Załącznik nr 1
do Zarządzenia nr 13/17
Wójta Gminy Duszniki
z dnia 2 marca 2017 r.

Polityka bezpieczeństwa Urzędu Gminy Duszniki

§ 1

Postanowienia ogólne

1. W celu zabezpieczenia danych osobowych gromadzonych i przetwarzanych w Urzędzie Gminy Duszniki wprowadza się „Politykę bezpieczeństwa Urzędu Gminy Duszniki" rozumianą jako zestaw praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji informacji wrażliwej jakimi są dane osobowe.
2. „Polityka bezpieczeństwa" obowiązuje wszystkich pracowników Urzędu Gminy Duszniki.
3. Wykonywanie postanowień tego dokumentu ma zapewnić właściwą reakcję, ocenę oraz udokumentowanie przypadków naruszenia bezpieczeństwa systemów oraz zapewnić właściwy tryb działania w celu przywrócenia bezpieczeństwa danych przetwarzanych w systemie informatycznym Urzędu.
4. Administratorem danych osobowych jest Wójt Gminy Duszniki.
5. Administrator danych osobowych jest obowiązany do zastosowania środków technicznych oraz organizacyjnych zapewniających ochronę przetwarzanych danych w Urzędzie Gminy Duszniki.
6. Administrator danych deklaruje dołożyć wszelkich starań, aby przetwarzanie odbywało się zgodnie z przepisami prawa.

§ 2

Podstawa prawna

1. Ustawa z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz.U. z 2016 r., poz. 922).
2. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024) - § 3 i § 4.

§ 3

Definicje

Ilekroć mowa w niniejszym dokumencie o:

1. Polityce, należy przez to rozumieć „Politykę bezpieczeństwa Urzędu Gminy Duszniki".
2. Urzędzie należy przez to rozumieć Urząd Gminy Duszniki.
3. Administratorze Bezpieczeństwa Informacji (ABI) - należy przez to rozumieć pracownika wyznaczonego przez Administratora danych - Wójta Gminy Duszniki do nadzorowania przestrzegania zasad ochrony danych osobowych oraz zgłoszonego Generalnemu Inspektorowi Ochrony Danych Osobowych.
4. Lokalnych Administratorach Bezpieczeństwa Informacji (LABI) - należy przez to rozumieć kierowników poszczególnych referatów w Urzędzie Gminy Duszniki.
5. Administratorze Systemu Informatycznego (ASI) - osoba wyznaczona przez administratora, odpowiedzialna za sprawność i konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych i techniczne bezpieczeństwo przetwarzania danych w sieci informatycznej. Dopuszcza się zlecanie zadań ASI osobom lub firmom zewnętrznym na podstawie umowy.
6. Użytkowniku systemu - należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie.

§ 4

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania danych oraz pomieszczenia, w których są przetwarzane.

1. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania danych oraz pomieszczenia, w których są przetwarzane– stanowi załącznik nr 6.

§ 5

Sposób przepływu danych

1. Stacje robocze w Urzędzie połączone są w sieć logiczną LAN.
2. Dostęp do poszczególnych zbiorów danych jest możliwy tylko przez użytkowników pracujących na stanowiskach komputerowych znajdujących się w pokojach wskazanych w załączniku nr 6.
3. W pokoju nr 6 znajduje się wydzielone pomieszczenie serwerowni, w którym znajdują się:
    - serwer Internetu,
    - serwer plików dla systemów baz danych SIGID,
    - Serwer dla pozostałych systemów baz danych, w tym zarządzania systemem ochrony F-Secure,
    - szafka krosowa - główny węzeł sieci (pozostałe dwa w pok. 4 i pok. nr 10),
    - stanowisko zarządzające – PC dla bezpiecznego i bezkonfliktowego prowadzenia czynności administracyjnych (zarządzania siecią),
4. Możliwe przepływy danych między oprogramowaniem przetwarzającym bazy danych zawierające dane osobowe:
    - System Ewidencji Ludności – Clanet > SIGID,
    - SIGID > Płatnik .

§ 6

Opis struktury zbiorów danych

1. Opis struktury zbiorów danych - stanowi załącznik nr 7.

§ 7

Potencjalne zagrożenia

1. Zbiory danych osobowych znajdujące się w Urzędzie Gminy Duszniki, a także sprzęt niezbędny do ich przechowywania i przetwarzania, są narażone na różne zagrożenia. W szczególności identyfikuje się następujące kategorie zagrożeń, którym mogą podlegać zasoby urzędu:
    a) naruszenie poufności danych zarówno przez pracowników, jak i osoby niezatrudnione w urzędzie, w tym również przez kradzież zasobu,
    b) niedostępność zbioru, znaczna degradacja jego istotnych parametrów funkcjonalnych lub utrata danych (zniszczenie zbioru) na skutek wystąpienia sił wyższych albo nieumyślnego, umyślnego lub przypadkowego działania,
    c) naruszenie integralności danych na skutek nieumyślnego, umyślnego lub przypadkowego działania,
    d) stosowanie niespójnych zasad (standardów, procedur) i środków ochrony systemów.

