Zarządzenie Nr 21.....
Wójta Gminy Miedziana Góra
z dnia...20.04.....2007 roku

w sprawie powołania komisji konkursowej w celu przeprowadzenia konkursu na stanowisko dyrektora Zespołu Szkół w Ćmińsku

Na podstawie art.18 ust.2 pkt.5 z dnia 8 marca 1990r.o samorządzie Gminnym /Dz.U.z 2001r.Nr 142,poz.1591 z późn.zm./,oraz art.36a ust.5 ustawy z dnia 7 września 1991r.o systemie oświaty/Dz.U.z 2004r.Nr 256, poz.2572 z późn.zm./uchwala się co następuje:

§ 1

Powołuje się Komisję do przeprowadzenia konkursu na stanowisko dyrektora **Zespołu Szkół w Ćmińsku**

1. przedstawiciele organu prowadzącego:

...Jan Szustak..... - przewodniczący komisji
...Feliks Januchta..... - członek komisji
...Jarosław Wałek..... ..... - członek komisji

2. przedstawiciele organu nadzoru pedagogicznego:

..Emilia Wojdyła..... - członek komisji
..Urszula Wojsław- Kozłowska..... - członek komisji
..Bożena Wróbel..... - członek komisji

3. przedstawiciele rady pedagogicznej:

...Marzena Zagdan..... - członek komisji
.. Teresa Ciszek..... - członek komisji

4. przedstawiciele rady rodziców:

....Edward Zbroszczyk..... - członek komisji
....Dorota Ciołak..... - członek komisji

5. przedstawiciel Związku Nauczycielstwa Polskiego:

.....Wojciech Ziębiński..... - członek komisji

6. przedstawiciel Związku Zawodowego NSZZ „ Solidarność „

.....Henryk Ślusarski.....- członek komisji

§ 2

Zadaniem komisji jest wyłonienie kandydata na stanowisko dyrektora Szkoły Podstawowej w Porzeczu

§ 3

Komisja działać będzie w oparciu o Regulamin określony w rozporządzeniu Ministra Edukacji Narodowej i Sportu z dnia 23 października 2003 r / Dz.U.Nr 189,poz.1855/, stanowiący załącznik do niniejszego Zarządzenia

§ 4

Wykonanie Zarządzenia powierza się kierownikowi ZOEAS

§ 5

Zarządzenie wchodzi w życie z dniem podjęcia.

WÓJT

mgr inż. Maciej Lubocki

Zarządzenie Nr.22...
Wójta Gminy Miedziana Góra
z dnia...20.04.....2007 roku

w sprawie powołania komisji konkursowej w celu przeprowadzenia konkursu na stanowisko dyrektora Szkoły Podstawowej w Porzeczu

Na podstawie art.18 ust.2 pkt.5 z dnia 8 marca 1990r.o samorządzie Gminnym /Dz.U.z 2001r.Nr 142,poz.1591 z późn.zm./,oraz art.36a ust.5 Ustawy z dnia 7 września 1991r.o systemie oświaty/Dz.U.z 2004r.Nr 256, Poz.2572 z późn.zm./uchwala się co następuje:

§ 1

Powołuje się Komisję do przeprowadzenia konkursu na stanowisko dyrektora Szkoły Podstawowej w Porzeczu

1. przedstawiciel organu prowadzącego:

   ...Jan Szustak..... - przewodniczący komisji
   ...Feliks Januchta..... - członek komisji
   ...Jarosław Wałek..... ..... - członek komisji
2. przedstawiciele organu nadzoru pedagogicznego:
   ..Emilia Wojdyła..... - członek komisji
   ..Urszula Wojsław- Kozłowska..... - członek komisji
   ..Bożena Wróbel..... - członek komisji
3. przedstawiciele rady pedagogicznej:
   ...Dorota Bielacha..... - członek komisji
   ...Stanisław Ciosek..... - członek komisji
4. przedstawiciele rady rodziców :
   ....Barbara Moćko..... - członek komisji
   ....Justyna Preka..... - członek komisji
5. przedstawiciel Związku Nauczycielstwa Polskiego:
   .....Wojciech Ziębiński..... - członek komisji
6. przedstawiciel Związku Zawodowego
   NSZZ „ Solidarność"
   .....Mirosław Walaszczyński.....- członek komisji

§ 2

Zadaniem komisji jest wyłonienie kandydata na stanowisko dyrektora Szkoły Podstawowej w Porzeczu

§ 3

Komisja działać będzie w oparciu o Regulamin określony w rozporządzeniu Ministra Edukacji Narodowej i Sportu z dnia 23 października 2003 r / Dz.U.Nr 189,poz.1855/, stanowiący załącznik do niniejszego Zarządzenia

§ 4

Wykonanie Zarządzenia powierza się kierownikowi ZOEAS

§ 5

Zarządzenie wchodzi w życie z dniem podjęcia.

WÓJT

mgr inż. Maciej Lubecki

Zarządzenie Nr.23...
Wójta Gminy Miedziana Góra
z dnia.....27.04.....2007 roku

w sprawie powołania komisji konkursowej w celu przeprowadzenia konkursu na stanowisko dyrektora Zespołu Szkół w Ćmińsku

Na podstawie art.18 ust.2 pkt.5 z dnia 8 marca 1990r.o samorządzie Gminnym /Dz.U.z 2001r.Nr 142,poz.1591 z późn.zm./,oraz art.36a ust.5 ustawy z dnia 7 września 1991r.o systemie oświaty/Dz.U.z 2004r.Nr 256, poz.2572 z późn.zm./uchwala się co następuje:

§ 1

Powołuje się Komisję do przeprowadzenia konkursu na stanowisko dyrektora **Zespołu Szkół w Ćmińsku**

1. przedstawiciele organu prowadzącego:

...Jan Szustak..... - przewodniczący komisji
...Feliks Januchta..... - członek komisji
...Jarosław Wałek..... ..... - członek komisji

2. przedstawiciele organu nadzoru pedagogicznego:

..Emilia Wojdyła..... - członek komisji
..Urszula Wojsław- Kozłowska..... - członek komisji
..Bożena Wróbel..... - członek komisji

3. przedstawiciele rady pedagogicznej:

...Marzena Zagdan..... - członek komisji
.. Teresa Ciszek..... - członek komisji

4. przedstawiciele rady rodziców:

....Edward Zbroszczyk..... - członek komisji
....Dorota Ciołak..... - członek komisji

5. przedstawiciel Związku Nauczycielstwa Polskiego:

.....Wojciech Ziębiński..... - członek komisji

6. przedstawiciel Związku Zawodowego NSZZ „ Solidarność „

.....Krzysztof Stępniewskii.....- członek komisji

§ 2

Zadaniem komisji jest wyłonienie kandydata na stanowisko dyrektora Szkoły Podstawowej w Porzeczu

§ 3

Komisja działać będzie w oparciu o Regulamin określony w rozporządzeniu Ministra Edukacji Narodowej i Sportu z dnia 23 października 2003 r / Dz.U.Nr 189,poz.1855/, stanowiący załącznik do niniejszego Zarządzenia

§ 4

Wykonanie Zarządzenia powierza się kierownikowi ZOEAS

§ 5

Zarządzenie wchodzi w życie z dniem podjęcia.

WÓJT

mgr inż. Maciej Lubecki

Zarządzenie Nr 23 /2007
Wójta Gminy w Miedzianej Górze
z dnia 23 maja 2007 roku

w sprawie zmian w budżecie gminy na rok 2007.

Na podstawie art. 30 ust. 2 pkt 4 ustawy z dnia 8 marca 1990 roku o samorządzie gminnym (tekst jednolity z 2001r Dz. U. Nr 142 poz. 1591 z póź. zm.) oraz art. 128 ust. 1 pkt 1 ustawy z dnia 30 czerwca 2005 roku o finansach publicznych (Dz. U. Nr 249 poz. 2104), Uchwały Rady Gminy Nr IV/28/07 z dnia 15 marca 2007 roku § 11, umowy zawartej w dniu 1 marca 2007 roku pomiędzy Wyższą Szkołą Ekonomi, Turystyki i Nauk Społecznych z siedzibą w Kielcach a Gminą Miedziana Góra, oraz pisma ŚUW Wydział Finansowy Znak:FN.I3011/37/2007, pisma ŚUW Wydział Finansowy Znak FN.I.3011/32/2007, zarządza się co następuje:

§ 1.

Zwiększa się dochody budżetowe o kwotę **151 290,00zł,**
w tym:

dział	010	rozdział	01095	§	2010	o kwotę	2 624,00
dział	801	rozdział	80195	§	2887	o kwotę	45 000,00
dział	801	rozdział	80195	§	2886	o kwotę	15 000,00
dział	852	rozdział	85295	§	2030	o kwotę	88 666,00

§ 2.

Zwiększa się wydatki budżetowe o kwotę **151 290,00zł,**
w tym:

dział	010	rozdział	01095	§	4430	o kwotę	2 572,00
dział	010	rozdział	01095	§	4210	o kwotę	52,00
dział	801	rozdział	80195	§	4177	o kwotę	8 625,00
dział	801	rozdział	80195	§	4176	o kwotę	2 875,00
dział	801	rozdział	80195	§	4217	o kwotę	20 475,00
dział	801	rozdział	80195	§	4216	o kwotę	6 825,00
dział	801	rozdział	80195	§	4247	o kwotę	750,00
dział	801	rozdział	80195	§	4246	o kwotę	250,00
dział	801	rozdział	80195	§	4307	o kwotę	15 150,00
dział	801	rozdział	80195	§	4306	o kwotę	5 050,00
dział	852	rozdział	85295	§	3110	o kwotę	88 666,00

§34.

Zarządzenie wchodzi w życie z dniem podjęcia.

WÓJT
mgr inż. Maciej Lubecki

Zarządzenie Nr 24/07
Wójta Gminy Miedziana Góra
z dnia 29 maja 2007 r.

w sprawie ustalenia " Zespołu do analizy oświadczeń majątkowych".

Na podstawie art. 24 h ust. 6 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U. z 2001 r. Nr 142, poz. 1591 z póź.zm.) zarządzam, co następuje:

§ 1.

Ustalam zespół do analizy oświadczeń majątkowych, zwany dalej "Zespołem" w składzie:
1) Mirosława Duda - Sekretarz Gminy
2) Teresa Reczyńska - Kierownik Referatu Organizacyjnego

§ 2.

Do obowiązków Zespołu należy:
1. wykonanie analizy oświadczeń majątkowych według zasady określonej w ustawie o samorządzie gminnym - art. 24 h ust. 8.
2. sporządzenie opinii zawierającej w szczególności informację o:
   1) osobach, które nie złożyły oświadczeń majątkowych lub złożyły je po terminie,
   2) nieprawidłowościach stwierdzonych w analizowanych oświadczeniach majątkowych, wraz z ich opisem i wskazaniem osób, które złożyły nieprawidłowe oświadczenia,
   3) przedstawienie Radzie Gminy informacji zgodnie z art. 24 h ust. 12 w terminie do 30 października 2007 roku.

§ 3.

Termin wykonania zarządzenia ustalam na dzień 5 czerwca 2007 roku, z wyjątkiem pkt 3 ust. 2 § 2.

§ 4.

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT
mgr inż. Maciej Lubecki

Zarządzenie Nr 26/2007

Wójta Gminy Miedziana Góra

z dnia 19 czerwca 2007 roku

w sprawie powołania stałej komisji inwentaryzacyjnej

§ 1

W celu sprawnego i prawidłowego przeprowadzenia inwentaryzacji powołuję stałą komisję inwentaryzacyjną w następującym składzie:

- Pani Mirosława Duda - przewodniczący komisji
- Pani Bożena Moćko - z-ca przewodniczącego komisji
- Pan Dominik Słoń - członek komisji

§ 2

Przewodniczącego komisji inwentaryzacyjnej zobowiązuje się do:

- sprawowania nadzoru nad przebiegiem i dokumentowaniem inwentaryzacji w celu zapewnienia sprawnego i terminowego przeprowadzenia inwentaryzacji,
- przeprowadzenia szkolenia i instruktażu przy współudziale Skarbnika Gminy wszystkich członków komisji i członków zespołów spisowych,
- objęcie szczegółową ewidencją i rozliczanie pobranych arkuszy spisowych.
- pobranie wyjaśnień od osób materialnie odpowiedzialnych, w przypadku wystąpienia różnić inwentaryzacyjnych,
- ustalenie przyczyn powstania różnic inwentaryzacyjnych i wnioskowanie w sprawie ich rozliczenia,
- sporządzenie sprawozdania z przygotowania, przebiegu i zakończenia czynności inwentaryzacyjnych.

§ 3

Na wniosek przewodniczącego komisji inwentaryzacyjnej zostaną powołane zespoły spisowe.

§ 4

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT

mgr inż. Maciej Lubecki

[redacted]

roku § 11, zarządza się co następuje:

§ 1.

Zmniejsza się wydatki budżetowe o kwotę **22 210zł,**
w tym:

dział	758	rozdział	75818	§	4810	o kwotę	15 210
dział	926	rozdział	92601	§	4300	o kwotę	7 000

§ 2.

Zwiększa się wydatki budżetowe o kwotę **22 210zł,**
w tym:

dział	010	rozdział	01010	§	4300	o kwotę	5 000
dział	700	rozdział	70004	§	4210	o kwotę	10 000
dział	854	rozdział	85415	§	3240	o kwotę	210
dział	926	rozdział	92601	§	4210	o kwotę	7 000

§34.

Zarządzenie wchodzi w życie z dniem podjęcia.

WÓJT

mgr inż. Maciej Lubecki

Zarządzenie Nr 27/2007
Wójta Gminy Miedziana Góra
z dnia 19 czerwca 2007 roku

w sprawie przeprowadzenia inwentaryzacji w Szkołach i Przedszkolu Gminy Miedziana Góra

Na podstawie art. 26–27 ustawy o rachunkowości z dnia 29 września 1994 roku (Dz. U. Nr 121, poz. 591 z późn. zm.) oraz Rozporządzenia Ministra Finansów z dnia 18 grudnia 2001 roku w sprawie zasad rachunkowości oraz planów kont dla budżetu państwa, budżetu jednostek samorządowych oraz niektórych jednostek sektora finansów publicznych Dz. U. Nr 153 poz. 1753 z późn. zm.) oraz Instrukcji inwentaryzacyjnej (Zarządzenie Nr 40/2006 Wójta Gminy z dnia 30 listopada 2006 roku).

zarządzam przeprowadzenie spisu z natury:

1. Nazwa obiektu i oznaczenie pomieszczenia, w którym przeprowadza się spis:
   - Szkoła Podstawowa w Kostomłotach II
   - Gimnazjum w Kostomłotach II
   - Przedszkole w Kosomłotach II
   - Szkoła Podstawowa w Ćmińku
   - Gimnazjum w Ćmińsku
   - Szkoła Podstawowa w Porzeczu
2. Rodzaj inwentaryzacji (okresowa, zdawczo-odbiorcza)
3. Rodzaj spisywanych składników
   - środki trwałe w użytkowaniu – wyposażenie
   - materiały i towary, paliwo i opał
4. Spis należy przeprowadzić wg stanu na dzień 31 sierpnia 2007 roku
5. Osobami odpowiedzialnymi za spisywanie składników majątku są Dyrektorzy Szkół i Przedszkola.
6. Termin zakończenia 31 sierpnia 2007 roku.
7. Do przeprowadzenia spisu z natury wymienionych składników majątkowych prosimy wyznaczyć zespoły spisowe.
8. Po zakończeniu spisu z natury należy złożyć sprawozdanie na piśmie do Stałej Komisji Inwentaryzacyjnej Urzędu Gminy.

WÓJT
mgr inż. Maciej Lubecki

ZARZĄDZENIE Nr 28/2007
WÓJTA GMINY MIEDZIANA GÓRA

z dnia 20 czerwca 2007

w sprawie wprowadzenia w Urzędzie Gminy Miedziana Góra

„Instrukcji przetwarzania danych osobowych"

Na podstawie art.33 ust.3 i 5 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (j.t. Dz.U. z 2001 nr 142 poz.1591 ze zmianami) w związku z art.36 ust.1 i 2 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (j.t Dz.U. z 2002 nr 101, poz.926) oraz § 3, § 4 i §5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. 2004 nr 100, poz.1024)

zarządzam, co następuje:

§1

Wprowadzam do stosowania **„Instrukcję przetwarzania danych osobowych"** w Urzędzie Gminy, zwaną dalej Instrukcją, określoną załącznikiem nr 1.

§ 2

1. Wykonanie zarządzenia powierzam Sekretarzowi Gminy.
2. Zobowiązuję Kierowników do wdrożenia zasad i procedur określonych w Instrukcji, o której mowa w § 1, w podległych referatach.
3. Zobowiązuję pracowników Urzędu do zapoznania się treścią niniejszego zarządzenia, a oświadczenia o zapoznaniu dołącza się do ich akt osobowych.

§3

Nadzór nad przestrzeganiem Instrukcji powierzam informatykowi, wykonującemu czynności Administratora Bezpieczeństwa Informacji w Urzędzie Gminy w Miedzianej Górze.

