ZARZĄDZENIE Nr 195/2016

WÓJTA GMINY LIPNO

z dnia 3.10.2016r.

w sprawie dokumentacji przetwarzania danych osobowych

Na podstawie art. 36 ust. 1 i 2 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tj. Dz. U. z 2016r. poz. 922 z późn. zm.)oraz § 3 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 2004 r. Nr 100, poz. 1024), zarządzam co następuje:

§ 1. Wdrażam „Politykę Bezpieczeństwa w Urzędzie Gminy Lipno" stanowiąca załącznik Nr 1 niniejszego zarządzenia.

§ 2. Wdrażam „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, w Urzędzie Gminy Lipno " stanowiąca załącznik Nr 2 niniejszego zarządzenia.

§ 3. Traci moc Zarządzenie Wójta Gminy Lipno Nr 126 / 2006r z 4.04.2006r w sprawie wprowadzenia do stosowania i wdrożenia „Polityki bezpieczeństwa danych osobowych" |i Nr 127 /2006r. 4.04.2006r w sprawie wprowadzenia do stosowania i wdrożenia „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych".

§ 4. Zarządzenie wchodzi w życie z dniem podpisania.

Załączniki
1. Polityka Bezpieczeństwa w Urzędzie Gminy Lipno
2. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, w Urzędzie Gminy Lipno

WÓJT
Jacek Kwiatkowski

Załącznik Nr 1 do Zarządzenia nr 195/2016 Wójta Gminy Lipno

ZATWIERDZAM"
Administrator Danych
Wójt
Jacek Kwaśniński
.....

POLITYKA BEZPIECZEŃSTWA

w URZĘDZIE GMINY LIPNO

Wersja 1.0

Część I – Wstęp

§ 1. Zgodnie z art. 39a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz. U. z 2016r., poz. 922 z późn. zm.), zwanej dalej „ustawą" oraz z § 3 ust. 1 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024), zwanego dalej „rozporządzeniem", ustanawia się „Politykę Bezpieczeństwa".

§ 2. Postanowienia ogólne

1. Celem Polityki jest stworzenie podstaw do właściwego wykonywania obowiązków Administratora Danych w zakresie zabezpieczenia i prawidłowej ochrony przetwarzanych danych osobowych.
2. Polityka określa zasady przetwarzania danych osobowych oraz ich zabezpieczenia, jako zestaw reguł i zaleceń regulujących sposób ich zarządzania, ochrony i dystrybucji w Urzędzie Gminy Lipno.
3. Politykę stosuje się do:
   a) Danych osobowych przetwarzanych w systemach informatycznych
   b) Danych osobowych przetwarzanych tradycyjnie
   c) Informacji dotyczących bezpieczeństwa przetwarzanych danych osobowych służących do uwierzytelniania w systemach informatycznych, w których są przetwarzane dane,
   d) Informacji dotyczących bezpieczeństwa przetwarzanych danych osobowych dotyczących wdrożonych zabezpieczeń technicznych i organizacyjnych

§ 3. Ilekroć w niniejszym dokumencie jest mowa o jednostce organizacyjnej, należy przez to rozumieć Urząd Gminy Lipno.

Część II – Zasady ogólne

§ 4. Ochrona danych osobowych realizowana jest poprzez zabezpieczenia fizyczne, organizacyjne, oprogramowanie systemowe, aplikacje oraz użytkowników.

§ 5. Utrzymanie bezpieczeństwa przetwarzanych danych osobowych w Urzędzie Gminy rozumiane jest jako zapewnienie ich poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z ochroną danych osobowych.

1. Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:
   a) poufność danych – rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom;
   b) integralność danych – rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
   c) rozliczalność danych – rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie;
   d) integralność systemu – rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej;
   e) dostępność informacji – rozumianą jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne;
   f) zarządzanie ryzykiem – rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych służących do przetwarzania danych osobowych.