2. Zadaniem regulacji zawartych w polityce jest zmniejszenie ryzyka płynącego z zagrożeń do akceptowalnego poziomu, to znaczy zminimalizowanie możliwości naruszenia bezpieczeństwa zasobów informacyjnych, umożliwienie wczesnego wykrycia takiego naruszenia, zminimalizowanie strat związanych z takim naruszeniem oraz sprawne usunięcie jego skutków.

§ 8

Zabezpieczenia

1. Zabezpieczenia budynku i poszczególnych pomieszczeń.
   a) Wejścia do budynku Urzędu są zabezpieczone zamkami drzwiowymi.
   b) W holu urzędu oraz w pok. nr 6, w którym znajduje się serwerownia, zastosowano urządzenia, które po wykryciu ruchu uruchamiają alarm.
   c) Poszczególne pokoje, w których odbywa się przetwarzanie danych i ich składowanie są wyposażone w niezależne zamki i muszą być zamykane podczas nieobecności pracownika.
   d) Po zakończeniu pracy osoba zamykająca pomieszczenie powinna przekazać klucz sprzątaczce, bądź umieścić go w specjalnie przeznaczonej gablotce.
   e) Wydzielone w pok. nr 6 pomieszczenie serwerowni, zabezpieczone zamkiem patentowym, wyposażone w system klimatyzacji (klucze dostępne tylko dla osób upoważnionych).

2. Zabezpieczenie systemu informatycznego.
   a) Serwer Internet'u – FireWall PC łączący WAN DSL (TP SA) z LAN (Urząd) skonfigurowany do bezpiecznej pracy (z wewnętrznym systemem ochrony antywirusowej), z monitoringiem komunikacji, zarządzany przez bezpieczne łącza przez firmę zewnętrzną.
   b) Serwer HP 2 szt. pod systemem Microsoft Serwer 2008 R2 – dla pozostałych systemów baz danych, w tym zarządzania systemem ochrony F-Secure.
   c) Szafka krosowa - główny węzeł sieci (pozostałe dwa w pok. 4 i pok. nr 10 zabezpieczone zamkami patentowymi).
   d) System autoryzacji dostępu (system haseł) do stanowisk pracy i zasobów sieciowych.
   e) System ochrony typu Client Security dla ochrony serwerów i stanowisk pracy w sieci.
   f) System archiwowania centralnego na dysku zewnętrznym.
   g) Stanowiska komputerowe w budynku Urzędu, podłączone w topologię sieci lokalnej zorganizowanej przez w/w zasoby centralne, każde stanowisko zasilane awaryjnie przez UPS, chronione przez system antywirusowy, dostępne dla użytkownika poprzez system autoryzacji dostępu.
   h) Dostęp do zbiorów danych znajdujących się na serwerze posiadają tylko stanowiska zlokalizowane w pokojach wskazanych w § 4.
   i) Stanowiska komputerowe w pomieszczeniach, gdzie mogą przebywać osoby nieupoważnione do przetwarzania danych osobowych (np. interesanci albo inni pracownicy Urzędu), powinny być umieszczone w sposób, który uniemożliwi takim osobom wgląd do tych danych. W pokoju, do którego dostęp mają petenci, monitory komputerowe ustawione są w ten sposób, by petenci nie widzieli zapisów na ekranie.
   j) W przypadku dłuższej bezczynności uruchamiane są tzw. wygaszacze ekranu lub blokowanie systemu, których dezaktywacja jest możliwa po podaniu prawidłowego hasła użytkownika.

k) Oprogramowanie wykorzystywane do przetwarzania danych posiada własny (dodatkowy, oprócz systemowego) system autoryzacji użytkownika.

l) Połączenie z bazami danych nie znajdującymi się na serwerze urzędu odbywa się poprzez bezpieczne łącze.

m) Kopie bezpieczeństwa wykonywane są raz w miesiącu na dyskach zewnętrznych i przechowywane są w zamykanej szafie w pokoju nr 6.

3. Zabezpieczenia organizacyjne.

a) Do Kierownictwa Urzędu należy zapewnienie odpowiednich pomieszczeń, stosownie zabezpieczonych i wyposażonych do przetwarzania i przechowywania danych osobowych, zaznajomienie pracowników z prawnymi oraz pracowniczymi konsekwencjami naruszenia bezpieczeństwa danych osobowych.

b) Administrator Danych swoją decyzją wyznacza Administratora Bezpieczeństwa Informacji Urzędu.

c) ABI realizuje zadania w zakresie ochrony danych.

d) Funkcje Lokalnych Administratorów Bezpieczeństwa Informacji pełnią kierownicy poszczególnych referatów.

e) Pracownicy Urzędu Gminy Duszniki, a w szczególności pracownicy upoważnieni do przetwarzania danych osobowych w systemie informatycznym jak i ręcznym, zobowiązani są do zapoznania się i przestrzegania Polityki.

