta w celu kontroli działania użytkowników (indywidualne identyfikatory i hasła, ograniczenia i kontrola dostępu do zbiorów danych, rejestracja zdarzeń w bazie);
- wykorzystuje się zabezpieczenia baz danych SQL

Na stacjonarnym sprzęcie stosuję się następujące zabezpieczenia:

- Hasło w BIOS-ie
- Hasła użytkowników systemu WINDOWS XP
- Ograniczony dostęp do systemu operacyjnego poprzez identyfikator i hasło zmieniana co 30 dni
- Wejście do aplikacji wymaga podania nazwy użytkownika oraz hasło
- W celu ochrony przed dostępem do danych komputera z sieci publicznej wykorzystuje się system zapory systemowej dla systemu operacyjnego WINDOWS XP – firewall. Stosuje się aktywną ochronę antywirusową w czasie rzeczywistym na każdym komputerze, na którym przetwarzane są dane osobowe. Aktualizacja przeprowadzana jest automatycznie przez system lub przez użytkownika stacji roboczej. Oprogramowanie antywirusowe, antyspamowe oraz antyspywerowe: NOD 32, AntiViren Kit GDATA, Spybot- Serach & Destroy 1.4, Ad-aware

[1] Zgodnie z art. 7 pkt 2a ustawy system informatyczny to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych. Pojęcie „system informatyczny" obejmuje elementy zaliczone do czterech kategorii. Są to:
1) urządzenia,
2) programy,
3) procedury przetwarzania informacji,
4) narzędzia programowe.
Urządzenie to „rodzaj mechanizmu lub zespół elementów, przyrządów służących do wykonania określonej czynności, ułatwiający pracę". Program – według znaczenia przyjmowanego w informatyce – to odpowiednio uporządkowana sekwencja instrukcji, mająca na celu wykonanie określonych zadań. Procedury przetwarzania informacji mogłyby być utożsamiane z programem, lecz wobec ich odrębnego wskazania w analizowanej definicji należy przyjąć, że są to procedury inne niż przyjęte w stosowanych w konkretnym przypadku programach. Narzędzia programowe także mieszczą się w kategorii oprogramowania.

Zastosowano następujące procedury ochronne w ramach systemu użytkowego na stanowiskach komputerowych wykorzystywanych do przetwarzania danych osobowych:

Stosuje się następujące zabezpieczenia organizacyjne przed dostępem do danych osób niepowołanych:

a) dostęp do danych mają wyłącznie pracownicy wyznaczeni przez Administratora Danych. Administrator Danych prowadzi ścisły rejestr tych pracowników obejmujący listę nazwisk użytkowników posiadających dostęp do danych.
b) pracownicy upoważnieni przez administratora danych osobowych do przetwarzania danych osobowych w wyżej podanym zakresie, posiadają odpowiednie wpisy do zakresów czynności, zapoznali się ZARZĄDZENIEM NR 0152/54 /2004 WÓJTA GMINY BOJSZOWY z dnia 20.09.2004r. w sprawie: polityki bezpieczeństwa ochrony danych osobowych i instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Gminy Bojszowy.
c) Wyznaczony został Administrator Bezpieczeństwa Informacji nadzorujący przestrzeganie zasad ochrony przetwarzania danych osobowych

3. Ewidencje

W ramach struktury organizacyjnej administratora danych prowadzone są następujące ewidencje wchodzące w skład dokumentacji z zakresu ochrony danych osobowych:

1) osoba upoważniona prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych,
2) ABi prowadzi ewidencje osób upoważnionych do systemów przetwarzających dane osobowe
3) administrator systemu prowadzi:

- przechowywaną w szafie o podwyższonej klasie odporności ewidencję haseł do stanowisk roboczych poszczególnych użytkowników oraz ich identyfikatorów,
- ewidencje: sprzętu komputerowego, komputerów stacjonarnych oraz przenośnych, nośników przenośnych oraz kluczy kryptograficznych.

V. Struktura zbiorów danych, sposób przepływu danych w systemie i zakres przetwarzania danych

1. Zbiór danych „Kadry i wynagrodzenia”

Zbiór ten obejmuje dane byłych i obecnych pracowników oraz osób świadczących usługi na rzecz administratora danych na innej podstawie niż stosunek pracy.

L.p.	Nazwa zbioru	Aktualnie zastosowany program do przetwarzania danych	sposób przepływu danych w systemie	zakres przetwarzania danych	Zakres uprawnień dla pracowników
38.	Urząd Stanu Cywilnego	PB_USC-baza danych SQL	*Brak*	– nazwiska i imiona, – imiona rodziców, – data urodzenia, – miejsce urodzenia, – adres zamieszkania lub pobytu, – numer ewidencyjny PESEL, – wykształcenie – seria i numery dowodów osobistych, – *Obywatelstwo* – *Stan cywilny* – *Płeć* – *Nazwiska rodowe rodziców* – *Miejsce zamieszkania i zameldowania każdego z rodziców w chwili urodzenia dziecka* – *Dane dotyczące wykształcenia rodziców dziecka* – *Dane dotyczące źródła utrzymania rodziców dziecka* – *Informacje dotyczące płci, ciężaru i długości dziecka* – *Informacje dotyczące porodu* – *Miejsce i data zawarcia małżeństwa* – *Nazwiska i imiona oraz nazwiska rodowe rodziców każdej z osób wstępujących w związek małżeński* – *Nazwiska i imiona świadków* – *Informacje o nazwiskach, które będą nosić osoby po zawarrciu małżeństwa* – *Prawomocne orzeczenie o rozwodzie, unieważnieniu małżeństwa, separacji* – *Nazwiska i imiona, miejsce zamieszkania osoby zgłaszającej zgon* – *Nazwisko: panieńskie, z poprzedniego małżeństwa, rodowe* – *Nazwisko i imię: ojca, matki, współmałżonka*	Dostęp do bazy wyłącznie pracownik USC 9Z-ca Kierownika USC) lub osoba zstępująca w czasie nieobecności. Każdy z pracowników ma swój login i hasło do sytemu