§ 4

Traci moc Zarządzenie Nr 9/99 z dnia 23 sierpnia 1999 w sprawie wykonania ustawy o ochronie danych osobowych w Urzędzie Gminy w Miedzianej Górze.

§5

Zarządzenie wchodzi w życie z dniem podpisania .

WÓJT
mgr inż. Marcin Lubecki

RADCA PRAWNY
Ewa Kobeszka
radca prawny

Załącznik nr 1
do Zarządzenia Nr 28/2007
Wójta Gminy Miedziana Góra
z dnia 20 czerwca 2007r.

INSTRUKCJA OCHRONY DANYCH OSOBOWYCH

Rozdział I

Zasady ogólne

§1

Przez użyte w Instrukcji następujące określenia należy rozumieć:

1) **Ustawa** – Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. 2002 r. Nr 101 poz. 926, ze zm.),
2) **Rozporządzenie** – Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych,
3) **Dane** – to surowe niepoddane analizie liczby, pojęcia, fakty, obrazy
4) **Dana** – to taka postać informacji, która może być przetworzona z użyciem sprzętu komputerowego
5) **Informacja** – jest wynikiem uporządkowania danych lub ich przeanalizowania w jakiś konkretny sposób
6) **Zbiór danych** - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
7) **Przetwarzanie danych** - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
8) **System informatyczny** - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
9) **Zabezpieczenie danych w systemie informatycznym** - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
10) **Usuwanie danych** - rozumie się przez to trwałe zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
11) **Administrator Danych Osobowych** - Wójt Gminy Miedziana Góra,
12) **Administrator Bezpieczeństwa Informacji** – Informatyk,
13) **Urząd** – Urząd Gminy w Miedzianej Górze,
14) **Kierownik** – Kierownik referatu, w której zatrudniony jest pracownik, przetwarzający dane osobowe,
15) **Pracownik komórki organizacyjnej** - pracownika samorządowego zatrudnionego w ramach stosunku pracy w Urzędzie bądź osobę wykonującą określone czynności:
    - w ramach umowy cywilnoprawnej na rzecz Urzędu
    - odbywanego stażu absolwenckiego
    - praktyki studenckiej, wolontariatu
16) **Zwrotna informacja telefoniczna** - czynności polegająca na:
    - przyjęciu wniosku telefonicznego o udostępnienia danych wraz z informacją o tożsamości, nazwie komórki organizacyjnej oraz numerze telefonu wnioskodawcy
    - oddzwonieniu ze stosowną informacją bądź danymi, po uprzednim sprawdzeniu prawdziwości i autentyczności wnioskodawcy.

    Procedura ta stosowana jest wyłącznie wewnątrz budynku Urzędu !!!

§2

Do kompetencji Administratora Danych Osobowych należy prowadzenie całokształtu spraw związanych z przetwarzaniem danych osobowych, a w szczególności:

1) udostępnianie danych osobowych,
2) kontrola i nadzór w zakresie przestrzegania zasad i procedur przetwarzania danych osobowych w Urzędzie, z uwzględnieniem kryterium celowości i adekwatności oraz warunków organizacyjno-technicznych,
3) rejestracja zbiorów danych osobowych w rejestrze Generalnego Inspektora Ochrony Danych Osobowych,
4) prowadzenie korespondencji z Generalnym Inspektorem Ochrony Danych Osobowych,
5) podpisywanie umowy o powierzenie danych osobowych podmiotowi zewnętrznemu oraz kontrolę przestrzegania prawa przez strony umowy,

§3

1. Administrator Bezpieczeństwa Informacji, z upoważnienia Administratora Danych Osobowych:
   1) zarządza i nadzoruje systemem informatycznym, gdzie przetwarzane są dane osobowe,
   2) ponosi odpowiedzialność za bezpieczeństwo danych osobowych i zbiorów danych osobowych w systemie informatycznym,
   3) podejmuje działania w przypadku naruszenia lub podejrzenia naruszenia systemu informatycznego.
2. Kierownik wykonuje czynności przetwarzania danych osobowych w ramach zbiorów, funkcjonujących w podległej komórce organizacyjnej, z upoważnienia Administratora Danych Osobowych, z wyłączeniem udostępniania danych osobowych.
3. Pracownik komórki organizacyjnej dokonuje czynności przetwarzania danych osobowych, z upoważnienia Administratora Danych Osobowych, w zakresie indywidualnych obowiązków pracowniczych bądź wskazanych czynności w umowie, z wyłączeniem czynności udostępniania danych osobowych.

Rozdział II

Obowiązki pracowników

§4

1. Obowiązek przestrzegania tajemnicy danych osobowych dotyczy wszystkich pracowników, którzy mają dostęp do informacji o charakterze danych osobowych.
2. Naruszenie zasad ochrony danych osobowych, w efekcie którego nastąpiło udostępnienie danych osobie nie upoważnionej, jest ciężkim naruszeniem obowiązków pracowniczych.

§5

1. Osoby, wymienione w §3 i §4, są zobowiązane do:
   1) zapoznania się z przepisami prawa w zakresie ochrony danych osobowych,
   2) stosowania określonych przez Administratora Danych Osobowych zasad, procedur oraz wytycznych mających na celu właściwe i adekwatne przetwarzanie danych
   3) należytego zabezpieczenia danych przed ich udostępnianiem osobom nieupoważnionym,
   4) zachowania szczególnej staranności w trakcie dokonywania operacji przetwarzania danych w celu ochrony interesów osób, których dane dotyczą.
2. Kierownik komórki organizacyjnej poza obowiązkami jest zobowiązany do:
   1) zapewnienia organizacyjno-technicznej ochrony danych osobowych,
   2) kontroli przestrzegania zasad i sposobu wykonywania operacji przetwarzania danych przez podległych pracowników,

3) sygnalizowania niezgodności aktów prawnych gminy oraz innych aktów wewnętrznych Urzędu z przepisami ustawowymi w zakresie ochrony danych osobowych i przedstawiania stosownych projektów zmian, mających na celu ich dostosowanie do regulacji ustawowej,

4) zwracanie się do Administratora Danych Osobowych, w przypadku wątpliwości co do stosowania przepisów prawnych z zakresu ochrony danych osobowych, o wiążące wytyczne.

Rozdział III

Procedury szczegółowe

§6

1. Administrator Danych Osobowych może upoważnić do udostępniania danych osobowych w zakresie szczegółowo określonych zbiorów Urzędu:
   1) Kierownika na umotywowany wniosek
   2) pozostałych pracowników komórek organizacyjnych na umotywowany wniosek
2. W okolicznościach zmiany zakresu obowiązku bądź stanowiska lub funkcji, Administrator Danych Osobowych cofa upoważnienie, o którym mowa w ust.1 na uzasadniony wniosek osób, których mowa w ust.1 pkt 1 i 2.
3. Wzór upoważnienia, o którym mowa w ust.1, stanowi załącznik nr 1 do niniejszej instrukcji.

§7

1. W przypadku przyjęcia do pracy nowego pracownika komórki organizacyjnej, którego zakres obowiązków obejmować będzie przetwarzanie danych osobowych, Kierownik zobowiązany jest zwrócić się do Administratora Danych Osobowych o wydanie upoważnienia (załącznik nr 3) do przetwarzania danych osobowych (załącznik nr 2).
2. Pracownik, któremu udzielono stosowne upoważnienie, o których mowa w ust.1, jest zobowiązany do podpisania oświadczenia, którego wzór stanowi załącznik nr 2 do niniejszej instrukcji.
3. W przypadku zmiany stanowiska, zakresu obowiązków pracowniczych, bądź w sytuacji określonej w § 12, która ma bezpośredni wpływ na rodzaj i zakres przetwarzanych danych, Kierownik zobowiązany jest bezzwłocznie skierować wniosek o wydanie bądź cofnięcie stosownego upoważnienia, którego wzór stanowi załącznik nr 3 do niniejszej instrukcji.

§8

1. W przypadku nawiązania stosunku pracy na stanowisku Kierownika komórki organizacyjnej, w zakresie której jest prowadzenie zbiorów danych osobowych Administrator Danych Osobowych wydaje upoważnienie do przetwarzania danych osobowych.
2. W przypadku zmiany na stanowisku Kierownika bądź w sytuacji określonej w § 9, Administrator Danych Osobowych wydaje bądź cofa stosowne upoważnienie, którego wzór stanowi załącznik nr 3 do niniejszej instrukcji

§9

Wypowiedzenie umowy o pracę przez pracodawcę powoduje wygaśnięcie upoważnienia do udostępniania danych, o którym mowa w § 6, oraz upoważnienia do przetwarzania danych, o którym mowa w §7, z dniem wręczenia wypowiedzenia umowy o pracę.

§ 10

1. Kadry Urzędu prowadzą ewidencję osób upoważnionych do przetwarzania danych, o których mowa §7 i §8
2. Informatyk zobowiązany jest do współpracy z kadrami w zakresie aktualizacji ewidencji, o której mowa w ust.1, a dotyczącej identyfikatorów pracowników, którzy posiadają upoważnienia.

§11

W przypadku konieczności utworzenia nowego zbioru danych, wynikającej z obowiązków nałożonych przepisami ustawy bądź nowymi zadaniami, Kierownik zobowiązany jest niezwłocznie - nie później jednak niż w ciągu 30 dni od dnia powstania obowiązku utworzenia zbioru - złożyć Administratorowi Danych Osobowych projekt wniosku o zarejestrowanie zbioru danych osobowych, którego wzór stanowi załącznik do Rozporządzenia, o którym mowa w § 1 pkt 2.

§12

1. W obiegu zewnętrznym dane osobowe udostępnia ze zbiorów zgodnie z powszechnie obowiązującymi w tym zakresie przepisami, Administrator Danych Osobowych lub osoba przez niego upoważniona, w trybie § 6 niniejszej instrukcji.
2. W obiegu wewnętrznym między komórkami organizacyjnymi Urzędu, chyba że przepisy szczególne stanowią inaczej, można udostępniać dane osobowe w następującym trybie:
informacje zawierające dane: imię, nazwisko, adres zamieszkania i inne o charakterze podstawowym, bezpośrednio identyfikujące osobę fizyczną może udostępnić pracownik przetwarzający dane w formie bezpośredniej lub telefonicznej, po sprawdzeniu tożsamości w procedurze „zwrotnej informacji telefonicznej".
3. Przekazywanie danych w trybie ust.2, może odbywa się tylko i wyłącznie w przypadku toczącego się postępowania administracyjnego bądź cywilnego w stosunku do osoby, której dane dotyczą.

§13

1. W umowach zawieranych przez komórki organizacyjne Urzędu, w przypadku zaistnienia okoliczności powierzenia danych osobowych podmiotowi zewnętrznemu w celu wykonania określonych czynności na tych danych, każdorazowo wymagany jest zapis o powierzeniu danych osobowych bądź zawarcie odrębnej umowy powierzenia.
2. W przypadkach, o których mowa w ust.1, właściwy Kierownik niezwłocznie, nie później jednak niż w ciągu 15 dni:
   1) przed podpisaniem umowy, w której został zawarty zapis o powierzeniu
   2) przed datą planowanego powierzenia danych, na podstawie odrębnej umowy powierzenia

   przekazuje Administratorowi Danych Osobowych projekt umowy, o której mowa w pkt 1 lub projekt umowy, o której mowa w pkt 2.

Rozdział IV

Zarządzanie systemem informatycznym służącym przetwarzaniu danych osobowych

§14

Uwzględniając kategorie danych osobowych oraz stopień bezpieczeństwa ich przetwarzania w systemie informatycznym Urzędu wprowadza się poziom wysoki.

§15

Do obowiązków Administratora Bezpieczeństwa Informacji należy wdrażanie i kontrola stosowania środków technicznych, służących do zabezpieczenia systemu informatycznego w celu realizacji wymogów rozliczalności, poufności i integralności, w szczególności :

1) nadawanie uprawnień użytkownikowi,
2) stosowanie mechanizmów uwierzytelnienia użytkownika,
3) kontrola dostępu do danych osobowych i zbiorów danych osobowych,
4) stosowanie środków ochrony w ramach oprogramowania urządzeń teletransmisyjnych, systemów, narzędzi i systemu użytkowego,
5) administrowanie sprzętem informatycznym,
6) zapewnianie właściwej obsługi sprzętowej i programowej komórek organizacyjnej w celu zapewnienia właściwego standardu jakości przetwarzania.

§16

Kierownik jest zobowiązany do:

1) każdorazowego informowania administratora bezpieczeństwa informacji planowanych przemieszczeniach sprzętu komputerowego i pracowników między pokojami (budynkami Urzędu, gdzie dokonuje się czynności przetwarzania danych).
2) zapewnienia odpowiednich warunków organizacyjno-technicznych w zakresie wyposażenia stanowisk pracy przetwarzających dane osobowe, umożliwiających zachowanie poufności informacji (dostęp do pomieszczeń, szaf z aktami),

3) nadzorowania warunków przechowywania wydruków zawierających dane osobowe, ich archiwizowania i okresowego niszczenia oraz przechowywania danych osobowych na dyskietkach i CD lub DVD-ROM-ach

4) wnioskowania o przyznanie podległemu pracownikowi sprzętu komputerowego, niezbędnego do wykonywania wyznaczonych czynności w systemie informatycznym i przyznanie identyfikatora.

§17

Szczegółowe wdrożenie programowych i sprzętowych rozwiązań w zakresie zabezpieczania danych osobowych w poszczególnych komórkach organizacyjnych zapewnia wyznaczony Informatyk.

§18

1. Administrator Bezpieczeństwa Informacji nadaje uprawnienia dostępu do systemu w formie identyfikatorów i haseł poszczególnym użytkownikom oraz rejestruje i wyrejestrowuje użytkowników w systemie informatycznym.
2. Identyfikator osoby, która utraciła uprawnienie do dostępu do danych osobowych, Informatyk jest zobowiązany niezwłocznie wyrejestrować, unieważnić jej hasło oraz podjąć inne stosowne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych.
3. Realizując obowiązki, o którym mowa w ust. 1 i 2, prowadzi się ewidencję identyfikatorów użytkowników.

§19

1. Każdy użytkownik, korzystający z systemu informatycznego zobowiązany jest do posługiwania się przydzielonym hasłem, zmienianym co miesiąc oraz identyfikatorem, który nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego nie powinien być przydzielany innym osobom.
2. Przydział hasła następuje raz w miesiącu, następnych zmian hasła dokonuje użytkownik pod kontrolą Informatyka.
3. Hasło, o którym mowa w ust.2, składa się z co najmniej 8 znaków.

§20

2. Użytkownik przystępując do pracy w systemie powinien podać dane dostępu do komputera i do użytkowanej aplikacji, zaś kończąc pracę prawidłowo zakończyć jego użytkowanie.
3. Użytkownik może posługiwać się jedynie programami autoryzowanymi, prowadzanych do systemu informatycznego w uzgodnieniu z Informatykiem.
4. Użytkownik wykonuje wydruki związane z przetwarzaniem danych osobowych wyłącznie w zakresie i ilości niezbędnej dla celów zawodowych w uzgodnieniu z przełożonym.
5. Użytkownik przechowuje wydruki z danymi osobowymi w zamykanych i zabezpieczonych sejfach bądź szafach.

§21

1. System informatyczny Urzędu przeprowadza automatycznie:

   1) tworzenie kopii zapasowych baz informatycznych,

   2) kontrolę antywirusową

   3) archiwizacją plików na dzień 31 grudnia każdego roku

2. W przypadku korzystania z nośników elektronicznych, pochodzącego od podmiotu zewnętrznego, użytkownik jest zobowiązany do **sprawdzania** go programem antywirusowym.
3. Nośniki elektroniczne są przechowywane przez czas ich użyteczności poza obszarem przetwarzania danych osobowych tzn. w Kancelarii Tajnej, a następnie dane z nich są usuwane bądź nośniki fizycznie niszczone.

§22

1. Archiwum plików, o którym mowa w § 21 ust.1 pkt 3 jest przechowywany przez okres 5 lat na odrębnych nośnikach informatycznych w Kancelarii Tajnej
2. Po upływie okresu, o którym mowa w ust.1, Administrator Bezpieczeństwa Informacji na wniosek Kierownika może przedłużyć okres przechowywania archiwum plików ze względu na ich znaczenie prawne, organizacyjne bądź techniczne dokumentów bądź zapisów tam zawartych.

§23

1. System informatyczny Urzędu jest zabezpieczony systemem typy firewall, który wprowadza instrumenty ochrony logicznej, w tym:
   1) kontrolę przepływu informacji między systemem a siecią publiczną
   2) monitoring działań zewnętrznych w stosunku do systemu informatycznego
2. Serwery, obsługujące system informatyczny, pracują, dokonując operacji w wydzielonych i zabezpieczonych pomieszczeniach, do których prawo wstępu posiada wyłącznie Informatyk.