f) Osoba zatrudniona składa oświadczenie o zapoznaniu się z przepisami i odpowiedzialności karnej za naruszenie ochrony danych osobowych oraz zachowaniu tajemnicy, którego wzór stanowi załącznik nr 1 do Polityki.

g) Fakt zapoznania się z Polityką pracownik potwierdza własnoręcznym podpisem na stosownym wykazie, którego wzór stanowi załącznik nr 2 do Polityki. Wykaz przechowuje ABI.

h) Osoby przetwarzające dane osobowe otrzymują upoważnienie do ich przetwarzania, którego wzór stanowi załącznik nr 3 do Polityki.

i) Upoważnienie, w którym określony jest zakres danych do przetwarzania, wydaje Wójt Gminy Duszniki.

j) Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych, której wzór stanowi załącznik nr 4 do Polityki. Ewidencję w formie elektronicznej prowadzi ABI.

k) Pracownikom wolno przebywać na terenie Urzędu tylko w godzinach ich pracy, a po godzinach pracy - po zawiadomieniu bezpośrednio przełożonego.

l) Przebywanie na terenie Urzędu w dni wolne od pracy wymaga zezwolenia Wójta.

m) Korzystanie z systemu informatycznego służącego do przetwarzania danych osobowych może odbywać się tylko w godzinach pracy Urzędu, a po godzinach pracy - po zawiadomieniu bezpośrednio przełożonego.

n) Wydruki zawierające dane osobowe powinny znajdować się w miejscu, które uniemożliwia dostęp osobom postronnym.

o) Wydruki zawierające dane osobowe po ustaleniu ich przydatności są niszczone w niszczarkach.

p) Po zakończeniu pracy, pracownicy zobowiązani są do niepozostawiania dokumentów na biurkach lub innych miejscach, umożliwiających łatwy dostęp. Dokumenty należy umieszczać w szafach.

q) Umowa z firmą zewnętrzną zajmującą się serwisem sprzętu komputerowego obejmuje klauzulę dotyczącą ochrony danych osobowych, a wszelkie prace na serwerach oraz stanowiskach, na których znajdują się dane osobowe prowadzone są pod nadzorem Administratora Systemu Informatycznego lub osoby przez niego wyznaczonej.

r) Wszelkie prace wykonywane przez firmy zewnętrzne, dotyczące serwisu oprogramowania służącego do przetwarzania danych osobowych prowadzone są pod nadzorem Administratora Systemu Informatycznego lub osoby przez niego wyznaczonej.

s) W przypadku, gdy uszkodzenie sprzętu zawierającego nośnik danych, na którym zapisane są dane osobowe wymusza konieczność przekazania go poza siedzibę urzędu, nośnik ten należy wymontować.

§ 9

Monitorowanie zabezpieczeń

1. Do monitorowania systemu zabezpieczeń, stosownie do swojego zakresu czynności, zobligowani są:
   a) Administrator danych,
   b) Administrator Bezpieczeństwa Informacji,
   c) Lokalni Administratorzy Bezpieczeństwa Informacji,
   d) Administrator Systemu Informatycznego.
2. W ramach monitoringu należy przeprowadzać następujące działania:
   a) okresowe sprawdzanie kopii bezpieczeństwa pod względem przydatności do odtworzenia danych,
   b) sprawdzanie stanu technicznego systemu komputerowego oraz oprogramowania, w tym pod kątem występowania zagrożeń zbiorów danych osobowych,
   c) sprawdzania częstotliwości zmian haseł,
   d) sprawdzanie przestrzegania przez pracowników zasad określonych w Polityce bezpieczeństwa.
3. Administrator Bezpieczeństwa Informacji przeprowadza kontrole dotyczące bezpieczeństwa zbiorów danych osobowych.
4. Na podstawie przeprowadzonych kontroli, o których mowa w pkt. 3 oraz raportów przedłożonych przez LABI, Administrator Bezpieczeństwa Informacji sporządza roczne sprawozdanie i przedstawia Administratorowi danych.

§ 10

Obowiązki Administratora danych

1. Do obowiązków Administratora danych należy w szczególności:
   a) zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym,
   b) zapobieganie zabraniu danych przez osobę nieuprawnioną,

c) zapobieganie przetwarzaniu danych z naruszeniem ustawy oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych,

d) zbieranie danych dla oznaczonych, zgodnych z prawem celów,

e) dbałość o merytoryczną poprawność danych i adekwatność w stosunku do celów, w jakich są przetwarzane,

f) określenie pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego,

g) opracowanie instrukcji określającej sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji,

h) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,

i) podejmowanie działań mających na celu zaznajomienie każdej osoby przetwarzającej dane osobowe z przepisami dotyczącymi ich ochrony.