§ 6. Administratorem danych osobowych przetwarzanych w Urzędzie Gminy Lipno jest Wójt Gminy.

Administrator danych osobowych powołuje administratora bezpieczeństwa informacji, którego zadania określa § 9.

§ 7. Definicje

1. Przez użyte w Polityce bezpieczeństwa określenia należy rozumieć:
   a) administrator danych osobowych – rozumie się Wójta Gminy Lipno;
   b) administrator bezpieczeństwa informacji (także ABI) – rozumie się przez to osobę wyznaczoną przez administratora danych osobowych, nadzorującą przestrzeganie zasad ochrony danych osobowych, w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;
   c) ustawa – rozumie się przez to ustawę z 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn.: Dz. U. z 2016 r. poz. 922);
   d) rozporządzenie – rozporządzenie 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. z 2004 r. nr 100, poz. 1024);
   e) dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
   f) zbiór danych osobowych – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
   g) przetwarzane danych – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;
   h) system informatyczny – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;
   i) system tradycyjny – rozumie się przez to zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji i wyposażenia i środków trwałych w celu przetwarzania danych osobowych na papierze;
   j) zabezpieczenie danych w systemie informatycznym – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
   k) administrator systemu informatycznego – rozumie się przez to osobę lub osoby, upoważnione przez administratora danych osobowych do administrowania i zarządzania systemami informatycznymi;
   l) użytkownik – rozumie się przez to upoważnionego przez administratora danych osobowych lub administratora bezpieczeństwa informacji (o ile został powołany), wyznaczonego do przetwarzania danych osobowych pracownika;
   m) identyfikator użytkownika (login) – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
   n) hasło – ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

§ 8. Deklaracja Administratora Danych Osobowych

1. ADO zobowiązuje się do podjęcia odpowiednich kroków, mających na celu zapewnienie prawidłowej ochrony danych osobowych, w szczególności do zapewnienia, ze przez cały okres ich przetwarzania, dane będą:
   a) Przetwarzane zgodnie z prawem
   b) Zbieranie dla oznaczonych, zgodnych z prawem celów i nie poddawanie dalszemu przetwarzaniu niezgodnemu z tymi celami
   c) Merytorycznie poprawne i adekwatne w stosunku do celów przetwarzania
   d) Przechowywanie w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania
   e) Zabezpieczone środkami technicznymi i organizacyjnymi, które zapewniają rozliczalność, integralność oraz poufność danych
2. Przy przetwarzaniu danych osobowych w systemach informatycznych urzędu należy stosować wysoki stopień bezpieczeństwa w rozumieniu § 6 ust. 4 Rozporządzenia

§ 9. Odpowiedzialność Administratora Danych Osobowych

1. Administrator Danych Osobowych jest odpowiedzialny za przetwarzanie i ochronę danych osobowych zgodnie z przepisami prawa, w tym wprowadzenie do stosowania procedur postępowania zapewniających prawidłowe przetwarzanie danych osobowych, rozumiane jako ochronę danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zmianą lub zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem Ustawy oraz utratą, uszkodzeniem lub zniszczeniem.
2. Do kompetencji Administratora Danych Osobowych należy w szczególności:
   a) Wyznaczenie Administratora Bezpieczeństwa Informacji
   b) Wyznaczenie Właścicieli zasobów danych osobowych
   c) Określenie celów i strategii ochrony danych osobowych
   d) Podział zadań i obowiązków związanych z organizacją danych osobowych
3. Do obowiązków Administratora Danych Osobowych należy:
   a) Zapewnienie szkoleń dla pracowników w zakresie przepisów o ochronie danych osobowych oraz zagrożeń związanych z ich przetwarzaniem
   b) Przyjmowanie i zatwierdzanie niezbędnych, wymaganych przez przepisy prawa dokumentów regulujących ochronę danych osobowych Urzędzie Gminy Lipno
   c) Nadawanie uprawnień pracownikom Urzędu oraz użytkownikom zewnętrznym do przetwarzania danych osobowych
   d) Zapewnienie środków finansowych na ochronę fizyczna pomieszczeń, w których przetwarzane są dane osobowe
   e) Zapewnienie środków finansowych niezbędnych do ochrony danych osobowych przetwarzanych w systemach informatycznych oraz zbiorach nieinformatycznych
   f) Zapewnienie środków finansowych na merytoryczne przygotowanie osób odpowiedzialnych za nadzór i ochronę danych osobowych
   g) Zapewnienie realizacji obowiązku zgłaszania i aktualizacji zbiorów danych osobowych do rejestracji GIODO