§24

1. Komputery przenośne, zostają przekazane do użytkowania wskazanym pracownikom po podpisaniu protokołu odbioru. Załącznik nr 4.
2. Zakazane jest tworzenie i przetwarzanie zbiorów danych osobowych na komputerach przenośnych.
3. Ewidencje sprzętu o którym mowa w ust. 1 prowadzi Informatyk.

§25

1. Naprawa sprzętu informatycznego odbywa się pod nadzorem Informatyka, który:
   1) sprawdza zawartość zbiorów, podejmując decyzje o sposobie ochrony zbiorów danych poprzez alternatywny wybór:
      a) bezpośredniego nadzoru Informatyka w czasie naprawy
      b) pozbawienie zapisu, uniemożliwiający ich odzyskanie
   2) wprowadza instrumenty ochrony, o których mowa w pkt 1 lit a lub b.
   3) nadzoruje sposób i zakres naprawy sprzętu
2. Likwidacja bądź przekazanie sprzętu komputerowego, na którym przetwarza się dane osobowe następuje bo całkowitym pozbawieniu zapisu danych bądź uszkodzenie w sposób uniemożliwiający ich odczytanie

§26

1. W pomieszczeniach, w których dokonuje się czynności przetwarzania danych, osoby nieuprawnione do dostępu do danych osobowych mogą przebywać wyłącznie w obecności osoby zatrudnionej przy przetwarzaniu tych danych i za zgodą Administratora Danych lub osoby przez niego upoważnionej.
2. Pomieszczenia, o których mowa w ust. 1, na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych, muszą być zamykane w sposób uniemożliwiających dostęp do nich osób postronnych.

§27

Urządzenia i systemy informatyczne służące przetwarzaniu danych muszą być, przez cały czas pracy, zabezpieczone przed utratą tych danych spowodowaną awarią zasilania lub zakłóceniami sieci zasilającej.

§28

Ekrany monitorów na stanowiskach z dostępem do danych osobowych, winny być automatycznie wyłączane po upływie, nie dłużej niż 3 minut nieaktywności użytkownika za pomocą systemowych wygaszaczy zabezpieczonych hasłem.

§29

1. Dla każdej osoby, której dane są przetwarzane w systemie informatycznym, powinny być automatycznie odnotowane:
   1) data pierwszego wprowadzenia danych tej osoby (data pierwszej umowy lub zatrudnienia)
   2) identyfikator użytkownika wprowadzającego dane
   3) dane odbiorców, którym dane zostały udostępnione, jeśli przewidziane jest ich udostępnianie innym podmiotom, chyba, że dane te traktuje się, jako dane jawne.
2. W uzasadnionych przypadkach, uniemożliwiających odnotowywanie, o którym mowa w ust.1 komórki organizacyjne prowadzą wydzielony rejestr odbiorów, którym udostępniono dane osobowe ze zbiorów
3. Nadzór na prawidłowością czynności odnotowania, określoną w ust.1, sprawuje Informatyk w uzgodnieniu z Kierownikiem komórki organizacyjnej.

Rozdział V

Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych

§1

Instrukcja jest przeznaczona dla osób zatrudnionych przy przetwarzaniu danych osobowych w systemie informatycznym.

§2.

Instrukcja określa tryb postępowania w przypadkach, gdy:

1. stwierdzono naruszenie zabezpieczenia systemu informatycznego,
2. stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej wskazują na naruszenie zabezpieczeń tych danych.

§3.

Każdy pracownik który stwierdzi lub podejrzewa naruszenie zabezpieczenia ochrony danych osobowych w systemie informatycznym, ma obowiązek niezwłocznego poinformowania o tym osobę zatrudnioną przy przetwarzaniu danych osobowych lub administratora bezpieczeństwa informacji bądź upoważnioną przez niego osobę.

§4.

Osoba przetwarzająca dane osobowe, która uzyskała informację lub sama stwierdziła naruszenie zabezpieczenia bazy danych osobowych w systemie informatycznym, zobowiązana jest niezwłocznie powiadomić o tym administratora bezpieczeństwa informacji lub inną upoważnioną przez niego osobę, a w przypadku ich nieobecności - bezpośrednio administratora danych osobowych.

§5.

Administrator bezpieczeństwa informacji lub inna upoważniona przez niego osoba powinna w pierwszej kolejności:

1. Zapisać wszelkie **informacje związane** z danym zdarzeniem, a szczególnie: dokładny czas uzyskania informacji o naruszeniu zabezpieczenia danych osobowych i czas samodzielnego wykrycia tego faktu.
2. Na bieżąco **wygenerować** i wydrukować (jeżeli zasoby systemu na to pozwalają) wszystkie **możliwe dokumenty i raporty,** które mogą pomóc w ustaleniu okoliczności zdarzenia, opatrzyć je datą i podpisem.
3. Przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, zwłaszcza do określenia skali zniszczeń i metody dostępu do danych osoby niepowołanej.

§6.

W celu **powstrzymania lub ograniczenia dostępu do danych osoby niepowołanej, należy niezwłocznie podjąć działania zmierzające do** zminimalizowania szkód i zabezpieczenia przed usunięciem śladów jej ingerencji, przez:

1. **fizyczne odłączenie** urządzeń i segmentów sieci, które mogły umożliwić dostęp do bazy danych osobie nie upoważnionej,
2. **wylogowanie** użytkownika podejrzanego o naruszenie zabezpieczenia ochrony danych,
3. **zmianę hasła** na konto administratora i użytkownika, poprzez które uzyskano nielegalny dostęp w celu uniknięcia ponownej próby włamania.

§7.

W celu **powstrzymania lub ograniczenia dostępu do danych osoby niepowołanej, należy niezwłocznie podjąć działania zmierzające do** zminimalizowania szkód i zabezpieczenia przed usunięciem śladów jej ingerencji, przez:

1. **fizyczne odłączenie** urządzeń i segmentów sieci, które mogły umożliwić dostęp do bazy danych osobie nie upoważnionej,
2. **wylogowanie** użytkownika podejrzanego o naruszenie zabezpieczenia ochrony danych,
3. **zmianę hasła** na konto administratora i użytkownika, poprzez które uzyskano nielegalny dostęp w celu uniknięcia ponownej próby włamania.

§8.

Po wyeliminowaniu bezpośredniego zagrożenia przeprowadza się **wstępną analizę stanu systemu** informatycznego w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych w systemie.

§9.

Administrator bezpieczeństwa informacji lub inna upoważniona przez niego osoba sprawdza:

1. stan urządzeń wykorzystywanych do przetwarzania danych osobowych,
2. zawartość zbioru danych osobowych,
3. sposób działania programu,
4. jakość komunikacji w sieci telekomunikacyjnej,
5. wykluczyć możliwość obecności wirusów komputerowych.

§10.

Po dokonaniu powyższych czynności administrator bezpieczeństwa informacji przeprowadza szczegółową analizę stanu systemu informatycznego obejmującego identyfikację:

1. rodzaju zaistniałego zdarzenia,
2. metody dostępu do danych osoby nie upoważnionej,
3. skali zniszczeń.

Następnie przywraca **normalny stan działania systemu,** przy czym, jeżeli nastąpiło uszkodzenie bazy danych, niezbędne jest odtworzenie jej z ostatniej kopii awaryjnej z zachowaniem wszelkich środków ostrożności, mających na celu uniknięcie ponownego uzyskania dostępu tą samą drogą przez osobę niepowołaną. W następnej kolejności przeprowadza szczegółową analizę w celu określenia przyczyny naruszenia ochrony danych osobowych oraz podejmuje działania mające na celu **wyeliminowanie podobnych zdarzeń w przyszłości.**

§11.

1. Jeżeli przyczyną zdarzenia był **błąd pracownika** przetwarzającego dane osobowe w systemie informatycznym, należy przeprowadzić dodatkowe szkolenie wszystkich osób biorących udział przy przetwarzaniu danych.
2. Jeżeli przyczyną zdarzenia było **uaktywnienie wirusa,** ustalić źródło jego pochodzenia oraz wykonać zabezpieczenia antywirusowe.
3. Jeżeli przyczyną zdarzenia było **zaniedbanie** ze strony pracownika zatrudnionego przy przetwarzaniu danych osobowych, zostaną zastosowane konsekwencje regulowane ustawą.
4. Jeżeli przyczyną zdarzenia było **włamanie w celu pozyskania** bazy danych osobowych, dokonuje się szczegółowej analizy wdrożonych środków zabezpieczających w celu zapewnienia skuteczniejszej ochrony bazy danych.
5. Jeżeli przyczyną zdarzenia był **zły stan urządzenia** lub sposób **działania programu,** niezwłocznie przeprowadza się kontrolne czynności serwisowo-programowe.

§12.

Administrator bezpieczeństwa informacji **przygotowuje szczegółowy raport** o przyczynach, przebiegu i wnioskach ze zdarzenia (dołączając ewentualne kopie dowodów dokumentujących to zdarzenie) oraz w określonym terminie od daty zaistnienia zdarzenia przekazuje go administratorowi danych osobowych jednostki.

Rozdział VI

Postanowienia końcowe

§ 1

Tworzy się Politykę bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Gminy w Miedzianej Górze, która stanowi załącznik nr 5

Polityka jest dokumentem wewnętrznym i jest objęta obowiązkiem zachowania w poufności przez wszystkie osoby, którym zostanie ujawniona.

§ 2

Tworzy się Instrukcję zarządzania systemem informatycznym służących do przetwarzania danych osobowych w Urzędzie Gminy w Miedzianej Górze, która stanowi załącznik nr 6

Instrukcja zarządzania jest dokumentem wewnętrznym i jest objęta obowiązkiem zachowania w poufności przez wszystkie osoby, którym zostanie ujawniona.

§ 3

Do spraw nieuregulowanych w instrukcji stosuje się przepisy o ochronie danych osobowych.

§ 4

Dokument nie wyłącza stosowania innych instrukcji dotyczących zabezpieczenia systemów bazodanowych.

§ 5

Integralną część niniejszej Instrukcji stanowią następujące załączniki:

1) Załącznik nr 1 – upoważnienie do udostępniania danych osobowych
2) Załącznik nr 2 – upoważnienie uprawniające do przetwarzania danych osobowych
3) Załącznik nr 3 – wniosek do Administratora Danych Osobowych o cofnięcie / wydanie upoważnienia do przetwarzania danych
4) Załącznik nr 4 – Protokół przekazania w użytkowanie komputera przenośnego
5) Załącznik nr 5 – Polityka bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Gminy w Miedzianej Górze
6) Załącznik nr 6 – Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy w Miedzianej Górze

Załącznik Nr 1

Upoważnienie

uprawniające do udostępniania danych osobowych

Na podstawie § 6 ust.1 Instrukcji Przetwarzania Danych Osobowych upoważniam Pana/Panią ..... do udostępnienia danych osobowych znajdujących się:

1) w systemie informatycznym*)
2) w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych*)

Dane mogą być udostępniane tylko zgodnie z Instrukcją Przetwarzania Danych Osobowych.

Miejsce przetwarzania danych osobowych: referat ..... pokój nr .....

Nazwa zbioru danych: .....

Niniejsze upoważnienia udzielam na okres .....

Miedziana Góra, dnia .....

.....
Administrator Danych Osobowych

*) – niepotrzebne skreślić

Oświadczenie

kierownika referatu .....

Niniejszym oświadczam, że zapoznałem się z Instrukcją Przetwarzania Danych Osobowych. Zapisów w niej zawartych zobowiązuję się przestrzegać z całą starannością i odpowiedzialnością.

.....
czytelny podpis

Miedziana Góra, dnia .....

Załącznik Nr 2

Upoważnienie

uprawniające do przetwarzania danych osobowych

Na podstawie art.37 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz.U. 2002, Nr 101 poz. 926, ze zm.) upoważniam Pana/Panią ..... do przetwarzania danych osobowych:

1) w systemie informatycznym*)
2) w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych*)

Miejsce przetwarzania danych osobowych: referat ..... pokój nr .....

Nazwa zbioru danych: .....

Miedziana Góra, dnia .....

.....
Administrator

*) – niepotrzebne skreślić

Oświadczenie

pracownika przetwarzającego dane osobowe

Niniejszym oświadczam, że zapoznałem się z Instrukcją Przetwarzania Danych Osobowych. Zapisów w niej zawartych zobowiązuję się przestrzegać z całą starannością i odpowiedzialnością.

.....
czytelny podpis

Miedziana Góra, dnia .....

Załącznik Nr 3

Wniosek

do Administratora Danych Osobowych
o cofnięcie / wydanie upoważnienia
uprawniającego do przetwarzania danych

Na podstawie § 7 ust.3 Instrukcji Przetwarzania Danych Osobowych oraz w związku z art.37 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz.U. 2002, Nr 101 poz. 926, ze zm.) zwracam się o cofnięcie/wydanie upoważnia dla Pana/Pani ..... przetwarzającego/ej dane osobowe:

1) w systemie informatycznym*)
2) w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych*)

Miejsce przetwarzania danych osobowych: referat ..... pokój nr .....

Nazwa zbioru danych: .....

.....
(czytelny podpis Kierownika)

*) – niepotrzebne skreślić

Załącznik Nr 4

Protokół
przekazania w użytkowanie komputera przenośnego

1. Zgodnie z Instrukcją Przetwarzania Danych Osobowych wprowadzoną Zarządzeniem nr 28/2007 Wójta Gminy Miedziana Góra z dnia 20 czerwca 2007przekazuję

Panu/i ..... w użytkowanie następujący sprzęt komputerowy:

1) komputer przenośny .....

2. Komputer będzie używany tylko do celów służbowych.
3. Komputer nie może być udostępniony osobie spoza pracowników Urzędu Gminy.
4. Urządzenie można udostępnić innemu pracownikowi tylko w budynku Urzędu Gminy i pod warunkiem, że posiada on kwalifikacje i doświadczenie w pracy z komputerem.
5. Komputer będzie zabezpieczony systemem haseł przed dostępem osób nieupoważnionych.
6. Zabraniam instalacji i używania oprogramowania innego niż służbowe, a zwłaszcza nielicencjonowanego, pochodzącego z niewiadomych źródeł, lub wobec którego istnieją jakiekolwiek wątpliwości, co do jego działania i składu.
7. Zabraniam tworzenia, nagrywania i przenoszenia na tym komputerze baz danych i innych plików zawierających jakiekolwiek dane osobowe.
8. Praca z danymi osobowymi możliwa jest tylko w budynku Urzędu Gminy, przy połączeniu sieciowym klient-serwer i za pisemnym upoważnieniem Administratora Danych Osobowych.
9. W przypadku wykrycia nieprawidłowości w działaniu sprzętu lub oprogramowania należy niezwłocznie powiadomić informatyka.

Uwagi końcowe

10. Zobowiązuję Pana/nią do zapewnienia urządzeniu odpowiednich warunków pracy i stosowania właściwych materiałów eksploatacyjnych, zgodnie z instrukcją obsługi załączoną przez producenta.
11. Ponosi Pan/i pełną odpowiedzialność materialną za wszelkie uszkodzenia tego urządzenia, powstałe wskutek niewłaściwego użytkowania.

Miedziana Góra, dnia .....

....
(pracownik otrzymujący komputer) (Wójt Gminy Miedziana Góra)

Załącznik Nr 5
do zarządzenia nr 28/2007
z dnia 20 czerwca 2007

Polityka bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Gminy w Miedzianej Górze

Spis treści

Definicje

Dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden z kilku specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.

Zbiór danych osobowych – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony (jego części znajdują się w różnych miejscach) lub podzielony funkcjonalnie (przetwarzany za pomocą programów realizujących różne funkcje).

Przetwarzanie danych osobowych – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, udostępnianie i usuwanie; zwłaszcza takie, które wykorzystuje się w systemach informatycznych.

System informatyczny – system przetwarzania informacji wraz ze związanymi z nimi ludźmi oraz zasobami technicznymi i finansowymi, które dostarcza i rozprowadza informacje. W szczególności systemem informacyjnym może być system, w którym nie będzie żadnego komputera, a wyłącznie dokumenty papierowe, skoroszyty oraz ludzie tam pracujący, wyposażenie pokoi, czy też organizacja pracy. Ochronie podlegają nie tylko informacje osobowe, ale także ludzie, zasoby techniczne i finansowe.

Bezpieczeństwo systemu informatycznego – wdrożenie stosowanych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą.

Administrator Danych Osobowych (ADO) – organ, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych osobowych. Administratorem danych jest Wójt, który ponosi pełnię odpowiedzialności wynikającej z przepisów ustawy o ochronie danych osobowych w odniesieniu do zbiorów danych osobowych znajdujących się w jego ustawowej dyspozycji.

Administrator Bezpieczeństwa Informacji (ABI) – należy przez to rozumieć pracownika urzędu wyznaczonego przez Administratora Danych Osobowych do nadzorowania przestrzegania zasad ochrony oraz wymagań w zakresie ochrony, wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych.

Administrator Systemów Informatycznych (ASI) – należy przez to rozumieć pracownika lub pracowników Informatyki odpowiedzialnych za stosowanie technicznych i organizacyjnych środków ochrony danych osobowych.

