Zarządzenie Nr 50/15
WÓJTA GMINY SIECIECHÓW
z dnia 1 października 2015r

w sprawie Polityki Bezpieczeństwa i zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy w Sieciechowie

Na podstawie art. 36 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. 2002 r. Nr 101 poz. 926 ze zm.) oraz § 3 i 9 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiada urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024), wprowadza się :

§ 1

1. Politykę Bezpieczeństwa w zakresie zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy w Sieciechowie stanowiącą załącznik Nr 1 do Zarządzenia;
2. Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy w Sieciechowie stanowiącą załącznik Nr 2 do Zarządzenia;
3. Instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych w Urzędzie Gminy w Sieciechowie, stanowiący załącznik Nr 3 do Zarządzenia
4. wzór upoważnienia do przetwarzania danych osobowych, stanowiący załącznik Nr 4 do Zarządzenia
5. wzór oświadczenia pracownika upoważnionego do przetwarzania danych osobowych stanowiący załącznik Nr 5 do Zarządzenia
6. wzór wniosku o udostępnienie danych ze zbioru danych osobowych załącznik Nr 6 do Zarządzenia

§ 2

1. Polityka Bezpieczeństwa informacji ma zastosowanie na wszystkich stanowiskach pracy, gdzie przetwarzane są dane osobowe lub praca odbywa się w systemie informatycznym Urzędzie Gminy w Sieciechowie
2. Zobowiązuję pracowników Urzędu Gminy w Sieciechowie do zapoznania się z treścią niniejszego Zarządzenia .

§ 3

Wykonanie Zarządzenia powierza się Administratorowi Bezpieczeństwa Informacji.

§ 4

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT
Marian Zbigniew Czerski

Załącznik Nr 1
Do Zarządzenia Nr 50
z dnia 1 października 2015r
Wójta Gminy Sieciechów

POLITYKA BEZPIECZEŃSTWA INFORMACJI

W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH

W URZĘDZIE GMINY W SIECIECHOWIE

ROZDZIAŁ I

Postanowienia ogólne

§ 1

1. Polityka Bezpieczeństwa Informacji Urzędu Gminy w Sieciechowie jest zbiorem zasad i procedur obowiązujących przy zbieraniu, przetwarzaniu i wykorzystywaniu danych osobowych we wszystkich zbiorach administrowanych przez Gminę. Odnosi się całościowo do problemu zabezpieczenia danych osobowych przetwarzanych tradycyjnie, jak i danych przetwarzanych w systemach informatycznych.
2. Przetwarzanie danych osobowych w Urzędzie Gminy w Sieciechowie jest dopuszczalne tylko pod warunkiem przestrzegania Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych i wydanych na jej podstawie przepisów wykonawczych oraz Zarządzenia Nr 50 Wójta Gminy Sieciechów a także przepisów wdrożonych w stosownych Instrukcjach.
3. Przetwarzanie danych osobowych przez pracowników i kontrahentów Urzędu Gminy w Sieciechowie służy realizacji zadań wynikających z Ustawy z dnia 8 marca 1990 roku o samorządzie gminnym (Dz.U. z 2013 poz.594 z póź. zm.)
   Celem Polityki Bezpieczeństwa danych osobowych, zwanych inaczej Instrukcją Ochrony Danych Osobowych, jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych w zakresie ochrony danych osobowych, sposobu przetwarzania w Urzędzie Gminy w Sieciechowie grupy informacji zawierającej dane osobowe.

§ 2

Określenia użyte w Polityce Bezpieczeństwa oznaczają:

- **komórka organizacyjna** – odpowiednio komórki organizacyjne - Referaty, o których mowa w „Regulaminie Organizacyjnym Urzędu Gminy w Sieciechowie"
- **dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej
- **przetwarzanie danych osobowych** – gromadzenie, utrwalanie, przechowywanie, opracowywanie, udostępnianie i usuwanie danych osobowych, zwłaszcza w systemach informatycznych
- **Administrator Danych** – Wójt Gminy Sieciechów
- **Administrator Bezpieczeństwa Informacji** – (ABI) osoba odpowiedzialna za bezpieczeństwo przetwarzania danych osobowych
- **Administrator Sieci** – osoba upoważniona do zarządzania systemem informatycznym (informatyk)
- **system informatyczny** – system przetwarzania danych osobowych w Urzędzie Gminy wraz z zasobami ludzkimi, technicznymi oraz finansowymi
- **zabezpieczenie systemu informatycznego** – wdrożenie stosownych środków administracyjnych, technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych a także ich utratą.

§ 3

Utrzymanie bezpieczeństwa przetwarzanych przez Urząd Gminy danych osobowych rozumiane jest jako zapewnienie ich poufności, integralności i uwierzytelnieniu na odpowiednim poziomie.
Miarą bezpieczeństwa jest wielkość ryzyka związanego z ochroną systemu informatycznego.

- **poufność** – rozumiana jest jako zapewnienie, że tylko uprawnieni pracownicy mają dostęp do informacji
- **integralność** – rozumiana jest jako zapewnienie dokładności i kompletności danych osobowych oraz metod ich przetwarzania
- **uwierzytelnienie** – rozumiane jest jako działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.
- **zarządzanie ryzykiem** – rozumiane jest jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informatycznych w których przetwarzane są dane osobowe.

ROZDZIAŁ II

ZAKRES POLITYKI BEZPIECZEŃSTWA

§ 4

1. W systemie informatycznym Urzędu Gminy przetwarzane są dane osobowe służące do wykonywania zadań z zakresu administracji publicznej.
2. Dane osobowe są przetwarzane i składowane zarówno w postaci manualnej jak i elektronicznej.
3. Polityka Bezpieczeństwa Informacji ma zastosowanie do całego systemu informacyjnego Urzędu Gminy , a w szczególności do:
   - wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są dane osobowe
   - informacji będących własnością Urzędu Gminy lub klientów Urzędu Gminy, o ile zostały przekazane na podstawie umów
   - wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie
4. Do stosowania zasad określonych przez dokumenty Polityki Bezpieczeństwa Informacji zobowiązani są wszyscy pracownicy w rozumieniu Kodeksu Pracy, konsultanci, stażyści oraz inne osoby mające dostęp do danych osobowych.

§ 5

Informacje niejawne nie są objęte zakresem niniejszej Polityki.