§ 10. 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.
2. Do kompetencji Administratora Bezpieczeństwa Informacji należy:
   a) Określenie zasad ochrony danych osobowych
   b) Wnioskowanie o ukaranie osób winnych naruszenia przepisów i zasad dotyczących ochrony danych osobowych

3. Do obowiązków Administratora Bezpieczeństwa Informacji należy:
   a) Nadzór nad wdrożeniem stosowanych środków organizacyjnych, technicznych i fizycznych w celu ochrony danych osobowych
   b) Wnioskowanie do ADO o nadawanie, zmienianie oraz cofanie uprawnień do przetwarzania danych osobowych uzgodnieniu z właścicielami zasobów dla pracowników oraz użytkowników zewnętrznych
   c) Prowadzenie dokumentacji opisującej zastosowaną ochronę danych osobowych (niniejsza Polityka i Instrukcja Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych) oraz:
      - ✓ Ewidencję osób upoważnionych przez Administratora Danych Osobowych do przetwarzania danych osobowych
      - ✓ Ewidencja zbiorów danych osobowych przetwarzanych w Urzędzie Gminy Lipno oraz programów zastosowanych do ich przetwarzania
      - ✓ Opis struktury zbiorów danych osobowych
      - ✓ Opis sposobów przepływu danych pomiędzy systemami
      - ✓ Oryginały i kopie dokumentów dotyczących ochrony danych osobowych (w tym kopie wniosków o rejestrację/aktualizację zbiorów danych do GIODO oraz uchwały, zarządzenia dotyczące danych osobowych)
      - ✓ Protokóły przeprowadzonych kontroli wewnętrznych i zewnętrznych w zakresie ochrony danych osobowych
   d) Zapoznanie pracowników Urzędu z przepisami i zasadami ochrony danych osobowych oraz informowanie o zagrożeniach związanych z ich przetwarzaniem
   e) Reprezentowanie Gminy w kontaktach z Biurem GIODO
   f) Przygotowanie zgłoszeń zbiorów danych osobowych do rejestracji w GIODO
   g) Reagowanie na zgłaszane incydenty związane z naruszeniem ochrony danych osobowych oraz analizowanie ich przyczyn i kierowanie wniosków dotyczących ukarania innych naruszeń
   h) Sprawdzenie wypełnienia obowiązków technicznych i organizacyjnych związanych z ochroną danych osobowych
4. Administrator Bezpieczeństwa Informacji w zakresie realizacji swoich obowiązków, ma prawo żądania od pozostałych osób, bez względu na rangę ich stanowiska udzielenia natychmiastowej pomocy w razie stwierdzenia, że doszło do naruszenia przepisów o ochronie danych osobowych które może skutkować postawieniem Urzędu albo Administratora Danych popełnienia jednego z przestępstw, wskazanych w Rozdziale 8 Ustawy
5. Sprawowanie nadzoru nad przestrzeganiem zastosowanych środków technicznych i organizacyjnych zapewniających ochronę danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochrona powinno być głównym zadaniem Administratora bezpieczeństwa Informacji