				– *Miejsce i godzina urodzenia* – *Data i numer aktu: urodzenia, małżeństwa, zgonu* – *Data, godzina, miejsce zgonu, odnalezienia zwłok* – *Nazwisko, imię, adres osoby zgłaszającej zgon* – *Miejsce wydania dowodu osobistego* – *Data unieważnienia aktu małżeństwa, urodzenia, zgonu* – *Imię nadane z urzędu* – *Data i numer orzeczenia sądu ustalającego ojcostwo, zaprzeczającego ojcostwo, przysposabiającego dziecko* – *Imię i nazwisko osoby przysposabiającej dziecko* – *Zmiana nazwiska dziecka*	
39.	PODATKI I OPŁATY	ZINTEGROWANY SYSTEM ZARZĄDZANIA KSAT 2000 – -BAZA DANYCH ORACLE	*Brak*	– nazwiska i imiona – adres zamieszkania lub pobytu – numer ewidencyjny PESEL – adres zamieszkania lub pobytu – numer identyfikacji podatkowej - NIP – rodzaj użytków rolnych, – klasy gruntu, – powierzchnia i adres gruntu, – nr karty podatnika (konto), – nr rejestrów geodezyjnych, – nazwisko, imię i adres użytkownika (płatnika), – kwota podatku, ulgi, – umorzenia i zaniechania oraz odroczenie terminu płatności podatku, – współmałżonek, dzieci, daty urodzenia, – nr karty gospodarstwa rolnego, – nr rejestracyjny pojazdu, marka, rodzaj, ładowność, nr silnika, pojemność, nr podwozia, rok produkcji, masa całkowita, barwa, data kupna – sprzedaży, grupa inwalidztwa, (do zwolnienia).	Dostęp do bazy posiadają wyłącznie pracownicy do spraw podatków i opłat oraz kasjer. Każdy z pracowników ma swój login i hasło do sytemu
40.	Ewidencja ludności i dowody osobiste	ZINTEGROWANY SYSTEM ZARZĄDZANIA KSAT 2000 – -BAZA DANYCH ORACLE IDL System dowody Osobiste	*Brak*	- nazwiska i imiona, - imiona rodziców, - data urodzenia, - miejsce urodzenia, - adres zamieszkania lub pobytu, - numer ewidencyjny PESEL, - wykształcenie - seria i numery dowodów osobistych, - Nazwisko rodowe rodziców	Dostęp do bazy wyłącznie pracownik Biura Ewidencji Ludności oraz oraz osoba zstępująca w czasie nieobecności. Każdy z pracowników ma swój login i hasło do sytemu

				- Imiona i nazwiska poprzednie - Stan cywilny - Nazwiska rodowe - Imię i nazwisko małżonka oraz jego nazwisko rodowe - Płeć - Obywatelstwo - Data nabycia i utraty obywatelstwa polskiego - Informacje potwierdzające posiadanie obywatelstwa polskiego - Dane dotyczące obowiązku wojskowego (stopień wojskowy, nazwa, seria i numer wojskowego dokumentu osobistego, oznaczenie wojskowej komendy uzupełnień, informacje zawarte w poświadczeniu o zgłoszeniu się do rejestracji przedpoborowych) - adres miejsca zameldowania na pobyt stały, data zameldowania, a w razie jego braku - zameldowania na pobyt czasowy trwający ponad dwa miesiące - Rysopis (wzrost, kolor oczu) - Nazwa organu wydającego, data wydania oraz termin ważności dowodu osobistego - *Wizerunek* -	
41.	Korespondencja – pisma przychodzące i wychodzące	System Elektronicznego obiegu Dokumentów MDOK – baza danych ORACLE		- nazwiska i imiona, - adres zamieszkania lub pobytu - numer identyfikacji podatkowej - NIP	Dostęp do bazy posiadają wszyscy pracownicy wg kategorii uprawnień przydzielonych w systemie. Każdy z pracowników ma swój login i hasło do sytemu
42.	System Informacji Oświatowej SIO	SIO	*Brak*	- data urodzenia - numer ewidencyjny PESEL - miejsce pracy, - zawód - wykształcenie - niepełnosprawność	Dostęp do bazy posiada wyłącznie Specjalista ds. edukacji oraz administrator systemu.
43.	*KADRY I PŁACE*	ZINTEGROWANY SYSTEM ZARZĄDZANIA KSAT 2000 – BAZA DANYCH ORACLE	*Brak*	- nazwiska i imiona, - imiona rodziców, - data urodzenia, - miejsce urodzenia, - adres zamieszkania lub pobytu, - numer ewidencyjny PESEL, - wykształcenie - seria i numery dowodów osobistych, - *Wizerunek* - numer telefonu - dowód osobisty (seria i nr, wydany przez, data wydania) - imię ojca - imię matki - stan cywilny i rodzinny	Dostęp do bazy posiadają : inspektor ds. kadrowych oraz inspektor ds. płac Każdy z pracowników ma swój login i hasło do sytemu

				- posiada gospodarstwo rolne - emeryt - rencista/ - obywatelstwo obce - dane osoby kontaktowej - wykształcenie - nazwa szkoły i rok ukończenia/ - staż pracy - historia prac - warunki zatrudnienia - wysokość wynagrodzenia - ukończone kursy - kary i nagrody - nieobecności w pracy - informacja o karalności - informacje o stanie zdrowia - dokument wojskowy, seria i numer, stopień wojskowy)/	
44.	*Rozliczenia z ZUS*	PŁATNIK	*Brak*	- PESEL - NIP - imię/nazwisko - Adres zamiesykania - data i miejsce urodzenia	

UDOSTĘPNIANIE DANYCH:

Dane ze zbiorów udostępniane są wyłącznie na podstawie przepisów prawa.

2. Poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym

Ze względu na fakt, że system informatyczny administratora danych połączony jest z siecią publiczną, zgodnie z § 6 ust. 4 rozporządzenia należy zapewnić wysoki poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym. Wynikające z tego konsekwencje trzeba uwzględnić w instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

VI. Strategia zabezpieczenia danych osobowych (działania niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych)

Dane gromadzone w budynku Urzędu Gminy Bojszowy w pomieszczeniu na parterze w zamykanych szafach metalowych, drzwi antywłamaniowe zamykane na klucz, rolety w oknach antywłamaniowe. Budynek chroniony jest alarmem przeciwpożarowym i antywłamaniowym, posiada dwustronne zasilanie elektryczne, instalacje odgromową i wyposażony jest w urządzenia gaśnicze.