Osoba upoważniona lub użytkownik systemu – osoba posiadająca upoważnienie 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.

Osoba uprawniona – osoba posiadająca uprawnienie wydane przez ADO na mocy którego wykonuje w jego imieniu określone czynności.

Sieć Lokalna (LAN) – sieć komputerowa o zasięgu lokalnym zwykle ogranicza się do jednego budynku lub kilku budynków w bezpośrednim sąsiedztwie.

Sieć rozległa (WAN) – rozległa sieć komputerowa.

Identyfikator użytkownika (LOGIN) – ciąg znaków literowych i cyfrowych, lub innych, jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.

Hasło (Password) – ciąg znaków literowych cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym,

Zalogowanie – uwierzytelnienie czyli działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

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 o ochronie danych osobowych,
- podmiotu, o którym mowa w art. 31 ustawy o ochronie danych osobowych,
- organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

Zwrotna informacja telefoniczna – czynności polegająca na:

- przyjęciu wniosku telefonicznego o udostępnienie danych wraz z informacją o tożsamości, nazwie komórki organizacyjnej , nazwie zamiejscowej komórki organizacyjnej, nazwie podległej jednostce organizacyjnej, numerze telefonu wnioskodawcy,
- oddzwonienie ze stosowna informacją bądź danymi, po uprzednim sprawdzeniu prawdziwości i autentyczności wnioskodawcy.

Wprowadzenie

Niniejszy dokument opisuje reguły dotyczące bezpieczeństwa danych osobowych zawartych w systemach informatycznych w Urzędzie Gminy w Miedzianej Górze. Opisane reguły określają granice dopuszczalnego zachowania wszystkich użytkowników systemów informatycznych wspomagających pracę Urzędu Gminy. Dokument zwraca uwagę na konsekwencje jakie mogą ponosić osoby przekraczające określone granice oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń. Odpowiednie zabezpieczenia, ochrona przetwarzanych danych, oraz niezawodność funkcjonowania są podstawowymi wymogami stawianymi współczesnym systemom informatycznym. Dokument „Polityka bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Gminy Miedziana Góra", zwanym dalej „Polityką bezpieczeństwa", wskazujący sposób postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych w systemach informatycznych, przeznaczony jest dla osób zatrudnionych przy przetwarzaniu tych danych.

Potrzeba jego opracowania wynika z §3 rozporządzenia Prezesa Rady Ministrów z dnia 25 lutego 1999 roku w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych (Dz. U. Nr 18 poz. 162) oraz §3 i §4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).

Polityka bezpieczeństwa określa tryb postępowania w przypadku, gdy:

- stwierdzono naruszenie zabezpieczenia systemu informatycznego,
- stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji sieci informatycznej mogą wskazywać lub sugerować naruszenie zabezpieczeń tych danych,

Polityka bezpieczeństwa obowiązuje wszystkich pracowników Urzędu Gminy w Miedzianej Górze. Wykonywanie postanowień tego dokumentu ma zapewnić właściwą reakcję, ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa systemów oraz zapewnić właściwy tryb działania w celu przywrócenia bezpieczeństwa danych przetwarzanych w systemach informatycznych Urzędu Gminy.

Niniejszy dokument jest zgodny z następującymi aktami prawnymi:

- ustawą z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. Z 2002 r. Nr 101, poz. 929 z późn. zm.),
- ustawą o ochronie informacji niejawnych z dnia 22 stycznia 1999r. (Dz. U. Nr 11, poz. 95 z późn. zm.),

- rozporządzeniem Prezesa Rady Ministrów z dnia 25 lutego 1999r. w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych (Dz. U. Nr 18 poz. 162).

Polityka bezpieczeństwa została oparta również na zapisach Polskiej Normy PN-ISO/IEC 17799, PN-I-02000 oraz PN-I-13335-1 określających praktyczne zasady zarządzania bezpieczeństwem informacji w obszarze technik informatycznych, która jako cel polityki bezpieczeństwa wskazuje „zapewnienie kierunków działania i wsparcie kierownictwa dla bezpieczeństwa informacji".

ROZDZIAŁ I

Zasady postępowania przy przetwarzaniu danych osobowych

1. Administrator Danych Osobowych, którym jest Wójt, wyznacza Administratora Bezpieczeństwa Informacji dla danych zawartych w systemach informatycznych Urzędu Gminy, zwanego dalej Administratorem Bezpieczeństwa Informacji

2. Administrator Danych Osobowych jest zobowiązany do:

- czuwania nad tym, by będące w jego posiadaniu dane osobowe były przetwarzane zgodnie z prawem,
- zastosowania niezbędnych środków technicznych i organizacyjnych w celu zapewnienia ochrony przetwarzanych w Urzędzie Gminy danych osobowych,
- sprawowania kontroli nad bezpieczeństwem oraz sposobem przetwarzania danych,
- rejestracji w Głównym Inspektoracie Ochrony Danych Osobowych, zbiorów danych przed przystąpieniem do ich przetwarzania, prowadzenia ewidencji osób zatrudnionych przy przetwarzaniu danych.

3. Administrator Bezpieczeństwa Informacji realizuje zadania w zakresie ochrony danych, a w szczególności:

- ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych Urzędu Gminy,
- podejmowania stosownych działań zgodnie z niniejszą Polityką bezpieczeństwa w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub na-ruszenia zabezpieczenia danych znajdujących się w systemie informatycznym,
- niezwłocznego informowania Administratora Danych Osobowych lub osoby przez niego upoważnionej o przypadkach naruszenia przepisów ustawy o ochronie danych osobowych,
- nadzoru i kontroli systemów informatycznych służących do przetwarzania danych osobowych i osób przy nim zatrudnionych,
- opracowania i wdrożenia programu szkolenia w zakresie zabezpieczenia systemu informatycznego,

4. Osoba zastępująca powyższe zadania realizuje tylko w przypadku nieobecności Administratorowi Bezpieczeństwa Informacji.

5. Osoba zastępująca składa Administratorowi Bezpieczeństwa Informacji relację z podejmowanych działań w czasie jego zastępstwa.

6. Kierownicy referatów Urzędu Gminy są zobowiązani do:

- współdziałania z Administratorem Bezpieczeństwa Informacji w zakresie przestrzegania instrukcji o której mowa w rozdziale VI,

- sprawowania nadzoru nad pracą podległych pracowników w zakresie wykonywania czynności służbowych w sposób zapewniający ochronę danych osobowych,
- zwracania się do administratora danych o rozstrzygnięcie w przypadku istotnych wątpliwości co do stosowania przepisów prawnych zakresu danych osobowych,
- niezwłocznego zawiadomienia ADO o konieczności utworzenia nowego zbioru danych osobowych, wymagającego rejestracji.

7. Pracownik upoważniony przez ADO do przetwarzania danych osobowych, jest zobowiązany do:

- odbycia wewnętrznego szkolenia dotyczącego przetwarzania i ochrony danych osobowych
- zapoznania się z przepisami prawa w zakresie ochrony danych osobowych,
- stosowania określonych przez administratora danych , procedur i środków mających na celu zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym,
- zachowania szczególnej staranności w trakcie wykonywania operacji przetwarzania danych w celu ochrony interesów osób, których te dane dotyczą,
- podporządkowania się poleceniom administratora bezpieczeństwa informacji oraz właściwego kierownika, w zakresie ochrony danych.

8. Czynności przetwarzania danych osobowych może dokonywać jedynie pracownik upoważniony przez ADO lub ABI . Wzór upoważnienia stanowi załącznik nr 1 do niniejszego dokumentu.

9. Bezpośredni nadzór nad przetwarzaniem danych osobowych w komórkach organizacyjnych Urzędu Gminy sprawują kierownicy referatów tych komórek, a w przypadku pracowników na samodzielnych stanowiskach Wójt, Zastępca Wójta – każdy w swoim pionie.

10. Pracownik, któremu administrator udzielił upoważnienia, o którym mowa w ust. 8 jest zobowiązany do podpisania oświadczenia. Wzór oświadczenia stanowi załącznik nr 2 do niniejszego dokumentu.

11. W przypadku zatrudnienia nowego pracownika, zmiany stanowiska, zmiany zakresu obowiązków pracowniczych, utworzenia nowego zbioru danych osobowych, zmiany sposobu przetwarzania danych lub w innych przypadkach, które wpływają bezpośrednio na rodzaj i zakres przetwarzania danych, kierownik jest zobowiązany bez-zwłocznie skierować wniosek do administratora danych osobowych o wydanie lub cofnięcie upoważnienia. W przypadku samodzielnych stanowisk pracy cofnięcia lub wydania upoważnienia dokonuje administrator danych. Wzór pisma o cofnięciu upoważnienia stanowi załącznik nr 3 do niniejszego dokumentu.

12. Wypowiedzenie umowy o pracę jest równoznaczne z cofnięciem upoważnienia do przetwarzania danych osobowych.

13. W obiegu wewnętrznym między referatami, a także pracownikami jednostek podległych Urzędowi Gminy wprowadza się następujące zasady udostępniania danych osobowych:

- informacje zawierające dane powszechnie dostępne może udostępnić pracownik przetwarzający dane w formie bezpośredniej lub telefonicznej, po sprawdzeniu tożsamości w procedurze "zwrotnej informacji telefonicznej",
- zgodę na udostępnienie danych osobowych w szerszym zakresie wyraża ADO.

14. W obiegu zewnętrznym zgodę na udostępnienie danych osobowych wyraża administrator danych zgodnie z powszechnie obowiązującymi przepisami.

15. Obowiązek przestrzegania tajemnicy danych osobowych spoczywa na wszystkich pracownikach, którzy mają do nich dostęp, również po ustaniu stosunku pracy.

16. ADO może przenieść obowiązek utrzymywania lub przetwarzania zbioru/zbiorów danych osobowych, na podmiot trzeci jednak musi się to odbyć za pośrednictwem stosownej umowy oraz z zachowaniem reguł bezpieczeństwa danych opisanych w niniejszym dokumencie.

17. Przetwarzanie danych osobowych sprzeczne z przepisami ustawy o ochronie danych osobowych może stanowić ciężkie naruszenie obowiązków pracowniczych.

18. Zbiory danych osobowych przetwarzane przez pracowników Urzędu Gminy w Miedzianej Górze nie będą udostępniane do celów komercyjnych.

ROZDZIAŁ II

Opis zdarzeń naruszających ochronę danych osobowych

1. Podział zagrożeń:

a) zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych,
b) zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora systemu informatycznego, awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych,
c) zagrożenia zamierzone, świadome i celowe – najpoważniejsze zagrożenia naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na:
d) nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu),
e) nieuprawniony dostęp do systemu z jego wnętrza,
f) pogorszenie jakości sprzętu i oprogramowania,

g) nieuprawniony przekaz danych,
h) bezpośrednie zagrożenie materialnych składników systemu.

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

a) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.,
b) niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie silnego pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,
c) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym fakt pozostawienia serwisantów bez nadzoru,
d) pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,
e) jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenie systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
f) nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,
g) stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
h) nastąpiła niedopuszczalna manipulacja danymi osobowymi w systemie,
i) ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń np. login użytkownika i jego hasło,
j) praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych – np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.,
k) ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. „bocznej furtki" (backdoor), itp.,
l) podmieniono, lub zniszczono nośniki z danymi osobowymi bez odpowiedniego upoważnienia lub w inny sposób niedozwolony skasowano lub skopiowano dane osobowe,
m) rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowano 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.).

3. Za naruszenie ochrony uważa się również stwierdzone nieprawidłowości w zakresie bezpieczeństwa miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, dyskietkach w formie niezabezpieczonej itp.

ROZDZIAŁ III

Zabezpieczenie danych osobowych

1. Administratorem Danych Osobowych zawartych i przetwarzanych w systemach informatycznych Urzędu Gminy Miedziana Góra jest Wójt.
2. Administrator Danych Osobowych jest zobowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w systemach informatycznych Urzędu Gminy, a w szczególności:
   - zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym,
   - zapobiegać przed zabraniem danych przez osobę nieuprawnioną,
   - zapobiegać przetwarzaniu danych z naruszeniem ustawy oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych.
3. Do zastosowanych środków technicznych należy:
   - przetwarzanie danych osobowych w wydzielonych pomieszczeniach położonych w strefie administracyjnej,
   - zabezpieczenie wejścia do pomieszczeń, o których mowa w pkt. wyżej,
   - szczególne zabezpieczenie centrum przetwarzania danych (komputer centralny, serwerownia) poprzez zastosowanie systemu kontroli dostępu,
   - wyposażenie pomieszczeń w szafy dające gwarancję bezpieczeństwa dokumentacji.
4. Do zastosowanych środków organizacyjnych należą przede wszystkim następujące zasady:
   - zapoznanie każdej osoby z przepisami dotyczącymi ochrony danych osobowych, przed dopuszczeniem jej do pracy przy przetwarzaniu danych osobowych,
   - przeszkolenie osób, o których mowa w w/w ustępie, w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochrona danych osobowych,
   - kontrolowanie otwierania i zamykania pomieszczeń, w którym są przetwarzane dane osobowe, polegające na otwarciu pomieszczenia przez pierwszą osobę, która rozpoczyna pracę oraz zamknięciu pomieszczenia przez ostatnią wychodzącą osobę.
5. Niezależnie od niniejszych zasad opisanych w dokumencie „Polityka bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Gminy Miedziana Góra" w zakresie bezpieczeństwa mają zastosowanie wszelkie wewnętrzne regulaminy lub instrukcje dotyczące bezpieczeństwa ludzi i zasobów informacyjnych oraz indywidualne zakresy zadań osób zatrudnionych przy przetwarzaniu danych osobowych w określonym systemie.

6. Wykaz pomieszczeń w których przetwarzane są dane osobowe stanowi załącznik nr 4 do niniejszego dokumentu.
7. Wykaz zbiorów przetwarzanych elektronicznie lub w inny sposób stanowi załącznik nr 5 a i b do niniejszego dokumentu.
8. Opis struktury zbiorów danych stanowi załącznik nr 6 do niniejszego dokumentu.
9. Sposób przepływu danych pomiędzy systemami stanowi załącznik nr 7 do niniejszego dokumentu.
10. Opis rejestracji baz danych stanowi załącznik nr 8 do niniejszego dokumentu.
11. Opis zabezpieczeń systemów informatycznych stanowi załącznik nr 9 do niniejszego dokumentu.

ROZDZIAŁ IV

Kontrola przestrzegania zasad zabezpieczenia danych osobowych

1. Administrator Danych Osobowych lub osoba przez niego wyznaczona, którą jest Administrator Bezpieczeństwa Informacji sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych wynikających z ustawy o ochronie danych osobowych oraz zasad ustanowionych w niniejszym dokumencie.
2. Administrator Bezpieczeństwa Informacji sporządza roczne plany kontroli zatwierdzone przez Administratora Danych Osobowych i zgodnie z nimi przeprowadza kontrole oraz dokonuje kwartalnych ocen stanu bezpieczeństwa danych osobowych.
3. Na podstawie zgromadzonych materiałów o których mowa w pkt. 2 ABI sporządza roczne sprawozdanie i przedstawia ADO.

ROZDZIAŁ V

Środki techniczne i organizacyjne

Część ta zawiera opis środków technicznych, organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych. Szczególny opis zawartości w „Instrukcji określającej sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem bezpieczeństwa informacji" (rozdział VI).

Środki organizacyjne

1. Dostęp do danych osobowych mogą mieć tylko i wyłącznie pracownicy posiadający pisemne, imienne upoważnienia podpisane przez ADO lub ABI.

2. Każdy z pracowników powinien zachować szczególną ostrożność przy przetwarzaniu, przenoszeniu wszelkich danych osobowych.
3. Należy chronić dane przed wszelkim dostępem do nich osób nieupoważnionych.
4. Pomieszczenia, w których są przetwarzane dane osobowe, muszą być zamykane na klucz.
5. Dostęp do kluczy powinni posiadać tylko upoważnieni pracownicy.
6. Dostęp do pomieszczeń możliwy jest tylko i wyłącznie w godzinach pracy urzędu. W wypadku, gdy jest wymagany poza godzinami pracy - możliwy jest tylko na podstawie pisemnego zezwolenia Administratora Danych Osobowych.
7. Dostęp do pomieszczeń, w których są przetwarzane dane osobowe mogą mieć tylko upoważnieni pracownicy urzędu.
8. W przypadku pomieszczeń do których dostęp mają również osoby nieupoważnione, mogą przebywać w tych pomieszczeniach TYLKO w obecności osób upoważnionych, i tylko w czasie wymaganym na wykonanie niezbędnych czynności.
9. Szafy w których przechowywane są dane osobowe muszą być zamykane na klucz.
10. Klucze do tych szaf powinni posiadać tylko upoważnieni pracownicy.
11. Szafy z danymi powinny być otwarte tylko na czas potrzebny na dostęp do danych a następnie powinny być zamykane.
12. Dane osobowe w formie papierowej mogą znajdować się na biurkach tylko na czas niezbędny na dokonanie czynności służbowych a następnie muszą być chowane do szaf.