§ 11. Odpowiedzialność Administratora Systemów Informatycznych
1. Rolę ASI pełni pracownik wyznaczony przez Administratora Danych Osobowych
2. Do kompetencji Administratora Systemów Informatycznych należy:
   a) Zabezpieczenie systemów przetwarzania danych osobowych zgłoszonych ASI, w zależności od kategorii przetwarzanych w tym systemie danych
   b) Zapewnienie poufności, integralności, dostępności i rozliczalności danych przetwarzanych w systemach informatycznych
3. Do obowiązku Administratora Systemów Informatycznych należy:
   a) Bieżący nadzór oraz zapewnienie optymalnej ciągłości działania systemu informatycznego w tym opracowanie procedur określających zarządzanie systemem informatycznym przetwarzającym dane osobowe

b) Reagowanie bez zbędnej zwłoki, w przypadku naruszenia bądź powstania zagrożenia bezpieczeństwa danych osobowych
c) Przeciwdziałanie próbom naruszenia bezpieczeństwa danych osobowych
d) Analizę raportów wszystkich zdarzeń w tym incydentów związanych z bezpieczeństwem systemów przetwarzania danych
e) Zapewnienie wszystkich wdrażanych systemów przetwarzania danych osobowych z Ustawą oraz niniejsza Polityką bezpieczeństwa i Instrukcją zarządzania systemem Informatycznym w Urzędzie Gminy Lipno
f) Instalację i konfigurację oprogramowania i sprzętu typu „stand - alone", sieciowego i serwerowego używanego do przetwarzania danych osobowych
g) Konfigurację i administrację oprogramowaniem systemowym i sieciowym zabezpieczającym dane osobowe przed nieupoważnionym dostępem
h) Nadzór nad czynnościami związanymi ze sprawdzaniem systemu pod kątem obecności szkodliwego oprogramowania
i) Nadzór nad systemem komunikacji w sieci komputerowej oraz przesyłaniem danych za pośrednictwem urządzeń teletransmisji
j) Nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe
k) Świadczenie pomocy technicznej w ramach oprogramowania a także serwis sprzętu komputerowego będącego na stanie Urzędu Gminy Lipno, służącego do przetwarzania danych osobowych
l) Diagnozowanie i usuwanie awarii sprzętu komputerowego oraz realizacje umów z firmami świadczącymi usługi pogwarancyjnego sprzętu komputerowego
m) Wykonywanie i zarządzanie kopiami oprogramowania systemowego i sieciowego
n) Nadzór nad wdrażaniem i zarządzaniem aplikacjami (przeglądanie, nadawanie, i odbieranie uprawnień użytkownikom, itp.), w których przetwarzane są dane osobowe
o) Zatwierdzanie wniosków zgłoszeń do rejestracji zbiorów danych osobowych w części E i F
p) Umożliwienie przeprowadzenia kontroli systemu informatycznego przez służby Biura Generalnego Inspektora Ochrony Danych Osobowych

§ 12. Odpowiedzialność właścicieli zasobów danych osobowych

1. Administrator Danych Osobowych wyznacza właścicieli zasobów danych osobowych, którzy są odpowiedzialni za ochronę przypisanych zbiorów danych osobowych w podległej komórce organizacyjnej
2. Do kompetencji właścicieli zasobów danych osobowych należy:
   a) Określenie celów w jakich mają być przetwarzane dane osobowe, zakresu oraz czasu trwania przetwarzania danych osobowych
   b) Określenie sposobu przetwarzania danych osobowych (czy w systemach informatycznych, czy w zbiorach nieinformatycznych)
   c) Ustalenie, czy przetwarzane dane dla określonego celu mają charakter niejawny lub zawierają dane wrażliwe
3. Do obowiązków właścicieli zasobów danych osobowych należy"
   a) Zapewnienie podstaw prawnych do przetwarzania danych osobowych od chwili zebrania danych osobowych do chwili ich usunięcia
   b) Zapewnienie aktualności, adekwatności oraz merytorycznej poprawności danych osobowych przetwarzanych w określonym przez nich celu
   c) Realizację obowiązku informowania o przetwarzaniu danych osobowych osób, których dane osobowe są pozyskiwane

d) Zapewnienie na żądanie uprawnionych osób, udostępnianie informacji o przetwarzanych danych osobowych oraz podmiotach, którym zostały one udostępnione
e) W przypadku utworzenia nowego zbioru danych osobowych lub jego aktualizacji przekazanie ABI stosownych informacji (część A – D wniosku)

