Z A R Z Ą D Z E N I E Nr 43)2013
Wójta Gminy Szczytniki
z dnia 2 września 2013r.

w sprawie: ***Polityki Bezpieczeństwa Informacji, Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych oraz Instrukcji postępowania przy przetwarzaniu danych osobowych w Urzędzie Gminy w Szczytnikach.***

Na podstawie art. 33 ust. 1 i 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (tj. Dz. U. 2013 r., poz. 594), art. 26 i art. 36 ust. 1 i 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm) oraz § 3 i § 9 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. z 2004r. Nr 100, poz. 1024) ***z a r z ą d z a się, co następuje:***

§ 1. Ustala się:

1) Politykę Bezpieczeństwa Informacji w Urzędzie Gminy w Szczytnikach, stanowiącą załącznik nr 1 do niniejszego Zarządzenia,
2) Instrukcję Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy w Szczytnikach, stanowiącą załącznik nr 2 do niniejszego Zarządzenia,
3) Instrukcję postępowania przy przetwarzaniu danych osobowych w odręcznych zbiorach ewidencyjnych w Urzędzie Gminy w Szczytnikach.

§ 2. Wyznacza się na Administratora Bezpieczeństwa Informacji (ABI) w Urzędzie Gminy w Szczytnikach Kierownika Referatu Administracyjno-Organizacyjnego UG P. Grażynę Kuchnicką.

§ 3. Polityka Bezpieczeństwa Informacji wraz z instrukcjami ma zastosowanie na wszystkich stanowiskach pracy, gdzie przetwarzane są dane osobowe. Obejmuje swoim zakresem całokształt spraw związanych z ochroną danych osobowych, finansowych, danych związanych z zarządzaniem technicznym oraz prawno – administracyjnym.

§ 4. Zobowiązuję Administratora Bezpieczeństwa Informacji do zapoznania wszystkich pracowników Urzędu Gminy w Szczytnikach z postanowieniami niniejszego zarządzenia wraz z załącznikami oraz do przestrzegania zasad zawartych w tym zarządzeniu.

§ 5. Traci moc Zarządzenie Nr 1/1999 Wójta Gminy Szczytniki z dnia 30 czerwca 1999r. w sprawie ochrony danych osobowych w systemie informatycznym służącym do przetwarzania danych osobowych.

§ 6. Zarządzenie wchodzi w życie z dniem podpisania.

Załącznik nr 1
do Zarządzenia Nr 43)2013
Wójta Gminy Szczytniki
z dnia 2 września 2013r**.**

POLITYKA BEZPIECZEŃSTWA INFORMACJI
URZĘDU GMINY W SZCZYTNIKACH

SPIS TREŚCI

WYKAZ ZAŁĄCZNIKÓW:

1) **Załącznik nr 1** – Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe stanowiących strefę administracyjną,

2) **Załącznik nr 2** – Wykaz zbiorów danych osobowych przetwarzanych elektronicznie i w inny sposób, ze wskazaniem programów zastosowanych do przetwarzania danych osobowych i wykazem pracowników przetwarzających,

3) **Załącznik nr 3** – Opis struktury zbiorów danych osobowych przechowywanych w systemach informatycznych oraz sposób przepływu danych pomiędzy systemami informatycznymi,

4) **Załącznik nr 4** – Wzór formularza stosowanego dla spełnienia przez Urząd Gminy w Szczytnikach obowiązków określonych w § 22 ust. 1 i 2 polityki bezpieczeństwa informacji,

5) **Załącznik nr 5** – Wzór formularza stosowanego dla spełnienia przez Urząd Gminy w Szczytnikach obowiązków określonych w § 23 ust. 1 i 2 polityki bezpieczeństwa informacji,

6) **Załącznik nr 6** – Wzór wniosku do administratora danych osobowych o upoważnienie imienne do przetwarzania danych osobowych. Wzór imiennego upoważnienia do przetwarzania danych osobowych. Wzór cofnięcia imiennego upoważnienia do przetwarzania danych osobowych,

7) **Załącznik nr 7** – Wzór oświadczenia osoby przetwarzającej dane osobowe o zachowaniu w tajemnicy danych, z którymi ma styczność oraz stosowanych przy przetwarzaniu danych osobowych środkach bezpieczeństwa,

8) **Załącznik nr 8** – Wzór oświadczenia osoby zatrudnionej przy przetwarzaniu danych osobowych na podstawie umowy zlecenia, umowy o dzieło lub innej umowy cywilnej o zachowaniu tajemnicy,

9) **Załącznik nr 9** – Wzór porozumienia zawieranego pomiędzy Wójtem Gminy Szczytniki, a pracownikiem zatrudnionym przy przetwarzaniu danych osobowych, w sprawie wykorzystania oddanego do dyspozycji sprzętu informatycznego, oprogramowania oraz zasobów sieci informatycznej.

10) **Załącznik nr 10** – Wzór oświadczenia pracownika po przeszkoleniu o zapoznaniu się z przepisami i procedurami.

11) **Załącznik nr 11 –** Wzór ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych.

12) **Załącznik nr 12** – Wzór raportu z naruszenia ochrony danych osobowych.

OPIS ZDARZEŃ NARUSZAJĄCYCH OCHRONĘ DANYCH OSOBOWYCH

Podział zagrożeń:

1) 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 ochrony danych.

2) Zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, awarie sprzętowe, błędy oprogramowania, pogorszenie jakości sprzętu i oprogramowania) - może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie ochrony danych.

3) Zagrożenia zamierzone - świadome i celowe działania powodujące naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na:

    - nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu),
    - nieuprawniony dostęp do systemu z jego wnętrza,
    - nieuprawnione przekazanie danych,
    - bezpośrednie zagrożenie materialnych składników systemu (np. kradzież sprzętu).

4) Naruszenie lub podejrzenie naruszenia systemu informatycznego, w którym przetwarzane są dane osobowe - następuje w sytuacji:

    - losowego lub nieprzewidzianego oddziaływania czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, itp.,

    - niewłaściwych parametrów środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,

    - awarii sprzętu lub oprogramowania, które wyraźnie wskazuje na umyślne działanie w kierunku naruszenia ochrony danych,

    - pojawienia się odpowiedniego komunikatu alarmowego,

    - podejrzenia nieuprawnionej modyfikacji danych w systemie lub innego odstępstwa od stanu oczekiwanego,

    - naruszenia lub próby naruszenia integralności systemu lub bazy danych w tym systemie,

- pracy w systemie wykazującej odstępstwa uzasadniające podejrzenie przełamania lub zaniechania ochrony danych osobowych - np. praca osoby, która nie jest formalnie dopuszczona do obsługi systemu,

- ujawnienia nieautoryzowanych kont dostępu do systemu,

- naruszenia dyscypliny pracy w zakresie przestrzegania procedur polityki bezpieczeństwa (np. nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, itp.).

5) Stwierdzone nieprawidłowości w zakresie zabezpieczenia fizycznego miejsc przechowywania i przetwarzania danych osobowych np.

- niezabezpieczone pomieszczenia,
- nienadzorowane, otwarte szafy, biurka, regały,
- niezabezpieczone urządzenia archiwizujące,
- pozostawianie danych w nieodpowiednich miejscach – kosze, stoły itp.

ROZDZIAŁ I
Postanowienia ogólne, definicje i objaśnienia

§ 1. Zawartość opracowania, podstawy prawne

1. Polityka Bezpieczeństwa Informacji Urzędu Gminy w Szczytnikach jest zbiorem zasad i procedur obowiązujących przy zarządzaniu, przetwarzaniu i wykorzystywaniu danych osobowych we wszystkich zbiorach danych osobowych administrowanych przez Urząd Gminy w Szczytnikach.

2. Polityka zawiera zestaw informacji dotyczących szacowania procesów przetwarzania danych osobowych oraz obowiązujących zabezpieczeń technicznych i organizacyjnych, zapewniających właściwą ochronę przetwarzania danych osobowych.

3. Podstawą do opracowania i wdrożenia dokumentu są:

   a) Konstytucja Rzeczypospolitej Polskiej,

   b) Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.),

   c) Rozporządzenie 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).

4. Polityka bezpieczeństwa informacji Urzędu Gminy w Szczytnikach zawiera między innymi:

   a) wykaz budynków i pomieszczeń, w których przetwarzane są dane osobowe, stanowiący załącznik nr 1 do niniejszej Polityki,

   b) wykaz zbiorów danych osobowych przetwarzanych elektronicznie lub w inny sposób, stanowiący załącznik nr 2 do niniejszej Polityki,

   c) opis struktury zbiorów danych osobowych przetwarzanych w systemach informatycznych oraz sposób przepływu danych pomiędzy systemami informatycznymi, stanowiący załącznik nr 3 do niniejszej Polityki.

5. Opracowaną Politykę stosuje się do danych osobowych:
   - przetwarzanych w systemach informatycznych,
   - przetwarzanych na nośnikach elektronicznych,
   - przetwarzanych w sposób tradycyjny.

6. Przetwarzanie danych osobowych w Urzędzie Gminy w Szczytnikach jest dopuszczalne wyłącznie pod warunkiem przestrzegania ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych i wydanych na jej podstawie przepisów wykonawczych oraz Zarządzeń Wójta .

§ 2. Definicje i pojęcia stosowane w polityce bezpieczeństwa informacji

1. Wszystkie pojęcia i definicje zawarte w Polityce znajdują wspólne powiązania ujęte w niniejszym dokumencie, są także powiązane z innymi dokumentami, które obowiązują w Urzędzie Gminy w Szczytnikach w zakresie ochrony danych osobowych.

2. Użyte w treści Polityki bezpieczeństwa informacji określenia oznaczają:

   1) **ADMINISTRATOR DANYCH OSOBOWYCH (ADO)** – Wójt Gminy Szczytniki – organ, jednostka organizacyjna, podmiot lub osoba, o którym mowa w art. 3 ustawy o ochronie danych osobowych, decydująca o celach i środkach przetwarzania danych osobowych, Osoba funkcyjna odpowiedzialna za całokształt zagadnień związanych z przetwarzaniem danych osobowych w administrowanych przez nią zbiorach danych,

   2) **ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI** (**ABI)** – osoba funkcyjna wyznaczona przez ADO, odpowiedzialna za nadzorowanie stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, w tym w szczególności za przeciwdziałanie dostępowi osób nieuprawnionych do systemu, w którym przetwarzane są dane osobowe oraz podejmowanie stosownych działań w przypadku wykrycia naruszeń w systemie ochrony danych osobowych odpowiednich do zagrożeń oraz kategorii danych objętych ochroną,

   3) **ADMINISTRATOR SYSTEMÓW INFORMATYCZNYCH (ASI)** – osoba wyznaczona przez ADO, odpowiedzialna za funkcjonowanie infrastruktury informatycznej, na którą składa się wyposażenie informatyczne oraz systemy i aplikacje informatyczne, za ich przeglądy, konserwację oraz za stosowanie technicznych i organizacyjnych środków bezpieczeństwa w systemach informatycznych.

   4) **BEZPIECZEŃSTWO PRZETWARZANIA DANYCH OSOBOWYCH** – zachowanie integralności, poufności i rozliczalności danych osobowych; ponadto należy brać pod uwagę inne cechy, w szczególności dostępność, niezawodność.

   5) **DANE OSOBOWE** – jest to jakakolwiek informacja, która daje możliwość bezpośrednio lub poprzez inne cechy identyfikację osoby fizycznej w konkretnym środowisku pracy,

   6) **GIODO** – Generalny Inspektor Ochrony Danych Osobowych.

   7) **INTEGRALNOŚĆ DANYCH** – właściwość zapewniająca pewność, iż nie dokonano zmiany lub zniszczenia danych w sposób nieautoryzowany,

   8) **NARUSZENIE OCHRONY DANYCH OSOBOWYCH** – jest to zamierzone lub niezamierzone naruszenie obowiązujących środków technicznych i organizacyjnych zastosowanych w celu ochrony danych osobowych. W szczególności, gdy stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, zasady funkcjonowania oprogramowania i komunikacji

w sieci telekomunikacyjnej, które mogą wskazywać na naruszenie ochrony danych osobowych.

9) **POUFNOŚĆ** – jest to właściwość dająca pewność, że do danych osobowych ma dostęp wyłącznie osoba upoważniona.

10) **ROZLICZALNOŚĆ –** jest to właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

11) **PRZETWARZANIE DANYCH OSOBOWYCH** – są to jakiekolwiek działania wykonywane na danych osobowych, w szczególności takie jak: utrwalanie, modyfikacja, opracowanie, pozyskiwanie, gromadzenie, wgląd, przenoszenie, utrwalanie, udostępnianie, usuwanie, opracowanie, zmienianie, przechowywanie i przekazywanie, a również te, które wykonuje się w systemach informatycznych, niezależnie od formy, w jakiej wykonywane są te czynności.

12) **USTAWA** – Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 roku (Dz**.** U. z 2002 roku Nr 101,poz.926 z późn.zm.).

13) **ROZPORZĄDZENIE**- rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz.1024).

14) **URZĄD** – Urząd Gminy w Szczytnikach, 62-865 Szczytniki 139.

15) **UŻYTKOWNIK SYSTEMU** – osoba posiadająca upoważnienie, identyfikator, hasło dostępu upoważniające do przetwarzania danych osobowych w systemie informatycznym,

16) **UŻYTKOWNIK ZEWNĘTRZNY** – osoba nie będąca zatrudniona w Urzędzie Gminy w Szczytnikach, nie będąca pracownikiem Urzędu Gminy w Szczytnikach*,* posiadająca uprawnienia do przetwarzania danych osobowych w związku z wykonywaniem obowiązków na stanowisku pracy.

17) **WŁAŚCICIEL ZASOBÓW DANYCH OSOBOWYCH** – osoba kierująca komórką organizacyjną, odpowiedzialna za ochronę danych osobowych przetwarzanych w podległej komórce. Osoba ta jest zobowiązana zastosować wszelkie środki techniczne i organizacyjne zapewniające właściwą ochronę przetwarzanych danych osobowych, stosowną do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczenie danych osobowych przed ich udostępnieniem osobie nieupoważnionej, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy o ochronie danych osobowych, przed nieautoryzowaną zmianą, utratą , uszkodzeniem lub zniszczeniem.

18) **SYSTEM INFORMATYCZNY** – jest to zespół współpracujących urządzeń (urządzenia komputerowe, drukujące, łączności, wraz z okablowaniem i oprogramowaniem) programów, procedur związanych z przetwarzaniem danych osobowych oraz narzędzi programowych zastosowanych w celu przetwarzania danych osobowych.