Bezpieczeństwo osobowe:

d) dostęp do danych mają wyłącznie pracownicy wyznaczeni przez Administratora Danych. Administrator Danych prowadzi ścisły rejestr tych pracowników obejmujący listę nazwisk użytkowników posiadających dostęp do danych.
e) pracownicy upoważnieni przez administratora danych osobowych do przetwarzania danych osobowych w wyżej podanym zakresie, posiadają odpowiednie wpisy do zakresów czynności, zapoznali się ZARZĄDZENIEM WÓJTA GMINY BOJSZOWY w sprawie: polityki bezpieczeństwa ochrony danych osobowych i instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Gminy Bojszowy.
f) Wyznaczony został Administrator Bezpieczeństwa Informacji nadzorujący przestrzeganie zasad ochrony przetwarzania danych osobowych

Do elementów zabezpieczenia danych osobowych w Urzędzie Gminy Bojszowy zalicza się:

- stosowane metody ochrony pomieszczeń, w których przetwarzane są dane osobowe (zabezpieczenia fizyczne),
- zabezpieczenie wszystkich procesów przetwarzania danych (w szczególności dokumentów papierowych i informatycznych),
- nadzór Administratora Bezpieczeństwa Informacji nad wprowadzonych zasadami i procedurami zabezpieczenia danych (zabezpieczenia organizacyjne)
- kompleksowe i całościowe traktowanie zabezpieczenia danych przez wszystkie podmioty i osoby biorące udział w przetwarzaniu danych,

W Urzędzie Gminy Bojszowy rozróżnia się następujące kategorie środków zabezpieczeń danych osobowych:

a. Zabezpieczenia fizyczne:

- Wprowadzono ochronę budynku, w którym znajduje się obszar przetwarzania danych osobowych,
- W pomieszczeniach obszaru przetwarzania danych nośniki z danymi (papierowe i informatyczne) przechowywane są w zamykanych szafach zamykanych na klucz, szafach metalowych oraz sejfach,
- Wszystkie pomieszczenia po godzinach pracy zamykane są na klucz, dodatkowe zabezpieczenia w pomieszczeniu KASY: karaty ,w szybach na parterze budynku folia antywłamaniowa, w pomieszczeniu USC, Ewidencji ludności rolety antywłamaniowe.
- Dodatkowo zabezpieczone jest pomieszczenie serwerowi, : dostęp do pomieszczeń mają jedynie osoby uprawnione, dodatkowo krata zabezpieczająca drzwi, instalacja przeciwpożarowa, rejestr wejść do serwerowni (osoby bez upoważnienia w obecności ABI lub osób upoważnionych).

b. Zabezpieczenia fizyczne procesów przetwarzania danych w dokumentacji papierowej:

- Dokumentacja papierowa zawierająca dane osobowe przechowywana w zamykanych szafach,
- Dokumentacja papierowa zawierająca dane osobowe jest udostępniania jedynie osobom do tego upoważnionym,
- Niszczenie dokumentacji papierowej w siedzibie urzędu za pomocą niszczarek.

c. Zabezpieczenia organizacyjne. Osoby upoważnione do przetwarzania danych osobowych, pracownicy i organizacja pracy

- Osobą odpowiedzialną za nadzór nad zabezpieczeniami danych jest Administrator Bezpieczeństwa Informacji (ABI);
- ABI na bieżąco kontroluje pracę systemu informatycznego z należytą starannością, zgodnie z aktualnie obowiązującą w tym zakresie wiedzą i z obowiązującymi procedurami;
- ABI na bieżąco kontroluje sposób zabezpieczenia fizycznego przechowywanych dokumentów z danymi osobowymi oraz informatycznych nośników danych osobowych.
- Nie rzadziej, niż raz na kwartał są prowadzone przez ABI kontrole stanu bezpieczeństwa systemów informatycznych i przestrzegania zasad ochrony informacji, a w przypadkach wykrycia rażących zaniedbań, ABI sporządza ich opis w formie protokołu i raportu i niezwłocznie przedkłada je Wójtowi.
- W Urzędzie Gminy obowiązuje następująca procedura nadawania upoważnień do przetwarzania danych osobowych:
    - przełożony upoważnionego (kierujący referatem) informuje Administratora Bezpieczeństwa Informacji o potrzebie nadania upoważnienia,
    - Wójt na podstawie projektu dokumentu przygotowanego przez Administratora Bezpieczeństwa Informacji podejmuje decyzje o upoważnieniu do przetwarzania danych osobowych i wydaje stosowny dokument, którego wzór stanowi załącznik nr 4 do Zarządzenie.
    - Osoba upoważniona prowadzi ewidencje osób upoważnionych do przetwarzania danych osobowych – wzór stanowi zał. Nr 5 do Zarządzenia.
    - Ustanie upoważnienia następuje na wniosek przełożonego osoby upoważnionej, po podjęciu decyzji przez Wójta lub działającego z jego upoważnienia Administratora Bezpieczeństwa Informacji.
    - Administrator Bezpieczeństwa Informacji prowadzi ewidencję osób upoważnionych, której wzór stanowi załącznik nr D do Polityki.
    - Powyższe zasady upoważnienia stosuje się do przetwarzania danych osobowych w kartotekach papierowych i w systemie informatycznym. W systemie informatycznym rejestracji użytkownika dokonuje administrator systemu.

W ramach zabezpieczenia danych osobowych ochronie podlegają:

- sprzęt komputerowy - serwer, komputery osobiste, drukarki i inne urządzenia zewnętrzne,
- oprogramowanie - kody źródłowe, programy użytkowe, systemy operacyjne, narzędzia wspomagające i programy komunikacyjne,
- dane zapisane na dyskach oraz dane podlegające przetwarzaniu w systemie,
- hasła użytkowników,
- pliki dziennych operacji systemowych i baz danych, kopie zapasowe i archiwa,
- użytkownicy i administratorzy, którzy obsługują i używają system,
- dokumentacja - zawierająca dane systemu, opisująca jego zastosowanie, przetwarzane informacje, itp.,
- wydruki,
- związana z przetwarzaniem danych dokumentacja papierowa, z której zawarte w niej dane są wprowadzane do systemu informatycznego lub też funkcjonują autonomicznie od niego.

ABI okresowo będzie analizował zagrożenia i ryzyko w celu weryfikacji środków zabezpieczających. Oprócz tego, administrator będzie okresowo dokonywać inwentaryzacji systemów informatycznych i zbiorów danych w celu zapewnienia aktualności polityki bezpieczeństwa.

W systemie informatycznym Urzędu Gminy w Bojszowach obowiązują zabezpieczenia na poziomie wysokim.

W przypadku stwierdzenia nieprawidłowości w zakresie zabezpieczenia danych osobowych Administrator Bezpieczeństwa Informacji ma prawo:

a) Pouczać i instruować osoby, które dopuściły się uchybień, a także wydawać im polecenia mające na celu przywrócenia stanu prawidłowego.
b) Zwracać się do Wójta o dokonanie zmian w zakresie stosowanych zabezpieczeń organizacyjnych i technicznych.
c) Przedstawiać Wójtowi raporty dotyczące stanu zabezpieczenia danych osobowych w urzędzie, w tym propozycję poprawiające bezpieczeństwo danych oraz wnioski dotyczące odpowiedzialności osób winnych uchybień.