ROZDZIAŁ III

DOKUMENTACJA POLITYKI BEZPIECZEŃSTWA INFORMACJI

§ 6

1. Dokumenty Polityki Bezpieczeństwa Informacji ustanawiają metody zarządzania oraz wymagania niezbędne do zapewnienia skutecznej i spójnej ochrony przetwarzanych informacji.
2. Polityka Bezpieczeństwa Informacji zawiera w szczególności:
   - Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar w którym przetwarzane są dane osobowe (Załącznik Nr 1 do Polityki bezpieczeństwa)
   - Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych (Załącznik Nr 2 do Polityki bezpieczeństwa)
   - Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania pomiędzy nimi (Załącznik Nr 3 do Polityki bezpieczeństwa)
   - Sposób przepływu danych pomiędzy poszczególnymi systemami (Załącznik Nr 4 do Polityki bezpieczeństwa)
   - Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.
3. Na zestaw dokumentów Polityki Bezpieczeństwa Informacji składa się:
   a) Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, opisująca sposób zarządzania systemem przetwarzania danych osobowych w Urzędzie Gminy
   b) Instrukcja postępowania w sytuacjach naruszenia ochrony danych osobowych opisująca tryb postępowania w sytuacjach naruszenia tego zabezpieczenia, a także uzasadnionego podejrzenia o przygotowanej próbie naruszenia danych osobowych.

ROZDZIAŁ IV

ZARZĄDZANIE DANYMI OSOBOWYMI W URZĘDZIE GMINY

§ 7

Administratorem Danych Osobowych Urzędu Gminy jest Wójt Gminy Sieciechów

§ 8

1. Wójt wyznacza osobę odpowiedzialną za bezpieczeństwo przetwarzania danych osobowych zwaną „Administratorem Bezpieczeństwa Informacji".
2. Obowiązki wynikające z ustawy o ochronie danych osobowych Wójt Gminy Sieciechów powierza Lokalnym Administratorom Danych czyli Kierownikom poszczególnych Referatów – w zakresie podległych im pracowników oraz Sekretarzowi Gminy.

3. Administrator Bezpieczeństwa Informacji realizuje zadania wynikające z ustawy z pomocą pracowników wymienionych w ust. 2.

4. Kierownicy jednostek odpowiadają za realizację wymagań obowiązujących przepisów prawa, dotyczących ochrony danych osobowych, z obowiązkiem współdziałania z Administratorem Bezpieczeństwa Informacji w zakresie swoich właściwości.
5. Dyrektorzy i Kierownicy samorządowych jednostek organizacyjnych Urzędu Gminy zobowiązani są do zapoznania podległych pracowników z treścią ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.), Polityką Bezpieczeństwa Informacji w zakresie przetwarzania danych osobowych, Instrukcją zarządzania systemem informatycznym w zakresie wymogów bezpieczeństwa przetwarzania danych osobowych oraz Instrukcją postępowania w sytuacji naruszenia ochrony danych osobowych.

§ 9

1. Do zadań Administratora Bezpieczeństwa Informacji z upoważnienia Wójta należy:
   - Prowadzenie ewidencji baz danych w systemach informatycznych, w których przetwarzane są dane osobowe w Urzędzie Gminy w Sieciechowie
   - Wydawanie i przechowywanie indywidualnych upoważnień osobom przetwarzającym dane osobowe w Urzędzie Gminy w Sieciechowie
   - Prowadzenie ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych w systemach informatycznych
   - Prowadzenie ewidencji miejsc przetwarzania danych osobowych i sposobu ich zabezpieczania
   - Zapewnienie zapoznania się i przeszkolenie osób zatrudnionych przy przetwarzaniu danych osobowych z przepisami dotyczącymi ochrony danych osobowych w Urzędzie Gminy w Sieciechowie
   - Rejestrowanie zbiorów danych osobowych w rejestrze Generalnego Inspektora Ochrony Danych Osobowych
2. W celu realizacji powierzonych zadań ABI ma prawo:
   - Nadzorować i kontrolować komórki organizacyjne w Urzędzie Gminy w Sieciechowie w zakresie właściwego zabezpieczenia systemów informatycznych oraz pomieszczeń w których przetwarzane są dane osobowe
   - Podejmować działania w przypadkach naruszenia bezpieczeństwa danych osobowych

ROZDZIAŁ V

DOSTĘP I PRZETWARZANIE DANYCH OSOBOWYCH W URZEDZIE GMINY

§ 10

Wszystkie osoby, których rodzaj wykonywanej pracy będzie wiązał się z dostępem do danych osobowych, przed przystąpieniem do pracy, podlegają przeszkoleniu w zakresie obowiązujących przepisów prawa dotyczących ochrony danych osobowych oraz obowiązujących w Urzędzie Gminy zasad ochrony danych osobowych.

§ 11

Osoby nie przestrzegające przepisów w zakresie ochrony danych osobowych podlegają, niezależnie od odpowiedzialności wynikającej z prawa pracy, sankcjom przewidzianym w Rozdziale 8 ustawy o ochronie danych osobowych.

§ 12

Za bezpieczeństwo danych osobowych odpowiedzialny jest każdy pracownik Urzędu Gminy.

§ 13

Systemy informatyczne, służące do przetwarzania danych osobowych, muszą spełniać wymogi obowiązujących aktów prawnych regulujących zasady gromadzenia i przetwarzania danych osobowych.

ROZDZIAŁ VI

OCHRONA PRZETWARZANIA DANYCH OSOBOWYCH - OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH

§ 14

1. Dane osobowe w Urzędzie Gminy w Sieciechowie przetwarzane są:
   - przy użyciu tradycyjnych środków pisarskich – dane osobowe gromadzone są w rejestrach, księgach zeszytach papierowych, segregatorach i przechowywane w zamykanych szafach i kasach pancernych
   - przy użyciu stacji roboczych na serwerach sieciowych pracujących wyłącznie w wewnętrznej sieci komputerowej oddzielonej fizycznie od sieci publicznej poprzez sprzętowy „firewall". Dostęp do danych następuje po autoryzacji polegającej na podaniu identyfikatora i hasła. (Środki bezpieczeństwa określa „Instrukcja zarządzania systemem informatycznym")

2. Do elementów zabezpieczenia danych osobowych w Urzędzie Gminy w Sieciechowie zalicza się:

a) stosowane metody ochrony pomieszczeń
   - ochrona budynku
   - zabezpieczenia fizyczne pomieszczeń, w których przetwarzane są dane osobowe :
     - zamykanie pomieszczeń na klucz
     - prowadzenie ewidencji wydawanych kluczy
     - przechowywanie dokumentów w szafach z zamkami
   - wprowadzenie kontroli dostępu do wszystkich stacji roboczych i pomieszczeń w których znajdują się serwery i węzły sieci oraz w których składowane są dane. Pomieszczenia objęte szczególną ochroną mogą być sprzątane w obecności pracowników wykonujących swoje obowiązki służbowe.