19) **ZBIÓR DANYCH OSOBOWYCH** – dane osobowe zgromadzone w usystematyzowany sposób, pozwalający na łatwe dotarcie do konkretnej informacji lub też każdy posiadający strukturę zestaw o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony czy podzielony funkcjonalnie.

20) **ZBIÓR NIEINFORMATYCZNY** – jest to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego czy zestaw jest rozproszony lub podzielony funkcjonalnie, prowadzony w formie nieelektronicznej, poza systemem informatycznym, w szczególności w formie kartoteki, skorowidza, księgi, wykazu a także w każdej innej formie w postaci zbioru.

21) **OSOBY ZATRUDNIONE PRZY PRZETWARZANIU DANYCH OSOBOWYCH** - wszystkie osoby, w tym użytkownicy systemu informatycznego, mające z racji wykonywanych obowiązków – dostęp do danych osobowych,

22) **USUWANIE DANYCH OSOBOWYCH** – niszczenie danych osobowych lub taka ich modyfikacja, która nie pozwala na ustalenie tożsamości osoby, której dane dotyczą,

23) **OBSZAR PRZETWARZANIA DANYCH OSOBOWYCH** – budynki, pomieszczenia lub części pomieszczeń w których są przetwarzane dane osobowe, zarówno w formie papierowej, jak i w systemie informatycznym,

24) **ZABEZPIECZENIE DANYCH W SYSTEMIE** – wdrożenie i eksploatacja stosowanych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,

25) **IDENTYFIKATOR UŻYTKOWNIKA (login)** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,

26) **HASŁO** - ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym,

27) **UWIERZYTELNIANIE** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu,

§ 3. 1. Celem realizowanej polityki bezpieczeństwa jest:

1) wskazanie podstaw dla właściwego wykonania obowiązków ABI w zakresie bezpieczeństwa i prawidłowej ochrony przetwarzanych danych osobowych,
1) zgodność z prawem i wymaganiami wynikającymi z obowiązujących aktów prawnych;
2) ustawiczne kształcenie pracowników w dziedzinie bezpieczeństwa informacji;
3) ciągłe monitorowanie systemów teleinformatycznych;
4) zarządzanie prawidłowym przepływem informacji;
5) wyciąganie konsekwencji za naruszenie polityki bezpieczeństwa

§ 4. Zasady ogólne:

1. Nadrzędną zasadą przy przetwarzaniu danych osobowych w Urzędzie Gminy w Szczytnikach jest ochrona danych przed nieuprawnionym dostępem, a także przestrzeganie zapisów związanych z przetwarzaniem danych osobowych, zawartych w ustawie o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (tj. Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.), aktach wykonawczych do ustawy oraz dokumentach wewnętrznych.

2. Ochronie podlegają zarówno zasoby danych osobowych w systemach informatycznych, jak i zawarte na wydrukach, w skorowidzach, kartotekach, aktach i innych zbiorach w formie papierowej.

3. Przetwarzanie danych osobowych jest możliwe wyłącznie w celu realizacji zadań statutowych Urzędu Gminy w Szczytnikach.

4. Obieg informacji zawierających dane osobowe, pomiędzy komórkami organizacyjnymi Urzędu musi odbywać się z zachowaniem zasad „Polityki Bezpieczeństwa Informacji w Urzędzie Gminy w Szczytnikach".

5. Każdy pracownik zatrudniony w Urzędzie Gminy w Szczytnikach (bez względu na formę zatrudnienia), a w szczególności osoby mające dostęp do danych osobowych z racji wykonywanych obowiązków, jest odpowiedzialny za ochronę tych danych przed niepowołanym dostępem, w tym do natychmiastowej reakcji na wszystkie próby ich nieautoryzowanego wykorzystania.

6. Nadzór nad realizacją założeń Polityki Bezpieczeństwa Informacji w Urzędzie Gminy w Szczytnikach sprawuje Administrator Bezpieczeństwa Informacji we współpracy z kierownikami tych komórek organizacyjnych, dla których przetwarzanie danych osobowych pozostaje w zakresie obowiązków pracowników.

7. Spełniając wymogi § 6 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. (Dz. U. z 2004 r. Nr 100, poz. 1024), poziom bezpieczeństwa określa się jako **średnio wysoki, wysoki.**

8. Wobec pracowników nie przestrzegających zasad Polityki Bezpieczeństwa Informacji w Urzędzie Gminy w Szczytnikach zostanie wszczęte postępowanie wynikające z odnośnych przepisów dotyczących odpowiedzialności dyscyplinarnej, cywilnej lub karnej, w zależności od rodzaju uchybienia i skali występujących w jego następstwie zagrożeń dla danych osobowych.

§ 5. Zadania Administratora Danych Osobowych

1. ADO zobowiązany jest do podjęcia wszelkich działań, których celem jest zapewnienie prawidłowej ochrony danych osobowych, w szczególności zapewnienie przetwarzania danych ze szczególną starannością realizując następujące zasady:

    1) Przetwarzanie zgodnie z przepisami prawa,
    2) Zbieranie danych dla określonych celów i nie poddawanie dalszemu przetwarzaniu niezgodnie z tymi celami,
    3) Dane będą merytorycznie poprawne i adekwatne w stosunku do celów , w jakich są przetwarzane,
    4) Przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, jednak nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania,
    5) Zabezpieczenie środkami technicznymi i organizacyjnymi, które zapewnią, rozliczalność, poufność i integralność.

2. DO określa zakres przetwarzanych danych osobowych w wydawanych zarządzeniach, regulaminach lub w indywidualnych umowach z podmiotami zewnętrznymi, którym zlecono przetwarzanie danych osobowych.

3. ADO przetwarza dane osobowe znajdujące się w administrowanych przez niego zbiorach w określonych celach i w określonym zakresie, jeżeli:

    a) jest to konieczne do realizacji określonych prawem zadań,
    b) jest to niezbędne do osiągnięcia uzasadnionych celów,

c) w innym celu i zakresie, jeśli osoba, której przetwarzane dane dotyczą, wyrazi na to pisemną zgodę.

4. W przypadkach szczególnych cel i zakres przetwarzanych danych mogą określać inne obowiązujące przepisy szczegółowe.

§ 6. Aktualizacja dokumentacji związanej z ochroną danych osobowych.

1. Niniejsza Polityka oraz wszystkie dokumenty z nią powiązane powinny być aktualizowane wraz ze zmianami w przepisach prawa dotyczącymi ochrony danych osobowych oraz zmianami wynikającymi z organizacji i funkcjonowania Urzędu Gminy w Szczytnikach.

2. W przypadku potrzeby wynikającej ze zdarzeń związanych z naruszeniem ochrony danych osobowych należy dostosować dokumentację do właściwych procedur, które w sposób skuteczny będą chroniły dane osobowe.

3. W każdym przypadku zmiany zapisów niniejszej Polityki wymagają aktualizacji innych dokumentów powiązanych z Polityką.

4. O wszelkich zmianach w dokumentacji powinien być informowany ADO, a w przypadku konieczności również powinny być zatwierdzane przez ADO.

§ 7. Zarządzanie ochroną danych osobowych

1. Celem właściwej realizacji zamierzeń, a także skutecznej ochrony danych osobowych należy stosować następujące obowiązki:

   1) Przeszkolić pracowników uprawnionych do przetwarzania danych osobowych w zakresie zasad bezpieczeństwa ,
   2) Przypisać użytkownikom określonych cech pozwalających na ich identyfikację w systemach informatycznych, dających możliwość dostępu do przetwarzania danych osobowych odpowiednio do zakresu upoważnienia,
   3) Okresowo kontrolować użytkowników i sposób postępowania przy przetwarzaniu danych osobowych,
   4) W przypadku stwierdzonych nieprawidłowości podejmować stosowne działania celem ich wyeliminowania,
   5) Na bieżąco wdrażać nowe rozwiązania organizacyjne i techniczne, które wzmocnią bezpieczeństwo przetwarzania danych osobowych.

2. W procesie nadzoru należy szczególnie uwzględniać zabezpieczenie w zakresie integralności, poufności oraz rozliczalności przetwarzania danych osobowych.

3. W procesie zarządzania należy stosować działania, które spowodują, że pracownicy, użytkownicy zewnętrzni będą:

   1) odpowiednio przygotowani i wprowadzeni do przetwarzania danych osobowych ,
   2) zapoznają się z obowiązującymi procedurami i zasadami przetwarzania danych osobowych w Urzędzie Gminy w Szczytnikach.
   3) na bieżąco informowani o wszelkich zmianach w procedurach,

§ 8. Dokumentacja powiązana z Polityką:

1. Na dokumentację powiązaną z procesem bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy w Szczytnikach składają się:

Lp.	NAZWA DOKUMENTU	ODPOWIEDZIALNY
1.	Upoważnienie do przetwarzania danych osobowych	ABI
2.	Ewidencja osób upoważnionych do przetwarzania danych osobowych.	ABI
3.	Ewidencja zbiorów danych osobowych oraz programów stosowanych do ich przetwarzania .	ABI
4.	Opis struktur zbiorów.	ASI
5.	• Wnioski związane ze zgłoszeniem zbioru do GIODO i ich aktualizacje, • obowiązujące przepisy prawa w zakresie ochrony danych osobowych, • zarządzenia ADO, • wzór legitymacji inspektora GIODO,	ABI
6.	Protokoły: • bieżącej i okresowej kontroli prowadzonej przez ABI, • kontroli zewnętrznych,	ABI
7.	Ewidencja przenośnych nośników informacji używanych przez pracowników.	ASI

§ 9. Obowiązki związane z dostępem do danych osobowych.

1. Dostęp do zbioru danych osobowych oraz ich przetwarzania mają tylko osoby wpisane do ewidencji prowadzonej przez Administratora Bezpieczeństwa Informacji.

2. Osoby zatrudnione w Urzędzie Gminy w Szczytnikach przy przetwarzaniu danych osobowych są zobowiązane do przechowywania danych osobowych we właściwych zbiorach, nie dłużej niż jest to niezbędne dla osiągnięcia celu ich przetwarzania.

3. Osoby zatrudnione w Urzędzie Gminy w Szczytnikach przy przetwarzaniu danych osobowych przy wykorzystaniu systemów informatycznych są zobowiązane do postępowania zgodnie z **„Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych**".

§ 10. Zakazy przetwarzania danych wrażliwych.

1. W zbiorach danych administrowanych przez Urząd Gminy w Szczytnikach zabrania się przetwarzania danych ujawniających:
   a) stan zdrowia,
   b) pochodzenie rasowe lub etniczne,
   c) poglądy polityczne,
   d) przekonania religijne lub filozoficzne,
   e) przynależność wyznaniową,
   f) przynależność partyjną lub związkową,
   g) kod genetyczny,
   h) nałogi,
   i) preferencje seksualne,

chyba że wymagają tego obowiązujące przepisy prawa lub osoba, której powyższe dane dotyczą wyraziła pisemną zgodę.

§ 11. Odpowiedzialność służbowa

1. Pracownik, który:
   1) przetwarza w zbiorze danych dane osobowe:

a) do których przetwarzania nie jest upoważniony,
b) których przetwarzanie jest zabronione,
c) niezgodne z celem stworzenia zbioru danych;

2) udostępnia lub umożliwia dostęp do danych osobowych osobom nieupoważnionym;
3) nie zgłasza administratorowi bezpieczeństwa informacji zbiorów danych podlegających rejestracji;
4) nie dopełnia obowiązku poinformowania osoby, której dane dotyczą, o przysługujących jej prawach;
5) uniemożliwia osobie, której dane dotyczą, korzystanie z przysługujących jej praw – podlega odpowiedzialności karnej zgodnie z ustawą oraz sankcjami określonymi w Kodeksie pracy.

ROZDZIAŁ II
Gromadzenie danych osobowych

§ 12. Uzyskiwanie danych osobowych

1. Dane osobowe przetwarzane w Urzędzie Gminy w Szczytnikach mogą być uzyskiwane bezpośrednio od osób, których te dane dotyczą lub z innych źródeł, w granicach dozwolonych przepisami prawa.

§ 13. Wykorzystanie danych osobowych

1. Zebrane dane osobowe mogą być wykorzystane wyłącznie do celów, dla jakich były, są lub będą zbierane i przetwarzane. Po wykorzystaniu dane osobowe powinny być przechowywane w formie uniemożliwiającej identyfikację osób, których dotyczą.

2. W przypadku konieczności udostępnienia dokumentów i danych, wśród których znajdują się dane osobowe niemające bezpośredniego związku z celem udostępnienia, należy bezwzględnie dokonać anonimizacji tych danych osobowych.

ROZDZIAŁ III
Obowiązek informacyjny i odpowiedzialność

§ 14. Odpowiedzialność osób na stanowiskach kierowniczych

1. Kierownicy komórek organizacyjnych Urzędu Gminy w Szczytnikach, w których są zbieranie i przetwarzane dane osobowe, są odpowiedzialni za poinformowanie osób, których dane osobowe przetwarzają o:

   a) adresie siedziby urzędu, pod którym dane są zbierane i przetwarzane,
   b) celu zbierania danych, dobrowolności lub obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej,
   c) prawie wglądu do treści swoich danych oraz możliwości ich poprawiania.

2. W przypadku zbierania danych osobowych nie bezpośrednio od osoby, której one dotyczą, osobę tę należy dodatkowo poinformować ponadto o źródle danych oraz o uprawnieniach wynikających z art. 32 ust. 1 pkt. 7 i 8 ustawy.

3. Wzór formularza stosowanego dla spełnienia przez Urząd Gminy w Szczytnikach obowiązków, o których mowa w ust. 1 i 2, stanowi załącznik nr 4 do niniejszej polityki bezpieczeństwa informacji.

§ 15. Odpowiedzialność Administratora Danych Osobowych.

1. Administrator Danych Osobowych jest odpowiedzialny za prawidłowe przetwarzanie danych osobowych i ich ochronę zgodnie z obowiązującymi przepisami prawa. Ponadto jest obowiązany do stosowania odpowiednich procedur zapewniających prawidłowe przetwarzanie danych osobowych, a także za zapewnienie ochrony przed zmianą, uszkodzeniem zniszczeniem danych osobowych przez nieuprawnioną osobę.