2. Administrator danych odpowiada za to, by zakres czynności osoby zatrudnionej przy przetwarzaniu danych osobowych określał odpowiedzialność tej osoby za:

   a) ochronę danych przed niepowołanym dostępem,

   b) nieuzasadnioną modyfikację lub zniszczenie danych,

   c) nielegalne ujawnienie danych.

   w stopniu odpowiednim do zadań realizowanych w procesie przetwarzania danych osobowych.

3. Zgłasza zbiory danych osobowych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych.

§ 11

Obowiązki Administratora Bezpieczeństwa Informacji

1. Do obowiązków Administratora Bezpieczeństwa Informacji należy w szczególności:

   a) nadzór na przestrzeganiem instrukcji określającej sposób zarządzania systemem informatycznym,

   b) przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane dane osobowe,

   c) podejmowanie odpowiednich działań w celu właściwego zabezpieczenia danych,

   d) badanie ewentualnych naruszeń w systemie zabezpieczeń danych osobowych,

   e) wdrożenie działań mających na celu zaznajomienie każdej osoby przetwarzającej dane z przepisami dotyczącymi ochrony danych osobowych, środkami technicznymi i organizacyjnymi wykorzystywanymi przy przetwarzaniu danych w systemach informatycznych,

   f) przeprowadzanie kontroli,

   g) sporządzanie raportów z naruszenia bezpieczeństwa,

   h) zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:

      - sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych,

- nadzorowanie opracowania i aktualizowania dokumentacji, o której mowa w art. 36 ust. 2, ustawy o ochronie danych osobowych oraz przestrzegania zasad w niej określonych,
- zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych,

i) prowadzenie rejestru zbiorów danych przetwarzanych przez Administratora danych, z wyjątkiem zbiorów, o których mowa w art. 43 ust. 1 ustawy o ochronie danych osobowych, zawierającego nazwę zbioru oraz informacje, o których mowa w art. 41 ust. 1 pkt 2-4a i 7 w/w ustawy .

§ 12

Obowiązki Administratora Systemu Informatycznego

1. Do obowiązków Administratora Systemu Informatycznego należy w szczególności przeprowadzanie lub nadzór nad firmą zewnętrzną w przypadku:
   a) naprawy, konserwacji oraz likwidacji urządzeń komputerowych zawierających dane osobowe,
   b) definiowania użytkowników i haseł dostępu w systemie,
   c) aktualizowania oprogramowania systemowego, chyba że aktualizacje wykonywane są automatycznie,
   d) aktualizowania oprogramowania antywirusowego, chyba że aktualizacje wykonywane są automatycznie,
   e) okresowe sprawdzanie kopii zapasowych pod kątem ich dalszej przydatności.

§ 13

Obowiązki Lokalnych Administratorów Bezpieczeństwa Informacji

1. Do zadań LABI należy:
   a) nadzór nad osobami pracującymi w referacie w zakresie przestrzegania Polityki bezpieczeństwa oraz instrukcji określającej sposób zarządzania systemem informatycznym i zasad w nich zawartych,
   b) zgłoszenie Administratorowi Bezpieczeństwa Informacji na temat: planowanego założenia nowych zbiorów danych osobowych, wnoszonych zmian do zbiorów zarejestrowanych,
   c) zgłaszanie Administratorowi danych konieczności wydania upoważnienia lub cofnięcie upoważnienia, pracownikowi, do przetwarzania danych znajdujących się w określonym zbiorze. W przypadku osób zatrudnionych na samodzielnych stanowiskach obowiązek taki dotyczy pracownika odpowiedzialnego za sprawy kadrowe.

§ 14

Zasady udostępniania danych osobowych

1. Administrator danych osobowych udostępnia dane osobowe przetwarzane we własnych zbiorach tylko osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.
2. Zbiory danych osobowych udostępnia się na pisemny, umotywowany wniosek, chyba że odrębne przepisy prawa stanowią inaczej.

3. Wniosek o udostępnienie danych osobowych powinien zawierać informacje umożliwiające wyszukanie żądanych danych osobowych w zbiorze oraz wskazywać ich zakres i przeznaczenie.
4. Wniosek o udostępnienie danych osobowych jest rozpatrywany przez lokalnego administratora bezpieczeństwa informacji.
5. Decyzję w sprawie udostępnienia danych podejmuje lokalny administrator bezpieczeństwa informacji lub - w przypadku nieobecności lokalnego administratora bezpieczeństwa informacji - Administrator Bezpieczeństwa Informacji.
6. Administrator danych osobowych może odmówić udostępnienia danych osobowych, jeżeli spowodowałoby to istotne naruszenia dóbr osobistych osób, których dane dotyczą, lub innych osób oraz jeżeli dane osobowe nie mają istotnego związku ze wskazanymi we wniosku motywami działania wnioskodawcy.
7. Administrator danych osobowych może powierzyć przetwarzanie danych osobowych innemu podmiotowi wyłącznie w drodze umowy zawartej w formie pisemnej.
8. Podmiot, o którym mowa w ust. 7, jest zobowiązany do zastosowania środków organizacyjnych i technicznych, zabezpieczających zbiór przed dostępem osób nieupoważnionych na zasadach określonych w przepisach o ochronie danych osobowych.
9. Podmiot, o którym mowa w ust. 7 jest zobowiązany przetwarzać dane osobowe wyłącznie w zakresie określonym w umowie.
10. W przypadkach opisanych w ust. 7-9 odpowiedzialność za ochronę przetwarzanych danych osobowych spoczywa na administratorze danych osobowych, co nie wyłącza odpowiedzialności podmiotu, z którym zawarto umowę z tytułu przetwarzania danych niezgodnie z ustawą.