Pracownicy i inne osoby upoważnione do przetwarzania danych osobowych w Urzędzie Gminy

Bojszowy są zobowiązani do:

a) Umożliwienia Administratorowi Bezpieczeństwa Informacji wykonywania jego zadań.
b) Stosować się do pouczeń i instrukcji ABI, o których mowa powyżej.

Najważniejszymi zastosowanymi środkami zabezpieczenia danych w systemach informatycznych są:

a) Zastosowano mechanizmy uwierzytelnienia użytkownika w systemie oraz kontroli dostępu do danych.
b) Zastosowano oprogramowanie zabezpieczające przed uzyskaniem nieuprawnionego dostępu do systemu informatycznego,
c) Zastosowano oprogramowanie antywirusowe,
d) Zastosowano zabezpieczenia przed awarią zasilania lub zakłóceniami w sieci zasilającej,
e) Urządzenia zawierające dane osobowe przeznaczone do likwidacji są pozbawiane zapisu tych danych,
f) System informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem,
g) Dane wykorzystywane do uwierzytelnienia nie są przesyłane w sieci publicznej,
h) Systemy służące do przetwarzania danych osobowych w Urzędzie Gminy Bojszowy powinny zapewniać odnotowanie:

- daty pierwszego wprowadzenia danych do systemu,
- identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba,
- źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą;
- informacji o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy o ochronie danych osobowych, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia.

Zasady zarządzania systemem informatycznym służącym do przetwarzania danych osobowych określa w Urzędzie Gminy Bojszowy dokument instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, w szczególności w zakresie:

1) określenia sposobu przydziału i zarządzania hasłami użytkowników;
2) określenia uprawnień użytkowników oraz sposobu ich rejestrowania i wyrejestrowania w systemie informatycznym;
3) zasad rozpoczęcia i zakończenia pracy w systemie;
4) ochrony antywirusowej;
5) przeglądów i konserwacji systemu;
6) postępowania w zakresie komunikacji w sieci komputerowej;
7) zarządzania systemem informatycznym;
8) przechowywania nośników informacji.

Instrukcje opracowuje i aktualizuje Administrator Bezpieczeństwa Informacji.

Zał. Nr 2
do Zarządzenia Nr 0152/61/2009
z dnia 12.02.2009r.

Instrukcja zarządzania systemami informatycznymi służącym do przetwarzania danych osobowych

SPIS TREŚCI

1. Cel instrukcji

Instrukcja określa sposób zarządzania systemem informatycznym, wykorzystywanym do przetwarzania danych osobowych, przez administratora danych – w celu zabezpieczenia danych osobowych przed zagrożeniami, w tym zwłaszcza przed ich udostępnieniem osobom nieupoważnionym, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.

2. Definicje

Ilekroć w instrukcji jest mowa o:

administratorze bezpieczeństwa informacji – rozumie się przez to osobę, której administrator danych powierzył pełnienie obowiązków administratora bezpieczeństwa informacji,

administratorze danych – rozumie się przez Wójta Gminy Bojszowy

administratorze systemu – rozumie się przez to kierownika działu informatyki,

osoba upoważniona prze Administratora Danych – osoba upoważniona do wykonywania niektórych czynności w imieniu Administratora Danych

haśle – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi,

identyfikatorze – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,

integralności danych – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,

odbiorcy danych – rozumie się przez to każdego, komu udostępniane są dane osobowe, z wyłączeniem:

- osoby, której dane dotyczą,
- osoby upoważnionej do przetwarzania danych,
- przedstawiciela, o którym mowa w art. 31a ustawy,
- podmiotu, o którym mowa w art. 31 ustawy,
- organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem,

osobie upoważnionej do przetwarzania danych osobowych – rozumie się przez to osobę, która upoważniona została do przetwarzania danych osobowych przez prezesa zarządu na piśmie,

poufności danych – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom,

przetwarzającym – rozumie się przez to podmiot, któremu zostało powierzone przetwarzanie danych osobowych na podstawie umowy zawieranej zgodnie z art. 31 ustawy,

raporcie – rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych,

rozliczalności – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,

rozporządzeniu – rozumie się przez to rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (DzU nr 100, poz. 1024),

sieci publicznej – rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 22 ustawy z dnia 21 lipca 2000 r. – Prawo telekomunikacyjne,

sieci telekomunikacyjnej – rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 23 ustawy z dnia 21 lipca 2000 r. – Prawo telekomunikacyjne (DzU nr 73, poz. 852 ze zm.),

serwisancie – rozumie się przez to firmę lub pracownika firmy zajmującej się sprzedażą, instalacją, naprawą i konserwacją sprzętu komputerowego,

systemie informatycznym administratora danych – rozumie się przez to sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych; w systemie tym pracuje co najmniej jeden komputer centralny i system ten tworzy sieć teleinformatyczną administratora danych,

teletransmisji – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej,

ustawie – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. DzU z 2002 r. nr 101, poz. 926 ze zm.),

uwierzytelnianiu – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu,

użytkowniku – rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych, której nadano identyfikator i przyznano hasło.

3. Poziom bezpieczeństwa

Uwzględniając kategorie danych osobowych oraz konieczność zachowania bezpieczeństwa ich przetwarzania w systemie informatycznym połączonym z siecią publiczną, wprowadza się „poziom wysoki" bezpieczeństwa w rozumieniu § 6 rozporządzenia.

4. Nadawanie i rejestrowanie (wyrejestrowywanie) uprawnień do przetwarzania danych w systemie informatycznym

Nadawanie i rejestrowanie uprawnień

a) Dostęp do systemu informatycznego służącego do przetwarzania danych osobowych może uzyskać wyłącznie osoba upoważniona do przetwarzania danych osobowych, zarejestrowana jako użytkownik w tym systemie przez administratora systemu na wniosek kierownika referatu .
b) Rejestracja użytkownika, o której mowa w pkt 1, polega na nadaniu identyfikatora i przydzieleniu hasła oraz wprowadzeniu tych danych do bazy użytkowników systemu.
c) Administrator systemu prowadzi rejestr pracowników który został nadany login do systemu.