Środki techniczne

1. Dostęp do komputerów na których są przetwarzane dane osobowe mogą mieć tylko upoważnieni pracownicy urzędu.
2. Stacje komputerowe na których przetwarzane są dane osobowe powinny mieć tak ustawione monitory, aby nie miały wglądu w dane osoby nieupoważnione.
3. Każdy plik w którym są zawarte dane osobowe powinien być zabezpieczony hasłem jeśli nie jest to przetwarzanie danych w systemie informatycznym.
4. W przypadku przetwarzania danych osobowych na komputerach przenośnych (notebook) należy zachować szczególną ostrożność przy ich przewożeniu.
5. Po zakończeniu pracy komputery (notebook) takie powinny być zabezpieczone w zamykanych na klucz szafach.
6. Komputerów tych nie należy wynosić poza budynek.
7. W wypadku potrzeby wyniesienia (np. notebook-a) wcześniej należy dane osobowe przenieść na komputer stacjonarny w miejscu pracy.
8. Nie należy udostępniać osobom nieupoważnionym tych komputerów.
9. W przypadku potrzeby przeniesienia danych osobowych pomiędzy komputerami należy dokonać tego z zachowaniem szczególnej ostrożności i za zgodą ABI.
10. Nośniki użyte do tego należy wyczyścić (skasować nieodwracalnie/zniszczyć), aby nie zostały na nich dane osobowe.
11. W wypadku niemożliwości skasowania danych z nośnika (płyta CD/DVD) należy taką płytę zniszczyć fizycznie (np. za pomocą odpowiedniej niszczarki).

12. W przypadku wykorzystania do przenoszenia dysków, dane należy kasować z tych dysków.
13. Niezabezpieczonych danych osobowych nie należy przesyłać drogą elektroniczną.
14. Sieć komputerowa powinna być zabezpieczona przed wszelkim dostępem z zewnątrz.
15. Do zabezpieczenia sieci należy stosować:
    - firewall,
    - adresowanie stacji roboczych tylko adresami prywatnymi, nieroutowalnymi,
    - systemy wykrywania włamań IDS,
    - logowanie wszelkich zdarzeń w dziennikach systemowych na serwerach i stacjach roboczych,
    - systemy antywirusowe i antyszpiegowskie,
    - zabezpieczenia skrzynek poczty elektronicznej hasłami "trudnymi" (min. 8 znaków w tym litery, cyfry, znaki dodatkowe),
    - zabezpieczenie przed dostępem na zewnątrz ze stacji roboczych do innych usług niż WWW, (zasada blokowania wszystkie i przepuszczania określonych usług w tym przypadku http, czyli port 80),
    - dostęp do poczty elektronicznej tylko na serwerach autoryzowanych przez Urząd Gminy,
    - zabezpieczenia stacji roboczych poprzez hasła w BIOS, w systemach MS Windows (autoryzacja użytkownika, login + hasło),
    - zabezpieczenie wszelkich systemów teleinformatycznych hasłami „trudnymi" (min. 8 znaków w tym litery, cyfry, znaki dodatkowe) zmienianymi pierwszego dnia roboczego każdego miesiąca,
    - ustawienie odpowiednich poziomów dostępu dla odpowiednich użytkowników w systemach teleinformatycznych, zmiany mogą zostać przeprowadzone tylko i wyłącznie przez administratora danego systemu (polityka ograniczonego zaufania).

ROZDZIAŁ VI

Instrukcja określająca sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem bezpieczeństwa informacji.

1. Określenie sposobu przydziału haseł dla użytkowników i częstotliwość ich zmiany oraz wskazanie osoby odpowiedzialnej za te czynności.
    - hasło nie powinno zawierać mniej niż 8 znaków,
    - hasło nie może być takie samo jak identyfikator,
    - hasło musi być zmieniane przynajmniej raz w miesiącu przez użytkownika, Administratora Bezpieczeństwa Informacji lub automatycznie przez system,
    - użytkownikowi nie wolno zapisywać hasła na papierze,

- użytkownik jest zobowiązany do utrzymania hasła w tajemnicy, również po utracie jego ważności,
- komputery nie pracujące w sieci muszą mieć hasło założone na BIOS,
- w przypadku czasowego opuszczenia stanowiska pracy, użytkownik powinien wylogować się z systemu, lub uruchomić wygaszacz ekranu zabezpieczony hasłem,
- za gospodarkę hasłami odpowiedzialny jest Administratora Bezpieczeństwa Informacji,
- hasło przy wpisywaniu nie może być wyświetlane na ekranie.

2. Określenie sposobu rejestrowania i wyrejestrowania użytkowników oraz wskazanie osoby odpowiedzialnej za te czynności.
   - administrator bezpieczeństwa informacji prowadzi ewidencję osób upoważnionych do przetwarzania danych , zawierającą ich identyfikatory, załącznik nr 12 do niniejszego dokumentu,
   - rejestracji użytkowników w systemie dokonuje administrator bezpieczeństwa informacji, lub osoba przez niego upoważniona,
   - zarejestrować można wyłącznie osoby, które administrator danych wpisał do ewidencji osób upoważnionych do przetwarzania danych,
   - wyłączenie z ewidencji osób upoważnionych do przetwarzania danych, obliguje administratora bezpieczeństwa informacji do odebrania dostępu do danych osobowych,
   - zalecane jest aby identyfikator składał się z pierwszej litery imienia i pierwszych pięciu liter nazwiska.
3. Procedury rozpoczęcia i zakończenia pracy.
   - ABI w porozumieniu z kierownikiem referatu, ustala czas pracy użytkownikom systemu, na pracę poza godzinami funkcjonowania urzędu musi wyrazić zgodę na piśmie kierownik jednostki, w formie upoważnienia jednorazowego lub stałego,
   - ABI, lub osoba przez niego upoważniona, nadzoruje rozpoczęcie i zakończenie pracy systemu informatycznego,
   - w pomieszczeniach gdzie przyjmowani są klienci , monitory powinny być tak ustawione, aby uniemożliwić osobie niepowołanej wgląd w dane,
   - dopuszcza się pozostawianie włączonego serwera w nocy, jeżeli pomieszczenie w którym on pracuje wyposażone jest w sprawny system powiadamiania p-poż, UPS oraz alarm antywłamaniowy.
   - kontrola wprowadzanych danych prowadzona jest na bieżąco na każdym stanowisku merytorycznym, nadzór prowadzi kierownik danej komórki organizacyjnej,
   - o przekazywaniu danych osobowych innym podmiotom decyduje ADO,
   - osoby, których dane są przetwarzane powinny mieć możliwość zapoznania się, na tablicy ogłoszeń, z przysługującymi im prawami wynikającymi z ustawy o ochronie danych osobowych.
4. Metoda i częstotliwość tworzenia kopii awaryjnych
   - za sporządzanie i bezpieczeństwo kopii odpowiedzialny jest ABI, lub osoba przez niego upoważniona,

- kopii należy dokonywać poprzez przegrywanie (backup) całej bazy danych (bez kompresji),
- w każdej chwili powinno być dostępnych jednocześnie pięć kopii: z ostatniego dnia, tygodnia, miesiąca, kwartału i roku. Kopie dzienne i tygodniowe należy zapisywać na dysku twardym a pozostałe na CD/DVD, bądź innym nośniku niemodyfikowalnym,
- kopie awaryjne może tworzyć jedynie administrator bezpieczeństwa informacji, lub osoba przez niego upoważniona,
- w czasie tworzenia kopii awaryjnej przez administratora, dostęp do bazy dla wszystkich użytkowników powinien być zablokowany,
- dyski wymienne z kopiami bezpieczeństwa powinny być wyjęte z komputera w czasie bieżącej pracy,
- ABI lub administrator systemu wykonuje backup lub archiwizacje systemu wykorzystując jak najlepiej swoje umiejętności.

Wprowadza się praktyczne zalecenia odnośnie do wykonania kopii bezpieczeństwa:

- przeprowadzić składowanie informacji regularnie,
- używać różnych typów nośników danych,
- kopie umieszczać w różnych, oddalonych od siebie miejscach,
- najlepiej do składowania wybrać tak nośnik, aby mógł w całości pomieścić kopie danych,
- przed składowaniem danych sprawdzić je programem antywirusowym,
- dokładnie opisywać składowane dane,
- trzymać nośniki z kopiami z daleka od źródeł pola magnetycznego i miejsc nasłonecznionych,
- sprawdzić, czy składowanie przebiegło prawidłowo,
- upewnić się, że nośnik jest niezależny od urządzenia, tzn. że dane mogą być przywrócone nie tylko na komputerze, z którego były pobrane,
- regularnie konserwować urządzenia do składowania.

5. Metody i częstotliwość sprawdzania obecności wirusów komputerowych oraz sposoby ich usuwania
   - za ochronę antywirusową odpowiedzialny jest administrator bezpieczeństwa informacji,
   - do ochrony antywirusowej należy stosować program antywirusowy, zainstalowany na komputerze, gdzie odbierana jest poczta elektroniczna i sprawdzane są wszystkie nośniki wymienne, przed ich uruchomieniem w sieci oraz na komputerach stacjonarnych,
   - sprawdzanie dostępnymi programami antywirusowymi odbywać się powinno przynajmniej raz w tygodniu (zalecane jest codzienne skanowanie komputera),
   - zalecane jest wykorzystanie programów pracujących w tle,
   - przy kontroli szczególną uwagę należy zwrócić na makra (dokumenty pakietów biurowych),

- każdą przesyłkę otrzymaną za pomocą transmisji danych (e-mail, ftp) należy sprawdzić programem antywirusowym,
- korzystanie z zewnętrznych nośników i źródeł informacji (dyskietek, dysków wymiennych, płyt CD, Internetu, poczty elektronicznej) może mieć miejsce wyłącznie po uzyskaniu zgody ABI,
- w przypadku wykrycia wirusa choćby na jednym komputerze, należy sprawdzić wszystkie stacje robocze w Urzędzie.

6. Sposób i czas przechowywania nośników informacji, w tym kopii zapasowych i wydruków.
   - nie należy magazynować zbędnych plików i wydruków, kopie bezpieczeństwa po upływie okresu przechowywania muszą być skasowane, lub fizycznie zniszczone w sposób uniemożliwiający odczytanie danych,
   - za zniszczenie zbędnych wydruków i innych dokumentów zawierających dane osobowe odpowiedzialny jest kierownik referatu, za skasowanie danych, lub zniszczenie nośników elektronicznych, odpowiedzialny jest ABI,
   - zbędne dokumenty konwencjonalne (papierowe) powinny być zniszczone w niszczarce dokumentów lub przekazane do utylizacji firmie uprawnionej,
   - kopie bezpieczeństwa na nośnikach wymiennych powinny być przechowywane w zamkniętej metalowej szafie,
   - kopie na nośnikach wymiennych nie powinny być przechowywane w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych eksploatowanych na bieżąco,
   - kopie awaryjne sprawdza się pod kątem ich dalszej przydatności do odtworzenia danych w przypadku awarii systemu – co najmniej jednorazowo po przegraniu danych,
   - wydruki należy przechowywać w pomieszczeniach, uniemożliwiających dostęp do nich przez osoby niepowołane,
   - kopie przechowuje się co najmniej:
     - dzienne przez siedem dni,
     - tygodniowe przez kolejny tydzień,
     - miesięczne przez kolejny miesiąc,
     - kwartalne przez kolejny kwartał,
     - roczne przez cały kolejny rok od daty sporządzenia.
   - osoba użytkująca przenośny komputer, służący do przetwarzania danych osobowych, obowiązana jest zachować szczególną ostrożność podczas transportu i przechowywania tego komputera, w celu zapobieżenia dostępowi do tych danych osobie niepowołanej, powinna zabezpieczyć dostęp do komputera hasłem i nie zezwalać na używanie komputera osobom, komputera nie należy pozostawiać w samochodzie,
7. Sposób dokonywania przeglądów i konserwacji systemu i zbioru danych osobowych
   - przeglądu i konserwacji dokonuje ABI, lub osoba przez niego upoważniona, przynajmniej dwa razy w roku,

- zasilacz UPS powinien zapewnić automatyczne zakończenie pracy i wyłączenie serwerów przy zaniku lub nadmiernym wahaniu napięcia – min. czas podtrzymania pracy wynosi 5 min,
- w przypadku przekazywania komputera z dyskiem lub innym nośnikiem danych osobowych do naprawy, należy nośnik zdemontować, zabezpieczyć dostęp hasłem, dokonać naprawy w obecności osoby upoważnionej przez administratora danych lub przekazać do naprawy firmie z która Urząd podpisuje odpowiednie dokumenty przekazania zbioru danych z zastrzeżeniem co do przetwarzania i wykorzystywania tych danych w przypadku przekazania nośnika innemu podmiotowi należy dane nieodwracalnie skasować,
- o wszelkich nieprawidłowościach, awariach, próbie lub naruszeniu bezpieczeństwa danych osobowych, użytkownik powinien niezwłocznie powiadomić ABI,
- do wydzielonej sieci energetycznej zasilającej system komputerowy nie wolno podłączać żadnych innych urządzeń (czajników elektrycznych, odkurzaczy, radioodbiorników),
- zabronione jest dokonywanie napraw sprzętu komputerowego samodzielnie przez pracowników urzędu.

8. Sposób postępowania w zakresie komunikacji w sieci komputerowej.
   - 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 (załącznik do Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 Kwietnia 2004 poz. 1024).
   - przy przydzielaniu uprawnień obowiązuje zasada „wszystko co nie jest dozwolone, jest zabronione",
   - Administrator Bezpieczeństwa Informacji z Administratorem Danych Osobowych określi zasoby dostępne dla każdego użytkownika,
   - użytkownicy powinni być przydzielani do odpowiedniej grupy roboczej, automatycznie w procesie logowania np. za pomocą skryptu logowania,
   - dostęp do serwerowni ma tylko ABI i pracownicy przez niego upoważnieni,
   - dostęp do konsoli serwera winien być zabezpieczony hasłem (min. 12 znaków, dostępnych w tablicy ASCII),
   - ABI winien monitorować pracę w sieci za pomocą dostępnego oprogramowania narzędziowego i plików .log (plik z informacjami przekazywanymi przez system/program dla użytkownika) ,
   - w pomieszczeniu, gdzie ustawiony jest serwer może pracować tylko ABI, lub osoby przez niego upoważnione,
   - nie wolno instalować na żadnym z komputerów w sieci urzędowej własnego oprogramowania bez zgody ABI,
   - użytkownicy nieuprawnieni nie powinni mieć dostępu do zasobów systemowych serwera, katalogów roboczych, danych i woluminów z poziomu systemu operacyjnego,

- dostęp do archiwalnych plików pocztowych, mających status poufnych (in-formacje handlowe) należy zabezpieczyć hasłem,
- wszystkie listy otrzymane pocztą elektroniczną należy przekazywać do kancelarii,
- w celu zwiększenia bezpieczeństwa transmisji danych osobowych należy stosować kryptografie,
- w czasie korzystania z Internetu za pośrednictwem linii komutowanej, stacja powinna być fizycznie odłączona od sieci lokalnej,
- uczestnictwo w internetowych grupach dyskusyjnych dozwolone jest jedynie za zgodą ABI,,
- komunikacja w sieci lokalnej musi umożliwiać identyfikację pracujących użytkowników.

ROZDZIAŁ VII

Instrukcja postępowania w sytuacji naruszenie ochrony danych osobowych

1. Niniejsze zasady określają tryb postępowania w przypadku gdy:
   - stwierdzono naruszenie zabezpieczenia systemu informatycznego lub naruszenie zabezpieczenia zbioru danych osobowych zebranych i przetwarzanych w innej formie,
   - stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej, mogą wskazywać na naruszenie zabezpieczeń tych danych.
2. Naruszeniu ochrony danych osobowych mogą świadczyć w szczególności następujące symptomy:
   - brak możliwości uruchomienia przez użytkownika aplikacji pozwalającej na dostęp do danych osobowych,
   - brak możliwości zalogowania się do tej aplikacji,
   - ograniczone, w stosunku do normalnej sytuacji, uprawnienia użytkownika aplikacji (np. brak możliwości wykonywania pewnych operacji normalnie dostępnych użytkownikowi) lub uprawnienia poszerzone w stosunku do normalnej sytuacji,
   - wygląd aplikacji inny niż normalnie,
   - inny zakres danych niż normalnie dostępny dla użytkownika - dużo więcej lub dużo mniej danych,
   - znaczne spowolnienie działania systemu informatycznego,
   - pojawienie się nie standardowych komunikatów generowanych przez system informatyczny,
   - ślady włamania lub prób włamania do obszaru, w którym przetwarzane są dane osobowe,
   - ślady włamania lub prób włamania do pomieszczeń, w których odbywa się przetwarzanie danych osobowych, w szczególności do serwerowni oraz do pomieszczeń, w których przechowywane są nośniki kopii awaryjnych,

- włamanie lub próby włamania do szafek, w których przechowywane są w postaci elektronicznej lub papierowej - nośniki danych osobowych,
- zagubienie lub kradzież nośnika danych osobowych.
- zagubienie lub kradzież nośnika materiału,
- kradzież sprzętu informatycznego, w którym przechowywane były dane osobowe,
- informacja z systemu antywirusowego o zainfekowaniu systemu informatycznego wirusami,
- fizyczne zniszczenie lub podejrzenie zniszczenia elementów systemu informatycznego przetwarzającego dane osobowe na skutek przypadkowych lub celowych działań albo zaistnienia siły wyższej.
- podejrzenie nieautoryzowanej modyfikacji danych osobowych przetwarzanych w systemie informatycznym.