2. Do kompetencji Administratora Danych Osobowych należy :
   1) Wyznaczenie Administratora Bezpieczeństwa Informacji – chyba ,że sam pełni tę funkcję,
   2) Wyznaczenie Właścicieli zasobów danych osobowych,
   3) Określenie celów o strategii działań w zakresie ochrony danych osobowych,
   4) Podział zadań i obowiązków związanych z organizacją ochrony danych osobowych.

3. Do obowiązków Administratora Danych Osobowych należy:
   1) Zapewnienie szkoleń dla pracowników w zakresie przepisów o ochronie danych osobowych oraz zagrożeń związanych z ich przetwarzaniem,
   2) Zatwierdzanie opracowanej dokumentacji związanej z ochroną danych osobowych w jednostce,
   3) Nadawanie upoważnień pracownikom oraz użytkownikom zewnętrznym do przetwarzania danych osobowych,
   4) Zapewnienie ochrony fizycznej pomieszczeń, w których są przetwarzane dane osobowe,
   5) Zapewnienie ochrony danych osobowych przetwarzanych w systemach informatycznych oraz nieinformatycznych,
   6) Zapewnienie środków na szkolenia osób funkcyjnych związanych z ochroną danych osobowych,
   7) Zapewnienie rejestracji zbiorów danych osobowych do GIODO oraz ich aktualizacji.

§ 16. Odpowiedzialność Administratora Bezpieczeństwa Informacji.

1. Administrator Danych Osobowych wyznacza Administratora Bezpieczeństwa Informacji, który nadzoruje przestrzeganie zasad ochrony danych osobowych zarówno w systemach informatycznych, jak również w zbiorach danych osobowych prowadzonych w formie papierowej i elektronicznej*,*

2. <u>Do kompetencji Administratora Bezpieczeństwa Informacji należy:</u>
   1) Określenie zasad ochrony danych osobowych,
   2) Kontrola komórek organizacyjnych Urzędu Gminy w Szczytnikach w zakresie właściwego zabezpieczenia systemów informatycznych oraz pomieszczeń, w których przetwarzane są dane osobowe,
   3) Wydawanie poleceń kierownikom komórek organizacyjnych Urzędu Gminy w Szczytnikach w zakresie bezpieczeństwa danych osobowych,
   4) Informowanie Administratora Danych Osobowych Urzędu Gminy w Szczytnikach o przypadkach naruszenia bezpieczeństwa danych osobowych,
   5) Żądanie od wszystkich pracowników Urzędu Gminy w Szczytnikach wyjaśnień w sytuacjach naruszenia bezpieczeństwa danych osobowych,
   6) Wnioskowanie o ukaranie osób winnych naruszenia przepisów i zasad dotyczących ochrony danych osobowych,

3. <u>Do obowiązków Administratora Bezpieczeństwa Informacji należy</u>:
   1) Nadzór nad wdrożeniem stosownych środków organizacyjnych, technicznych i fizycznych w celu ochrony przetwarzanych danych osobowych,

2) Nadawanie, zmienianie oraz cofanie uprawnień do przetwarzania danych osobowych na wniosek Właścicieli zasobów po akceptacji Administratora Danych Osobowych dla pracowników oraz użytkowników zewnętrznych,
3) Nadzór nad zapewnieniem przez Właścicieli zasobów danych osobowych dostosowania funkcjonalności systemów przetwarzających dane osobowe do wymagań określonych w rozporządzeniu,
4) Prowadzenie dokumentacji opisującej zastosowaną ochronę danych osobowych (Polityka oraz wynikające z niej instrukcje i procedury),
5) Zapoznawanie pracowników z przepisami i zasadami ochrony danych osobowych oraz informowanie o zagrożeniach związanych z ich przetwarzaniem oraz przeszkolenie ich w tym zakresie,
6) Reprezentowanie ADO w kontaktach z GIODO.
7) Przygotowywanie wniosków zgłoszeniowych zbiorów danych osobowych do rejestracji w Biurze GIODO.
8) Reagowanie na zgłaszane incydenty związane z naruszeniem ochrony danych osobowych oraz analizowanie ich przyczyn i kierowanie wniosków dla ADO.
9) Kontrola oraz sprawdzanie wypełnienia obowiązków technicznych i organizacyjnych związanych z ochroną danych osobowych,
10) Ścisła współpraca z Administratorem Systemu Informatycznego w zakresie przetwarzania danych osobowych w systemach informatycznych,

4. Administrator Bezpieczeństwa Informacji w zakresie realizacji swoich obowiązków, ma prawo żądania od pracowników bezzwłocznej pomocy w razie stwierdzenia naruszenia przepisów o ochronie danych osobowych, które mogłoby skutkować odpowiedzialnością karną zawartą w Rozdziale 8 Ustawy.

§ 17. Odpowiedzialność Administratora Systemów Informatycznych.

1. Obowiązki ASI pełni pracownik wyznaczony przez Administratora Danych Osobowych.
2. Do zakresu obowiązków Administratora Systemów Informatycznych należy:
   1) Zabezpieczenie systemów przetwarzania danych osobowych zgłoszonych ASI, w zależności od kategorii przetwarzanych w tym systemie danych.
   2) Zapewnienie poufności, integralności, dostępności i rozliczalności danych przetwarzanych w systemach informatycznych.
   3) Bieżący nadzór oraz zapewnianie optymalnej ciągłości działania systemu informatycznego w tym opracowanie procedur określających zarządzanie systemem informatycznym przetwarzającym dane osobowe.
   4) W przypadku powstania zagrożenia ochrony danych osobowych bezzwłoczne podjęcie stosowanych działań.
   5) Przeciwdziałanie próbom naruszenia bezpieczeństwa danych osobowych.
   6) Analiza raportów wszelkich zdarzeń w tym incydentów związanych z bezpieczeństwem systemów przetwarzania danych.
   7) Zapewnienie zgodności wszystkich wdrażanych systemów przetwarzania danych osobowych z Ustawą, Rozporządzeniem, Polityką bezpieczeństwa i Instrukcją Zarządzania Systemem Informatycznym.
   8) Instalację i konfigurację oprogramowania i sprzętu używanego do przetwarzania danych osobowych.
   9) Konfigurację i administrację oprogramowaniem systemowym i sieciowym zabezpieczającym dane osobowe przed nieupoważnionym dostępem.
   10) Nadzór nad czynnościami związanymi ze sprawdzaniem systemu pod kątem obecności szkodliwego oprogramowania.
   11) Nadzór nad systemem komunikacji w sieci komputerowej oraz przesyłaniem danych za pośrednictwem urządzeń teletransmisji.

12) Nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe.
13) Przyznawanie na wniosek Właściciela zasobów, za zgodą Administratora Danych Osobowych i zatwierdzeniu przez Administratora Bezpieczeństwa Informacji ściśle określonych praw dostępu do danych osobowych w danym systemie.
14) Udzielanie pomocy w ramach realizacji serwisu dla potrzeb Urzędu Gminy w Szczytnikach.
15) Diagnozowanie i usuwanie awarii sprzętu komputerowego oraz realizacja umów z firmami świadczącymi usługi pogwarancyjnego sprzętu komputerowego.
16) Wykonywanie i zarządzanie kopiami awaryjnymi oprogramowania systemowego (w tym danych osobowych oraz zasobów umożliwiających ich przetwarzanie) i sieciowego.
17) Wykonywanie i przechowywanie dokumentacji należącej do kompetencji ASI.
18) Nadzór nad wdrożeniem i zarządzanie aplikacjami (przeglądanie, nadawanie i odbieranie uprawnień użytkownikom, itp.), w których przetwarza się dane osobowe.
19) Wspólnie z ABI współdziałanie w wypełnianiu wniosków zgłoszeń do rejestracji zbiorów danych osobowych w części E i F.
20) Współpraca w trakcie kontroli GIODO w zakresie dotyczącym systemu informatycznego.

§ 18. Odpowiedzialność Właścicieli Zasobów Danych Osobowych.

1. Administrator Danych Osobowych wyznacza Właścicieli zasobów danych osobowych, którzy są odpowiedzialni za ochronę przypisanych i przetwarzanych zbiorów danych osobowych w podległej komórce organizacyjnej.

2. <u>Do kompetencji Właścicieli zasobów danych osobowych należy:</u>
   1) Określanie celów w jakich mają być przetwarzane dane osobowe, zakresu oraz czasu trwania przetwarzania danych osobowych.
   2) Określenie sposobu przetwarzania danych osobowych (czy w systemach informatycznych czy w zbiorach nieinformatycznych).
   3) Ustalenie, czy dane przetwarzane dla określonego celu mają charakter danych podlegających szczególnej ochronie.

3. <u>Do obowiązków Właścicieli zasobów danych osobowych należy:</u>
   1) Zapewnienie niezbędnych uprawnień do przetwarzania danych osobowych.
   2) Zapewnienie aktualności, adekwatności oraz merytorycznej poprawności danych osobowych przetwarzanych w określonym przez nich celu.
   3) Realizację obowiązku informacyjnego o przetwarzaniu danych osobowych osób, których dane osobowe są pozyskiwane.
   4) Zapewnienie na żądanie uprawnionych osób, udostępnianie informacji o przetwarzanych danych osobowych oraz podmiotach, którym zostały one udostępnione.
   5) Zapewnienie złożenia przez pracowników oświadczenia o znajomości przepisów o ochronie danych osobowych oraz zobowiązania do zachowania w tajemnicy danych osobowych oraz informacji na temat zabezpieczania danych osobowych.
   6) Zapewnienie uzyskania przez pracowników przetwarzających dane osobowe, upoważnienia do przetwarzania danych osobowych.
   7) Współpraca i informowanie ABI oraz ASI w przypadku utworzenia nowego zbioru danych osobowych ustalenie, kogo dotyczą dane osobowe, jaki jest ich zakres (np. imię i nazwisko, adres zamieszkania, NIP, PESEL itp.), cel przetwarzania oraz komu dane osobowe mają być udostępniane.
   8) Przygotowanie wniosku do rejestracji/aktualizacji zbioru do GIODO w części A-D.
   9) Wnioskowanie do Administratora Danych Osobowych o nadanie upoważnień dla pracowników podległej komórki organizacyjnej.
   10) Prowadzenie ewidencji, o której mowa w § 8 w odniesieniu do Właścicieli zasobów.

§ 19. Odpowiedzialność pracowników i użytkowników systemu.

1. W celu osiągnięcia i utrzymania wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych konieczne jest szczególne zaangażowanie ze strony każdego pracownika i użytkownika zewnętrznego w zakresie ochrony danych osobowych.

2. Pracownicy oraz użytkownicy zewnętrzni są zobowiązani do informowania o wszelkich podejrzeniach naruszenia lub zauważonych naruszeniach oraz słabościach systemu przetwarzającego dane osobowe bezpośrednio do Administratora Bezpieczeństwa Informacji.

3. Pracownicy / użytkownicy zewnętrzni są zobowiązani do:

   1) Postępowania zgodnie z Polityką.
   2) Zachowania w tajemnicy danych osobowych oraz informacji o sposobach ich zabezpieczenia.
   3) Ochrony danych osobowych oraz środków przetwarzających dane osobowe przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem.

4. Wykonywania niezbędnych działań i w procesie przetwarzania danych celem zapewnienia właściwej ich ochrony, w tym celu powinni:

   1) Przestrzegać procedur związanych z otwieraniem i zamykaniem pomieszczeń, a także z wejściem do obszarów przetwarzania danych osobowych osób nieupoważnionych.
   2) Informować Administratora Bezpieczeństwa Informacji lub pracowników ochrony o podejrzanych osobach poruszających się w obszarze przetwarzania danych osobowych,
   3) Pracownicy powinni na podstawie dokonanej identyfikacji ewentualnych zagrożeń, przedkładać Administratorowi Bezpieczeństwa Informacji projekty i propozycje nowych rozwiązań, których celem jest zwiększenie poziomu bezpieczeństwa ochrony danych osobowych.

§ 20. Odpowiedzialność za naruszenie zasad ochrony danych osobowych.

1. Rozdział 8 Ustawy a także art. 266 Kodeksu Karnego określa odpowiedzialność pracownika w przypadku naruszenia ochrony danych osobowych.

2. Zgodnie z art. 100 §2 pkt 5 Kodeksu Pracy – obowiązkiem pracownika jest przestrzeganie tajemnic prawnie chronionych określonych w odrębnych przepisach.

3. Ciężkie naruszenie obowiązków pracowniczych może skutkować rozwiązaniem umowy o pracę z winy pracownika bez wypowiedzenia umowy o pracę.

§ 21. Szkolenia

1. Przed rozpoczęciem przetwarzania danych osobowych każdy pracownik, stażysta, praktykant powinien zostać przeszkolony przez Administratora Bezpieczeństwa Informacji. Szkolenie powinno obejmować następujące zagadnienia:

   1) obowiązujące przepisy w zakresie o ochronie danych osobowych,
   2) procedury oraz zasady przetwarzania danych osobowych,
   3) procedury dotyczące bezpiecznego przetwarzania danych osobowych w systemach informatycznych.
   4) zasady użytkowania oprogramowania, urządzeń i systemów informatycznych służących do przetwarzania danych osobowych.
   5) rodzaje zagrożeń jakie mogą być związane z przetwarzaniem danych osobowych w systemach informatycznych,
   6) zasady dostępu do pomieszczeń, w których przetwarzane są dane osobowe,

7) zasady i sposób postępowania w przypadku naruszenia ochrony danych osobowych lub systemu informatycznego.
8) odpowiedzialność w przypadku naruszenia ochrony danych osobowych.

2. Szkolenia należy przeprowadzać nie rzadziej niż dwa razy do roku ,a także każdorazowo w przypadku osoby nowozatrudnionej, stażystów i praktykantów.

§ 22. Zgoda na przetwarzanie danych osobowych

1. Materiały dotyczące innej niż ustawowa działalność Urzędu Gminy w Szczytnikach mogą być wysyłane tylko do tych osób, które wcześniej wyraziły zgodę na piśmie na przetwarzanie ich danych osobowych w tym celu.

2. Kandydaci do pracy w Urzędzie Gminy w Szczytnikach w procesie rekrutacji są zobowiązani podpisać pisemną zgodę na przetwarzanie ich danych osobowych.

3. Dokumenty złożone w celu określonym w ust. 2 są przechowywane w komórce organizacyjnej, która przetwarza te dane i są włączane do akt osobowych pracownika.

4. Wzór formularza stosowanego dla spełnienia przez Urząd Gminy w Szczytnikach obowiązków wymienionych w ust. 1 i 2, stanowi załącznik 4 do niniejszej polityki bezpieczeństwa informacji.