Wyrejestrowywanie uprawnień

a) Wyrejestrowania użytkownika z systemu informatycznego dokonuje administrator systemu na wniosek kierownika referatu lub pracownika działu kadr..
b) Wyrejestrowanie, o którym mowa w ust. 1, może mieć charakter czasowy lub trwały.
c) Wyrejestrowanie następuje poprzez:
   - zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe),
   - usunięcie danych użytkownika z bazy użytkowników systemu (wyrejestrowanie trwałe).
d) Czasowe wyrejestrowanie użytkownika z systemu informatycznego musi nastąpić w razie zawieszenia w pełnieniu obowiązków służbowych.
e) Przyczyną czasowego wyrejestrowania użytkownika z systemu informatycznego może być:
   - wypowiedzenie umowy o pracy,
   - wszczęcie postępowania dyscyplinarnego względem osoby upoważnionej do przetwarzania danych osobowych.
f) Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy lub innego stosunku prawnego, w ramach którego zatrudniony był użytkownik.

5. Metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

Identyfikator

a) Identyfikator składa się z: pierwszej litery imienia oraz nazwisk W identyfikatorze pomija się polskie znaki diakrytyczne.
b) W przypadku zbieżności nadawanego identyfikatora z identyfikatorem wcześniej zarejestrowanego użytkownika administrator systemu, za zgodą administratora bezpieczeństwa informacji, nadaje inny identyfikator, odstępując od zasady określonej w pkt 1.

Hasło użytkownika

a) Hasło powinno składać się z unikalnego zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne. Hasło nie może być identyczne z identyfikatorem użytkownika ani jego imieniem lub nazwiskiem.
b) Hasła w systemie zmienia się co 30 dni; administrator bezpieczeństwa informacji może, w uzasadnionych sytuacjach, polecić dokonanie zmiany hasła przez użytkownika.

Zabrania się użytkownikom systemu udostępniania swojego identyfikatora i hasła innym osobom oraz korzystania przez osoby upoważnione do przetwarzania danych osobowych z identyfikatora lub hasła innego użytkownika.

Hasło administratora

Hasło administratora systemu przechowywane jest w zamkniętej kopercie w szafie o podwyższonym stopniu odporności, zamykanej na klucz, do którego ma dostęp wyłącznie Wójt, Administrator systemu, ABI, osoba upoważniona przez Wójta.

6. Procedury rozpoczęcia, zawieszenia i zakończenia pracy, przeznaczone dla użytkowników systemu

- Tryb pracy na poszczególnych stacjach roboczych

c) Rozpoczęcie pracy na stacji roboczej następuje po włączeniu komputera, a następnie wprowadzeniu indywidualnego, znanego tylko użytkownikowi, hasła i identyfikatora. Hasło

BIOS, następnie login do sytemu operacyjnego, następnie wejście do aplikacji zawierającej dane osobowe po podaniu loginu i hasła.

d) W pomieszczeniu, w którym przetwarzane są dane osobowe, mogą znajdować się osoby postronne tylko w obecności pracownika posiadającego stosowne upoważnienie do przetwarzania danych osobowych
e) Przed osobami postronnymi należy chronić ekrany komputerów (ustawienie monitora powinno uniemożliwiać pogląd), wydruki leżące na biurkach oraz w otwartych szafach.
f) Monitory komputerów wyposażone są we włączające się po 10 minutach od przerwania pracy wygaszacze ekranu. Wznowienie wyświetlenia następuje dopiero po wprowadzeniu odpowiedniego hasła.
g) W przypadku opuszczenia stanowiska pracy użytkownik obowiązany jest aktywizować wygaszacz ekranu lub w inny sposób zablokować stację roboczą.
h) Obowiązuje zakaz robienia kopii całych zbiorów danych; całe zbiory danych mogą być kopiowane tylko przez administratora systemu lub automatycznie przez system, z zachowaniem procedur ochrony danych osobowych.
i) Jednostkowe dane mogą być kopiowane na nośniki magnetyczne, optyczne i inne po ich zaszyfrowaniu i przechowywane w zamkniętych na klucz szafach. Po ustaniu przydatności tych kopii dane należy trwale skasować lub fizycznie zniszczyć nośniki, na których są przechowywane.
j) Jednostkowe dane mogą być przekazywane pocztą elektroniczną pomiędzy komputerami administratora danych a komputerami przenośnymi użytkowników tylko po ich zaszyfrowaniu.
k) Przesyłanie danych osobowych pocztą elektroniczną może odbywać się tylko w postaci zaszyfrowanej.
l) Obowiązuje zakaz wynoszenia na jakichkolwiek nośnikach całych zbiorów danych oraz szerokich z nich wypisów, nawet w postaci zaszyfrowanej.
m) Przetwarzając dane osobowe, należy odpowiednio często robić kopie robocze danych, na których się właśnie pracuje, tak by zapobiec ich utracie.
n) Zakończenie pracy na stacji roboczej następuje po wprowadzeniu danych tego dnia przetwarzanych w odpowiednie obszary serwera, a następnie prawidłowym wylogowaniu się użytkownika i wyłączeniu komputera oraz odcięciu napięcia w zasilaczu awaryjnym (UPS) i listwie.
o) Przed opuszczeniem pokoju należy:
   - zniszczyć w niszczarce lub schować do zamykanych na klucz szaf wszelkie wykonane wydruki zawierające dane osobowe,
   - schować do zamykanych na klucz szaf wszelkie akta zawierające dane osobowe,
   - umieścić klucze do szaf w ustalonym, przeznaczonym do tego miejscu,
   - zamknąć okna.
a) Opuszczając pokój, należy zamknąć za sobą drzwi na klucz. Klucz od pokoju zawiesić w gablocie do tego przeznaczonej lub przekazać sprzątaczce.

Tryb pracy na komputerach przenośnych

Na komputerach przenośnych zabrania się przetwarzania danych osobowych. W uzasadnionych przypadkach dopuszczalna jest praca na komputerach przenośnych wyłącznie za zgoda Administratora Danych.

a) ile to możliwe, przy przetwarzaniu danych osobowych na komputerach przenośnych obowiązują procedury określone w niniejszej instrukcji, dotyczące pracy na komputerach stacjonarnych.
b) Użytkownicy, którym zostały powierzone komputery przenośne, powinni chronić je przed uszkodzeniem, kradzieżą i dostępem osób postronnych, szczególną ostrożność należy zachować podczas ich transportu.
c) Obowiązuje zakaz używania komputerów przenośnych przez osoby inne niż użytkownicy, którym zostały one powierzone.
d) Praca na komputerze przenośnym możliwa jest po wprowadzeniu hasła i indywidualnego identyfikatora użytkownika.
e) Użytkownicy są zobowiązani zmieniać hasła w komputerach przenośnych nie rzadziej niż raz na 30 dni.
f) Pliki zawierające dane osobowe przechowywane na komputerach przenośnych są zaszyfrowane i opatrzone hasłem dostępu.
g) Obowiązuje zakaz przetwarzania na komputerach przenośnych całych zbiorów danych lub

szerokich z nich wypisów, nawet w postaci zaszyfrowanej.