3. ujawnieniu danych osobowych decyduje:
   - dane osobowe zostają ujawnione, gdy stają się znane w całości lub części pozwalającej na określenie osobom nie uprawnionym tożsamości osoby, której dane dotyczą.
   - w stosunku do danych, które zostały zagubione, pozostawione bez nadzoru poza obszarem bezpieczeństwa należy przeprowadzić postępowanie wyjaśniające, czy dane osobowe należy uznać za ujawnione.
4. Każdy pracownik Urzędu Gminy biorący udział w przetwarzaniu danych osobowych w systemie informatycznym jest odpowiedzialny za bezpieczeństwo tych danych.
   - w szczególności osoba, która zauważyła zdarzenie mogące być przyczyną naruszenia ochrony danych osobowych lub mogących spowodować naruszenie bezpieczeństwa danych, zobowiązana jest do natychmiastowego poinformowania Administratora Bezpieczeństwa Informacji lub innej osoby wskazanej przez niego.
   - osoba zatrudniona w Urzędu Gminy, która stwierdzi lub podejrzewa naruszenie zabezpieczenia ochrony danych osobowych w systemie informatycznym (lub przetwarzanych w inny sposób), powinna niezwłocznie poinformować o tym Administratora Bezpieczeństwa Informacji lub osobę zatrudnioną przy przetwarzaniu danych osobowych, albo inną upoważnioną przez niego osobę.
   - Administrator Bezpieczeństwa Informacji jest odpowiedzialny za przygotowanie i opublikowanie wykazu osób, które mogą być informowane w przypadku wystąpienia zagrożenia danych osobowych.
   - w przypadku niemożliwości zawiadomienia Administratora Bezpieczeństwa Informacji lub osób przez niego upoważnionych, pracownik winien powiadomić bezpośredniego przełożonego.
5. Informacja o pojawieniu się zagrożenia lub wystąpieniu zagrożenia danych osobowych.
   - informacja przekazywana jest przez pracownika osobiście, telefonicznie lub pocztą elektroniczną,
   - informacja, o której mowa w w/w podpunkcie powinna zawierać imię i nazwisko osoby zgłaszającej oraz zauważone symptomy zagrożenia,
   - w przypadku gdy zgłoszenie o podejrzeniu zaistnienia incydentu otrzyma osoba inna niż ABI, jest ona obowiązana poinformować o tym fakcie ABI.

- pracownik może zostać poproszony przez ABI o potwierdzenie zauważonego faktu na piśmie.

6. Czynności „pierwszej reakcji" użytkownika zgłaszającego naruszenie.
   - do czasu przybycia Administratora Bezpieczeństwa Informacji lub upoważnionej przez niego osoby, zgłaszający:
     - niezwłocznie podejmuje czynności niezbędne do powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnia w działaniu również ustalenie przyczyn lub sprawców,
     - zabezpiecza dostęp do miejsca lub urządzenia przez osoby trzecie,
     - wstrzymuje pracę na komputerze na którym zaistniało naruszenie ochrony oraz nie uruchamia bez koniecznej potrzeby komputerów i innych urządzeń, których funkcjonowanie w związku naruszeniem ochrony zostało wstrzymane,
     - nie zmienia położenia przedmiotów, które pozwalają stwierdzić naruszenie ochrony lub odtworzyć jej okoliczności,
     - podejmuje, stosownie do zaistniałej sytuacji, inne niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych,
     - podejmuje inne działania przewidziane określone w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących naruszeniu,
     - wstępnie udokumentować zaistniałe naruszenie.
   - dokonywanie zmian w miejscu naruszenia ochrony jest dopuszczalne jeżeli zachodzi konieczność ratowania osób lub mienia albo zapobieżenia grożącemu niebezpieczeństwu.

7. Administrator Bezpieczeństwa Informacji lub osoba przez niego upoważniona, niezwłocznie po uzyskaniu sygnału o naruszeniu danych osobowych, powinien:
   - zapoznać się z zaistniałą sytuacją i dokonać wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy Urzędu Gminy,
   - zapisać wszelkie informacje związane z danym zdarzeniem,
   - na bieżąco wygenerować i wydrukować wszystkie możliwe dokumenty i raporty, które mogą pomóc w ustaleniu okoliczności zdarzenia,
   - przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, zwłaszcza do określenia skali zniszczeń i metody dostępu do danych osoby niepowołanej,
   - dokonać fizycznego odłączenia urządzeń i segmentów sieci, które mogły umożliwić dostęp do bazy danych osobie nie uprawnionej,
   - wylogować użytkownika podejrzanego o naruszenie zabezpieczenia ochrony danych,
   - dokonać zmiany hasła na konto ABI i użytkownika, poprzez które uzyskano nielegalny dostęp w celu uniknięcia ponownej próby włamania,
   - zażądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
   - rozważyć możliwość i potrzebę powiadomienia o zaistniałym naruszeniu ADO,

- nawiązać bezpośredni kontakt, jeżeli zachodzi taka potrzeba, ze specjalistami spoza Urzędu,
- zamknąć i opieczętować urządzeń, w których przechowywane są dane osobowe w formie cyfrowej.

8. Administrator Bezpieczeństwa Informacji podejmuje działania zmierzające do wyjaśnienia zgłoszonego zdarzenia. W szczególności może on dokonywać, w zależności od zgłoszonego zdarzenia:
   - wizji lokalnej w zakresie adekwatnym do rodzaju zgłoszonego zdarzenia,
   - przeprowadzenia wywiadów z pracownikami w celu ustalenia zaistniałych faktów,
   - przeprowadzenia analizy poprawności funkcjonowania systemu informatycznego, jeżeli zgłoszone zdarzenie było związane z nieprawidłowym jego funkcjonowaniem,
   - przeprowadzenia analizy zapisu zdarzeń w systemie informatycznym z uwzględnieniem zapisu operacji realizowanych przez użytkowników,
   - przeprowadzenia analizy danych przetwarzanych w systemie informatycznym, jeżeli zgłoszone zdarzenie mogło być spowodowane utratą dostępności lub integralności przetwarzanych danych,
   - sporządzenia dokumentacji fotograficznej,
   - zabezpieczenia danych przetwarzanych w systemie informatycznym dotkniętym incydentem, w szczególności danych konfiguracyjnych tego systemu,
   - zebrania innych materiałów pozwalających na wyjaśnienie przyczyn zaistnienia incydentu, jego charakteru i potencjalnych skutków,
9. Po wykonaniu czynności, o których mowa w pkt. 7 i w pkt. 8, Administrator Bezpieczeństwa Informacji jest zobowiązany do podjęcia kroków w celu:
   - wyjaśnienia zdarzenia - w szczególności czy miało miejsce naruszenie ochrony danych osobowych,
   - wyjaśnienia przyczyn naruszenia bezpieczeństwa danych osobowych i zebranie ewentualnych dowodów - w szczególności, gdy zdarzenie było związane z celowym działaniem pracowników bądź osób trzecich,
   - zabezpieczenia systemu informatycznego przed dalszym rozprzestrzenianiem się zagrożenia,
   - usunięcie skutków incydentu i przywrócenie pierwotnego stanu systemu informatycznego (to jest sprzed incydentu).
10. Czynności „pierwszej reakcji" Administratora Bezpieczeństwa Informacji

ABI przystępuje do usuwania skutków incydentu i przywrócenia prawidłowego przebiegu procesu przetwarzania danych osobowych. W szczególności działania związane z usuwaniem skutków incydentu mogą obejmować:

- przeprowadzenie naprawy sprzętu informatycznego,
- rekonfigurację sprzętu informatycznego,
- wprowadzenie poprawek do oprogramowania,
- rekonfigurację oprogramowania,
- odtworzenie danych z kopii awaryjnych,

- modyfikację danych w celu odtworzenia ich integralności,
- wycofanie z użycia materiału kryptograficznego,
- inne naprawy urządzeń wchodzących w skład infrastruktury informatycznej wspomagających lub zabezpieczających działanie systemu informatycznego.

11. Administrator Bezpieczeństwa Informacji może odstąpić od usuwania skutków incydentu, jeżeli został on spowodowany działaniem celowym, a całkowite wyjaśnienie zdarzenia i wyciągnięcie konsekwencji wobec sprawców jest istotniejsze niż przerwa w działaniu systemu. Istniejący stan systemu informatycznego jest niezmieniany w celach dowodowych do czasu wyjaśnienia sprawy.
12. Przy usuwaniu skutków incydentu z wykorzystaniem odtwarzania danych z kopii awaryjnych Administrator Bezpieczeństwa Informacji obowiązany jest upewnić się, że odtworzone dane zostały zapisane przed wystąpieniem incydentu - w szczególności dotyczy to przypadków odtwarzania systemu po infekcji wirusowej.
13. Osoby upoważnione.
    - w sytuacjach wyjątkowych wszystkie powyżej opisane działania związane z usuwaniem skutków incydentu i wyjaśnianiem jego przyczyn mogą być realizowane przez osoby upoważnione przez Administratora Bezpieczeństwa Informacji.
    - ABI odpowiada za sporządzenie listy pracowników mających prawo do podejmowania odpowiednich kroków w razie wystąpienia incydentu w sytuacji, gdy nie mogą one być wykonane osobiście przez niego.
14. Raporty i powiadomienia.
    - ABI określa, na podstawie przeprowadzonych wyjaśnień, przyczyny zaistnienia incydentu,
    - jeżeli incydent był spowodowany celowym działaniem, ABI jest zobowiązany do pisemnego powiadomienia Wójta Gminy - Administratora Danych lub Zastępcę Wójta,
    - Wójt Gminy - Administrator Danych 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.
15. Korzystanie z urządzeń po naruszeniu ochrony.

Zgodę na uruchomienie komputerów i innych urządzeń lub dokonanie zmian w miejscu naruszenia ochrony wyraża ABI lub osoba przez niego upoważniona.

16. Czynności końcowe - obserwacja.

System informatyczny, którego prawidłowe działanie zostało odtworzone, powinien zostać poddany szczegółowej obserwacji w celu stwierdzenia całkowitego usunięcia symptomów incydentu. W czasie jej trwania użytkowanie systemu informatycznego powinno być ograniczone do niezbędnego minimum.

Okres kwarantanny, o którym mowa powyżej , jest uzależniony charakterem incydentu i specyfiką systemu informatycznego - jest on każdorazowo określany przez Administratora Bezpieczeństwa Informacji.

17. Czynności końcowe - dokumentacja.
   - ABI dokumentuje w raporcie każdy zaistniały przypadek naruszenia ochrony danych osobowych,
   - dokumentacja, o której mowa powyżej, obejmuje następujące informacje:
     - imię i nazwisko osoby zgłaszającej incydent,
     - imię i nazwisko osoby przyjmującej zgłoszenie incydentu,
     - datę i godzinę przyjęcia zgłoszenia incydentu,
     - określenie czasu i miejsca incydentu,
     - opis zgłoszonego incydentu oraz okoliczności towarzyszące,
     - przyczyny wystąpienia naruszenia,
     - opis podjętych działań naprawczych,
     - wyniki przeprowadzonego badania wyjaśniającego,
     - ocenę skuteczności przeprowadzonego postępowania naprawczego,
     - podjęte środki techniczne, organizacyjne i dyscyplinarne w celu zapobiegania w przyszłości naruszenia ochrony danych osobowych.
     - wzór raportu, o którym mowa w ust.17, określa załącznik nr 10 do Polityki Bezpieczeństwa.

18. Czynności końcowe - analiza.

Administrator Bezpieczeństwa Informacji w oparciu o posiadaną dokumentację, odpowiedzialny jest za przeprowadzenie przynajmniej raz w roku analizy zaistniałych incydentów w celu:

- określenia skuteczności podejmowanych działań wyjaśniających i naprawczych.
- określenia wymagań działań zwiększających bezpieczeństwo systemu informatycznego i minimalizujących ryzyko zaistnienia incydentów.
- określenia potrzeb w zakresie szkoleń użytkowników systemu informatycznego przetwarzającego dane osobowe.

ROZDZIAŁ VIII

Postanowienia końcowe

1. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie dyscyplinarne.
2. Administrator Bezpieczeństwa Informacji zobowiązany jest prowadzić ewidencję osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych wg wzoru stanowiącego załącznik nr 11 do niniejszego dokumentu.

3. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, w szczególności przez osobę, która wobec naruszenia zabezpieczenia systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym Administratora Bezpieczeństwa.
4. Orzeczona kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia Administratora Bezpieczeństwa Informacji nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2002r. Nr 101, poz. 926 ze zm.) oraz możliwość wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
5. W sprawach nieuregulowanych niniejszym dokumentem mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2002r. Nr 101, poz. 926), rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024) oraz rozporządzenie Ministra Sprawiedliwości z dnia 28 kwietnia 2004r. w sprawie sposobu technicznego przygotowania systemów i sieci do przekazywania informacji – do gromadzenia wykazów połączeń telefonicznych i innych przekazów informacji oraz sposobów zabezpieczenia danych informatycznych (Dz. U. Nr 100, poz. 1023).

Załącznik Nr 1
do Polityki Bezpieczeństwa

.....
(pieczątka)

UPOWAŻNIENIE

Na podstawie art. 37 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.) upoważniam Panią/a zatrudnioną/ego w ..... na stanowisku ..... do przetwarzania danych osobowych.

Zadania i czynności do wykonania:

1. Ochrona danych osobowych w systemie informatycznym i ręcznym, a w szczególności przeciwdziałanie dostępowi osób niepowołanych oraz przeciwdziałanie w przypadku wykrycia naruszeń zabezpieczeń systemu zgodnie z ustawą o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.).
2. Przestrzeganie zasad określonych w instrukcji określającej sposób zarządzania systemem informatycznym i ręcznym. (Rozdział VI)
3. Przestrzeganie zasad określonych w instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych. (Rozdział VII)
4. Przestrzeganie zachowania w tajemnicy danych osobowych uzyskanych w okresie zatrudnienia w związku z upoważnieniem do przetwarzania danych osobowych, także po ustaniu stosunku pracy.
5. W szczególności przetwarzanie danych osobowych w następujących zbiorach danych (numer i nazwa): ..... .

.....
(data i podpis administratora)

.....
(data i podpis pracownika)

Załącznik Nr 2
do Polityki Bezpieczeństwa

...., dnia ..... r.
(imię i nazwisko)

.....
(referat)

OŚWIADCZENIE

Oświadczam, że zapoznałem(łam) się z przepisami prawa dotyczącymi ochrony danych osobowych, a w szczególności z ustawą z 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. 2002 Nr 101, poz. 926 ze zm.) oraz rozporządzeniem ministra spraw wewnętrznych i administracji z 29 kwietnia 2004 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemu informatyczne, służące do przetwarzania danych osobowych (Dz. U Nr 100, poz. 1024) i zobowiązuję się do ich przestrzegania.

Oświadczam ponadto, że zapoznałem(łam) się z Polityką bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Gminy Miedziana Góra wprowadzoną zarządzeniem nr 28/2007 Wójta Gminy Miedziana Góra z dnia 20 czerwca 2007 r. oraz Instrukcją przetwarzania danych osobowych.

Świadomy(a) odpowiedzialności porządkowej i karnej oświadczam, że znane mi dane osobowe będę przetwarzać zgodnie z prawem, i nie dopuszczę do bezprawnego naruszenia tajemnicy również w sytuacji, gdy ustanie moje zatrudnienie w:

Urząd Gminy Miedziana Góra
ul. Urzędnicza 18
26-085 Miedziana Góra

Otrzymałem(łam) dnia:

.....
(data i podpis pracownika)

Załącznik Nr 3
do Polityki Bezpieczeństwa

....., dnia ..... r.

WYCOFANIE UPOWAŻNIENIA

Na podstawie art.37 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002r. Nr 101, poz. 926 ze zm.) w związku z: .....
.....
.....
.....
cofam upoważnienie Pana/Pani .....
zatrudnionego/zatrudnionej w ..... na stanowisku.....
do przetwarzania danych osobowych, wynikającego z zakresu obowiązków pracowniczych.