§ 15

Odpowiedzialność służbowa

1. Pracownik, który:
   a) przetwarza w zbiorze danych dane osobowe:
   - do których przetwarzania nie jest upoważniony,
   - których przetwarzanie jest zabronione,
   - niezgodne z celem stworzenia zbioru danych;

   a) udostępnia lub umożliwia dostęp do danych osobowych osobom nieupoważnionym,
   b) nie zgłasza zbiorów danych podlegających rejestracji,
   c) nie dopełnia obowiązku poinformowania osoby, której dane dotyczą, o przysługujących jej prawach,
   d) uniemożliwia osobie, której dane dotyczą, korzystanie z przysługujących jej praw, podlega odpowiedzialności karnej zgodnie z ustawą oraz sankcjami określonymi w Kodeksie pracy.

§ 16

Postępowanie w przypadku naruszenia ochrony danych osobowych

1. Każdy pracownik Urzędu, który poweźmie wiadomość w zakresie naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane osobowe, bądź posiada informację mogącą mieć wpływ na bezpieczeństwo danych osobowych jest zobowiązany fakt ten niezwłocznie zgłosić Administratorowi Bezpieczeństwa Informacji.
2. W razie niemożliwości zawiadomienia Administratora Bezpieczeństwa Informacji, należy powiadomić bezpośredniego przełożonego.
3. W przypadku wykrycia naruszenia ochrony danych osobowych Administrator Bezpieczeństwa Informacji informuje kierownictwo Urzędu o zaistniałym zdarzeniu oraz przeprowadza wstępne

dochodzenie, po czym sporządza raport opisujący okoliczności zdarzenia, którego wzór stanowi załącznik nr 5 do Polityki. Jeśli zdarzenie ma charakter przestępstwa sprawa kierowana jest do organów ścigania.

……..
(imię i nazwisko pracownika)

……..

……
(adres)

Oświadczenie

Ja niżej podpisany(a) oświadczam, że zapoznałem(łam) się z :

- treścią definicji danych osobowych w rozumieniu art. 6 Ustawy z dnia 29.08.1997 r., o ochronie danych osobowych (Dz.U. z 2016 r., poz. 922),
- z Polityką bezpieczeństwa i Instrukcją zarządzania systemem informatycznym, obowiązującymi w Urzędzie Gminy Duszniki, a w szczególności z oprogramowaniem zainstalowanym na stanowisku pracy.

Oświadczam, że zostałem(łam) poinformowany(a):

- o zasadach zachowania w tajemnicy danych osobowych, do których mam/ będę miał(a) dostęp w związku z wykonywaniem przeze mnie zadań służbowych i obowiązków pracowniczych w Urzędzie Gminy Duszniki, zarówno w trakcie obecnie wiążącego mnie stosunku pracy, stażu, praktyki, jak i po ustaniu zatrudnienia,
- o fakcie prowadzenia przez mojego pracodawcę monitoringu udostępnionego mi do użytku służbowego sprzętu komputerowego wraz z oprogramowaniem oraz konsekwencjach służbowych wynikających z wykorzystywania go niezgodnie z przeznaczeniem.

Oświadczam, że jestem świadomy odpowiedzialności karnej, o której mowa w artykułach: 278 § 2 oraz 293 w związku z 291 oraz art. 292 ustawy z dnia 6 czerwca 1997 r. kodeks karny (Dz. U. z 2016 r., poz. 1137 ze zm.) oraz odpowiedzialności karnej i cywilnej przewidzianej w artykułach: 116 i następnych ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2016 r., poz. 666, ze zm.) za niezgodne z prawem korzystanie, rozpowszechnianie, utrwalanie, uzyskiwanie lub zwielokrotnianie oprogramowania.

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

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

……
(data i podpis pracownika)

Wykaz osób, które zostały zapoznane z „Polityką bezpieczeństwa Urzędu Gminy Duszniki" przeznaczoną dla osób zatrudnionych przy przetwarzaniu danych osobowych.
(wzór)

Lp.	*Nazwisko i imię*	*Stanowisko*	*Data*	*Podpis*

Upoważnienie
Nr…….