b) zabezpieczenia procesów przetwarzania danych osobowych
   - przetwarzanie danych następuje w wyznaczonych pomieszczeniach
   - przetwarzanie danych następuje przez wyznaczone do tego celu osoby

c) zabezpieczenia organizacyjne:

- osobą odpowiedzialną za bezpieczeństwo przetwarzania danych osobowych jest Administrator Bezpieczeństwa Informacji (ABI)
- Administrator Bezpieczeństwa Informacji i współpracujący z nim administratorzy – kierownicy Referatów i Sekretarz Gminy na bieżąco kontrolują pracę systemu informatycznego zgodnie z obowiązującymi procedurami.
- Administrator Systemu (informatyk) nadaje uprawnienia do dostępu do sytemu w formie identyfikatora i hasła poszczególnym użytkownikom w systemie informatycznym, na wniosek Naczelnika Wydziału.

d) organizacja pracy przy przetwarzaniu danych osobowych
- wykaz pracowników Urzędu Gminy w Sieciechowie uprawnionych do przetwarzania danych osobowych znajduje się u Administratora Bezpieczeństwa Informacji
- przetwarzać dane osobowe mogą jedynie pracownicy, którzy posiadają stosowne upoważnienie przyznane przez Administratora Danych (AD) a wydane przez Administratora Bezpieczeństwa Informacji (ABI)
- w trakcie przetwarzania danych osobowych, pracownik osobiście jest odpowiedzialny za bezpieczeństwo powierzonych mu danych
- przed przystąpieniem do realizacji zadań związanych z przetwarzaniem danych osobowych, pracownik powinien sprawdzić, czy posiadane przez niego dane były należycie zabezpieczone oraz czy zabezpieczenia te nie były naruszone.
- w trakcie przetwarzania danych osobowych, pracownik winien dbać o należyte ich zabezpieczenie przed możliwością wglądu, bądź zmiany przez osoby do tego celu nieupoważnione.
- po zakończeniu przetwarzania danych osobowych każdy pracownik winien należycie zabezpieczyć dane przed możliwością dostępu do nich osób nieupoważnionych.

e) W przypadku naruszenia zabezpieczenia danych osobowych obowiązuje „Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych w Urzędzie Gminy w Sieciechowie"

2. W ramach zabezpieczenia danych osobowych ochronie podlegają:
a) sprzęt komputerowy – serwery, komputery, drukarki,
b) oprogramowanie
c) dane zapisane na dyskach oraz dane podlegające przetwarzaniu w systemie
d) hasła użytkowników
e) związana z przetwarzaniem danych osobowych dokumentacja papierowa
f) kopie zapasowe i archiwa

3. Środkami zabezpieczenia danych osobowych w systemach informatycznych są:
a) hasła dostępu do systemu
b) hasła dostępu do aplikacji
c) wygaszacze ekranu chronione hasłem
zaś dla dokumentów papierowych – należy stosować zasadę „czystego biurka"

4. Dla zapewnienia niezawodności systemu informatycznego wprowadza się procedury awaryjne.

5. Osobą posiadającą najważniejsze uprawnienia w systemie informatycznym jest Administrator Systemu – informatyk, który jest uprawniony do instalowania i usuwania oprogramowania systemowego i narzędziowego oraz nadawania identyfikatorów i haseł.

ROZDZIAŁ VII
ZASADY UDOSTĘPNIANIA DANYCH OSOBOWYCH

§ 15

1. W przypadku konieczności udostępniania danych osobowych, Administrator Danych udostępnia posiadane dane osobowe, osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.
2. Dane osobowe mogą być udostępnione innym osobom niż wymienione w ust. 1, jeżeli w sposób wiarygodny uzasadnią potrzebę posiadania tych danych, a ich udostępnienie nie naruszy praw i wolności osób, których dane dotyczą.
3. Dane osobowe udostępnia się na pisemny wniosek chyba, że przepis innej ustawy stanowi inaczej.
4. Udostępnione dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem dla którego zostały udostępnione.

ROZDZIAŁ VIII

REJESTRACJA ZBIORÓW DANYCH OSOBOWYCH

§ 16

Kierownicy komórek organizacyjnych w Urzędzie Gminy, w których przetwarzane są dane osobowe są zobowiązani do zgłaszania Administratorowi Bezpieczeństwa Informacji:
- planowanego rejestrowania nowych zbiorów danych osobowych
- wnoszenia zmian zbiorów już zarejestrowanych

ROZDZIAŁ VIII

ARCHIWIZOWANIE INFROMACJI ZAWIERAJĄCYCH DANE OSOBOWE

§ 17

Zasady archiwizacji i brakownia dokumentów reguluje Rozporządzenie Ministra Kultury z dnia 16 września 2002 r. w sprawie postępowania z dokumentacją, zasad jej klasyfikowania i kwalifikowania oraz zasad i trybu przekazywania materiałów archiwalnych do archiwów państwowych (Dz. U. Nr 167, poz. 1375).

WYKAZ BUDYNKÓW, POMIESZCZEŃ lub części pomieszczeń TWORZĄCYCH OBSZAR < W KTÓRYCH SĄ PRZETWARZANE, PRZECHOWYWANE, NISZCZONE DANE OSOBOWE W UZRZĘDZIE GMINY W SIECIECHOWIE

a/ pomieszczenia znajdujące się w budynku Jednostki przy ul. Rynek 16

- (biura) pokoje nr : 1,2, 3, 4,5, 6,7, 8, 9,10,11,12

b/ budynek przy ul. 11 Listopada 2 Gminna Biblioteka Publiczna 1, 2

- (biura) pokoje nr : GOPS 3,4 GK 6 , Księgowość Oświatowa 10

Załącznik Nr 2

Do polityki bezpieczeństwa

danych osobowych w Urzędzie Gminy w Sieciechowie

WYKAZ ZBIORÓW DANYCH OSOBOWYCH WRAZ ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO ICH PRZETWARZANIA

W URZĘDZIE GMINY W SIECIECHOWIE

Lp.	Zbiór danych	Programy zastosowane do przetwarzania/forma rejestru	Lokalizacja zbioru	Miejsce przetwarzania danych

Załącznik Nr 3

do polityki bezpieczeństwa

danych osobowych w Urzędzie Gminy w Sieciechowie

OPIS STRUKTURY ZBIORÓW DANYCH WSKAZUJĄCY ZAWARTOŚĆ POSZCZEGÓLNYCH PÓL INFORMACYJNYCH I POWIĄZANIA MIĘDZY NIMI

Lp.	Nazwa zbioru danych osobowych	Nazwa podzbioru danych osobowych	Pola informacyjne
			•

Załącznik Nr 4 do polityki bezpieczeństwa
danych osobowych w Urzędzie Gminy w Sieciechowie

SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY POSZCZEGÓLNYMI SYSTEMAMI

System/Moduł "A"	System/Moduł „B"	Kierunek przepływu danych osobowych	Sposób przesyłania danych osobowych

Załącznik Nr 2
do Zarządzenia Nr 50
Wójta Gminy Sieciechów
z dnia 1 października 2015r

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy w Sieciechowie

ROZDZIAŁ I
Postanowienia ogólne

§ 1

Niniejsza instrukcja określa zasady zarządzania każdym systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy w Sieciechowie oraz przetwarzaniu danych osobowych zawartych w innych zbiorach.