Otrzymałem(łam) dnia:

.....
(data i podpis pracownika)

Załącznik Nr 4
do Polityki Bezpieczeństwa

Wykaz pomieszczeń lub części pomieszczeń w których przetwarzane są dane

Lp.	Nr. pokoju	Referat / samodzielne stanowisko (imię i nazwisko)	Określenie części pomieszczenia, w którym przetwarza się, lub archiwizuje dane
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			

Załącznik Nr 5a
do Polityki Bezpieczeństwa

Wykaz zbiorów przetwarzanych w inny sposób niż elektronicznie

Lp.	Nr. pokoju	Referat / samodzielne stanowisko (imię i nazwisko)	Rodzaj danych / cel przetwarzania	Nazwa zbioru
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				

Załącznik Nr 5b
do Polityki Bezpieczeństwa

Wykaz zbiorów przetwarzanych elektronicznie

Lp.	Nr. pokoju	Referat / samodzielne stanowisko (imię i nazwisko)	Nazwa urządzenia i program zastosowany do przetwarzania (urządzenie / system / program / wersja)	Nazwa zbioru / Cel przetwarzania
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				

Załącznik Nr 6
do Polityki Bezpieczeństwa

Opis struktury zbiorów danych

Zgodnie z §4 pkt 3 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 Kwietnia 2004 r. (Dz. U. Nr 100, poz. 1024), dla każdego zidentyfikowanego zbioru danych powinien być wskazany opis struktury zbioru i zakres informacji gromadzonych w danym zbiorze. Opisy poszczególnych pól informacyjnych w strukturze zbioru danych powinny jednoznacznie wskazywać jakie kategorie danych są w nich przechowywane.

W §4 pkt 3 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. (Dz. U. Nr 100, poz. 1024) wyraźnie wskazano, że w polityce bezpieczeństwa ma być zawarty opis struktury zbiorów wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi. Opis ten może być przedstawiony w postaci formalnej, w postaci graficznej pokazującej istniejące powiązania pomiędzy obiektami, jak również opisu tekstowego.

Opis struktury zbioru danych powinien znajdować się w dokumentacji technicznej eksploatowanych systemów. Dokumentacja może być załączona w formie elektronicznej lub papierowej.

Załączniki:

1. .....
2. .....
3. .....
4. .....
5. .....

Załącznik Nr 7
do Polityki Bezpieczeństwa

Sposób przepływu danych pomiędzy systemami

Załącznik Nr 8
do Polityki Bezpieczeństwa

Opis rejestracji baz danych

W przypadku konieczności przetwarzania danych w nowej bazie danych, wymagana jest konsultacja z Administratorem Bezpieczeństwa Informacji (ABI). W przypadku konieczności rejestracji bazy danych w Generalnym Inspektoracie Danych Osobowych, rejestracja następuje na wniosek danego referatu.

Każdy referat powinien prowadzić dokumentację opisującą bazy danych osobowych przetwarzanych w wydziale.

Dokumentacja winna zawierać:

- nazwę bazy,
- imię i nazwisko osoby tworzącej,
- datę utworzenia,
- ewentualną datę zakończenia przetwarzania danych,
- podstawę prawną przetwarzania,
- cel przetwarzania,
- listę osób przetwarzających dane,
- zakres danych osobowych zawartych w bazie,
- przewidywany czas użytkowania bazy (stały, okresowy, jednorazowy),
- informacje o ewentualnym przekazywaniu danych (komu, kiedy, w jakim celu, podstawa prawna, jaki zakres przekazania danych),
- dodatkowe ważne informacje (zmiany osób uprawnionych itp.).

Załącznik Nr 9
do Polityki Bezpieczeństwa

Opis zabezpieczeń systemów informatycznych

1. W celu ochrony przed utratą danych w Urzędzie Gminy Miedziana Góra stosowane są następujące zabezpieczenia:
   a) odrębne zasilanie sprzętu komputerowego,
   b) ochrona serwerów przed zanikiem (wahaniami) zasilania poprzez stosowanie zasilaczy zapasowych UPS,
   c) ochrona newralgicznych elementów sieciowych (switchy) przed zanikiem zasilania,
   d) ochrona przed utratą zgromadzonych danych przez robienie codziennych kopii zapasowych na taśmach magnetycznych, dyskach przenośnych lub płytach CD/DVD, z których w przypadku awarii odtwarzane są dane i system operacyjny,
   e) ochrona przed awarią podsystemu dyskowego poprzez używanie macierzy dyskowych (mirroring),
2. Zabezpieczenia przed nieautoryzowanym dostępem do baz danych Urzędu Gminy Miedziana Góra:
   a) wszystkie gniazdka lokalnej sieci komputerowej są galwanicznie oddzielone od szkieletu sieci komputerowej. Podłączenie (zkrosowanie) danego użytkownika do szkieletu sieci komputerowej dokonuje Administrator Bezpieczeństwa Informacji, lub osoba przez niego upoważniona,
   b) aby uzyskać dostęp do zasobów sieci, należy zwrócić się do Administratora Bezpieczeństwa z wnioskiem w którym podane będą dane nowego użytkownika oraz zasoby jakie mają być udostępnione,
   c) w systemie informatycznym Urzędu Gminy zastosowano podwójną autoryzację użytkownika. Pierwszej autoryzacji należy dokonać w momencie uzyskania dostępu do serwera Urzędu podając login oraz hasło, drugiej autoryzacji należy dokonać uruchamiając program użytkowy, podając login użytkownika oraz hasło. Dostęp do wybranej bazy danych uzyskuje się dopiero po poprawnym podwójnym zalogowaniu się do systemu informatycznego.
3. Zabezpieczenia przed nieautoryzowanym dostępem do baz danych Urzędu Gminy poprzez Internet.

W zakresie dostępu do sieci wewnętrznej Urzędu Gminy z rozległej sieci Internet zastosowano środki ochrony przed podsłuchiwaniem, penetrowaniem i atakiem z zewnątrz. Zastosowano firewall na routerze, który ma za zadanie uwierzytelnianie źródła przychodzących pakietów oraz ich filtrowanie w oparciu o adres IP i inne parametry. Zablokowano wszystkie nieużywane porty celem zmniejszenia potencjalnych luk, które mogą być wykorzystane przez osobę próbującą uzyskać nieautoryzowany dostęp do sieci wewnętrznej. Ruch pakietów, oraz otwarte porty zostały określone przez Administratora Bezpieczeństwa.

Firewall zapisuje do logu fakt zaistnienia wyjątkowych zdarzeń i śledzi ruch pakietów przechodzących przez router. dostęp do sieci zewnętrznej jest ustalony indywidualnie na wniosek pisemny, lub ustny użytkownika. Oprócz filtra pakietów (firewall) zastosowano system wykrywający obecność wirusów w poczcie elektronicznej.

W efekcie zapewnione jest:

- zabezpieczenie sieci przed atakiem z zewnątrz poprzez blokowanie wszystkich zbędnych portów,
- objęcie ochroną antywirusową wszystkich danych ściąganych z sieci Internet na stacjach lokalnych,
- zapisywanie do logów połączeń użytkowników z siecią Internet.

4. Postanowienia końcowe.
   a) do pomieszczeń w których następuje przetwarzanie danych osobowych mają dostęp tylko uprawnione osoby bezpośrednio związane z nadzorem nad serwerami, lub aplikacjami. Dostęp ten powinien być kontrolowany za pomocą drzwi z elektronicznym zamkiem szyfrowym,
   b) zabezpieczenie przed nieuprawnionym dostępem do danych, prowadzone jest przez ABI zgodnie z przyjętymi procedurami nadawania uprawnień do systemu informatycznego,
   c) osoby mające dostęp do danych powinny posiadać zaświadczenie o przebytym szkoleniu z zakresu ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997r.,
   d) w pomieszczeniach w których znajdują się serwery powinna być zamontowana klimatyzacja, która zapewni właściwą temperaturę i wilgotność powietrza dla sprzętu komputerowego,
   e) w pobliżu wejścia do pomieszczenia z serwerami i innymi urządzeniami powinna znajdować się gaśnica, która jest okresowo napełniana i kontrolowana przez stosownego specjalistę.

Załącznik Nr 10
do Polityki bezpieczeństwa

Raport nr ..... / .....

z naruszenia bezpieczeństwa systemu informatycznego

w Urzędzie Gminy Miedziana Góra

1. Data: ..... Godzina: .....
(dd.mm.rrrr) (00:00)

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

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

3. Lokalizacja zdarzenia:

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

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

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

5. Podjęte działania:

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

6. Przyczyny wystąpienia zdarzenia:

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

7. Postępowanie wyjaśniające:

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

8. Ocena skuteczności przeprowadzonego postępowania naprawczego:

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

9. Podjęte środki techniczne, organizacyjne i dyscyplinarne w celu zapobiegania w przyszłości podobnym naruszeniom ochrony danych osobowych:

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

.....
(data i podpis
Administratora Bezpieczeństwa Informacji)

Załącznik Nr 11
do Polityki Bezpieczeństwa

Wzór wykazu osób które zapoznały się z „Polityką bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Gminy Miedziana Góra."

Wykaz osób, które zostały zapoznane z **„Polityką bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Gminy Miedziana Góra"**, przeznaczonej dla osób zatrudnionych przy przetwarzaniu tych danych.

Przyjąłem/am/ do wiadomości i stosowania zapisy Polityki bezpieczeństwa.

Nr upoważnienia	Nazwisko i Imię	Data nadania	Upoważniający	Data odebrania	Odbierający

.....
(data i podpis
Administratora Bezpieczeństwa Informacji)

Załącznik Nr 12
do Polityki Bezpieczeństwa

Ewidencja osób upoważnionych do przetwarzania danych.

Lp.	Imię	Nazwisko	Identyfikator
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

.....

(data i podpis
Administratora Bezpieczeństwa Informacji)

załącznik nr 6 do
Zarządzenia Nr 28/2007
z dnia 20 czerwca 2007

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych w Urzędzie Gminy w Miedzianej Górze

I. Podstawa Prawna

Niniejsza Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych w Urzędzie Gminy w Miedzianej Górze zwana dalej Instrukcją reguluje sposób zarządzania systemem informatycznym służącym do przetwarzania danych (w tym danych osobowych i innych prawnie chronionych) z uwzględnieniem wymogów określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100 poz. 1024), rozporządzeniu Ministra Rozwoju Regionalnego i Budownictwa z dnia 16 lipca 2001r. w sprawie zgłaszania prac geodezyjnych i kartograficznych, ewidencjonowania systemów i przechowywania kopii zabezpieczających bazy danych, a także ogólnych warunków umów o udostępnianie tych baz (Dz.U. Nr 78, poz. 837)

II. Cel instrukcji

Instrukcja określa zasady zarządzania systemami informatycznymi służącymi do przetwarzania danych (w tym danych osobowych i innych prawnie chronionych) w Urzędzie Gminy w Miedzianej Górze.
Celem utworzenia instrukcji jest podniesienie poziomu bezpieczeństwa systemów informatycznych, w których są prowadzone i przetwarzane dane oraz określenie odpowiedzialności użytkowników za prawidłowe działanie tych systemów i bezpieczeństwo przetwarzania w nim danych osobowych.

Uwzględniając kategorie przetwarzanych danych oraz zagrożenia wprowadza się w Urzędzie Gminy w Miedzianej Górze zwanym dalej Urzędem wysoki poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym.

III. Administratorzy.

1. Administratorem danych w Urzędzie Gminy w Miedzianej Górze jest Wójt Gminy

2. Funkcję Administratora bezpieczeństwa informacji pełni osoba wyznaczona przez Wójta Gminy

3. Decyzję o udostępnieniu danych innemu podmiotowi podejmuje każdorazowo administrator danych

IV. Uprawnienia do przetwarzania danych, metody i środki uwierzytelniania.

1. Do przetwarzania danych uprawnione są jedynie osoby posiadające pisemne upoważnienie zwane dalej „użytkownikami".

2. Przed przystąpieniem do przetwarzania danych osobowych każdy użytkownik systemu musi zapoznać się z :
   - ustawą z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U.z 2002r. Nr 101, poz. 926 ze zm.),
   - Polityką Bezpieczeństwa Informacji Urzędu Gminy w Miedzianej Górze,
   - niniejszym dokumentem

3. Dostęp do komputera (utworzenie konta w systemie operacyjnym komputera) będzie przyznawany na podstawie uprawnień lub na podstawie upoważnienia.

4. Podstawowym sposobem uwierzytelniania w systemach informatycznych w Urzędzie jest login i hasło użytkownika. Zasady tworzenia haseł określa procedura „Zasady tworzenia i postępowania z hasłami do systemów informatycznych obowiązujące w Urzędzie Gminy w Miedzianej Górze" stanowiąca załącznik nr 1 do niniejszego dokumentu.

5. Dostęp do danych przetwarzanych w postaci elektronicznej możliwy jest po wielostopniowym uwierzytelnieniu użytkownika:
   1) dostęp do komputera zabezpieczony jest hasłem zapisanym w systemie BIOS komputera,
   2) dostęp do systemu operacyjnego wymaga pełnego uwierzytelnienia użytkownika (login i hasło),
   3) dostęp do systemów w których przetwarzane są dane (ze szczególnym uwzględnieniem danych osobowych i innych danych prawnie chronionych), wymaga pełnego uwierzytelnienia użytkownika (login i hasło).

6. Dostęp do systemów operacyjnych serwerów, na których przetwarzane są dane (ze szczególnym uwzględnieniem danych osobowych) możliwy jest wyłącznie dla pracowników obsługi informatycznej Urzędu po podaniu identyfikatora i hasła użytkownika.

V. Środki ochrony systemów informatycznych

1. Ochrona antywirusowa.

    1) Wszystkie komputery oraz serwery wyposażone są w system antywirusowy posiadający funkcje automatycznej, codziennej aktualizacji bazy wirusów oraz bieżącego skanowania każdego uruchomionego programu i otwieranego pliku.
    2) Za instalację systemu antywirusowego odpowiedzialny jest pracownik obsługi informatycznej Urzędu.

2. Ochrona na styku sieci wewnętrznej z siecią Internet.

    1) Ze względu na wagę posiadanych danych i ich bezpieczeństwo stosuje się zasadę separacji lokalnej sieci wewnętrznej Urzędu od sieci Internet za pomocą sprzętowej zapory wysokiej klasy, posiadającej funkcje blokowania portów, wykrywania wirusów, filtrowania treści oraz mechanizm wykrywania i zapobiegania włamaniom. Dodatkowo cała poczta elektroniczna przychodząca do Urzędu jest filtrowana pod kątem zawartości wirusów oraz niepożądanych treści (spamu) przez sprzętowy system antyspamowy.
    2) Szeroki dostęp do Internetu posiadają wyłącznie wydzielone stanowiska podłączone do sieci odseparowanej od sieci wewnętrznej, w której przetwarzane są dane osobowe.
    3) Stanowiska podłączone do sieci wewnętrznej, w której przetwarzane są dane osobowe podłączane są do Internetu wyłącznie w szczególnie uzasadnionych wypadkach i tylko do tych zasobów, które są niezbędne do realizowania określonych zadań, Głównego Urzędu Statystycznego, Regionalnej Izby Rozrachunkowej, Elektronicznej Platformy Usług Administracji Publicznej i inne zgodnie z potrzebami.
    4) W przypadku konieczności przesyłania danych osobowych lub innych danych prawnie chronionych przy użyciu sieci Internet należy stosować metody zabezpieczenia tych danych poprzez ich szyfrowanie lub kompresję z użyciem hasła

3. Ochrona przed awarią zasilania.

    1) Wszystkie serwery, komputery, urządzenie peryferyjne i urządzenia aktywne sieci komputerowej zasilane są z dedykowanej sieci elektrycznej odpowiednio zabezpieczonej. Niedopuszczalne jest używanie sieci komputerowej do podłączania innych urządzeń, zwłaszcza urządzeń dużej mocy (czajniki, urządzenia grzewcze).
    2) Serwery, na których przetwarzane są dane, zabezpiecza się przed utratą danych spowodowanych awarią zasilania poprzez zainstalowanie zasilaczy awaryjnych z mechanizmem automatycznego zamykania systemu w przypadku braku zasilania. Zasilaniem awaryjnym objęte są także wszystkie elementy aktywne sieci.

VI. Archiwizacja danych.

Dane zabezpiecza się przed utratą spowodowaną awarią zasilania, sprzętu lub sieci komputerowej poprzez tworzenie kopii zapasowych. Zasady tworzenia kopii zapasowych opisuje załącznik nr 2

VII. Zasady wykonywania przeglądów, napraw i konserwacji systemu.

1. Dla zachowania ciągłości pracy i bezpieczeństwa danych przeprowadza się kontrole, przeglądy, naprawy i konserwacje platformy sprzętowej i programowej.

2. Przeglądy i konserwacje systemu i zbiorów danych dokonywane są przez pracownika obsługi informatycznej Urzędu lub w przypadku uzasadnionej potrzeby przez osoby posiadające odpowiednie kwalifikacje w tym zakresie.

3. Naprawy i zmiany w systemie informatycznym przeprowadzane przez serwis zewnętrzny prowadzone są pod nadzorem pracownika obsługi informatycznej Urzędu, jeżeli jest to możliwe – w siedzibie Urzędu a jeżeli jest to niemożliwe po podpisaniu umowy powierzenia przetwarzania danych osobowych także poza siedzibą Urzędu.