Działając na podstawie uprawnień nadanych mi w …….. w sprawie ochrony danych osobowych art. 37 ustawy o Ochronie Danych Osobowych, upoważniam

Panią/ Pana Imię i Nazwisko ……
do przetwarzania danych/obsługi:
systemu informatycznego / nieinformatycznego oraz urządzeń wchodzących w jego skład zlokalizowanych w Urzędzie Gminy Duszniki służących do przetwarzania danych osobowych zawartych w zbiorze noszącym nazwę.....
na okres …….
identyfikator…….

Wyżej wymieniona osoba została zapoznana z obecnie obowiązującymi przepisami dotyczącymi ochrony danych osobowych i dopuszczona jest do ich przetwarzania jedynie w zakresie określonym w ustawie z dnia 29.08.1997r, o ochronie danych osobowych (Dz. U. z 2016 r., poz. 922) i wydanych do niej przepisach wykonawczych oraz w Zarządzeniu …….. w sprawie ochrony danych osobowych.

Wymieniona osoba została wpisana do ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych w Urzędzie Gminy Duszniki.

Wzór

Ewidencja osób upoważnionych

L.p.	Imię Nazwisko	Numer upoważnienia	Nazwa zbioru	Okres dostępu	Uwagi
1					
2					
….					

Załącznik nr 5 do Polityki bezpieczeństwa Urzędu Gminy Duszniki

Raport z naruszenia bezpieczeństwa systemu informatycznego w Urzędzie Gminy Duszniki (wzór)

1. Data: …… Godzina: ……
(dd.mm.rr) (gg:mm)

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

……
(imię, nazwisko, stanowisko służbowe, nazwa użytkownika (jeśli występuje))

3. Lokalizacja zdarzenia:

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

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

……

……

……..

5. Przyczyny wystąpienia zdarzenia:

……

……

……..

6. Podjęte działania:

……

……

……

7. Postępowanie wyjaśniające:

……
……
……
……..

……
(data, podpis Administratora bezpieczeństwa informacji)

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania danych oraz pomieszczenia, w których są przetwarzane

Wszystkie zbiory wymienione w poniższej tabeli przetwarzane są w budynku Urzędu Gminy Duszniki, ul. Sportowa 1, 64 – 550 Duszniki.

Lp.	Zbiór danych	Nazwa oprogramowania	Nr pokoju
1	Ewidencja ludności i rejestr wyborców	System Ewidencji Ludności – Clanet Gliwice	5*
2	Rejestr aktów stanu cywilnego	PB USC (PTH TECHNIKA Sp. z o.o.)	5*
3	Baza osób składających wnioski w sprawie wydania dowodów osobistych	System Wydawania Dowodów Osobistych (WASKO S. A.)	5**
4	Rejestr płatników podatku od nieruchomości, leśnego, rolnego	SIGID Sp. z o.o.	5,6,7,8,9*
5	Rejestr osób (pracowników) do celów kadrowych		
6	Baza płatników podatku od środków transportowych		
7	Ewidencja osób prowadzących działalności gospodarczej		
8	Baza płatników składek ZUS (pracowników)	Płatnik (PROKOM Software S. A.)	8
9	Baza danych klientów Urzędu Gminy Duszniki	System obiegu dokumentów SODAN	1,2,3,4,5,6,7,8, 9,10,11,14,15 *
10	System Ewidencji Gruntów - wykreślony	GEO-INFO 7 moduł i.EGiB	4***
11	Zbiór danych osób podlegających kwalifikacji wojskowej	Zbiór prowadzony w formie papierowej	11
12	Zbiór danych oświadczeń majątkowych osób zobowiązanych do ich składania	Zbiór prowadzony w formie papierowej	10
13	Zbiór danych oświadczeń majątkowych radnych	Zbiór prowadzony w formie papierowej	10
14	Ewidencja osób , którym wydano zaświadczenie o nadaniu numeru porządkowego	Internetowy Manager Punktów Adresowych firmy Geosystem	4****
15	Rejestr umów dzierżawy	Zbiór prowadzony w formie papierowej	4
16	Rejestr umów	Zbiór prowadzony w formie papierowej	3
17	Rejestr skarg i wniosków	Zbiór prowadzony w formie papierowej	10
18	Zbiór danych płatników opłaty za gospodarowanie odpadami komunalnymi	SIGID	8

19	Rejestr decyzji o warunkach zabudowy zagospodarowania terenu oraz decyzji o lokalizacji inwestycji celu publicznego	Zbiór prowadzony w formie papierowej	4
20	Rejestr spraw dotyczących usunięcia drzew i krzewów	Rejestr prowadzony w pliku EXCEL	3
21	Rejestr rolników poszkodowanych w wyniku klęsk żywiołowych	Rejestr prowadzony w formie papierowej oraz w pliku EXCEL	4
22	Informacje o wyrobach zawierających azbest	Zbiór prowadzony w formie papierowej	4
23	Wykaz zbiorników bezodpływowych i przydomowych oczyszczalni ścieków	Zbiór prowadzony w formie papierowej	4
24	Rejestr korespondencji wychodzącej.	Rejestr prowadzony w formie papierowej oraz w pliku EXCEL	14