ROZDZIAŁ IV
Udzielanie informacji o przetwarzaniu danych osobowych

§ 23. Kontrola własnych danych osobowych

1. Osobom, których dane osobowe przetwarza się w zbiorze danych Urzędu Gminy w Szczytnikach, przysługuje zgodnie z Ustawą, prawo kontroli ich danych osobowych, a w szczególności prawo do uzyskania wyczerpujących informacji na temat tych danych.

2. Każda osoba, która wystąpi z wnioskiem o otrzymanie informacji, powinna otrzymać odpowiedź w formie pisemnej, w terminie nie dłuższym niż 30 dni od daty wpływu wniosku do Urzędu Gminy w Szczytnikach .

3. Informacji, o której mowa w ust. 1, udziela się na formularzu stanowiącym załącznik nr 5 do niniejszej polityki bezpieczeństwa informacji.

§ 24. Obowiązek uzupełniania danych

W przypadku gdy dane osoby są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są zbędne do realizacji celu, dla którego zostały zebrane, Administrator Danych Osobowych jest zobowiązany do ich uzupełnienia, uaktualnienia, sprostowania lub usunięcia.

ROZDZIAŁ V
Zbiory danych osobowych - rejestracja w Biurze GIODO

§ 25. Obowiązki kierowników komórek organizacyjnych

1. Kierownicy komórek organizacyjnych Urzędu Gminy w Szczytnikach oraz pracownicy na samodzielnych stanowiskach pracy, w których przetwarzane są dane osobowe, są zobowiązani do zgłoszenia ABI informacji na temat:

a) planowanego założenia nowych zbiorów danych osobowych wymagających rejestracji,
b) wnoszonych zmian do zbiorów już zarejestrowanych.

2. Ostateczną decyzję o zarejestrowaniu zbioru w Krajowym Rejestrze Zbiorów prowadzonych przez GIODO podejmuje ABI,

3. ABI przygotowuje projekt zgłoszenia zbioru, powiadamia ADO o potrzebie zgłoszenia lub aktualizacji zbioru, po akceptacji ADO zgłasza zbiór do Krajowego Rejestru Zbiorów,

4. Po zgłoszeniu zbioru ABI dokonuje uzupełnień w wykazie zbiorów, który jest prowadzony przez ABI,

5. Zgłoszeniu podlegają wszystkie zbiory prowadzone w systemie informatycznym lub w sposób tradycyjny za wyjątkiem tych zbiorów, które są zawarte w art. 43 ust.1 ustawy o ochronie danych osobowych,

6. Rejestracji można dokonać wypełniając wniosek w formie papierowej lub z wykorzystaniem platformy e-giodo znajdującej się na stronie www.giodo.gov.pl

ROZDZIAŁ VI
Ochrona przetwarzania danych osobowych

§ 26. Zasada szczególnej staranności

1. Każdy pracownik dla właściwego sposobu i zasad przetwarzania danych osobowych zobowiązany jest do zachowania szczególnej staranności przy przetwarzaniu danych osobowych, a w szczególności:
   1) stosowanie wszelkich metod zabezpieczeń wynikających z Polityki,
   2) zabezpieczenie wydruków elektronicznych a także tych , które mogą być tworzone w trakcie kserowania, kopiowania,
   3) udzielanie informacji zawierających dane osobowe tylko osobom, podmiotom uprawnionym,
   4) prowadzenie rozmów telefonicznych w sposób bezpieczny, na zasadzie by osoba nieuprawniona nie pozyskiwała informacji jeżeli nie jest ona dla niej przeznaczona,

§ 27. Miejsca i pomieszczenia przeznaczone do przetwarzania danych osobowych

1. Dane osobowe można przetwarzać wyłącznie w miejscach bezpiecznych i będących pod właściwym nadzorem osoby, która przetwarza i nadzoruje przetwarzanie danych osobowych,

2. Pomieszczenia bezpieczne to takie, które nie są pozostawione bez nadzoru odpowiedzialnego pracownika,
   1) pomieszczenie biurowe,
   2) archiwum,
   3) pomieszczenie, w którym znajdują się zbiory danych osobowych ,

3. Pomieszczenia, w których są przetwarzane dane osobowe są zamykane na klucz podczas nieobecności osoby upoważnionej/nadzorującej,

4. Obiekt jak i pomieszczenia są zabezpieczone fizycznie zgodnie z obowiązującymi procedurami i potrzebami.

5. W przypadku potrzeby należy zastosować dodatkowe zabezpieczenie fizyczne takie jak: kraty, rolety antywłamaniowe, szczególnie w przypadku pomieszczeń usytuowanych na parterze budynku,

6. Pomieszczenie powinno być wyposażone w sprzęt p.pożarowy,

7. W przypadku wykonywania prac naprawczych, remontowych, montażowych przez firmy zewnętrzne, pomieszczenie jest pod stałym nadzorem osoby upoważnionej-pracownika urzędu,

8. Przechowywanie kopii zapasowych powinno być realizowane w innym pomieszczeniu niż znajdują się zasoby podstawowe,

9. Każdy pracownik w przypadku zauważenia uchybień w zabezpieczeniu pomieszczenia zobowiązany jest niezwłocznie poinformować o tym fakcie ABI.

§ 28. Przechowywanie imiennych upoważnień do przetwarzania danych osobowych

1. Administrator Danych Osobowych Urzędu Gminy w Szczytnikach zobowiązany jest do wydawania, ewidencjonowania i przechowywania imiennych upoważnień do przetwarzania danych osobowych oraz cofniętych upoważnień. Upoważnienie może zostać wydane na czas określony lub do odwołania. Wzory formularza upoważnienia i formularza cofnięcia upoważnienia stanowią załącznik nr 6 do niniejszej polityki bezpieczeństwa informacji.

2. ADO Urzędu Gminy w Szczytnikach zobowiązany jest do zbierania, ewidencjonowania i przechowywania:

   a) oświadczeń osób przetwarzających dane osobowe o zachowaniu w tajemnicy danych, z którymi mają styczność oraz środkach bezpieczeństwa stosowanych przy przetwarzaniu danych osobowych. Wzór formularza oświadczenia stanowi załącznik nr 7 do niniejszej Polityki,

   b) oświadczeń osób zatrudnianych na podstawie umowy zlecenia, umowy o dzieło lub innej umowy cywilnej o zachowaniu tajemnicy. Wzór formularza oświadczenia stanowi załącznik nr 8 do niniejszej Polityki,

   c) porozumień zawartych z osobami zatrudnionymi przy przetwarzaniu danych osobowych w zakresie wykorzystania oddanego im do dyspozycji sprzętu informatycznego, oprogramowania oraz zasobów sieci informatycznej. Wzór formularza porozumienia stanowi załącznik nr 9 do niniejszej polityki bezpieczeństwa informacji.

3. Brak ważnego upoważnienia, o którym mowa w ust. 1 oraz brak podpisanych oświadczeń lub porozumienia, o których mowa w ust. 2, uniemożliwia powierzenie pracownikowi wykonywania zadań i obowiązków związanych z przetwarzaniem danych osobowych.

4. ABI prowadzi dla pracowników szkolenia z zakresu obowiązujących przepisów prawa i procedur zawartych w Polityce,

5. Pracownik po przeszkoleniu podpisuje oświadczenie o zapoznaniu się z przepisami i procedurami. Wzór oświadczenia stanowi załącznik nr 10 do Polityki Bezpieczeństwa.

6. Upoważnienie oraz oświadczenie jest przechowywane w aktach osobowych, oraz w dokumentacji ABI,

§ 29. Ewidencja osób upoważnionych

1. ABI prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych ,

2. Ewidencja jest prowadzona przez ABI na bieżąco i starannie,
3. Ewidencja zawiera: Wzór stanowi załącznik Nr 11 do Polityki Bezpieczeństwa.
   - Lp.
   - Imię i nazwisko osoby upoważnionej ,
   - Stanowisko
   - Komórka organizacyjna
   - Data przeszkolenia
   - Nr upoważnienia imiennego
   - Data nadania upoważnienia,
   - Data ustania upoważnienia,
   - Zakres upoważnienia,
   - Login/hasło użytkownika,

ROZDZIAŁ VII
Zasady udostępniania danych osobowych

§ 30. Osoby uprawnione do wglądu do danych osobowych

Administrator Danych Osobowych udostępnia dane osobowe przetwarzane we własnych zbiorach tylko osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.

§ 31. Tryb udostępniania danych osobowych

1. Zbiory danych osobowych podmiotom zewnętrznym udostępnia się na pisemny, umotywowany wniosek, chyba że odrębne przepisy prawa stanowią inaczej.

2. Wniosek o udostępnienie danych osobowych powinien zawierać informacje, umożliwiające wyszukanie żądanych danych osobowych w zbiorze oraz wskazywać ich zakres i przeznaczenie.

3. W przypadku udostępniania danych osobowych na zewnątrz ABI dokonuje oceny sposobu przygotowania danych, a także analizuje sposób i prawidłowość przygotowania danych do udostępnienia,

4.. Wniosek o udostępnienie danych osobowych jest rozpatrywany przez ABI, który jednocześnie prowadzi ewidencję wniosków.

4. Decyzję w sprawie udostępnienia danych podejmuje ABI.

5. Dane osobowe przekazywane na zewnątrz są przekazywane listem poleconym za zwrotnym poświadczeniem odbioru lub innym bezpiecznym sposobem określonym wymogami prawa lub umową,

6. Fakt udostepnienia danych należy udokumentować pisemnie poprzez wykonanie pisma przewodniego lub notatki urzędowej,

§ 32. Odmowa udostępnienia danych osobowych

1. Administrator Danych Osobowych może odmówić udostępnienia danych osobowych, jeżeli spowodowałoby to:

   1) ujawnienie wiadomości zawierających informacje niejawne,
   2) zagrożenie dla obronności lub bezpieczeństwa państwa, życia i zdrowia ludzi lub bezpieczeństwa i porządku publicznego,

3) zagrożenie dla podstawowego interesu gospodarczego lub finansowego państwa,
4) istotne naruszenie dóbr osobistych osób, których dane dotyczą, lub innych osób oraz jeżeli dane osobowe nie mają istotnego związku ze wskazanymi we wniosku motywami działania wnioskodawcy.

§ 33. Powierzenie przetwarzania danych osobowych

1. Administrator Danych Osobowych może powierzyć przetwarzanie danych osobowych innemu podmiotowi wyłącznie w drodze umowy zawartej w formie pisemnej na zasadach określonych w art. 31 ust. 1 uodos,

2. Powierzenie danych występuje wówczas, gdy podmiot zewnętrzny ma dostęp do danych osobowych przetwarzanych przez Urząd,

3. Podmiot, o którym mowa w ust. 1, jest zobowiązany do zastosowania środków organizacyjnych i technicznych, zabezpieczających zbiór przed dostępem osób nieupoważnionych na zasadach określonych w przepisach o ochronie danych osobowych.

4. Podmiot, o którym mowa w ust. 1, jest zobowiązany przetwarzać dane osobowe wyłącznie w zakresie określonym w umowie.

5. W przypadkach opisanych w ust. 1– 3 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.

5. Przy kontroli zgodności przetwarzanych danych przez upoważniony przez administratora danych osobowych podmiot, o którym mowa w ust. 1, stosuje się odpowiednio przepisy art. 14–19 ustawy.

6. Umowa powierzenia danych osobowych, o której mowa w ust. 1 powinna zawierać następujące warunki i zawierać:

   1) cel i zakres przetwarzania danych osobowych,
   2) sposoby zabezpieczenia danych i zasady ich przetwarzania ,
   3) zasady organizacyjne i techniczne jakie powinien spełnić podmiot, któremu powierzono przetwarzanie danych osobowych,
   4) odpowiedzialność podmiotu, któremu powierzono dane osobowe za nieprawidłowe przetwarzanie danych osobowych,
   5) prawo do kontroli podmiotu, któremu powierzono dane osobowe przez przedstawiciela Urzędu,

7. Projekt umowy powierzenia przygotowuje ABI.

8. ABI przed powierzeniem danych osobowych dokonuje kontroli stanu zabezpieczeń w jednostce , której dane osobowe będą powierzone .

Rozdział VIII

Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

§ 34. 1. Administrator Danych Osobowych jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych a w szczególności:

1) zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym.
2) zapobiegać przed zabraniem danych przez osobę nieuprawnioną.
3) zapobiegać przetwarzaniu danych z naruszeniem ustawy oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych.

2. Do zastosowanych środków technicznych i organizacyjnych w Urzędzie Gminy w Szczytnikach należą:

1) Przetwarzanie danych osobowych w wydzielonych pomieszczeniach położonych w strefie administracyjnej, o której mowa w zał. 1, klucze od pomieszczeń znajdują się w posiadaniu upoważnionych pracowników,

2) Zabezpieczenie wejścia do pomieszczeń, o których mowa w zał. 1 w postaci zamykania pomieszczeń na czas nieobecności pracowników upoważnionych,

3) Szczególne zabezpieczenie centrum przetwarzania danych – pomieszczenie o nr 4⁄1 (komputer centralny, serwerownia) w postaci podwójnych drzwi (I drzwi wejściowe do pomieszczenia - dostęp upoważnieni pracownicy urzędu, II drzwi do serwera, routera i pozostałych elementów – dostęp ograniczony do dwóch osób: Administratora Danych i osoby upoważnionej zajmującej się obsługą informatyczną w gminie),

4) Wyposażenie pomieszczeń w szafy zamykane dające gwarancję bezpieczeństwa dokumentacji, klucze od szaf po zakończeniu pracy przekazywane są do sekretariatu Wójta i przechowywane w szafie metalowej w gabinecie Administratora Danych Osobowych - dostęp ograniczony do dwóch osób: Administratora Danych i upoważniony pracownik sekretariatu,

5) Klucze od pomieszczeń i szaf wykonane są w dwóch egzemplarzach jeden w dyspozycji upoważnionego pracownika, drugi zdeponowany w zamkniętej kopercie w szafie metalowej w gabinecie Administratora Danych- dostęp ograniczony do dwóch osób: Wójta i upoważniony pracownik sekretariatu,

6) Wejście główne do budynku urzędu zabezpieczone jest w postaci dwóch zamków kluczowych, klucze sporządzone są w trzech kompletach będących w posiadaniu: Administratora Danych i osób upoważnionych, na każdy komplet kluczy prowadzona jest ewidencja w której wskazane są osoby będące aktualnie w ich posiadaniu, przekazanie kluczy między pracownikami upoważnionymi odbywa się po stosownym wpisie w ewidencji.