h) Użytkownicy przetwarzający dane osobowe na komputerach przenośnych obowiązani są do systematycznego wprowadzania tych danych w określone miejsca na serwerze administratora danych, a następnie do trwałego usuwania ich z pamięci powierzonych komputerów przenośnych.
i) Obowiązuje zakaz samodzielnej modernizacji oprogramowania i sprzętu w powierzonych komputerach przenośnych. Wszelkie zmiany mogą być dokonywane tylko pod nadzorem administratora systemu, stosownie do wymagań niniejszej instrukcji. W razie wystąpienia usterek w pracy komputerów przenośnych lub w razie wystąpienia konieczności aktualizacji ich oprogramowania należy zgłosić to administratorowi systemu.
j) Komputery przenośne wyposażone są w odpowiednie programy ochrony antywirusowej, których aktualizację sugeruje automatycznie system.

7. Procedury tworzenia kopii zapasowych

a) W systemie informatycznym wykorzystującym technologię klient-serwer kopie zapasowe wykonuje się po stronie serwera.
b) Dostęp do kopii bezpieczeństwa ma tylko ABI oraz Informatyk.
c) Pozostałe kopie tworzy się na oddzielnych nośnikach informatycznych. W kolejnych latach zakupić odrębny serer do przechowywania baz danych poza systemem KSAT 2000.
d) Nośniki zawierające kopie zapasowe należy oznaczać jako „Kopia zapasowa dzienna/tygodniowa/miesięczna" wraz z podaniem daty sporządzenia.

Częstotliwość wykonywania kopii

Kopie zapasowe tworzy się:

4) codziennie – na koniec dnia kopię wszystkich danych, które uległy zmianie tego dnia,
5) raz w tygodniu – na koniec tygodnia kopię wszystkich aplikacji,

raz w miesiącu – na koniec miesiąca kopię zarówno danych, jak i aplikacji.

Testowanie kopii

W celu zapewnienia poprawności wykonywanych kopii bezpieczeństwa należy co najmniej raz na kwartał poddać testowi cyklicznie wybraną kopię. Próba polega na odtworzeniu danych w warunkach testowych i sprawdzeniu, czy jest możliwość odczytania danych.

Przechowywanie kopii

a) Kopie zapasowe tygodniowe przechowuje się w Serwerowi w sejfie ognioodpornym administratora danych. Pozostałe kopie zapasowe przechowuje się w szafie o podwyższonym stopniu odporności, do której dostęp posiada wyłącznie administrator bezpieczeństwa informacji oraz administrator systemu i upoważnieni przez niego pracownicy. Każde wydanie i przyjęcie kopii jest odnotowywane w rejestrze depozytów.
b) Zabrania się przechowywania kopii zapasowych w pomieszczeniach przeznaczonych do przechowywania zbiorów danych pozostających w bieżącym użytkowaniu. Jednocześnie kopie zapasowe muszą być odpowiednio zabezpieczone fizycznie (sejf ognioodporny w zabezpieczonym pomieszczeniu).

Kopie zapasowe mogą być przechowywane tylko w tych pomieszczeniach, w których jest zainstalowany system wykrywania pożaru.

Likwidacja nośników zawierających kopie

a) Nośniki zawierające nieaktualne kopie danych, będące poza wykazem cyklicznych kopii, likwiduje się. W przypadku nośników jednorazowych, takich jak płyty CD-R, DVD-R, likwidacja polega na ich fizycznym zniszczeniu w taki sposób, by nie można było odczytać ich zawartości. Nośniki wielorazowego użytku, takie jak dyski twarde, dyskietki, płyty CD-RW, DVD-RW, można wykorzystać ponownie do celów przechowywania kopii bezpieczeństwa po uprzednim usunięciu ich zawartości.
b) Nośniki wielorazowego użytku nienadające się do ponownego użycia należy zniszczyć fizycznie.

8. Przechowywanie elektronicznych nośników informacji zawierających dane osobowe

a) Zbiory danych przechowywane są generalnie na serwerze obsługującym system informatyczny administratora danych. Wszelkie dane przetwarzane w pamięci poszczególnych stacji roboczych oraz komputerów przenośnych są niezwłocznie umieszczane w odpowiednich miejscach na serwerze, przydzielonych każdemu użytkownikowi przez administratora systemu.
b) Zakazuje się przetwarzania danych osobowych na zewnętrznych nośnikach magnetycznych, optycznych i innych oraz ich przesyłania pocztą elektroniczną bez uprzedniego zaszyfrowania.

c) Na nośnikach, o których mowa w pkt 2, dopuszczalne jest przetwarzanie jedynie jednostkowych danych osobowych.
d) W przypadku posługiwania się nośnikami danych pochodzącymi od podmiotu zewnętrznego użytkownik jest zobowiązany do sprawdzenia go programem antywirusowym na wyznaczonym w tym celu stanowisku komputerowym oraz do oznakowania tego nośnika.
e) Nośniki magnetyczne raz użyte do przetwarzania danych osobowych nie mogą być wykorzystywane do innych celów mimo usunięcia danych i podlegają ochronie w trybie niniejszej instrukcji.
f) Nośniki magnetyczne z zaszyfrowanymi jednostkowymi danymi osobowymi są na czas ich użyteczności przechowywane w zamkniętych na klucz szafach, a po wykorzystaniu dane na nich zawarte są trwale usuwane lub nośniki te są niszczone.
g) Nośniki informatyczne przechowywane są w miejscach, do których dostęp mają wyłącznie osoby upoważnione do przetwarzania danych osobowych.

9. Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

a) Sprawdzanie obecności wirusów komputerowych w systemie informatycznym oraz ich usuwanie odbywa się przy wykorzystaniu oprogramowania zainstalowanego na serwerach, stacjach roboczych oraz komputerach przenośnych przez administratora systemu.
b) Oprogramowanie, o którym mowa w pkt 1, sprawuje ciągły nadzór (ciągła praca w tle) nad pracą systemu i jego zasobami oraz serwerami i stacjami roboczymi.
c) Niezależnie od ciągłego nadzoru, o którym mowa w pkt 2, administrator systemu nie rzadziej niż raz na tydzień przeprowadza pełną kontrolę obecności wirusów komputerowych w systemie oraz jego zasobach, jak również w serwerach i stacjach roboczych.
d) Do obowiązków administratora systemu należy aktualizacja oprogramowania antywirusowego oraz określenie częstotliwości automatycznych aktualizacji definicji wirusów, dokonywanych przez to oprogramowanie.
e) Użytkownik jest obowiązany zawiadomić administratora systemu o pojawiających się komunikatach, wskazujących na wystąpienie zagrożenia wywołanego szkodliwym oprogramowaniem.
f) Użytkownicy mogą korzystać z zewnętrznych nośników danych zakupionych prze Administratora Danych po uprzednim sprawdzeniu zawartości nośnika oprogramowaniem antywirusowym.
g) Dostęp do internetu możliwy jest na kilku stacjach roboczych, specjalnie chronionych urządzeniem sprzętowym z wbudowanym programem Firewall i translacją adresów NAT.

10. Kontrola nad wprowadzaniem, dalszym przetwarzaniem i udostępnianiem danych osobowych

1) System informatyczny umożliwia sporządzenie i wydrukowanie dla każdej osoby, której dane są przetwarzane w systemie, raportu zawierającego:
- datę pierwszego wprowadzenia danych do systemu administratora danych,
- identyfikator użytkownika wprowadzającego te dane,
- źródła danych – w przypadku zbierania danych nie od osoby, której one dotyczą,
- informacje o odbiorcach danych, którym dane osobowe zostały udostępnione,
- sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 ustawy.

Odnotowanie informacji, o których mowa w pkt 3), następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.

11. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych

a) Przeglądu i konserwacji systemu dokonuje informatyk..
b) Przeglądu pliku zawierającego raport dotyczący działalności aplikacji bądź systemu (log systemowy) administrator systemu dokonuje nie rzadziej niż raz w miesiącu.
c) Przeglądu i sprawdzenia poprawności zbiorów danych zawierających dane osobowe dokonuje użytkownik przy współudziale administratora systemu nie rzadziej niż raz na kwartał.
d) Zapisy logów systemowych powinny być przeglądane przez administratora systemu codziennie oraz każdorazowo po wykryciu naruszenia zasad bezpieczeństwa.
e) Kontrole i testy przeprowadzane przez administratora bezpieczeństwa informacji powinny obejmować zarówno dostęp do zasobów systemu, jak i profile oraz uprawnienia poszczególnych użytkowników.

12. Naprawy urządzeń komputerowych z chronionymi danymi osobowymi

a) Wszelkie naprawy urządzeń komputerowych oraz zmiany w systemie informatycznym

administratora danych przeprowadzane są – o ile to możliwe – przez informatyka.

b) Naprawy i zmiany w systemie informatycznym administratora danych przeprowadzane przez serwisanta prowadzone są pod nadzorem administratora systemu w siedzibie administratora danych (jeśli to możliwe) lub poza siedzibą administratora danych, po uprzednim nieodwracalnym usunięciu danych w nich przetwarzanych, a jeśli wiązałoby się to z nadmiernymi utrudnieniami, to po podpisaniu umów powierzenia przetwarzania danych osobowych.

c) Jeśli nośnik danych (dysk, dyskietka, płyta lub inne) zostanie uszkodzony i nie można go odczytać ani usunąć z niego danych, należy go zniszczyć mechanicznie w niszczarce.

13. Postępowanie w przypadku stwierdzenia naruszenia bezpieczeństwa systemu informatycznego

1) Użytkownik zobowiązany jest zawiadomić administratora bezpieczeństwa informacji lub informatyka o każdym naruszeniu lub podejrzeniu naruszenia bezpieczeństwa systemu, a w szczególności o:
   - naruszeniu hasła dostępu i identyfikatora (system nie reaguje na hasło lub je ignoruje bądź można przetwarzać dane bez wprowadzenia hasła),
   - częściowym lub całkowitym braku danych albo dostępie do danych w zakresie szerszym niż wynikający z przyznanych uprawnień,
   - braku dostępu do właściwej aplikacji lub zmianie zakresu wyznaczonego dostępu do zasobów serwera,
   - wykryciu wirusa komputerowego w przypadku niemożności jego usunięcia lub wyleczenia pliku zainfekowanego,
   - zauważeniu elektronicznych śladów próby włamania do systemu informatycznego,
   - znacznym spowolnieniu działania systemu informatycznego,
   - podejrzeniu kradzieży sprzętu komputerowego lub dokumentów zawierających dane osobowe,
   - zmianie położenia sprzętu komputerowego,
   - zauważeniu śladów usiłowania lub dokonania włamania do pomieszczeń lub zamykanych szaf.
2) Do czasu przybycia na miejsce administratora bezpieczeństwa informacji należy:
   - o ile istnieje taka możliwość, niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego zdarzenia, a następnie uwzględnić w działaniu również ustalenie jego przyczyn lub sprawców,
   - rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
   - zaniechać – o ile to możliwe – dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,
   - zastosować się do instrukcji i regulaminów lub dokumentacji aplikacji, jeśli odnoszą się one do zaistniałego przypadku,
   - przygotować opis incydentu,
   - nie opuszczać bez uzasadnionej przyczyny miejsca zdarzenia do czasu przybycia administratora bezpieczeństwa informacji lub osoby przez niego wskazanej.
3) Administrator bezpieczeństwa informacji po otrzymaniu zawiadomienia, o którym mowa w pkt 1, powinien niezwłocznie:
   - przeprowadzić postępowanie wyjaśniające w celu ustalenia okoliczności naruszenia ochrony danych osobowych,
   - podjąć działania chroniące system przed ponownym naruszeniem,
   - w przypadku stwierdzenia faktycznego naruszenia bezpieczeństwa systemu sporządzić raport naruszenia bezpieczeństwa systemu informatycznego administratora danych, a następnie niezwłocznie przekazać jego kopię administratorowi danych.
4) Administrator bezpieczeństwa informacji w uzgodnieniu z administratorem systemu może zarządzić, w razie potrzeby, odłączenie części systemu informatycznego dotkniętej incydentem od pozostałej jego części.
5) W razie odtwarzania danych z kopii zapasowych administrator systemu obowiązany jest upewnić się, że odtwarzane dane zapisane zostały przed wystąpieniem incydentu (dotyczy to zwłaszcza przypadków infekcji wirusowej).
6) Administrator danych po zapoznaniu się z raportem, o którym mowa w pkt 4 lit. c, podejmuje decyzję o dalszym trybie postępowania, powiadomieniu właściwych organów oraz podjęciu innych szczególnych czynności zapewniających bezpieczeństwo systemu informatycznego

administratora danych bądź zastosowaniu środków ochrony fizycznej.