*) Baza danych fizycznie jest położona na serwerze w pokoju nr 6.
**) Baza danych położona na serwerze MSWIA
***)Baza danych na serwerze Starostwa Powiatowego w Szamotułach
****) Dane na serwerze zewnętrznym firmy Geo-system

Opis struktury zbiorów danych

Lp.	Zbiór danych	Nazwa oprogramowania	Opis struktury zbiorów
1	Ewidencja ludności i rejestr wyborców	System Ewidencji Ludności – Clanet Gliwice	W zbiorze danych przetwarzane są dane osobowe mieszkańców gminy w zakresie: a) dane adresowe klienta (imię, nazwisko, kod pocztowy, miejscowość, ulica, nr domu) oraz b) dane dotyczące miejsca, daty urodzenia, nr PESEL, imiona rodziców, nazwisko rodowe, stan cywilny
2	Rejestr aktów stanu cywilnego	PB USC (PTH TECHNIKA Sp. z o.o.)	W zbiorze danych przetwarzane są dane osobowe klientów w zakresie: a) dane adresowe klienta (imię, nazwisko, kod pocztowy, miejscowość, ulica, nr domu) oraz b) dane dotyczące miejsca, daty urodzenia, nr PESEL , daty i miejsca zgonu oraz c) dane dotyczące stanu cywilnego i dat zmiany tego stanu
3	Baza osób składających wnioski w sprawie wydania dowodów osobistych	System Wydawania Dowodów Osobistych (WASKO S. A.)	W zbiorze danych przetwarzane są dane osobowe klientów zakresie: a) dane adresowe klienta (imię, nazwisko, kod pocztowy, miejscowość, ulica, nr domu) oraz b) dane dotyczące miejsca, daty urodzenia, nr PESEL , imiona rodziców, nazwisko rodowe, stan cywilny
4	Rejestr płatników podatku od nieruchomości, leśnego, rolnego	SIGID Sp. z o.o.	W zbiorze danych przetwarzane są dane osobowe klientów w zakresie: a) dane adresowe klienta (imię, nazwisko, kod pocztowy, miejscowość, ulica, nr domu) oraz b) dane dotyczące numeru NIP i nr rachunku klienta oraz c) dane dotyczące nieruchomości klienta od których odprowadzany jest podatek
5	Rejestr osób (pracowników) do celów kadrowych		W zbiorze danych przetwarzane są dane osobowe pracownika w zakresie: a) dane adresowe pracownika (imię, nazwisko, kod pocztowy, miejscowość, ulica, nr domu) oraz b) dane dotyczące numeru NIP i nr rachunku pracownika oraz c) dane dotyczące zatrudnienia pracownika w tym staż pracy, okres zatrudnienia, wynagrodzenie pracownika itp.
6	Baza płatników podatku od środków transportowych		W zbiorze danych przetwarzane są dane osobowe klientów w zakresie: a) dane adresowe klienta (imię, nazwisko, kod pocztowy, miejscowość, ulica, nr domu) oraz b) dane dotyczące numeru NIP i nr rachunku klienta oraz c) dane dotyczące środków transportu klienta od których odprowadzany jest podatek
7	Ewidencja osób prowadzących działalności		W zbiorze danych przetwarzane są dane osobowe klientów w zakresie: a) dane adresowe klienta (imię, nazwisko, kod pocztowy, miejscowość, ulica, nr domu)