7) Wejście zapasowe, zamknięte na stałe, klucze zdeponowane w szafie metalowej u Wójta,

3. Niezależnie od niniejszych zasad opisanych w dokumencie "Polityka bezpieczeństwa informacji w Urzędzie Gminy w Szczytnikach" 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.

Rozdział IX

Postępowanie w przypadku naruszenia ochrony danych osobowych lub podejrzenia naruszenia ochrony danych osobowych

§ 35. 1. Pracownicy Urzędu są zobowiązani do szczególnej staranności przy przetwarzaniu danych osobowych.

2. Pracownicy każdorazowo przed przystąpieniem do pracy są zobowiązani do dokonania oceny oględzin stanowiska pracy pod kątem, czy nie dokonano jakichkolwiek nieuprawnionych działań związanych z ochroną danych osobowych przez osoby nieuprawnione.

§ 36. 1. Na fakt naruszenia lub próby naruszenia zabezpieczeń systemu informatycznego mogą wskazywać:

1) Stan stacji roboczej-zdarzenia losowe (np. brak zasilania, pożar, problemy z uruchomieniem, itp.).
2) Wszelkiego rodzaju różnice w funkcjonowaniu systemu programu (np. komunikaty informujące o błędach, brak dostępu do funkcji programu, nieprawidłowości w wykonywanych operacjach),
3) Różnice w zawartości zbioru danych osobowych (np. brak lub nadmiar danych).
4) Jakości komunikacji w sieci telekomunikacyjnej (gwałtowne opóźnienia lub przyspieszenia wykonywanych czynności),
5) Próba nieuprawnionego logowania lub inny sygnał wskazujący na próbę lub działanie wskazujące na nielegalny dostęp do systemu,
6) Stwierdzenie braku sprzętu informatycznego, jego części lub nośników zewnętrznych zawierających dane osobowe (wydruki, pamięć zewnętrzna, płyty CD, dysk twardy ,itp.),
7) Naruszenie lub próba naruszenia integralności, poufności lub rozliczalności danych i systemu,
8) Niezamierzona zmiana lub utrata danych zapisanych na nośnikach jako kopie zapasowe,
9) Inne sytuacje nadzwyczajne.

§ 37. 1. W przypadku stwierdzenia naruszenia lub próby naruszenia:

a) zabezpieczenia systemu informatycznego,
b) technicznego stanu urządzeń,
c) zawartości zbioru danych osobowych,
d) ujawnienia metody pracy lub sposobu działania programu,
e) jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych,
f) innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np.: zalanie, pożar, itp.)

osoba zatrudniona przy przetwarzaniu danych osobowych zobowiązana jest do :

a) niezwłocznego powiadomienia o powyższym zdarzeniu ABI,
b) zablokowania komputera w sposób uniemożliwiający dalszą pracę w systemie - utrzymania sprzętu w taki sposób, aby uniemożliwić dostęp do niego innym osobom,
c) zabezpieczenia materiałów, dokumentów aby uniemożliwić dostępu osobom nieuprawnionym i dalszym stratom,
d) udokumentować wstępnie zaistniałe naruszenie,
e) nie opuszczania bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora Bezpieczeństwa lub osoby upoważnionej.

2. Administrator Bezpieczeństwa Informacji i osoba przełożona pracownika przejmują nadzór nad pracą w systemie odsuwając jednocześnie od pracy pracownika, który dotychczas pracował na stanowisku, na którym stwierdzono naruszenie zabezpieczenia danych.

3. Administrator Bezpieczeństwa Informacji analizuje przyczyny i stopień naruszenia systemu zabezpieczeń, ocenia sytuację, dokonuje oględzin stanowiska pracy, pomieszczenia, określa skutki, na którym doszło do naruszenia lub próby naruszenia danych osobowych oraz podejmuje dalsze działania stosowne do potrzeb i zaistniałej sytuacji.
4. W przypadkach stwierdzenia naruszenia lub próby naruszenia zabezpieczeń ABI niezwłocznie powiadamia o tym Administratora Danych, a także zabezpiecza systemy informatyczne przed dalszym ich naruszaniem.

5. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych. Administrator Bezpieczeństwa lub osoba go zastępująca:
   1) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy Urzędu Gminy.
   2) może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem.
   3) rozważa celowość i potrzebę powiadamia o zaistniałym naruszeniu Administratora Danych.
   4) nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba, ze specjalistami spoza Urzędu.

6. Administrator Bezpieczeństwa dokumentuje zaistniały przypadek naruszenia lub próby naruszenia oraz sporządza raport (załącznik nr 12 do niniejszej Polityki), który powinien zawierać w szczególności:
   1) wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem,
   2) lokalizacja zdarzenia (określenie czasu i miejsca naruszenia i powiadomienia),
   3) określenie rodzaju naruszenia oraz okoliczności towarzyszących,
   4) wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania,
   5) wstępną ocenę przyczyn występowania naruszenia,
   6) ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.

7. Raport, o którym mowa w ust. 6, ABI niezwłocznie przekazuje Administratorowi Danych, a w przypadku jego nieobecności osobie uprawnionej.

8. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu lub próbie naruszenia ABI zasięga niezbędnych opinii i proponuje postępowanie naprawcze, a w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.

9. Zaistniałe naruszenie lub próba naruszenia może stać się przedmiotem szczegółowej, zespołowej analizy prowadzonej przez Kierownictwo Urzędu Gminy, Administrator Bezpieczeństwa Informacji, Pełnomocnika ds. Ochrony Informacji Niejawnych.

10. Analiza, o której mowa w ust. 9, powinna zawierać wszechstronną ocenę zaistniałego naruszenia, wskazanie, odpowiedzialnych, wnioski co do ewentualnych przedsięwzięć proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

Rozdział X
Zbiory danych osobowych

§ 38. 1. W rozumieniu Ustawy o ochronie danych osobowych zbiorem danych osobowych jest każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

2. Dane osobowe przetwarzane są w zbiorach z wykorzystaniem systemów informatycznych lub w kartotekach ewidencyjnych.

3. Zbiory danych osobowych są zlokalizowane w pomieszczeniach Urzędu.

4. Wykaz systemów i aplikacji związanych z przetwarzaniem danych osobowych oraz struktury zbiorów danych osobowych i opis struktur wskazujący zawartość poszczególnych pól powinien być prowadzony przez Administratora Systemów informatycznych.

4. Administrator Systemów Informatycznych prowadzi dokumentację związaną ze sposobem i zasadami współpracy i przepływu danych pomiędzy poszczególnymi systemami.

6. ABI jest zobowiązany do bieżącego zgłaszania zbiorów do Krajowego Rejestru Zbiorów prowadzonego przez Generalnego Inspektora Ochrony Danych Osobowych, a także ich aktualizacji w przypadku takiej potrzeby.

§ 39. Ochrona danych osobowych w zbiorach nieinformatycznych

1. Zbiory i dane przetwarzane w tych zbiorach to takie dane, które są przetwarzane w formie tradycyjnej bez wykorzystywania systemów informatycznych .

2. Dane osobowe w formie dokumentów i wydruków podlegają ochronie, a także odpowiedniemu ich zabezpieczeniu w meblach biurowych zamykanych na klucz.

3. Dokumenty, wydruki podlegające zniszczeniu należy zniszczyć skutecznie, tak by osoba nieuprawniona nie mogła zapoznać się z treścią tych dokumentów lub wydruków.

4. W trakcie niszczenia dokumentów należy przestrzegać przepisów Ustawy o narodowym Zasobie Archiwalnym i przepisów wykonawczych do ustawy.

§ 40. Kontrole prowadzone przez Generalnego Inspektora Ochrony danych Osobowych

1. Zgodnie z art. 12 Ustawy o ochronie danych osobowych, Generalny Inspektor ochrony Danych Osobowych ma uprawnienia do kontroli przetwarzania danych osobowych z przepisami o ochronie danych osobowych, a także wydawania decyzji administracyjnych i rozpatrywania skarg w sprawach wykonywania przepisów o ochronie danych osobowych.

2. W celu wykonywania zadań, o których mowa w pkt.1 upoważnieni pracownicy Biura mają prawo:

    1) wstępu, w godzinach od 6°° do 22°°, za okazaniem imiennego upoważnienia i legitymacji służbowej, do pomieszczenia, w którym zlokalizowany jest zbiór danych, oraz pomieszczenia, w którym przetwarzane są dane poza zbiorem danych, i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z ustawą,
    2) żądać złożenia pisemnych lub ustnych wyjaśnień oraz wzywać i przesłuchiwać osoby w zakresie niezbędnym do ustalenia stanu faktycznego,
    3) wglądu do wszelkich dokumentów i wszelkich danych mających bezpośredni związek z przedmiotem kontroli oraz sporządzania ich kopii,

4) przeprowadzania oględzin urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych,
5) zlecać sporządzanie ekspertyz i opinii.

3. Administrator Danych jest zobowiązany do umożliwienia przeprowadzenia kontroli.

4. W toku kontroli kontrolujący ma prawo wglądu do zbioru danych osobowych za pośrednictwem Administratora Bezpieczeństwa Informacji.

5. Kontrolę przeprowadza się po okazaniu imiennego upoważnienia wraz z legitymacją służbową.

6. Imienne upoważnienie powinno zawierać:
   1) wskazanie podstawy prawnej przeprowadzenia kontroli,
   2) oznaczenie organu kontroli,
   3) imię i nazwisko, stanowisko służbowe osoby upoważnionej do przeprowadzenia kontroli oraz numer jej legitymacji służbowej,
   4) określenie zakresu przedmiotowego kontroli,
   5) oznaczenie podmiotu objętego kontrolą albo zbioru danych, albo miejsca poddawanego kontroli,
   6) wskazanie daty rozpoczęcia i przewidywanego terminu zakończenia kontroli,
   7) podpis Generalnego Inspektora,
   8) pouczenie kontrolowanego podmiotu o jego prawach i obowiązkach,
   9) datę i miejsce wystawienia imiennego upoważnienia.

7. Z czynności kontrolnych inspektor sporządza protokół, którego jeden egzemplarz doręcza kontrolowanemu.

8. Protokół podpisują inspektor i kontrolowany Administrator Danych .

9. W razie odmowy podpisania protokołu inspektor czyni o tym wzmiankę w protokole , a wówczas można w terminie 7 dni , przedstawić swoje stanowisko na piśmie Generalnemu Inspektorowi Ochrony Danych Osobowych.

Rozdział XI
Postanowienia końcowe

§ 41. W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tj. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz przepisy wykonawcze do Ustawy.

Załącznik nr 1
do Polityki Bezpieczeństwa Informacji

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe , stanowiących strefę administracyjną.

Dane osobowe przetwarzane są w Urzędzie Gminy w Szczytnikach, w budynku znajdującym się w Szczytnikach, w pomieszczeniu zajmowanym przez referaty i samodzielne stanowiska w sposób tradycyjny i za pomocą systemów informatycznych.

1) REFERAT INFRASTRUKTURY I OCHRONY ŚRODOWISKA
2) SAMODZIELNE STANOWISKO DS. PROFILAKTYKI I ROZWIĄZYWANIA PROBLEMÓW ALKOHOLOWYCH
2) REFERAT FINANSÓW / SKARBNIK GMINY
3) WÓJT GMINY / SEKRETARIAT URZĘDU / Z-CA WÓJTA GMINY
4) REFERAT ADMINISTRACYJNO – ORGANIZACYJNY / PRZEWODNICZĄCY RADY/ RADCA PRAWNY
5) REFERAT FINANSÓW - PODATKI/ BIURO OBSŁUGI RADY
6) REFERAT SPRAW OBYWATELSKICH

Lp.	**Nazwa jednostki organizacyjnej - adres - budynek**	**Nazwa Referatu / samodzielnego stanowiska Nr pomieszczenia przetwarzania danych osobowych**
1.	**Urząd Gminy w Szczytnikach** 62-865 Szczytniki 139	➢ **Referat Infrastruktury i Ochrony Środowiska – 2** ➢ **Samodzielne stanowisko ds. profilaktyki i rozwiązywania problemów alkoholowych – 2** ➢ **Pomieszczenie służbowe/archiwum – 2/1** ➢ **Referat Finansów/Skarbnik Gmin – 3** ➢ **Wójt Gminy/ Sekretariat/Z-ca Wójta – 4** ➢ **Pomieszczenie służbowe/serwerownia – 4/1** ➢ **Referat Administracyjno-Organizacyjny /Przewodniczący Rady Gminy/Radca prawny – 5** ➢ **Referat Finansów-Podatki/Biuro Rady Gminy – 6** ➢ **Referat Spraw obywatelskich – 7** ➢ **Pomieszczenie służbowe/Archiwum – 7/1**

Załącznik nr 2

do Polityki Bezpieczeństwa Informacji

Wykaz zbiorów danych osobowych przetwarzanych elektronicznie lub w inny sposób ze wskazaniem programów zastosowanych do przetwarzania danych osobowych i wykazem pracowników przetwarzających.