7) Administrator bezpieczeństwa informacji i administrator systemu zobowiązani są do informowania administratora danych o awariach systemu informatycznego, zauważonych przypadkach naruszenia niniejszej instrukcji przez użytkowników, a zwłaszcza o przypadkach posługiwania się przez użytkowników nieautoryzowanymi programami, nieprzestrzegania zasad używania oprogramowania antywirusowego, niewłaściwego wykorzystania sprzętu komputerowego lub przetwarzania danych w sposób niezgodny z procedurami ochrony danych osobowych.
8) Administrator bezpieczeństwa informacji składa raz w miesiącu informacje o przeprowadzonych działaniach oraz raz w roku administratorowi danych kompleksową analizę zarządzania systemem informatycznym.

14. Postanowienia końcowe

a) W sprawach nieokreślonych niniejszą instrukcją należy stosować instrukcje obsługi i zalecenia producentów aktualnie wykorzystywanych urządzeń i programów.
b) Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się przed dopuszczeniem do przetwarzania danych z niniejszą instrukcją oraz złożyć stosowne oświadczenie, potwierdzające znajomość jej treści.

Niezastosowanie się do procedur określonych w niniejszej instrukcji przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52 kodeksu pracy.

Niniejsza instrukcja wchodzi w życie z dniem podpisania.

Zał. Nr 3
do Zarządzenia Nr 0152/61/2009
z dnia 12.02.2009r.

Bojszowy, dn ……..

UPOWAŻNIENIE Nr ……..

Upoważniam Pana/ią ……
– …….
stanowisko służbowe

Do przetwarzania danych osobowych na stacjonarnym sprzęcie komputerowym (edytory tekstu, arkusze kalkulacyjne itp.) oraz kartotekach, skorowidzach itp. zgodnie z powierzonym Pani zakresem czynności z dnia…… . ABI nada Pani hasło i indywidualny login przyporządkowany wyłącznie Pani i tylko Pani może go używać. Zabrania się udostępniania hasła i loginu innemu pracownikowi.

1. Zobowiązuję Pana/Panią do dbania o bezpieczeństwo powierzonych mu do przetwarzania, archiwizowania lub przechowywania danych zgodnie z obowiązującą w Urzędzie Polityką Bezpieczeństwa, regulaminami i instrukcjami wewnętrznymi, w tym m. in.:
   a) Chronić dane przed dostępem osób nieupoważnionych,
   b) Chronić dane przed przypadkowym lub nieumyślnym zniszczeniem, utratą lub modyfikacją,
   c) Chronić nośniki magnetyczne i optyczne oraz wydruki komputerowe przed dostępem osób nieupoważnionych oraz przed przypadkowym zniszczeniem,
   d) Utrzymywać w tajemnicy powierzone identyfikatory, hasła, częstotliwość ich zmiany oraz szczegóły technologiczne systemów także po ustaniu zatrudnienia w Urzędzie.
   e) Archiwizować dane,
2. Zabrania się pod rygorem odpowiedzialności służbowej i karnej:

a) Ujawniać dane – w tym dane osobowe zawarte w obsługiwanych systemach,
b) Kopiować bazy danych lub ich części poza przewidzianymi kopiami bezpieczeństwa,
c) Zabrania się przetwarzania danych w sposób inny niż opisany instrukcją.
d) Instalacji nielegalnego oprogramowania mogącego naruszyć bezpieczeństwo danych osobowych

……
(podpis Administrator Danych)

OŚWIADCZENIE

1. Stwierdzam własnoręcznym podpisem, że znana mi jest treść przepisów:
   a) ustawy o ochronie danych osobowych :(tekst pierwotny Dz. U. 1997 r. Nr 133 poz. 883),
   b) ustawy o ochronie informacji niejawnej z dn. 5.08.2010r. (Dz. U.2010. Nr 182 poz. 1228 z póź. zmianami)
   c) rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100 poz. 1024 z 2004 r.) oraz odpowiedzialności karnej za naruszenie ochrony danych osobowych.
   d) zapoznałem się z przyjętą polityką bezpieczeństwa i instrukcji zarządzania systemami informatycznymi.
2. Jednocześnie zobowiązuję się nie ujawniać wiadomości, z którymi zapoznałem/zapoznałam się z racji wykonywanej pracy w Urzędzie Gminy, a w szczególności nie będę:
   a) ujawniać danych zawartych w eksploatowanych w Urzędzie systemach informatycznych, zwłaszcza danych osobowych znajdujących się w tych systemach,
   b) ujawniać szczegółów technologicznych używanych w Urzędzie systemów oraz oprogramowania,
   c) instalował oprogramowania innego niż użytkowany bez pisemnego uzgodnienia z Administratorem Bezpieczeństwa Informacji ABI.

d) udostępniać osobom nieupoważnionym nośniki magnetyczne i optyczne oraz wydruki komputerowe,
e) kopiować lub przetwarzać danych w sposób inny niż dopuszczony obowiązującą instrukcją.

……..
(podpis pracownika)

Zał. Nr 4
do Zarządzenia Nr 0152/61/2009
z dnia 12.02.2009r.

SPIS UPOWAŻNIEŃ WYDANYCH

ZGODNIE Z ZARZĄDZENIEM NR 0152/61 /2009 WÓJTA GMINY BOJSZOWY z dnia 12.09.2009r. w sprawie: polityki bezpieczeństwa ochrony danych osobowych i instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania osobowych ochrony danych osobowych.

L.p.	Nazwisko i imię	Stanowisko	Numer upoważnienia	Data ważności	Uwagi
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					

Zał. Nr 5
do Zarządzenia Nr 0152/61/2009
z dnia 12.02.2009r

EWIDENCJA OSÓB UPOWAŻNIONYCH
DO SYSTEMÓW PRZETWARZAJĄCYCH DANE OSOBOWYCH W URZĘDZIE GMINY BOJSZOWY

Niniejszy dokument stanowi wykonanie art.39 ust.l ustawy z dnia 29 sierpnia 1997 r. o *ochronie danych osobowych* (Dz.U. z 2002 r. Nr 101, poz. 926 ze zm.)

Na podstawie art. 37 ustawy o ochronie danych osobowych do przetwarzania danych dopuszczone zostały następujące osoby:

L.p.	Nazwisko i imię	Stanowisko	Numer upoważnienia do przetwarzani8a danych osobowych	Identyfikator w systemie	Data ważności	Przedłużenie ważności/data wygaśnięcia	Zakres upoważnienia – dostęp do bazy danych	Uwagi
1.								
2.								
3.								
4.								
5.								