	gospodarczej		oraz b) dane dotyczące prowadzonej działalności gospodarczej w tym nazwa , miejsce wykonywania, nr NIP, itp.
8	Baza płatników składek ZUS (pracowników)	Płatnik (PROKOM Software S. A.)	W zbiorze danych przetwarzane są dane osobowe pracownika w zakresie: a) dane adresowe pracownika (imię, nazwisko, kod pocztowy, miejscowość, ulica, nr domu) oraz b) dane dotyczące numeru NIP pracownika oraz c) dane dotyczące składek ZUS pracownika
9	Baza danych klientów Urzędu Gminy Duszniki	System obiegu dokumentów SODAN	W zbiorze danych przetwarzane są dane osobowe klientów w zakresie: a) dane adresowe klienta (imię, nazwisko, kod pocztowy, miejscowość, ulica, nr domu) oraz b) wszystkich składanych przez danego klienta wniosków oraz wysyłanych do klienta odpowiedzi
10	System Ewidencji Gruntów -wykreślony	wykreślony	wykreślony
11	Zbiór danych osób podlegających kwalifikacji wojskowej	Zbiór prowadzony w formie papierowej	W zbiorze danych przetwarzane są dane osobowe klientów w zakresie: a) dane adresowe klienta (imię, nazwisko, kod pocztowy, miejscowość, ulica, nr domu) oraz b) dane osobowe c) dane dotyczące o przydatności do służby wojskowej
12	Zbiór danych oświadczeń majątkowych osób zobowiązanych do ich składania	Zbiór prowadzony w formie papierowej	W zbiorze danych przetwarzane są dane osobowe klientów w zakresie: a) dane adresowe klienta (imię, nazwisko, kod pocztowy, miejscowość, ulica, nr domu) oraz b) dane dotyczące stanu cywilnego, majątku, zatrudnienia , prowadzonej działalności
13	Zbiór danych oświadczeń majątkowych radnych	Zbiór prowadzony w formie papierowej	W zbiorze danych przetwarzane są dane osobowe klientów w zakresie: c) dane adresowe klienta (imię, nazwisko, kod pocztowy, miejscowość, ulica, nr domu) oraz d) dane dotyczące stanu cywilnego, majątku, zatrudnienia , prowadzonej działalności
14	Ewidencja osób , którym wydano zaświadczenie o nadaniu numeru porządkowego	Zbiór prowadzony na serwerze firmy Geo - system	W zbiorze danych przetwarzane są dane osobowe klientów w zakresie: a) dane adresowe klienta (imię, nazwisko, kod pocztowy, miejscowość, ulica, nr domu) oraz b) dane dotyczące nadane nr porządkowego (nr porządkowy , miejscowość, ulica, nr działki)
15	Rejestr umów dzierżawy	Zbiór prowadzony w formie papierowej	W zbiorze danych przetwarzane są dane osobowe klientów w zakresie: a) dane adresowe klienta (imię, nazwisko, kod pocztowy, miejscowość, ulica, nr domu) oraz b) dane dotyczące dzierżawionej powierzchni
16	Rejestr umów	Zbiór prowadzony w formie papierowej	W zbiorze danych przetwarzane są dane osobowe klientów w zakresie: a) dane adresowe klienta (imię, nazwisko, kod pocztowy, miejscowość, ulica, nr domu) oraz b) umowa dotycząca zadań wykonywanych przez klienta

17	Rejestr skarg i wniosków	Zbiór prowadzony w formie papierowej	W zbiorze danych przetwarzane są dane osobowe klientów w zakresie: a) dane adresowe klienta (imię, nazwisko, kod pocztowy, miejscowość, ulica, nr domu) oraz b) skargi i wnioski mieszkańców
18	Zbiór danych płatników opłaty za gospodarowanie odpadami komunalnymi	SIGID Sp. z o.o.	W zbiorze danych przetwarzane są dane osobowe klientów w zakresie: a) dane adresowe klienta (imię, nazwisko, kod pocztowy, miejscowość, ulica, nr domu) oraz b) dane liczby osób zamieszkujących nieruchomości oraz sposobu zbierani odpadów
19	Rejestr decyzji o warunkach zabudowy zagospodarowania terenu oraz decyzji o lokalizacji inwestycji celu publicznego	Zbiór prowadzony w formie papierowej oraz pliku WORD	W zbiorze danych przetwarzane są dane osobowe klientów w zakresie: a) dane adresowe klienta (imię, nazwisko, kod pocztowy, miejscowość, ulica, nr domu) oraz b) dane dotyczące miejsca planowanego przedsięwzięcia
20	Rejestr spraw dotyczących usunięcie drzew i krzewów	Rejestr prowadzony w formie papierowej oraz w pliku EXCEL	W zbiorze danych przetwarzane są dane osobowe klientów w zakresie: a) dane adresowe klienta (imię, nazwisko, kod pocztowy, miejscowość, ulica, nr domu) oraz b) dane dotyczące miejsca wycinki oraz podsadzenia w zamian drzew i krzewów
21	Rejestr rolników poszkodowanych w wyniku klęsk żywiołowych	Rejestr prowadzony w formie papierowej oraz w pliku EXCEL	W zbiorze danych przetwarzane są dane osobowe klientów w zakresie: a) dane adresowe klienta (imię, nazwisko, kod pocztowy, miejscowość, ulica, nr domu) oraz b) dane dotyczące terenu obszaru wystąpienia szkody,
22	Informacje o wyrobach zawierających azbest	Rejestr prowadzony w formie papierowej oraz w pliku EXCEL	W zbiorze danych przetwarzane są dane osobowe klientów w zakresie: a) dane adresowe klienta (imię, nazwisko, kod pocztowy, miejscowość, ulica, nr domu) oraz b) dane dotyczące wyrobów zawierających azbest
23	Wykaz zbiorników bezodpływowych i przydomowych oczyszczalni ścieków	Rejestr prowadzony w formie papierowej oraz w pliku EXCEL	W zbiorze danych przetwarzane są dane osobowe klientów w zakresie: a) dane adresowe klienta (imię, nazwisko, kod pocztowy, miejscowość, ulica, nr domu) oraz b) dane dotyczące zbiorników bezodpływowych i przydomowych oczyszczalni ścieków
24	Rejestr korespondencji wychodzącej	Rejestr prowadzony w formie papierowej oraz w pliku EXCEL	W zbiorze danych przetwarzane są dane osobowe klientów w zakresie: a) dane adresowe klienta (imię, nazwisko, kod pocztowy, miejscowość, ulica, nr domu)