§ 2

Ilekroć w instrukcji jest mowa o:

- **zbiorze danych** – rozumie się każdy posiadający strukturę zestaw danych o charakterze osobowym
- **przetwarzaniu danych** – rozumie się przez to operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, usuwanie, itp.
- **danych osobowych** – rozumie się przez to, każdą informację dotyczącą osoby fizycznej, pozwalającą na określenie tożsamości tej osoby
- **użytkowniku** – rozumie się przez to osobę upoważnioną do dostępu i przetwarzania danych osobowych
- **Administratorze Danych** - rozumie się przez to Wójta Gminy Sieciechów, a także inne osoby wskazane przez Wójta do administrowania określonymi zbiorami danych osobowych
- **Administratorze Bezpieczeństwa Informacji** – rozumie się osobę odpowiedzialną za bezpieczeństwo przetwarzania danych osobowych w systemie informatycznym, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń
- **Administratorze Sieci** – rozumie się przez to osobę upoważnioną do administrowania siecią informatyczną (Informatyk)
- **Administratorze Systemu** – należy przez to rozumieć pracownika administrującego serwerami i systemami w których przetwarzane są dane osobowe
- **systemie informatycznym** – należy przez to rozumieć, system przetwarzania danych w Urzędzie Gminy w Sieciechowie wraz ze związanymi z nimi ludźmi oraz zasobami technicznymi i finansowymi, który dostarcza i rozprowadza informacje
- **zabezpieczeniu systemu informatycznego** – należy przez to rozumieć wdrożenie stosownych środków administracyjnych, technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą

- **sieci lokalnej** – należy przez to rozumieć zespół co najmniej dwóch komputerów, bez dostępu do sieci publicznej, wspólnie administrowanych
- **sieci publicznej** – należy rozumieć sieć służącą do powszechnej wymiany informacji z użytkownikami publicznymi

ROZDZIAŁ II

Organizacja przetwarzania danych osobowych

§ 3

1. Do pracy przy przetwarzaniu danych osobowych mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie zatwierdzone przez Administratora Danych i wydane przez Administratora Bezpieczeństwa Informacji na podstawie aktualnego zakresu obowiązków, znajdującego się w aktach osobowych pracownika.

§ 4

1. Administrator Bezpieczeństwa Informacji (ABI) działa w zakresie Polityki Bezpieczeństwa Informacji w Urzędzie Gminy w Sieciechowie oraz :
   - odpowiada za bezpieczeństwo danych osobowych w systemach informatycznych oraz w kartotekach, skorowidzach, księgach i innych zbiorach ewidencyjnych w zakresie zgodności zasad postępowania przy przetwarzaniu danych osobowych
   - czuwa nad wdrażaniem niniejszej instrukcji w systemach informatycznych Urzędu Gminy, w których przetwarzane są dane osobowe oraz dba o bieżące jej uaktualnianie stosownie do zmieniających się technologii informatycznych oraz zagrożeń bezpieczeństwa systemów informatycznych
   - sprawuje nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których dane są przetwarzane oraz kontrolą przebywających w nim osób
   - określa strategię zabezpieczania systemów informatycznych Urzędu Gminy
   - sprawuje nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych osobowych
   - sprawuje nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych na których zapisane są dane osobowe
   - identyfikuje i analizuje zagrożenia oraz ryzyka, na które narażone może być przetwarzanie danych osobowych w systemach informatycznych Urzędu Gminy
   - określa potrzeby w zakresie zabezpieczenia systemów informatycznych, w których przetwarzane są dane osobowe
   - sprawuje nadzór nad bezpieczeństwem danych zawartych w komputerach przenośnych, dyskach wymiennych, palmtopach, w których przetwarzane są dane osobowe
   - sprawuje nadzór nad obiegiem oraz przechowywaniem dokumentów zawierających dane osobowe
   - sprawdza działanie zabezpieczeń wdrożonych w celu ochrony danych osobowych w systemach informatycznych
   - rejestruje wniosek Kierownika Referatu o przyznaniu uprawnień użytkownikowi do przetwarzania danych osobowych (wg wzoru)
   - prowadzi ewidencję baz danych w systemach informatycznych, w których przetwarzane są dane osobowe

- prowadzi ewidencję osób zatrudnionych przy przetwarzaniu danych osobowych w systemach informatycznych
- prowadzi ewidencję miejsc przetwarzania danych osobowych w systemach informatycznych
- prowadzi rejestr zbiorów danych Urzędu (przetwarzanych metodą tradycyjną i w systemach informatycznych)
- prowadzi dokumentację wykonywanych czynności.

§ 5

Lokalni Administratorzy Danych – Kierownicy poszczególnych Referatów stwarzają właściwe warunki organizacyjno-techniczne gwarantujące bezpieczeństwo systemów informatycznych w podległych im komórkach organizacyjnych, w szczególności poprzez:

1. Wykonywanie zaleceń Administratora Bezpieczeństwa Informacji Urzędu Gminy w Sieciechowie w zakresie ochrony danych osobowych
2. Określanie indywidualnych obowiązków i odpowiedzialności osób zatrudnionych przy przetwarzaniu danych osobowych, wynikających z ustawy o ochronie danych osobowych
3. Zabezpieczanie pomieszczeń, w których przetwarzane są dane osobowe w systemach informatycznych przed dostępem osób niepowołanych
4. Przekazywanie na bieżąco Administratorowi Bezpieczeństwa Informacji zaktualizowanych informacji dotyczących;
   a) gromadzonych w systemach informatycznych danych osobowych
   b) listy osób pracujących przy przetwarzaniu danych osobowych
   c) lokalizacji pomieszczeń, w których przetwarzane są dane osobowe
   d) rodzaju systemów informatycznych funkcjonujących w zakresie ich działania
   e) listy identyfikatorów osób biorących udział przy przetwarzaniu danych osobowych w podległych im systemach informatycznych
   f) czynności serwisowych wykonywanych w podległych systemach informatycznych
   g) zdarzeń wpływających na bezpieczeństwo systemów informatycznych, w tym: wykrytych wirusów, koni trojańskich, nielegalnego oprogramowania, awarii systemu informatycznego, stwierdzenia faktu korzystania z systemu informatycznego przez osobę nieuprawnioną
5. Stwarzanie warunków organizacyjno – technicznych umożliwiających spełnienie wymogów wynikających z obowiązywania ustawy o ochronie danych osobowych.
6. Określanie zasad i ewidencji wykonywania czynności serwisowych w systemach informatycznych w podległych Wydziałach
7. Przygotowywanie zgłoszeń rejestracji zbioru danych do Generalnego Inspektoratu Danych Osobowych i przekazywanie tych informacji Administratorowi Bezpieczeństwa Informacji.

§ 6

Administrator Sieci komputerowej opracowuje i na bieżąco uaktualnia szczegółowe instrukcje zarządzania systemami informatycznymi w podległych systemach informatycznych, które powinny zawierać w szczególności:

1. Sposób przydziału haseł dla użytkowników poszczególnych systemów informatycznych i częstotliwość ich zmiany oraz wskazanie osoby odpowiedzialnej za te czynności
2. Określenie sposobu rejestrowania i wyrejestrowania użytkowników systemu

3. Procedury rozpoczęcia i zakończenia pracy
4. Metody i częstotliwość wykonywania kopii awaryjnych
5. Metody i częstotliwość sprawdzania systemów informatycznych na obecność wirusów komputerowych oraz metodę ich usuwania
6. Sposób i czas przechowywania nośników informatycznych, w tym kopii informatycznych i wydruków
7. Sposób postępowania w zakresie komunikacji w sieci komputerowej
8. Wnioskowanie do Administratora Bezpieczeństwa Informacji w sprawie procedur bezpieczeństwa i standardów zabezpieczeń
9. Prowadzenie profilaktyki antywirusowej i zabezpieczeń typu „firewall"

ROZDZIAŁ III

Ogólne zasady eksploatacji systemów informatycznych

§ 7

1. System informatyczny w Urzędu Gminy w Sieciechowie może być używany tylko na potrzeby wykonywania zadań z zakresu administracji publicznej.
2. System informatyczny stanowią środki przetwarzania informacji wraz ze związanymi z nim ludźmi oraz zasobami technicznymi i finansowymi, czyli urządzeniami komputerowymi i innymi służącymi do przetwarzania danych osobowych i informacji z nimi związanymi.
3. Przetwarzanie danych osobowych obejmuje operacje polegające na ich zbieraniu, utrwalaniu, zmianie, przechowywaniu, opracowywaniu, udostępnianiu i usuwaniu.
4. Wszystkie stacje robocze pracujące w systemie informatycznym w Starostwie muszą być zgodne ze sprzętową oraz programową konfiguracją zarejestrowaną przez Administratora Bezpieczeństwa Informacji.
5. Stacje robocze działające w systemie informatycznym w Starostwie muszą mieć możliwość blokowania dostępu do systemu oraz możliwość zastosowania zabezpieczonego hasłem wygaszacza ekranu automatycznie uruchamianego po określonym czasie braku aktywności użytkownika.
6. W pomieszczeniach, gdzie przebywają osoby postronne, monitory stanowisk dostępu do danych z systemu informatycznego w Starostwie powinny być ustawione w sposób uniemożliwiający tym osobom wgląd w dane.

§ 8

Miejscem przetwarzania danych osobowych są pomieszczenia pracy komórek organizacyjnych - Referatów Urzędu Gminy w Sieciechowie znajdujące się w budynkach przy ulicy Rynek 16 i 11 Listopada 2

§ 9

Infrastruktura sieciowa składa się z okablowania strukturalnego w budynkach Urzędu Gminy z siecią internetową oraz instalacją zasilającą urządzenia komputerowe.

§ 10

W systemie informatycznym w Urzędzie Gminy wykorzystywany jest sprzęt komputerowy określony w szczegółowej specyfikacji technicznej prowadzonej przez Administratora Systemu czyli informatyka.

§ 11

Środkami przetwarzania danych osobowych są oprócz komputerów również drukarki, skanery, modemy, niszczarki dokumentów, dokumenty papierowe, skorowidze, kartoteki, rejestry, itp.

§ 12

W skład systemu informatycznego wchodzą aplikacje użytkowe ujęte w szczegółowej specyfikacji technicznej prowadzonej przez Administratora Systemu oraz kartoteki, decyzje, rejestry prowadzone ręcznie lub komputerowo przy użyciu aplikacji biurowych w poszczególnych Referatach Gminy.

ROZDZIAŁ IV

Przyznanie praw dostępu

§13

1. Prawo dostępu do poszczególnych systemów informatycznych mogą mieć wyłącznie osoby, które posiadają pisemne upoważnienie zatwierdzone przez Administratora Danych Osobowych – Wójta Gminy Sieciechów i wydane przez Administratora Bezpieczeństwa Informacji.
2. Żądanie przyznania jak i zmiany praw dostępu do systemu informatycznego musi być udokumentowane pisemnie w formie wniosku sporządzonego przez Kierownika Referatu lub Sekretarza skierowanego poprzez Administratora Bezpieczeństwa Informacji do Administratora Danych Osobowych.
3. Komórka Kadrowa winna informować ABI o zmianach stanowisk pracy przez osoby dopuszczone do przetwarzania danych osobowych.
4. Prawo dostępu przyznane użytkownikom, którzy nie są pracownikami mają charakter czasowy i mogą być przyznane na okres odpowiadający wykonywanemu zadaniu.
5. Specjalne prawa dostępu muszą być ściśle ograniczone do osób, które bezpośrednio odpowiadają za administrację poszczególnych systemów informatycznych i ich bezpieczeństwo.
6. Dostęp do systemu informatycznego w Urzędzie Gminy powinien być zabezpieczony przez system identyfikatora i hasło użytkownika.
7. Identyfikator przydzielany jest użytkownikowi przez Administratora Systemu na podstawie pisemnego wniosku właściwego Kierownika Referatu w celu uaktualnienia ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych zgodnie z art. 37 i 39 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.
8. Administrator Systemu informatycznego (odcinka systemu, aplikacji) przechowuje dokument (wniosek) stanowiący podstawę przydziału (zablokowania) identyfikatora i dokonuje odpowiedniego wpisu do prowadzonego rejestru użytkowników systemu informatycznego.
9. W przypadku zakończenia pracy w Urzędzie Gminy stosuje się procedurę wyrejestrowania użytkownika z systemu. Wykonanie tej operacji jest jednoznaczne z uniemożliwieniem dostępu do systemu dla pracownika, z którym rozwiązano umowę o pracę.