§ 13. Odpowiedzialność pracowników i użytkowników systemu

1. W celu osiągnięcia i utrzymania wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych konieczne jest zaangażowanie ze strony każdego pracownika i użytkownika zewnętrznego w zakresie ochrony danych osobowych
2. Pracownicy Urzędu Gminy oraz użytkownicy zewnętrzni są zobowiązani do informowania o wszelkich podejrzeniach naruszenia lub zauważonych naruszeniach oraz słabościach systemu przetwarzania danych osobowych do Administratora Bezpieczeństwa Informacji
3. Pracownicy / użytkownicy zewnętrzni są zobowiązani do:
   a) Postępowania zgodnie z Polityką
   b) Zachowania w tajemnicy danych osobowych oraz informacji o sposobach ich zabezpieczenia
   c) Ochrony danych osobowych oraz środków przetwarzających dane osobowe przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem
   d) Wykonania konkretnych działań i procesów w celu zapewnienia ochrony danych osobowych
4. Pracownicy / użytkownicy zewnętrzni powinni mieć świadomość możliwości zaistnienia sytuacji naruszenia ochrony danych osobowych. W tym celu powinni:
   a) Przestrzegać procedur związanych z otwieraniem i zamykaniem pomieszczeń, a także z wejściem do obszarów przetwarzania danych osobowych osób nieupoważnionych
   b) Informować ABI (sekretariat) o podejrzanych osobach
   c) Pracownicy / użytkownicy zewnętrzni powinni na podstawie dokonanej identyfikacji ewentualnych zagrożeń, przekładać ABI projekty i propozycje nowych rozwiązań, których celem jest zwiększenie poziomu ochrony danych osobowych

§ 11. Szkolenia w zakresie ochrony danych osobowych

1. Przed rozpoczęciem przetwarzania danych osobowych pracownik powinien zostać przeszkolony przez ABI z :
   a) Przepisów o ochronie danych osobowych
   b) Zasad przetwarzania danych osobowych
   c) Procedur dotyczących bezpiecznego przetwarzania danych osobowych w systemach informatycznych
   d) Zasad użytkowania urządzeń i systemów informatycznych służących do przetwarzania danych osobowych
   e) Zagrożenia na jakie może być narażone przetwarzanie danych osobowych
   f) Zasady dostępu do pomieszczeń, w których przetwarzane są dane osobowe
   g) Sposób postępowania w przypadku naruszenia ochrony danych osobowych lub systemu informatycznego
   h) Odpowiedzialności z tytułu naruszenia ochrony danych osobowych

§ 12. Sankcje za naruszenie zasad ochrony danych osobowych

1. Naruszenie zasad ochrony danych osobowych przez pracownika / użytkownika zewnętrznego może skutkować postawieniem mu zarzutu popełnienia, jednego z przestępstw określonych w Rozdziale 8 Ustawy lub przestępstwa określonego w art.266 Kodeksu Karnego
2. Pracownik dopuszczający się nieuprawnionego ujawnienia lub wykorzystania danych osobowych w sposób sprzeczny z ich przeznaczeniem (np. wykorzystanie do celów prywatnych) czy tez ich przetwarzania w sposób niezgodny z przyjętymi w Urzędzie procedurami może zostać ukarany karą upomnienia lub karą nagany
3. W razie ciężkiego naruszenia obowiązku zachowania danych osobowych w tajemnicy lub przetwarzania ich w sposób rażąco sprzeczny z przyjętymi zasadami i procedurami, ADO może rozwiązać bez wypowiedzenia umowy o pracę z winy pracownika