Lp.	Nazwa zbioru/nr księgi rejestrowej – data zarejestrowania w GIODO	Sposób gromadzenia	Nazwa programu	Pracownicy przetwarzający	Lokalizacja bazy danych/ nr pomieszczenia przetwarzania danych
1.	Ewidencja ludności i dowody osobiste gminy Szczytniki 043797 z dnia 22.01.2001r.	Forma papierowa i elektroniczna	System Ewidencji Ludności PB ewid.	Referat Spraw Obywatelskich	Serwerownia – 4⁄1 UG w Szczytnikach - 7
2.	Urząd Stanu Cywilnego w Szczytnikach 043020 z dnia 12.01.2001r.	Forma papierowa i elektroniczna	Komputerowy System Rejestracji Aktów Stanu Cywilnego USC PB_USC	Referat Spraw Obywatelskich	Serwerownia – 4⁄1 UG w Szczytnikach - 7
3.	Ewidencja przedpoborowych i poborowych w UG w Szczytnikach 043008 z dnia 12.01.2001r.	Forma papierowa i elektroniczna	System Ewidencji Ludności PB ewid.	Referat Spraw Obywatelskich	Serwerownia – 4⁄1 UG w Szczytnikach - 7
4.	Rejestr świadczeń osobistych i rzeczowych na rzecz obrony w Urzędzie Gminy Szczytniki 043008 z dnia 12.01.2001r.	Forma papierowa i elektroniczna	System Ewidencji Ludności PB ewid.	Referat Spraw Obywatelskich	Serwerownia – 4⁄1 UG w Szczytnikach - 7
5.	**Pracownicy urzędu gminy, osoby ubiegające się o pracę**	Forma papierowa i elektroniczna	Zintegrowany System informatyczny dla administracji - Płace, Płatnik ZUS	Referat Finansów Referat Administracyjno-Organizacyjny	Serwerownia – 4⁄1 UG w Szczytnikach - 3, 5
6.	**Radni Gminy i Sołtysi**	Forma papierowa	Zintegrowany System informatyczny dla administracji	Biuro Rady Gminy Referat Finansów - podatki	UG w Szczytnikach – 6
7.	Ewidencja skarg i wniosków Gminy Szczytniki	Forma papierowa	Zintegrowany System informatyczny dla administracji	Referat Administracyjno-Organizacyjny	UG w Szczytnikach – 5

	024181 z dnia 26.07.2000r.				
8.	Oświadczenia o stanie majątkowym radnych Gminy Szczytniki 024179 z dnia 26.07.2000r.	Forma papierowa	Zintegrowany System informatyczny dla administracji	Referat Administracyjno-Organizacyjny /Biuro Rady Gminy	UG w Szczytnikach – 6
9.	**Dzierżawcy i użytkownicy wieczyści gruntów gminnych**	Forma papierowa	Zintegrowany System informatyczny dla administracji PODATKI – GOMiG (Gospodarka Odpadami Miasta i Gminy)	Referat Infrastruktury i Ochrony Środowiska	UG w Szczytnikach – 2
10.	**Najemcy lokali mieszkalnych**	Forma papierowa		Referat Infrastruktury i Ochrony Środowiska	UG w Szczytnikach – 2
11.	Rejestr decyzji o w o warunkach zabudowy i zagospodarowania terenu. 032426 z dnia 28.09.2000r.	Forma papierowa		Referat Infrastruktury i Ochrony Środowiska	UG w Szczytnikach – 2
12.	Ewidencja pozwoleń na wycięcie drzew i krzewów 024174 z dnia 26.07.2000r.	Forma papierowa		Referat Infrastruktury i Ochrony Środowiska	UG w Szczytnikach – 2
13.	Ewidencja zatwierdzonych projektów podziału nieruchomości i rozgraniczeń nieruchomości 042962 z dnia 12.01.2001r.	Forma papierowa		Referat Infrastruktury i Ochrony Środowiska	UG w Szczytnikach – 2
14.	Ewidencja miejscowości, ulic i adresów gminy Szczytniki 127197 z dnia 21.12.2012r.	Forma papierowa		Referat Infrastruktury i Ochrony Środowiska	UG w Szczytnikach – 2
15.	Ewidencja właścicieli psów agresywnych 024170 z dnia 26.07.2000r.	Forma papierowa		Referat Infrastruktury i Ochrony Środowiska	UG w Szczytnikach – 2
16.	**Płatnicy opłaty za usuwanie odpadów komunalnych**	Forma papierowa I elektroniczna	Zintegrowany System informatyczny dla administracji PODATKI – GOMiG (Gospodarka Odpadami Miasta i Gminy)	Referat Infrastruktury i Ochrony Środowiska	Serwerownia – 4⁄1 UG w Szczytnikach – 2, 3, 6
17.	**Wnioskujący o wydanie zezwolenie na uprawę maku**	Forma papierowa		Referat Infrastruktury i Ochrony Środowiska	UG w Szczytnikach – 2

18.	**Odbiorcy usługi dostarczania wody i odbioru ścieków**	Forma papierowa I elektroniczna	Zintegrowany System informatyczny dla administracji Woda i Wodnik	Referat Infrastruktury i Ochrony Środowiska Referat Finansów	Serwerownia – 4⁄1 UG w Szczytnikach – 2,3
19.	Ewidencja właścicieli gruntów (nieruchomości i gospodarstw rolnych), budynków, podatników i opłat lokalnych Gminy Szczytniki 024169 z dnia 26.07.2000r. Podatnicy podatku rolnego i leśnego Podatnicy podatku od nieruchomości . Podatnicy podatku drogowego	Forma papierowa i elektroniczna	Zintegrowany system informatyczny dla administracji - Podatki	Referat Infrastruktury i Ochrony Środowiska Referat Finansów	Serwerownia – 4⁄1 UG w Szczytnikach - 2, 3, 6
20.	**Wnioskujący o zwrot podatku akcyzowego za paliwo rolnicze**	Forma papierowa i elektroniczna	Zintegrowany system informatyczny dla administracji - Podatki	Referat Finansów	Serwerownia – 4⁄1 UG w Szczytnikach - 6
21.	Ewidencja zamówień publicznych 058672 z dnia 26.07.2000r.	Forma papierowa		Referat Infrastruktury i Ochrony Środowiska	UG w Szczytnikach - 2
22.	Ewidencja numerów porządkowych nieruchomości 042960 z dnia 22.01.2001r.	Forma papierowa		Referat Infrastruktury i Ochrony Środowiska	UG w Szczytnikach - 2
23.	Ewidencja zezwoleń na sprzedaż napojów alkoholowych 059948 z dnia 02.12.2003r.	Forma papierowa		Referat Infrastruktury i Ochrony Środowiska	UG w Szczytnikach - 2
24.	Ewidencja zaświadczeń wydawanych w Urzędzie Gminy Szczytniki 24164 z dnia 26.07.2000r.	Forma papierowa I elektroniczna	System Ewidencji Ludności PB ewid.	Referat Infrastruktury i Ochrony Środowiska Referat Finansów - Podatki Referat Spraw Obywatelskich Referat Administrac.Organiz.	UG w Szczytniki – 2,3,5,6,7

Załącznik nr 3

do Polityki Bezpieczeństwa Informacji

Opis struktury zbiorów danych osobowych przechowywanych w systemach informatycznych oraz sposób przepływu danych pomiędzy systemami informatycznymi.

Lp.	Nazwa zbioru/nazwa programu/miejsce	Opis zbioru – pola danych wskazujące zawartość poszczególnych pól informacyjnych	Pole powiązania – przepływu danych między poszczególnymi systemami
1.	Ewidencja ludności i dowody osobiste gminy Szczytniki */System Ewidencji Ludności PB ewid.* Referat SO	nazwisko, imiona, nazwisko rodowe, nazwiska poprzednio używane, PESEL, data i miejsce urodzenia, imiona i nazwiska rodowe rodziców, obywatelstwo, stan cywilny, informacje o dzieciach, adres zamieszkania lub pobytu [miejscowość, ulica, numer domu, kod pocztowy], seria i nr dowodu osobistego, zawód, wykształcenie, miejsce pracy.	
2.	Urząd Stanu Cywilnego w Szczytnikach */Komputerowy System Rejestracji Aktów Stanu Cywilnego USC PB_USC/RSO* Referat SO	nazwisko, imiona, nazwisko rodowe, nazwiska poprzednio używane, PESEL, data i miejsce urodzenia, imiona i nazwiska rodowe rodziców, stan cywilny, miejsce zamieszkania, nr i seria dowodu osobistego, wykształcenie, nazwisko panieńskie, nazwisko z poprzedniego małżeństwa ,miejsce i godzina urodzenia, dala i nr aktu urodzenia, aktu małżeństwa, aktu zgonu, płeć, imię i nazwisko współmałżonka.	
3.	Ewidencja przedpoborowych i poborowych w UG w Szczytnikach */System Ewidencji Ludności PB ewid.* Referat SO	imiona, nazwisko, imię ojca, rok urodzenia, miejsce stałego lub czasowego pobytu,	
4.	Rejestr świadczeń osobistych i rzeczowych na rzecz obrony w Urzędzie Gminy Szczytniki */System Ewidencji Ludności PB ewid.* Referat SO	imiona, nazwisko, imię ojca, data urodzenia, miejsce zamieszkania, nr i seria dowodu osobistego,	
5.	**Pracownicy urzędu gminy, osoby ubiegające się o pracę /***Zintegrowany System informatyczny dla administracji - Płace, Płatnik ZUS* Referat AO, Referat F	nazwisko, imiona, nazwisko panieńskie, miejsce zamieszkania [miejscowość, ulica, numer domu, kod pocztowy], PESEL, NIP, data i miejsce urodzenia, imiona rodziców, data zatrudnienia, narodowość, obywatelstwo, wykształcenie, wysokość wynagrodzenia, stopień niepełnosprawności, liczba dzieci, historia zatrudnienia, telefon	

6.	**Radni Gminy i Sołtysi-** */Zintegrowany System informatyczny dla administracji* Biuro RG, Referat F	imiona, nazwisko, miejsce zamieszkania - adres,	
7.	Ewidencja skarg i wniosków Gminy Szczytniki */Zintegrowany System informatyczny dla administracji* Referat AO	imiona, nazwisko, miejsce zamieszkania – adres,	
8.	Oświadczenia o stanie majątkowym radnych Gminy Szczytnik */Zintegrowany System informatyczny dla administracji* Referat AO, Biuro RG	imiona, nazwisko, imię ojca, data i miejsce urodzenia, stanowisko, miejsce zamieszkania – adres [miejscowość, ulica, numer domu, kod pocztowy], kraj,	
9.	**Dzierżawcy i użytkownicy wieczyści gruntów gminnych/** *Zintegrowany System informatyczny dla administracji PODATKI – GOMiG (Gospodarka Odpadami Miasta i Gminy)* Referat IOŚ	imiona. nazwisko, data urodzenia, miejsce zamieszkania, seria i nr dowodu osobistego, nr działki,	
10.	**Najemcy lokali mieszkalnych** Referat IOŚ	imiona i nazwisko właściciela, miejsce zamieszkania, nr i położenie działki, nr lokalu, dochody	
11.	Rejestr decyzji o warunkach zabudowy i zagospodarowania terenu. Referat IOŚ	Imiona, nazwisko właściciela, miejsce zamieszkania, nr i położenie działki,	
12.	Ewidencja pozwoleń na wycięcie drzew i krzewów Referat IOŚ	Imię, nazwisko, miejsce zamieszkania, nr telefonu,	
13.	Ewidencja zatwierdzonych projektów podziału nieruchomości i	Imię. nazwisko, miejsce zamieszkania, nr działki	

	rozgraniczeń nieruchomości Referat IOŚ		
14.	Ewidencja miejscowości, ulic i adresów gminy Szczytniki Referat IOŚ	Imię, nazwisko, miejsce zamieszkania,	
15.	Ewidencja właścicieli psów agresywnych Referat IOŚ	Imię, nazwisko, miejsce zamieszkania,	
16.	**Płatnicy opłaty za odbiór i zagospodarowanie odpadów komunalnych/** *Zintegrowany System informatyczny dla administracji GOMiG* *Referat IOŚ*	Imię, nazwisko, miejsce zamieszkania, PESEL, nr telefonu,	
17.	**Wnioskujący o wydanie zezwolenie na uprawę maku** Referat IOŚ	Imię, nazwisko, miejsce zamieszkania	
18.	Ewidencja dodatków mieszkaniowych Referat IOŚ	Imię, nazwisko, miejsce zamieszkania	
19.	**Odbiorcy usługi dostarczania wody i odbioru ścieków/** *Zintegrowany System informatyczny dla administracji Woda i Wodnik* Referat IOŚ	Imię i nazwisko, miejsce zamieszkania, nr działki,	
20.	Ewidencja właścicieli gruntów (nieruchomości i gospodarstw rolnych), budynków, podatników i opłat lokalnych Gminy Szczytniki Podatnicy podatku rolnego i leśnego Podatnicy podatku od nieruchomości	Imię, imię drugie, nazwisko, miejsce zamieszkania [miejscowość, ulica, numer domu, kod pocztowy], imię ojca, PESEL, NIP, powierzchnia gospodarstwa, działki, nieruchomości, wysokość podatku, wysokość zaległości	

	Podatnicy podatku drogowego / *Zintegrowany system informatyczny dla administracji – Podatki* Referat F - podatki		
21.	**Wnioskujący o zwrot podatku akcyzowego za paliwo rolnicze /** *Zintegrowany system informatyczny dla administracji – Podatki* Referat F - podatki	Imię, imię drugie, nazwisko, miejsce zamieszkania [miejscowość, ulica, numer domu, kod pocztowy],PESEL, NIP, nr i seria dowodu osobistego, organ wydający do, obywatelstwo, wielkość powierzchni gospodarstwa- użytków rolnych, numer rachunku bankowego,	
22.	Ewidencja zamówień publicznych Referat IOŚ		
23.	Ewidencja numerów porządkowych nieruchomości Referat IOŚ	Imię, nazwisko, miejsce zamieszkania, nr działki,	
24.	Ewidencja zezwoleń na sprzedaż napojów alkoholowych Referat IOŚ	Imię, nazwisko, miejsce zamieszkania, nr w rejestrze ewidencji działalności gospodarczej,	
25.	Ewidencja zaświadczeń wydawanych w Urzędzie Gminy Szczytniki/ *System Ewidencji Ludności PB ewid.* Referat IOŚ Referat F- podatki Referat SO Referat AO	Imię, nazwisko, miejsce zamieszkania [miejscowość, ulica, numer domu, kod pocztowy], wielkość gospodarstwa [ha fizyczne, przeliczeniowe] dochód z gospodarstwa	
26.	Ewidencja i informacja o działalności gospodarczej CEIODG Referat IOŚ	Imię, imię drugie, nazwisko, miejsce zamieszkania [miejscowość, ulica, numer domu, kod pocztowy],nazwisko rodowe, imię matki, imię ojca, data i miejsce urodzenia, PESEL, NIP, nr i seria dowodu osobistego, adres miejsca zameldowania.	Centralna Ewidencja i Informacja o Działalności Gospodarczej, ZUS, KRUS, GUS
27.	Baza azbestowa Referat IOŚ	Imię i nazwisko, miejsce zamieszkania, nr działki	Baza azbestowa prowadzona przez Ministerstwo Gospodarki

Załącznik nr 4
do Polityki Bezpieczeństwa Informacji

Wzór formularza stosowanego dla spełnienia przez Urząd Gminy w Szczytnikach obowiązków określonych w § 22 ust. 1 i 2 Polityki Bezpieczeństwa Informacji,

ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH

Na podstawie art. 23 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tj. Dz.U. z 2002r. nr 101, poz. 926 z późn. zm.)

wyrażam zgodę na przetwarzanie moich danych osobowych w tym:

1. informacji zawartych w aktach osobowych pracownika i innych dokumentach pracowniczych,
2. danych zawartych w programie kadrowym/płacowym/zusowskim w celach prowadzenia polityki kadrowo-płacowej zakładu.