§ 14

1. Identyfikator dla użytkownika przydzielany zostaje przez Administratora Systemu na podstawie pisemnego wniosku Kierownika Referatu lub Sekretarza.
2. Identyfikator składa się minimum z sześciu znaków.

§ 15

Pierwsze hasło dla użytkownika zakładane jest przez Administratora Systemu podczas wprowadzenia jego identyfikatora do systemu. Następnie użytkownik powinien zmienić hasło wg określonych zasad:

- hasło jest obowiązkowe dla każdego użytkownika posiadającego identyfikator w systemie i jest zakładane jednocześnie z utworzeniem identyfikatora dla użytkownika
- po założeniu hasła przez Administratora Systemu, użytkownik ma obowiązek zarejestrować się do systemu i zmienić hasło.
- hasło powinno składać się z unikalnego zestawu co najmniej ośmiu znaków i powinno zawierać małe i wielkie litery oraz cyfry lub znaki specjalne
- przy wpisywaniu hasła nie jest ono wyświetlane na ekranie
- w przypadku ujawnienia hasła musi ono zostać niezwłocznie zmienione
- hasło musi być zmieniane przynajmniej raz w miesiącu (nie rzadziej niż co 30 dni)
- hasła użytkowników muszą być zapisywane w systemie w postaci zaszyfrowanej

§ 16

1. Hasła użytkowników należą do nich samych.
2. W przypadku potrzeby zabezpieczenia dostępu do systemu Kierownik Referatu decyduje o deponowaniu hasła.

§ 17

Kartoteki, decyzje, rejestry, itp. tworzone za pomocą aplikacji biurowych (pakiet MS Office) są chronione przy użyciu haseł systemowych i haseł zakładanych przez użytkownika dla poszczególnych dokumentów wg instrukcji dostępnej w pakiecie MS Office.

§ 18

Rejestrowanie użytkownika odbywa się obowiązkowo, gdy rozpoczyna on pracę w systemie. Polega to na wprowadzeniu identyfikatora i hasła objętego tajemnicą i znanego tylko użytkownikowi, na podstawie których system stwierdza tożsamość użytkownika. Po poprawnym zarejestrowaniu użytkownik może wykonywać wszystkie czynności, na jakie pozwalają przydzielone mu prawa dostępu.

§ 19

Rozpoczęcie pracy w systemie informatycznym odbywa się poprzez:

- Przygotowanie stanowiska pracy
- Włączenie stacji roboczej – komputera
- Wprowadzenie swojego identyfikatora i hasła

Po zakończeniu pracy w systemie należy:

- Zamknąć aplikację
- Odłączyć się od zasobów systemowych
- Zakończyć pracę systemu operacyjnego
- Wyłączyć komputer

Zawieszenie pracy w systemie odbywa się poprzez jeden z wymienionych sposobów:

- Włączenie wygaszacza ekranu
- Wylogowanie się z systemu
- Wylogowanie się z otwartych aplikacji i systemu

Przy dłuższej przerwie należy wyłączyć stację roboczą.
Wychodząc z pomieszczenia, w którym przetwarzane są dane z systemu informatycznego należy sprawdzić czy zamknięte są okna i wejście do pomieszczenia.

§ 20

1. Przy korzystaniu z Internetu w Urzędzie Gminy należy stosować następujące zasady:
   - Z wnioskiem uzasadniającym potrzebę wyposażenia stanowiska pracy w Internet występuje Kierownik Referatu.
   - Połączenia sieci wewnętrznej z siecią zewnętrzną – Internetem mogą być wykonywane tylko za pośrednictwem systemów „firewall" o odpowiednich parametrach zainstalowanych w Urzędzie Gminy.

2. Użytkownicy zobowiązani są do zachowania szczególnej ostrożności przy pracy z pocztą elektroniczną. W przypadku jakichkolwiek wątpliwości, szczególnie przy załącznikach, należy przed uruchomieniem skontaktować się z Administratorem Systemu.

ROZDZIAŁ V
Kopie awaryjne

§ 21

1. Awaryjne kopie baz danych należy tworzyć systematycznie w celu zabezpieczenia zbiorów danych osobowych przed niezamierzoną ich utratą oraz możliwością odtworzenia.
2. Kopie awaryjne powinny być sporządzane po każdej modyfikacji.
3. Kopie awaryjne mogą być użyte dla odbudowy systemu uszkodzonego w skutek awarii twardego dysku lub innych problemów.
4. Przechowywane awaryjne kopie baz danych muszą być ewidencjonowane i aktualizowane przez Administratora Systemu lub użytkowników.

ROZDZIAŁ VI
Wydruki

§ 22

1. W przypadku wykonywania wydruków ze zbioru danych osobowych wykonawca jest zobowiązany do zachowania wszelkich niezbędnych działań w celu niedopuszczenia do ich ujawnienia lub utraty a w szczególności do nie pozostawiania ich nie zamkniętych bez dozoru.
2. Wydruki zawierające dane z systemu informatycznego po zakończeniu pracy powinny być przechowywane w zamkniętych szafach.
3. Wydruki i kserokopie dokumentów nie wykorzystane, wadliwe a zwierające dane z systemu informatycznego muszą być bezwzględnie niszczone w sposób uniemożliwiający ich odtworzenie.
4. Drukarki nie mogą być pozostawione bez kontroli jeśli są lub wkrótce będą drukowane na nich dane osobowe.

ROZDZIAŁ VII
Zabezpieczenie oprogramowania

§ 23

1. Na wszystkich komputerach Urzędu Gminy dopuszcza się instalację tylko legalnego, licencjonowanego oprogramowania. Dopuszczone do zainstalowania programy użytkowe do przetwarzania danych osobowych obejmuje prowadzony rejestr. Zabrania się instalowania oprogramowania bez zgody ABI.
2. Dopuszcza się instalację nowego oprogramowania do przetwarzania danych osobowych lub aktualizacji istniejących pod warunkiem spełnienia określonych wymagań. Instalacji lub aktualizacji dokonuje Administrator Systemu lub osoba przez niego upoważniona.
3. Za samodzielne zainstalowanie oprogramowania odpowiada użytkownik.