VIII. Inne środki ochrony danych.

1. Płyty CD, pamięci zewnętrzne lub inne nośniki informatyczne zawierające dane przeznaczone do likwidacji użytkownik pozbawia wcześniej zapisu tych danych a gdy jest to niemożliwe uszkadza w sposób uniemożliwiający odczytanie. Jeżeli wymienione nośniki przeznaczone są do przekazania innemu podmiotowi nieuprawnionemu do otrzymania danych należy pozbawić je wcześniej zapisu tych danych.

2. Dyski twarde przeznaczone do likwidacji pracownik obsługi informatycznej Urzędu niszczy mechanicznie w sposób uniemożliwiający odczyt danych.

3. W przypadku zbiorów danych osobowych przetwarzanych w postaci plików tekstowych lub arkuszy kalkulacyjnych dane te należy zabezpieczyć hasłem (mechanizm dostępny w pakietach biurowych oraz w archiwizatorach np. 7z). W uzasadnionych przypadkach pracownicy obsługi informatycznej udostępniają program umożliwiający szyfrowanie plików i nośników danych.

4. Użytkownik przenośnego komputera służącego do przetwarzania danych osobowych lub innych prawnie chronionych zobowiązany jest do zachowania szczególnej ostrożności podczas transportu, zabezpieczenia komputera hasłem, oraz nieudostępniania komputera osobom nieupoważnionym do dostępu do danych. Użytkownik przenośnego sprzętu komputerowego używanego poza obszarem przetwarzania danych zobowiązany jest do prawidłowego zabezpieczenia danych na nim zawartych poprzez zastosowanie mechanizmów zabezpieczania dokumentów hasłami (mechanizm dostępny w pakietach biurowych) lub stosować kompresję danych z zabezpieczeniem hasłem (mechanizm dostępny w archiwizatorach np. 7z). W uzasadnionych przypadkach należy stosować mechanizm szyfrowania dysku, pracownicy obsługi informatycznej udostępniają program umożliwiający szyfrowanie nośników danych.

5. W pomieszczeniu, w którym przetwarzane są dane osobowe lub inne prawnie chronione, osoby nieupoważnione mogą przebywać tylko za zgodą i w towarzystwie użytkownika, niedopuszczalne jest pozostawienie w pomieszczeniu osób nieupoważnionych bez nadzoru ze strony pracowników Urzędu. W przypadku opuszczenia tych pomieszczeń winny być one bezwzględnie zamykane na klucz. Przebywanie w obszarze przetwarzania danych osób nieuprawnionych jest dopuszczalne za zgodą administratora danych lub w obecności osoby uprawnionej do przetwarzania danych.

6. Monitory w pomieszczeniach, w których przebywają osoby nieupoważnione do dostępu do danych winny być ustawione w sposób uniemożliwiający tym osobom wgląd do danych.

7. Ekrany monitora jest automatycznie wygaszany po upływie max. 10 minut od momentu zaprzestania pracy, a powtórne jego wyświetlenie możliwe po podaniu hasła.

8. Wydruki i dokumenty zawierające dane powinny być zabezpieczone przed przypadkowym odczytaniem przez osoby nieupoważnione, i przechowywane w szafach wyposażonych w zamki.

9. Wydruki zawierające dane przeznaczone do usunięcia użytkownik niszczy w stopniu uniemożliwiającym ich odczytanie.

10. W udostępnionych zasobach sieciowych komputerów (katalog Public) nie wolno przechowywać plików zawierających dane osobowe lub inne dane prawnie chronione.

IX. Udostępnianie i monitorowanie dostępu do danych osobowych.

1. Decyzję o udostępnieniu danych osobowych za każdym razem podejmuje Administrator danych

2. Udostępnienie danych osobowych może odbyć się zgodnie z obowiązującymi przepisami prawa regulującymi zasady przetwarzania konkretnych zbiorów danych. Udostępnienie może odbyć się wyłącznie na pisemny wniosek. W przypadku braku określenia wzoru wniosku o udostępnienie danych osobowych w odrębnych przepisach regulujących przetwarzanie konkretnych danych, pismo adresowane na Administratora Danych powinno zawierać określenie podmiotu występującego o udostępnienie danych, podstawę udostępnienia danych osobowych, informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz zakres danych i cel ich udostępnienia.

3. Jeżeli udostępnienie danych następuje bezpośrednio z systemu informatycznego, system umożliwia dokonanie wpisu do rejestru potwierdzającego zakres i cel udostępnienia danych, nazwę podmiotu, któremu dane zostały udostępnione i datę udostępnienia.

4. Nie stosuje się zasad zawartych w pkt. 1-3 gdy:

   a) przetwarzane w zbiorze dane są danymi jawnymi w rozumieniu ustawy o ochronie danych osobowych,
   b) dane udostępniane są osobie której bezpośrednio dotyczą,
   c) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

5. System umożliwia automatyczną rejestrację daty wprowadzenie danych osobowych do systemu oraz identyfikatora użytkownika

X. Postępowanie w przypadku naruszenia ochrony danych osobowych.

1. Użytkownik zobowiązany jest zawiadomić Administratora Bezpieczeństwa Informacji o każdym naruszeniu lub podejrzeniu naruszenia bezpieczeństwa systemu, a w szczególności o:

   a) naruszeniu hasła dostępu i identyfikatora (system nie reaguje na hasło lub je ignoruje bądź można przetwarzać dane bez wprowadzania hasła),
   b) częściowym lub całkowitym braku danych albo dostępie do danych w zakresie szerszym niż wynikający z przyznanych uprawnień,
   c) braku dostępu do właściwej aplikacji lub zmianie zakresu wyznaczonego dostępu do zasobów serwera,
   d) wykryciu wirusa komputerowego,
   e) zauważeniu elektronicznych śladów próby włamania do systemu informatycznego Administratora Danych,
   f) znacznym spowolnieniu działania systemu informatycznego,
   g) podejrzeniu kradzieży sprzętu komputerowego lub dokumentów zawierających dane osobowe,
   h) zmianie położenia sprzętu komputerowego,
   i) zauważeniu śladów usiłowania lub dokonania włamania do pomieszczeń lub zamykanych szaf,
   j) wskazującym na naruszenie zabezpieczeń stanie urządzenia, zawartości zbioru danych osobowych, sposobie działania programu, lub pogorszeniu jakości komunikacji w sieci telekomunikacyjnej.

2. Pracownik zobowiązany jest do:

   a) zawiadomienia o powyższym Administratora Bezpieczeństwa Informacji i swojego przełożonego,
   b) zablokowanie komputera w sposób uniemożliwiający dalszą pracę w systemie,
   c) utrzymania sprzętu w taki sposób, aby uniemożliwić do niego dostęp innym osobom.

3. Administrator Bezpieczeństwa Informacji po otrzymaniu zawiadomienia powinien:

   a) przeprowadzić postępowanie wyjaśniające, w celu ustalenia okoliczności naruszenia ochrony danych osobowych, ustalenia przyczyn oraz skutków,
   b) podjąć działania chroniące system przed ponownym naruszeniem,
   c) podjąć działania w celu przywrócenia stanu przed ujawnieniem naruszenia zabezpieczeń systemu,

d) w przypadku stwierdzenia faktycznego naruszenia bezpieczeństwa systemu sporządzić raport z naruszenia bezpieczeństwa systemu informatycznego a następnie niezwłocznie przekazać jego kopie Administratorowi Danych.

4. Administrator Bezpieczeństwa Informacji może zarządzić, w razie potrzeby, odłączenie części systemu informatycznego dotkniętej incydentem od pozostałej jego części.

5. W razie odtwarzania danych z kopii zapasowych Administrator Bezpieczeństwa Informacji 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, podejmuje decyzję o dalszym trybie postępowania, powiadomieniu właściwych organów oraz podjęciu innych, szczególnych czynności zapewniających bezpieczeństwo systemu informatycznego bądź zastosowaniu środków ochrony fizycznej.

1. **Załączniki.**

Załącznik nr 1 – Zasady tworzenia i postępowania z hasłami do systemów informatycznych obowiązujące w Urzędzie Gminy w Miedzianej Górze

Załącznik nr 2 – Zasady tworzenia kopii zapasowych do systemów informatycznych obowiązujące w Urzędzie Gminy w Miedzianej Górze

załącznik nr 1
do Instrukcji zarządzania

Zasady tworzenia i postępowania z hasłami do systemów informatycznych obowiązujące

w Urzędzie Gminy w Miedzianej Górze

1. Wszystkie hasła, jakie występują w systemie i są związane z eksploatacją podlegają okresowej zmianie, nie rzadziej niż raz w miesiącu. Hasła podlegające zmianie:
   a) hasła Administratora Systemu Informatycznego dostępu do serwera systemu,
   b) hasła Operatorów Systemu dostępu do aplikacji,
2. Zmiana haseł określonych w punktach a i b poprzedniego ustępu powinna być wymuszana poprzez konfigurację kont użytkowników lub przez aplikację użytkową.
3. Hasło powinno zawierać, co najmniej 6 znaków a jego treść nie powinna umożliwiać identyfikacji użytkownika systemu i musi być utajniona.
4. Hasła dostępu do konfiguracji stacji roboczych i serwera są zmieniane nie rzadziej niż raz
   w miesiącu, w sposób identyczny dla wszystkich stacji przez Administratora Systemu Informatycznego.

załącznik nr 2

do Instrukcji zarządzania

Zasady tworzenia kopii zapasowych

1. Zabezpieczenie danych systemu polega na stworzeniu kopii zabezpieczających plików zawierających *dane osobowe*, na wymienialnym nośniku, w stacji posiadającej dostęp do danych systemu. Kopie zabezpieczające danych systemu można wykonywać na nośnikach dopuszczonych przez Administratora Systemu Informatycznego.
2. Kopie oprogramowania systemu wykonuje się niezależnie dla wszystkich serwerów systemu.
3. Zasady oznaczania kopii zabezpieczających:
   a) po wykonaniu kopii zabezpieczającej każdy nośnik musi być opisany na obudowie lub opakowaniu i przechowywany w opakowaniu,
   b) fakt wykonania każdej kolejnej kopii na kasecie należy umieścić w opisie kasety,
4. Ewidencja wykonywania kopii zabezpieczających:

   Fakt wykonania każdej kopii zabezpieczającej, względnie potwierdzenie automatycznego wykonania kopii przez system, należy umieścić w *Wykazie Wykonywania Kopii Zabezpieczających.*
5. Wykonywanie kopii zabezpieczających w systemie informatycznym:
   a) zakres wykonywania kopii zabezpieczających:
      1) wykonywanie kopii danych systemu obejmuje wszystkie pliki znajdujące się w katalogach określonych w *Opisie Systemu* jako dane systemu,
      2) wykonywanie kopii oprogramowania systemu obejmuje wykonanie fizycznej kopii wszystkich elementów oprogramowania systemu informatycznego, w sposób umożliwiający odtworzenie aktualnego stanu systemu,
   b) częstotliwość i sposób wykonywania i okres przechowywania kopii zabezpieczających określi Administrator Systemu Informatycznego i dołączy do *Wykazu Wykonywania Kopii Zabezpieczających*, w szczególności należy przestrzegać następujących zasad:
      1) kopie oprogramowania systemu i danych systemu powinny być wykonywane w dwóch jednakowych egzemplarzach,
      3) kopie zabezpieczające dane systemu powinny być w szczególności wykonywane:
         a. przed wprowadzeniem nowej wersji oprogramowania,
         b. przed wykonaniem niestandardowych czynności związanych z bazą danych (np. uruchomienie oprogramowania sprawdzającego lub przywracającego integralność bazy danych, itd.),
      4) kopie zabezpieczające oprogramowanie systemu powinny być w szczególności wykonywane:
         a. po zainstalowaniu i skonfigurowaniu systemu,
         b. po każdorazowej zmianie w konfiguracji systemu.
6. Zasady określające sposoby deponowania i wykorzystywania kopii zabezpieczających:

a) nośniki zawierające kopie zabezpieczające podlegają zdeponowaniu w opakowaniu zapieczętowanym przez Administratora Systemu Informatycznego, wraz z numerem oraz wykazem kopii, które zawierają. Dopuszcza się inny sposób zdeponowania kopii, zatwierdzony przez Administratora Bezpieczeństwa Informacji.

b) kopie zabezpieczające należy deponować w ognioodpornych szafach pancernych pomieszczenia bezpieczeństwa, przeznaczonych do przechowywania nośników magnetycznych,

c) w wypadku konieczności wykorzystania kopii zabezpieczającej do odtworzenia oprogramowania systemu lub danych systemu należy:

1) pobrać stosowną kopię,

2) po zakończeniu odtwarzania oprogramowania systemu lub danych systemu należy przekazać kopię zabezpieczającą do miejsca zdeponowania wraz z protokołem stwierdzającym jej użycie.

d) dopuszcza się wielokrotne użycie nośnika do wykonywania kopii zabezpieczających. Administrator Systemu Informatycznego zobowiązany jest zachować następujący tryb postępowania:

1) należy wyselekcjonować nośniki, które mogą podlegać ponownemu użyciu z uwzględnieniem minimalnego okresu przechowywania kopii,

2) należy skasować poprzednią zawartość nośnika w sposób uniemożliwiający odtworzenie – nośnik od chwili skasowania jest traktowany jako nowy,

e) w wypadku otwarcia opakowania, w którym zdeponowano kopię zabezpieczającą, należy po zamknięciu ponownie go zapieczętować. Fakt każdorazowego otwarcia opakowania należy opisać na opakowaniu,

f) za poprawne wykonanie czynności Administratora Systemu Informatycznego, w związku z odtwarzaniem oprogramowania systemu z kopii zabezpieczających, odpowiada Administrator Bezpieczeństwa Informacji.

7. Przechowywanie nośników oprogramowania, dyskietek startowych itp.

a) Oryginały nośników oprogramowania i dyskietek startowych wraz z dokumentacją należy deponować w szafie. Zaleca się wykonanie kopii awaryjnych tych nośników do stosowania w celach użytkowych.

b) Oprogramowanie i dyskietki startowe należy przechowywać zgodnie z zasadami przechowywania kopii zabezpieczających, z następującymi zastrzeżeniami:

1) opakowanie, w którym przechowuje się oprogramowanie winno zawierać:

a. dokładny opis nośników – rodzaj, ilość i nazwy jeśli występują,

b. dokładny opis dokumentacji – tytuły, ilość pozycji,

8. Licencje na używane w systemie oprogramowanie należy przechowywać w szafie w sposób uporządkowany oraz pozwalający na łatwe określenie ilości oprogramowania licencyjnego oraz sposobu (miejsca) jego użytkowania.

9. Nośniki zawierające kopie zabezpieczające nie nadające się do kolejnego użycia należy poddać likwidacji

Ewidencja osób dopuszczonych do przetwarzania danych osobowych w systemie informatycznym

1. **Referat spraw obywatelskich**
   - Anna Karczewska – kierownik referatu **pok. Nr 23**

2. **Urząd Stanu Cywilnego**
   - Teodozja Wiśniewska – kierownik USC **pok. Nr 24**
   - Anna karczewska – z-ca kierownika USC **pok. Nr 23**

3. **Referat Organizacyjny**
   - Teresa Reczyńska – kierownik referatu **pok. Nr 22**
   - Michał Tokar – Informatyk **pok. Nr 10**

4. **Referat Finansowy**
   - Szymon Sikora – (skarbnik gminy) kierownik referatu **pok. Nr 9**
   - Janina Mróz – inspektor ds. podatków i opłat **pok. Nr 2**
   - Jadwiga Moćko - inspektor ds. księgowości budżetowej **pok. Nr 3**
   - Barbara Piątek - inspektor ds. podatków i opłat **pok. Nr 2**
   - Justyna Błaszczyk - inspektor ds. księgowości budżetowej **pok. Nr 3**
   - Dorota Wójcik.- podinspektor ds. działalności gospodarczej **pok. Nr 13**
   - Anna Słoń - podinspektor ds. płac **pok. Nr 11**
   - Mirosława Wiśniewska - inspektor ds. księgowości podatków i opłat **pok. Nr 1**

5. **Referat infrastruktury technicznej i budownictwa**
   - Irena Danieluk – kierownik referatu **pok. Nr 5**
   - Tomasz Bucki - podinspektor ds. budownictwa **pok. Nr 6**
   - Joanna Jońska - podinspektor ds. rolnictwa i ochrony przyrody **pok. Nr 7**
   - Andrzej Adamski - inspektor ds. nieruchomości i geodezji **pok. Nr 8**

Oświadczenie

Oświadczam iż zapoznałam/em się z treścią zarządzenia Wójta Gminy Miedziana Góra nr 28/2007 z dnia 20 czerwca 2007 wdrażających stosowanie ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Zobowiązuję się do bezwzględnego przestrzegania zasad zawartych w zarządzeniu, posiadam pełną świadomość postępowania - zgodnie z przyjętymi zasadami oraz zobowiązuje się do minimalizowania zagrożeń wynikających z błędów ludzkich.

Miedziana Góra dn. ....

Data Podpis