Niniejsza zgoda ważna jest od dnia …… i wygasa z dniem ustania stosunku pracy, a ponadto może być w każdym czasie zmieniona lub odwołana.

Na podstawie art. 32 ust. 1 pkt 6 ustawy o ochronie danych osobowych pracownikowi przysługuje prawo do żądania:

- uzupełnienia,
- uaktualnienia,
- sprostowania danych osobowych,
- czasowego lub stałego wstrzymania przetwarzania danych,
- usunięcia danych, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji celu, dla którego zostały zebrane.

Zobowiązuję się zachować w tajemnicy w/wymienione dane osobowe oraz sposoby ich zabezpieczenia

.....
(data i podpis upoważnionego)

Załącznik nr 5
do Polityki Bezpieczeństwa Informacji

Wzór formularza stosowanego dla spełnienia przez Urząd Gminy w Szczytnikach obowiązków określonych w § 23 ust. 1 i 2 Polityki Bezpieczeństwa Informacji,

WNIOSEK
O UDOSTEPNIENIE DANYCH ZE ZBIORU DANYCH OSOBOWYCH

1. Wniosek do Kierownika Urzędu Gminy w Szczytnikach

2. Wnioskodawca .....
.....
(nazwa firmy i jej siedziba albo nazwisko, imię i adres zamieszkania wnioskodawcy, ew. 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. 29 ust. 1 ustawy o ochronie danych osobowych:
.....
.....
……* ☐ ew. cd. w załączniku nr ……

4. Wskazanie przeznaczenia dla udostępnionych danych:
.....
.....
.....* ☐ ew. cd. w załączniku nr ……

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

6. Zakres żądanych informacji ze zbioru:
.....
.....
..... * ☐ ew. cd. w załączniku nr ……

7. Informacje umożliwiające wyszukanie w zbiorze żądanych danych:
.....
.....
..... * ☐ ew. cd. w załączniku nr ……

_____
**Jeżeli TAK, to zakreśla kwadrat literą „x"*
(miejsce na znaczki opłaty skarbowej)

……
(data, podpis i ewentualnie pieczęć wnioskodawcy)

Załącznik nr 6

do Polityki Bezpieczeństwa Informacji

Upoważnienie do przetwarzania danych osobowych.

U P O W A Ż N I E N I E Nr ……

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz § 28 ust. 1 Zarządzenia Nr 43/2013 Wójta Gminy Szczytniki z dnia 2 września 2013r. w sprawie Polityki Bezpieczeństwa Informacji, Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych oraz Instrukcji postępowania przy przetwarzaniu danych osobowych w Urzędzie Gminy w Szczytnikach zgodnie z zakresem czynności i złożonego oświadczenia w sprawie znajomości przepisów dotyczących ochrony danych osobowych

U p o w a ż n i a m

Pana/Panią: ……

zatrudnionego/ą na stanowisku ……

do przetwarzania danych osobowych, gromadzonych w systemie informatycznym/nie informatycznym w …… obsługi

(nazwa komórki organizacyjnej)

systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych w następujących zbiorach.

Lp.	PEŁNA NAZWA ZBIORU

Powyższe upoważnienie wydaje się na okres do ……

(wpisać na jaki okres lub bezterminowo)

Administrator Danych Osobowych

…… …… ……

(miejscowość) *(data)*

Załącznik nr 6

do Polityki Bezpieczeństwa Informacji

Odwołanie Upoważnienia do przetwarzania danych osobowych.

O D W O Ł A N I E U P O W A Ż N I E N I A Nr ……

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz § 28 ust. 1 Zarządzenia Nr 43/2013 Wójta Gminy Szczytniki z dnia 2 września 2013r. w sprawie Polityki Bezpieczeństwa Informacji, Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych oraz Instrukcji postępowania przy przetwarzaniu danych osobowych w Urzędzie Gminy w Szczytnikach zgodnie z zakresem czynności i złożonego oświadczenia w sprawie znajomości przepisów dotyczących ochrony danych osobowych

O d w o ł u j ę

Upoważnienie Nr ……. Pana/Pani ……..

zatrudnionego/ej na stanowisku ……

do przetwarzania danych osobowych gromadzonych w systemie informatycznym/nie informatycznym w …… obsługi

(nazwa komórki organizacyjnej)

systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych w następujących zbiorach.

Lp.	PEŁNA NAZWA ZBIORU

Administrator Danych Osobowych

…… …… ……

(miejscowość) *(data)*

Załącznik nr 7
do Polityki Bezpieczeństwa Informacji.

Oświadczenie osoby przetwarzającej dane osobowe o zachowaniu w tajemnicy danych, z którymi ma styczność oraz stosowanych przy przetwarzaniu danych osobowych środkach bezpieczeństwa.

O Ś W I A D C Z E N I E

Imię i nazwisko	
Stanowisko służbowe	
Nazwa komórki organizacyjnej	

Stwierdzam własnoręcznym podpisem, że zapoznałem/am/ się z „Polityką Bezpieczeństwa Informacji" w Urzędzie Gminy w Szczytnikach, Instrukcją Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych oraz Instrukcją postępowania przy przetwarzaniu danych osobowych w Urzędzie Gminy w Szczytnikach.

Jednocześnie, zgodnie z przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) zobowiązuję się do ochrony przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem, danych osobowych przetwarzanych w Urzędzie Gminy w Szczytnikach oraz do zachowania ich w tajemnicy w czasie trwania jak i po ustaniu zatrudnienia.

Równocześnie oświadczam, że zostałem(am) poinformowany(a) o odpowiedzialności służbowej i karnej w przypadku naruszenia przepisów.

....
(imię, nazwisko i podpis osoby przyjmującej oświadczenie) *(data i podpis składającego oświadczenie)*

Załącznik nr 8
do Polityki Bezpieczeństwa Informacji

Oświadczenie osoby zatrudnionej przy przetwarzaniu danych osobowych na podstawie umowy zlecenia, umowy o dzieło lub innej umowy cywilnej o zachowaniu tajemnicy,

O Ś W I A D C Z E N I E
OSOBY UPOWAŻNIONEJ DO PRZETWARZANIA DANYCH OSOBOWYCH

Ja niżej podpisany/a oświadczam, że:

1) przed uzyskaniem dostępu do danych osobowych w związku z zatrudnieniem mnie na podstawie umowy zlecenia, umowy o dzieło lub innej umowy cywilno-prawnej, zapoznałem/am się z przepisami dotyczącymi:
   - Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.),
   - Rozporządzeniem 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),
   - Dokumentem „Polityka Bezpieczeństwa Informacji w Urzędzie Gminy w Szczytnikach.
   - Dokumentem „Instrukcja Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych oraz Instrukcja postępowania przy przetwarzaniu danych osobowych w Urzędzie Gminy w Szczytnikach.

2) znana mi jest treść art. 6 ustawy o ochronie danych osobowych, zgodnie z którym za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
3) potwierdzam fakt odbycia szkolenia z ochrony danych osobowych,
4) zobowiązuję się do przestrzegania przepisów o ochronie danych osobowych, w tym w szczególności do niedokonywania bez upoważnienia: odczytu, modyfikacji, powielania, usuwania, zapisywania na nośnikach oraz przekazywania danych w dowolnej formie,
5) mam świadomość ciążącego na mnie obowiązku zachowania w tajemnicy, w okresie zatrudnienia oraz po ustaniu zatrudnienia, danych osobowych, do których uzyskałem/am dostęp oraz sposobów ich zabezpieczenia,
6) przyjmuje do wiadomości, że niedotrzymanie powyższych zobowiązań, będzie stanowiło naruszenie przepisów karnych ustawy o ochronie danych osobowych oraz podstawowych obowiązków pracowniczych i dlatego spowoduje skierowanie zawiadomienia o podejrzeniu popełnienia przestępstwa oraz/ lub rozwiązanie umowy cywilnoprawnej.

.....	.....
(imię, nazwisko i podpis osoby przyjmującej oświadczenie)	*(data i podpis składającego* oświadczenie)

Załącznik nr 9
do Polityki Bezpieczeństwa Informacji

Wzór porozumienia – umowy zawieranego/ej pomiędzy Wójtem Gminy Szczytniki a pracownikiem zatrudnionym przy przetwarzaniu danych osobowych, w sprawie wykorzystania oddanego do dyspozycji sprzętu informatycznego, oprogramowania oraz zasobów sieci informatycznej.

POROZUMIENIE/UMOWA
POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH[1]

§ 1. 1. Na podstawie art. 31 ust. 1 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tj. Dz. U z 2002 r. Nr 101, poz. 926 z późn.zm.) administrator danych powierza przetwarzającemu przetwarzanie danych osobowych, zgromadzonych w bazie danych klientów administratora danych.

2. Administrator danych udziela przetwarzającemu upoważnienia do upoważniania pracowników do przetwarzania danych osobowych zgodnie z § 6.

§ 2. 1. Przetwarzający zobowiązuje się przetwarzać dane osobowe, o których mowa w § 1 ust. 1. wyłącznie w celu wysyłania korespondencji reklamowej oraz wykonania niniejszej umowy.

2. Przetwarzający zobowiązuje się przetwarzać dane osobowe wyłącznie w następującym zakresie:

- imię i nazwisko,
- adres zamieszkania.
-

3. Wprowadzanie nowych rekordów do bazy danych klientów administratora danych może następować tylko z uwzględnieniem danych osobowych, o których mowa w § 2 ust. 1, i nie stanowi zmiany zakresu przetwarzanych danych osobowych oraz nie wymaga zmiany niniejszej umowy.

§ 3. 1. Przed rozpoczęciem przetwarzania danych osobowych przetwarzający zobowiązuje się do przeprowadzenia uproszczonego audytu wewnętrznego.

2. Audyt przeprowadza zespół ds. ochrony danych, w którego skład wchodzi trzech pracowników wskazanych przez administratora danych, w tym ABI jako przewodniczący oraz dwóch pracowników wskazanych przez przetwarzającego.

3. Raport z prac zespołu przekazuje się zarówno administratorowi danych, jak i przetwarzającemu w ciągu 2 dni od dnia jego sporządzenia, zgodnie z harmonogramem, o którym mowa w § 3 ust. 4.

4. Harmonogram audytu stanowi załącznik nr 2 do niniejszej umowy.

[1] Wzór umowy zawiera tylko postanowienia ściśle związane z ochroną danych osobowych. Pominięto postanowienia precyzujące obowiązki przetwarzającego, związane ze świadczeniem usług.

5. Jeśli raport, o którym mowa w § 3 ust. 3, wskazuje na niezgodności systemu informatycznego przetwarzającego z rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z 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 z późn. zm.), to administrator danych może odstąpić od umowy na piśmie z zachowaniem siedmiodniowego terminu.

6. W razie odstąpienia od umowy przetwarzający zapłaci karę umowną w wysokości ……..

§ 4. 1. Przetwarzający zobowiązuje się dołożyć szczególnej staranności przy przetwarzaniu powierzonych danych osobowych, w tym zwłaszcza przyjąć i wdrożyć dokumentację określoną przez administratora danych, w której skład wchodzi:

- polityka bezpieczeństwa,
- instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

2. Przyjęcie i wdrożenie dokumentacji określonej w § 4 ust. 1 nastąpi nie później niż w ciągu 60 dni od dnia zakończenia audytu, o którym mowa w § 3.

3. Przyjęcie i wdrożenie dokumentacji oznacza dostosowanie przekazanych przez administratora danych wzorów dokumentacji, o której mowa w § 4 ust. 1, do struktury organizacyjnej przetwarzającego, opublikowanie dostosowanej dokumentacji, zaznajomienie z nią osób upoważnionych do przetwarzania danych osobowych u przetwarzającego oraz przeprowadzenie szkoleń dla tych osób, zgodnie z polityką bezpieczeństwa.

4. W razie niewykonania obowiązku przyjęcia i wdrożenia dokumentacji, o której mowa w § 2 ust. 1, przetwarzający zapłaci karę umowną w wysokości ..... za każdy dzień opóźnienia.

§ 5. 1. Przetwarzający zobowiązany jest wyznaczyć administratora bezpieczeństwa informacji w ciągu 7 dni od dnia zawarcia niniejszej umowy.

2. Kandydat do pełnienia funkcji administratora bezpieczeństwa informacji może być wyznaczony dopiero po uprzednim zaakceptowaniu jego osoby przez administratora danych**.**

3. W razie niewykonania obowiązku wyznaczenia administratora bezpieczeństwa informacji przetwarzający zapłaci karę umowną w wysokości ..... za każdy dzień opóźnienia. Nie dotyczy to sytuacji, w której niewykonanie obowiązku wyznaczenia administratora bezpieczeństwa informacji jest wynikiem niezaakceptowania przez administratora danych więcej niż trzech kandydatów przedstawionych do pełnienia funkcji administratora bezpieczeństwa informacji.

§ 6. 1. Przetwarzający może upoważniać do przetwarzania danych osobowych zawartych w bazie danych klientów administratora danych tylko pracowników, którzy podpisali zobowiązania do nieujawniania informacji o:

a. dokumentacji określonej w § 4 ust. 1,
b. danych osobowych, do których uzyskają dostęp w związku z wykonywaniem

obowiązków pracowniczych.
2. Przetwarzający zobowiązuje się nie upoważniać do przetwarzania danych osobowych osób nieposiadających statusu pracownika.

3. Imienne upoważnienia do przetwarzania danych osobowych wydawane będą przez przetwarzającego.

4. Lista osób upoważnionych, o których mowa w ust. 1, będzie każdorazowo uaktualniana i przedkładana administratorowi danych.

§ 7. 1. Administrator danych obowiązany jest przekazać przetwarzającemu bazę danych klientów administratora danych na dysku DVD-R w terminie 2 dni od wdrożenia dokumentacji, o której mowa w § 4.

2. Administrator danych zobowiązuje się do przesyłania w drodze teletransmisji aktualizacji i nowych rekordów w celu uaktualnienia i uzupełnienia danych osobowych w bazie danych klientów administratora danych.

3. Szczegółowe zasady przekazywania danych osobowych w drodze teletransmisji po uzgodnieniu przez strony zostaną zamieszczone w załączniku do niniejszej umowy.

4. Przetwarzający obowiązany jest niezwłocznie wprowadzać aktualizacje i nowe rekordy do bazy danych klientów administratora danych. (...)

§ 8. 1. Każda ze stron może rozwiązać niniejszą umowę za wypowiedzeniem na koniec miesiąca z zachowaniem trzymiesięcznego okresu wypowiedzenia.