ROZDZIAŁ VIII

Ochrona i znaczenie sprzętu informatycznego

§ 24

1. Sprzęt komputerowy używany w systemie informatycznym w Urzędzie Gminy powinien być fizycznie chroniony przed kradzieżą, zniszczeniem lub niewłaściwym używaniem. Bezpośrednio odpowiedzialny jest za to użytkownik tego sprzętu.
2. Użytkownicy sami nie mogą demontować komputerów oraz dokonywać zmiany komponentów sprzętu komputerowego. Te prace wykonują uprawnione osoby.
3. Sprzęt komputerowy używany w systemie informatycznym w Starostwie nie może być przenoszony bez zgody Kierownika Referatu lub Sekretarza i ABI.
4. Każde urządzenie używane w systemie informatycznym w Urzędzie Gminy musi być oznaczone w celu jego identyfikacji.
5. Za bezpieczeństwo komputera przenośnego odpowiedzialny jest jego użytkownik.
6. Działania pracowników serwisu muszą się odbyć w obecności Administratora Systemu lub osoby przez niego upoważnionej.

ROZDZIAŁ IX

Nośniki informacji

§ 25

1. Za pobrany komputerowy nośnik informacji oraz bezpieczeństwo zapisanych na nim danych odpowiada użytkownik, który pobrał dany nośnik i posiada go na swoim stanie.
2. Autoryzowane nośniki informacji po zakończeniu pracy przechowywane powinny być w sposób zapewniający bezpieczeństwo zapisanych na nim danych.
3. Uszkodzone nośniki informacji - dyskietki, płyty CD lub inne zawierające dane osobowe nie mogą być użytkowane. Muszą być odpowiednio zabezpieczone przed nieuprawnionym udostępnieniem a następnie zniszczone lub naprawione pod nadzorem Administratora Bezpieczeństwa Informacji.
4. Użytkownik komputera w Urzędzie Gminy zobowiązany jest do używania w pracy dyskietek i CD zakupionych przez Starostwo i przechowywania na nich tylko danych związanych z charakterem pracy.
5. Dopuszcza się do stosowania lub stosowanie pamięci masowych, streamerów oraz innych urządzeń i nośników umożliwiających wykonywanie kopii zapasowych w systemach informatycznych zakupionych przez Urząd Gminy.

ROZDZIAŁ X

Systemy awaryjne

§ 26

1. Dla wszystkich elementów systemu informatycznego powinna być zainstalowana odpowiednia ochrona przeciwpożarowa.
2. Każdy komputer powinien być podłączony do wydzielonych gniazd z zasilaniem prądowym.
3. Serwery i stacje robocze powinny być chronione zasilaniem awaryjnym (UPS).

ROZDZIAŁ XI

Ochrona danych osobowych w poszczególnych referatach i komórkach organizacyjnych

§ 27

1. W zakresie dotyczącym poszczególnych referatów i komórek organizacyjnych uszczegółowienie zasad ochrony danych osobowych mogą stanowić referatowe instrukcje ochrony danych osobowych.
2. Instrukcje referatów nie mogą być sprzeczne z postanowieniami niniejszej Instrukcji i wymagają akceptacji Administratora Bezpieczeństwa Informacji.

ROZDZIAŁ XII

Postanowienia końcowe

§ 28

1. Każda informacja o naruszeniu systemu bezpieczeństwa wymaga zgłoszenia i wszczęcia postępowania wyjaśniającego przez Administratora Bezpieczeństwa Informacji.
2. Postępowanie w sytuacji naruszenia ochrony danych osobowych określa odrębna Instrukcja, stanowiąca Załącznik Nr 3do Zarządzenia Nr 50 z dnia 1 października 2015r Wójta Gminy Sieciechów
3. Postanowienia instrukcji dotyczą w odpowiednim zakresie również postępowania przy przetwarzaniu danych osobowych zgromadzonych w zbiorach prowadzonych w innej formie.
4. Wszyscy pracownicy zobowiązani są do ochrony tajemnic prawnie chronionych, co potwierdzają własnoręcznym podpisem złożonym w chwili przyjęcia do pracy.
5. Wszyscy pracownicy są zobowiązani do przestrzegania zasad ochrony fizycznej dokumentów i materiałów zawierających dane osobowe.
6. Nieprzestrzeganie postanowień tej Instrukcji oraz brak nadzoru nad bezpieczeństwem informacji stanowi naruszenie obowiązków pracowniczych i może być przyczyną odpowiedzialności dyscyplinarnej określonej przepisami Kodeksu Pracy.
7. Ujawnienie informacji osobie nieupoważnionej, pociąga za sobą odpowiedzialność karną określoną przepisami Kodeksu karnego.
8. Jeżeli skutkiem działania użytkownika jest szkoda, sprawca ponosi odpowiedzialność materialną na warunkach określonych w przepisach Kodeksu Pracy oraz Kodeksu Cywilnego.

Załącznik Nr 3
do Zarządzenia Nr 50
Wójta Gminy Sieciechów
z dnia 1 października 2015r

Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych w Urzędzie Gminy w Sieciechowie

§ 1

Instrukcja niniejsza ma zastosowanie w sytuacjach:

1. stwierdzonego naruszenia zabezpieczenia danych osobowych w systemie informatycznym lub innym zbiorze danych.
2. podejrzenia naruszenia zabezpieczenia danych osobowych w systemie informatycznym lub innym zbiorze danych.

§ 2

Naruszenie zabezpieczenia danych osobowych w systemie informatycznym lub innym zbiorze danych stwierdza się, gdy wystąpiły między innymi:

1. nieuprawniony dostęp do danych osobowych
2. udostępnienie danych osobowych osobom nieupoważnionym
3. zmiany, kopiowanie lub uszkodzenie danych osobowych dokonane przez osoby nieuprawnione
4. kradzież nośników informacji zawierających dane osobowe (np. dysków, dyskietek, płyt CD, płyt DVD, wydruków komputerowych)

§ 3

Za okoliczności, które wskazują na naruszenie zabezpieczenia danych osobowych w systemie informatycznym lub innym zbiorze danych, uważa się między innymi:

1. nieuzasadnione korzystanie z zasobów systemu informatycznego lub innego zbioru danych
2. nieuzasadnione ujawnienie danych osobowych
3. ujawnienie wirusów komputerowych lub innych programów, które mogą mieć negatywny wpływ na funkcjonowanie systemu informatycznego
4. wydarzenia obniżające stan bezpieczeństwa systemu informatycznego lub innego zbioru danych (np. awaria zasilania)

§ 4

Osoba upoważniona do przetwarzania danych osobowych w systemie informatycznym lub innym zbiorze danych, która stwierdzi lub podejrzewa naruszenie zabezpieczenia danych zobowiązana jest do:

1. niezwłocznego poinformowania o tym fakcie Administratora Bezpieczeństwa Informacji określonego dalej skrótem ABI i swojego bezpośredniego przełożonego
2. w przypadku nieobecności ABI, niezwłocznego poinformowania o tym fakcie Administratora Systemu i swojego bezpośredniego przełożonego
3. zaprzestania pracy w systemie informatycznym lub innym zbiorze danych do momentu otrzymania od ABI decyzji o możliwości wznowienia pracy.

§ 5

1. ABI po uzyskaniu informacji, o której mowa w §4 zawiadamia o naruszeniu zabezpieczenia danych osobowych Administratora Danych (AD) Urzędzie Gminy w Sieciechowie oraz podejmuje działania w celu rozpoznania naruszenia zabezpieczenia danych, a w szczególności ustala, czy miało miejsce naruszenie ochrony danych osobowych, a w sytuacji nie potwierdzenia podejrzeń dokonuje analizy systemu zabezpieczeń i przeprowadza szkolenie użytkownika.
2. ABI w przypadku stwierdzenia naruszenia zabezpieczenia danych osobowych w systemie informatycznym lub innym zbiorze danych:
   - podejmuje działania służące ograniczeniu szkód wywołanych naruszeniem ochrony danych osobowych
   - zabezpiecza dane wskazujące na naruszenie zabezpieczenia danych osobowych
   - ustala okoliczności naruszenia ochrony danych osobowych
   - analizuje rodzaj, zakres i źródło naruszenia ochrony danych osobowych
   - podejmuje działania naprawcze
   - bada przyczyny naruszenia ochrony danych osobowych i podejmuje działania mające na celu wyeliminowanie podobnych zdarzeń zagrażających bezpieczeństwu danych.

§6

W przypadku nieobecności ABI wszelkie czynności określone w §4 i §5 podejmuje w jego zastępstwie Administrator Systemu.

§7

Administrator Bezpieczeństwa Informacji po czynnościach, o których mowa w §5, sporządza i przedstawia Administratorowi Danych raport o stwierdzeniu naruszenia zabezpieczenia danych osobowych w systemie informatycznym lub innym zbiorze danych w ciągu 14 dni od daty jego zaistnienia. Raport powinien zawierać następujące dane i informacje:

1. imię i nazwisko, stanowisko i miejsce zatrudnienia osoby, która zgłosiła naruszenie zabezpieczenia danych osobowych w systemie informatycznym lub innym zbiorze danych
2. datę i godzinę powiadomienia o naruszeniu zabezpieczenia danych osobowych
3. opis podjętych działań mających na celu ustalenie zakresu naruszenia zabezpieczenia danych osobowych
4. opis podjętych działań naprawczych

§8

Administrator Bezpieczeństwa Informacji jest odpowiedzialny za przechowywanie materiałów, o których mowa w §5 dokumentujących zaistniałe naruszenie oraz podejrzenie naruszenia zabezpieczenia danych w systemie informatycznym lub innym zbiorze danych.

Załącznik Nr 4
do Zarządzenia Nr 50 Wójta
Gminy Sieciechów z dnia
1października2015r

.....
(miejscowość, dat

.....
(pieczęć jednostki organizacyjnej)

Nr rej. .....

Upoważnienie do przetwarzania danych osobowych

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

.....
(imię i nazwisko)

Zatrudnionego/nej na stanowisku.....

w .....
(oznaczenie jednostki i komórki organizacyjnej)

do przetwarzania, w ramach wykonywanych obowiązków służbowych, niżej wymienionych zbiorów danych osobowych w okresie: od..... do.....; bezterminowo:

l.p.	Nazwa zbioru	Postać zbioru	Nazwa programu	Identyfikator

Wymieniona osoba zostaje wpisana do ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych w Urzędzie Gminy w Sieciechowie

Rozwiązanie stosunku pracy jest równoznaczne z cofnięciem upoważnienia do przetwarzania danych osobowych.

.....
(pieczęć i podpis administratora danych)

Wykonano w 3 egzemplarzach:
Egz. Nr 1 – pracownik
Egz. Nr 2 – akta personalne pracownika
Egz. Nr 3 – Administrator Bezpieczeństwa Informacji

Otrzymałam/em dnia .....
Podpis pracownika .....

Załącznik Nr 5
Do Zarządzenia Nr 50
Wójta Gminy Sieciechów
Z dnia 1 października 2015r

.....

.....
(pieczęć jednostki organizacyjnej)

ADMINISTRATOR DANYCH OSOBOWYCH

w miejscu

Na podstawie art. 37 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz.U. 2002 r. Nr 101 poz. 926, ze zm.)

proszę o upoważnienie Pani / Pana:

.....
(imię i nazwisko)

.....
(stanowisko)

do przetwarzania, w ramach wykonywanych obowiązków służbowych, niżej wymienionych zbiorów osobowych w okresie: od..... do.....; bezterminowo

L.p.	Nazwa zbioru	Postać zbioru	Nazwa programu

.....
(podpis kierownika Referatu lub Sekretarza)

.....
(Administrator Danych Osobowych)

Wzór wniosku o udostępnienie danych ze zbioru danych osobowych

WNIOSEK O UDOSTĘPNIENIE DANYCH ZE ZBIORU DANYCH OSOBOWYCH

1. Wniosek

do.....

.....

.....

(dokładne oznaczenie administratora danych)

2.Wnioskodawca.....

.....

.....

.....

(nazwa firmy i jej siedziba albo nazwisko, imię i adres zamieszkania wnioskodawcy nr ewidencyjny NIP oraz nr REGON)

3. Podstawa prawna upoważniająca do pozyskania danych albo wskazanie wiarygodnie uzasadnionej potrzeby posiadania danych w przypadku osób innych niż wymienione w art. ust. 1 o ochronie danych osobowych:

.....

.....

.....

.....

4. Wskazanie przeznaczenia dla udostępnienia danych:

.....

.....

5. Oznaczenie lub nazwa zbioru, z którego mają być udostępnione dane:

.....

.....

6. Zakres żądanych informacji ze

zbioru:.....

.....

.....

.....

.....

7. Informacje umożliwiające wyszukanie w zbiorze

danych:.....

.....

.....

.....

.....

(data, podpis i ew. pieczęć wnioskodawcy)

Załącznik Nr 6
do Zarządzenia Nr 50
z dnia 1 października 2015r
Wójta Gminy Sieciechów