2. W terminie 14 dni od rozwiązania umowy przetwarzający obowiązany jest przekazać administratorowi danych bazę danych klientów administratora danych na dysku DVD-R, uaktualnioną na dzień rozwiązania umowy, oraz usunąć trwale wszystkie dane osobowe przetwarzane w bazie danych klientów administratora danych z systemu informatycznego oraz posiadanych nośników.

3. W terminie określonym w ust. 2 przetwarzający obowiązany jest przekazać administratorowi danych także kopie zapasowe bazy danych klientów administratora danych, sporządzone zgodnie z polityką bezpieczeństwa.(...)

Załącznik Nr 10 –

do Polityki Bezpieczeństwa Informacji

Oświadczenie pracownika po przeszkoleniu o zapoznaniu się z przepisami i procedurami w zakresie ochrony danych osobowych

.....
(miejscowość, data)

.....
(imię i nazwisko)
.....
(stanowisko)

O Ś W I A D C Z E N I E

Ja niżej podpisany/a oświadczam, że:
przed uzyskaniem dostępu do danych osobowych w Urzędzie Gminy w Szczytnikach w związku z:
……
……
……
……
zapoznałem/a się z przepisami dotyczącymi:

- Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.),
- Dokumentem „Polityka Bezpieczeństwa Informacji w Urzędzie Gminy w Szczytnikach.
- Dokumentem „Instrukcja Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych oraz Instrukcja postępowania przy przetwarzaniu danych osobowych w Urzędzie Gminy w Szczytnikach.
- Zostałem przeszkolony z zakresu ochrony danych osobowych.

.....
(data i czytelny podpis)

Załącznik Nr 11 –
do Polityki Bezpieczeństwa Informacji

E W I D E N C J A

OSÓB ZATRUDNIONYCH PRZY PRZETWARZANIU DANYCH OSOBOWYCH W URZĘDZIE GMINY W SZCZYTNIKACH

Lp.	Imię i nazwisko osoby upoważnionej	Stanowisko	Komórka organizacyjna	Data przeszkolenia	Nr upoważnienia imiennego	Data nadania upoważnienia	Data ustania upoważnienia	Zakres upoważnienia*	Login/hasło użytkownika

*** Zakres upoważnienia:**

wgląd	**D**
wprowadzanie	**W**
Modyfikacja	**M**
usuwanie	**U**

Załącznik Nr 12
do Polityki Bezpieczeństwa Informacji

Raport z naruszenia ochrony danych osobowych.

R a p o r t
z naruszenia ochrony danych osobowych

1. Data: ..... Godzina: .....
(dzień, miesiąc, rok) *(00:00)*

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

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

3. Lokalizacja zdarzenia:

.....
(określenie czasu i miejsca naruszenia i powiadomienia (np. nr pokoju, nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

.....
.....

5. Podjęte działania i jego opis:
.....
.....

6. Przyczyny wystąpienia zdarzenia:
.....
.....

7. Postępowanie wyjaśniające i naprawcze:
.....
.....

.....
(*data, podpis Administratora Bezpieczeństwa Informacji)*

Załącznik Nr 2
do Zarządzenia Nr 43)2013
Wójta Gminy Szczytniki
z dnia 2 września 2013r.

I N S T R U K C J A

ZARZĄDZANIA SYSTEMEM INFORMATYCZNYMI SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W URZĘDZIE GMINY W SZCZYTNIKACH

Niniejszy dokument opisuje reguły zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych u Urzędzie Gminy w Szczytnikach.

Podstawa prawna:
- art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz. U. z 2002 r. Nr 101. poz. 926 ze zm.),
- 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).

§ 1. „Instrukcja zarządzania systemem informatycznym w Urzędzie Gminy w Szczytnikach" zwana dalej „Instrukcją" obowiązuje wszystkich pracowników Urzędu Gminy, którzy w związku z wykonywaną pracą przetwarzają dane osobowe w systemach informatycznych.

§ 2. 1. Za dane osobowe w rozumieniu ustawy o ochronie danych osobowych uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
2. Przez przetwarzanie danych rozumie się jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza takie, które wykonuje się w systemach informatycznych.
3. Przez zbiór danych rozumie się każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

§ 3. 1. W Urzędzie Gminy dane osobowe przetwarzane są w systemach informatycznych w celach związanych z wykonywaniem zadań ustawowych.
2. Przetwarzanie danych osobowych jest niezbędne do wykonywania określonych prawem zadań realizowanych dla dobra publicznego. Dane przetwarzane są zgodnie z prawem, zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami. Przetwarzanie danych jest merytorycznie poprawne i adekwatne do celów, w jakich są przetwarzane.

ROZDZIAŁ I
PROCEDURY NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH
I REJESTROWANIA TYCH UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM ORAZ WSKAZANIE OSOBY ODPOWIEDZIALNEJ ZA TE CZYNNOŚCI.

§ 4. 1. Osoba dopuszczona do obsługi systemu informatycznego oraz urządzeń wchodzących w skład, służących do przetwarzania danych winna posiadać upoważnienie wydane przez Administratora Danych.

2. Indywidualny zakres czynności osoby zatrudnionej przy przetwarzaniu danych osobowych powinien określać zakres odpowiedzialności tej osoby za ochronę tych danych przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem w stopniu odpowiednim do zadań tej osoby przy przetwarzaniu danych osobowych.
3. Przed dopuszczeniem do pracy przy przetwarzaniu danych osobowych każda osoba powinna być zaznajomiona z przepisami dotyczącymi ochrony danych osobowych i z niniejszą instrukcją.
4. Wprowadza się rejestr osób zatrudnionych przy przetwarzaniu danych osobowych oraz osób pracujących w systemie.
5. Rejestr prowadzony jest przez Administratora Bezpieczeństwa Informacji (ABI) w postaci elektronicznej i papierowej.
6. Administratorem Bezpieczeństwa Informacji jest wyznaczony przez Wójta pracownik zatrudniony w Urzędzie Gminy.

§ 5. 1. Administrator Bezpieczeństwa Informacji określa sposób przydziału haseł dla użytkowników.
2. Wykazy haseł przechowuje Administrator Bezpieczeństwa Informacji w sposób uniemożliwiający dostęp osób nieuprawnionych.

ROZDZIAŁ 2
STOSOWANE METODY I ŚRODKI UWIERZYTELNIENIA ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZENIEM I UŻYTKOWANIEM

§ 6. 1. W systemie informatycznym służącym do przetwarzania danych osobowych stosuje się mechanizmy kontroli dostępu do tych danych.
2. Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się, aby:
   a) w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator:
   b) dostęp do danych możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.

§ 7. 1. **Identyfikator** użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.
2. W przypadku gdy do uwierzytelnienia użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni (jeden miesiąc). Hasło składa się z 8 znaków (w tym co najmniej jednej cyfry i jednej dużej litery).

ROZDZIAŁ 3
PROCEDURY ROZPOCZĘCIA ZAWIESZENIA I ZAKOŃCZENIA PRACY PRZEZNACZONE DLA UŻYTKOWNIKÓW SYSTEMU

§ 8. Procedura rozpoczęcia i zakończenia pracy na danym stanowisku odbywa się przez logowanie do sieci i wylogowanie z sieci.

ROZDZIAŁ 4

PROCEDURY TWORZENIA KOPII ZAPASOWYCH ZBIORÓW DANYCH ORAZ PROGRAMÓW I NARZĘDZI PROGRAMOWYCH SŁUŻĄCYCH DO ICH PRZETWARZANIA

§ 9. 1. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych.

2. Kopie zapasowe:
   a) przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem:
   b) usuwa się niezwłocznie po ustaniu ich użyteczności.

§ 10. 1. Kopie bezpieczeństwa baz danych są wykonywane codziennie, kopie bezpieczeństwa systemu operacyjnego oraz dyskietki ratunkowe wykonywane są raz w miesiącu.

2. Kopie bezpieczeństwa przechowywane są w szafie metalowej w okratowanym zamkniętym pomieszczeniu.

§ 11. Wydruki z danymi i nośnikami informacji przechowywane są w warunkach uniemożliwiających dostęp do nich osobom niepowołanym.

ROZDZIAŁ 5

SPOSÓB ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO PRZED DZIAŁALNOŚCIĄ OPROGRAMOWANIA, KTÓREGO CELEM JEST UZYSKANIE NIEUPRAWNIONEGO DOSTĘPU DO SYSTEMU INFORMATYCZNEGO.

§ 12. 1. System informatyczny służący do przetwarzania danych osobowych zabezpiecza się w szczególności przed:
   a) działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego:
   b) utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

2. Zabezpieczenia, o których mowa w ust. 1 polegają w szczególności na:
   a) sprawdzaniu obecności wirusów komputerowych w systemach informatycznych przy pomocy oprogramowania antywirusowego.
   b) używaniu oprogramowania typu firewall.
   c) przydzielaniu każdemu użytkownikowi systemów informatycznych indywidualnego identyfikatora oraz hasła.
   d) używania zasilaczy awaryjnych.

ROZDZIAŁ 6

SPOSÓB REALIZACJI WYMOGÓW, O KTÓRYCH MOWA W § 7 UST 1 PKT 4 ROZPORZĄDZENIA

§ 13. 1. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie – system ten zapewnia odnotowanie:
   a) daty pierwszego wprowadzenia danych do systemu.
   b) identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba.
   c) źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą.

d) informacji o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych.
e) sprzeciwu, o którym mowa w art. 32 ust, 1 pkt 8 ustawy.

2. Odnotowanie informacji, o których mowa w ust. 1 pkt 1 i 2, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.
3. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w ust 11.
4. W przypadku przetwarzania danych osobowych, w co najmniej dwóch systemach informatycznych, wymagania, o których mowa w ust. 1 pkt 4, mogą być realizowane w jeden z nich lub w odrębnym systemie informatycznym przeznaczonym do tego celu.

§ 14. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia należy zniszczyć w sposób uniemożliwiający ich odczytanie.

ROZDZIAŁ 7
PROCEDURY WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMÓW ORAZ NOŚNIKÓW INFORMACJI SŁUŻĄCYCH DO PRZETWARZANIA DANYCH.

§ 15. Przegląd i konserwacja systemu i zbioru danych osobowych odbywa się na bieżąco.

§ 16. 1. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:

a) Likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
b) Przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
c) Naprawy – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez Administratora Danych.

§ 17. Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem, o którym mowa w § 4 pkt 1 rozporządzenia, w tym stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.

§ 18. Administrator Bezpieczeństwa Informacji monitoruje w imieniu Administratora Danych wdrożone zabezpieczenia systemu informatycznego.

Załącznik nr 3
do Zarządzenia Nr 43/)013
Wójta Gminy Szczytniki
z dnia 2 września 2013r.

I N S T R U K C J A

POSĘPOSTOWANIA PRZY PRZTWARZANIU DANYCH OSOBOWYCH W ODRĘBNYCH ZBIORACH EWIDENCYJNYCH W URZĘDZIE GMINY W SZCZYTNIKACH

Niniejszy dokument opisuje reguły postępowania przy przetwarzaniu danych osobowych w odręcznych zbiorach ewidencyjnych w Urzędzie Gminy w Szczytnikach.

Podstawa prawna:
- art. 36 ustawy z dnia 29.08.1997r. o ochronie danych osobowych (tj. Dz. U. z 2002 r. Nr 101. poz. 926 z późn. zm.)

§ 1. „Instrukcja postępowania przy przetwarzaniu danych osobowych w odręcznych zbiorach ewidencyjnych w Urzędzie Gminy w Szczytnikach" zwana dalej „Instrukcją" obowiązuje wszystkich pracowników Urzędu Gminy, którzy w związku z wykonywaną pracą przetwarzają dane osobowe w odręcznie prowadzonych zbiorach ewidencyjnych, a w szczególności w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych.

§ 2. 1. Za dane osobowe w rozumieniu ustawy o ochronie danych osobowych uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

1. Przez przetwarzanie danych rozumie się jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie.
2. Przez zbiór danych rozumie się każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

§ 3. 1. Przetwarzanie danych osobowych w Urzędzie Gminy w Szczytnikach odbywa się wyłącznie, gdy jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa, a w szczególności:

2. W celu wydania decyzji administracyjnych lub innych orzeczeń w postępowaniu administracyjnym.
3. W zakresie niezbędnym do wykonywania zadań odnoszących się do zatrudnienia pracowników i innych osób.
4. W zakresie niezbędnym do prawidłowej obsługi organów Gminy.

§ 4. 1. Dostęp do danych osobowych przetwarzanych w danym referacie ma wyłącznie kierownik tego referatu oraz upoważniony pracownik.

2. Pracownik zatrudniony przy przetwarzaniu danych osobowych na stanowisku pracy związanym z przetwarzaniem danych osobowych zobowiązany jest zabezpieczyć dane osobowe przed dostępem osób nieuprawnionych.

3. W razie nieobecności w pracy pracownika zatrudnionego przy przetwarzaniu danych osobowych dostęp do danych może mieć wyjątkowo osoba zastępująca pracownika nieobecnego.

§ 5. Każdy z pracowników zatrudnionych przy przetwarzaniu danych osobowych obowiązany jest do zachowania ich w tajemnicy – obowiązek ten istnieje również po ustaniu zatrudnienia oraz zabezpieczenia ich przed udostępnieniem osobom nie upoważnionym, zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem.

§ 6. 1**.** Zbiory danych osobowych w odręcznych zbiorach ewidencyjnych winny być zarejestrowane w Biurze Generalnego Inspektora Ochrony Danych Osobowych.

2. W przypadku tworzenia nowego zbioru danych osobowych Kierownik merytorycznego referatu (pracownik samodzielny) powinien zgłosić ten fakt do Z-cy Wójta Gminy w celu przygotowania zgłoszenia zbioru do Generalnego Inspektora Ochrony Danych Osobowych.

§ 7. Udostępnienie danych osobowych ze zbioru innym podmiotom i osobom fizycznym może mieć miejsce wyłącznie na zasadach określonych w ustawie.

§ 8. Za przestrzeganie zasad bezpieczeństwa danych osobowych w referatach odpowiedzialni są kierownicy, a także pracownicy na samodzielnych stanowiskach pracy.

§ 9. Kontrolę wewnętrzną przestrzegania zasad określonych w niniejszej instrukcji przeprowadza wyznaczony pracownik przez Administratora Danych Osobowych (Wójta).