Część III – Zasady przetwarzania i ochrony danych osobowych

§ 13. Przetwarzanie danych osobowych

1. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby upoważnione przez Administratora Danych Osobowych. Wzór upoważnienia stanowi załącznik nr 6.
2. Administrator Bezpieczeństwa Informacji prowadzi ewidencję osób upoważnionych do ich przetwarzania. Wzór ewidencji stanowi załącznik Nr 8.
3. Osoby, które zostały upoważnione do przetwarzania danych, są zobowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia.
4. Każda osoba, mająca dostęp do danych osobowych przetwarzanych w Urzędzie Gminy jest zobowiązana do zapoznania się z niniejszym dokumentem.
5. Dokumenty zawierające dane osobowe przechowywane w formie papierowej, upoważnione osoby przechowują w obszarze przetwarzania danych w szafach zamykanych na klucz. W przypadku konieczności zniszczenia papierowych dokumentów zawierających dane osobowe, ich zniszczenie dokonuje się poprzez pocięcie w niszczarce.
6. Zasady przetwarzania danych osobowych w systemie informatycznym określone są w „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Lipno".

§ 14. Rejestracja zbiorów danych osobowych

1. Upoważnieni pracownicy są zobowiązani do wnioskowania do ABI zamiaru utworzenia nowego zbioru danych osobowych wraz ze wskazaniem podstawy przetwarzania danych, uzasadnieniem celowości, zakresu i sposobu zbierania danych osobowych
2. ABI weryfikuje wniosek o utworzenie nowego zbioru danych osobowych oraz analizuje nowy zbiór danych pod kątem obowiązku zgłoszenia zbioru GIODO
3. W sytuacji, jeżeli rejestracja nowopowstałego zbioru lub zbioru wymagającego aktualizacji danych osobowych jest ustawowo wymagana, właściciel zbioru przygotowuje projekt zgłoszenia zbioru danych osobowych (zgłoszenia zmian do rejestracji) zmiany w GIODO w części A-D
4. Zgłoszenie (zmiana) wniosku zgłoszenia zbioru do rejestracji przez GIODO w części E-F jest przygotowywana przez Administratora Systemów Informatycznych odpowiedzialnego za odpowiednie zabezpieczenie danych w systemie informatycznym Urzędu

5. Sprawdzony przez ABI projekt zgłoszenia zbioru danych osobowych do rejestracji w GIODO jest przekazany Administratorowi Danych Osobowych do podpisu
6. ADO zgłasza wniosek o rejestrację do GIODO, wyznacza właściciela zasobów danych osobowych dla zarejestrowanego zbioru danych osobowych
7. ABI uzupełnia Politykę, dokumenty z nią powiązane i pozostałe dokumenty obowiązujące w Urzędzie.

§ 15. Udostępnianie Danych Osobowych

1. Udostępnienie danych osobowych podmiotowi zewnętrznemu może nastąpić wyłącznie po pozytywnym zweryfikowaniu ustawowych przesłanek dopuszczalności takiego udostępnienia, przez co rozumie się w szczególności pisemny wniosek podmiotu uprawnionego.

§ 16. Powierzenie przetwarzania danych

1. Zlecenie podmiotowi zewnętrznemu przetwarzania danych osobowych może nastąpić wyłącznie w ramach umowy powierzenia przetwarzania danych osobowych, zgodnie z art. 31 ustawy.

§ 17. Przetwarzanie danych osobowych w obszarach bezpiecznych

1. Dane osobowe w Urzędzie Gminy Lipno mogą być przetwarzane wyłącznie w pomieszczeniach przetwarzania danych osobowych
2. Do pomieszczeń przetwarzania danych zalicza się:
   a) Serwerownię
   b) Pomieszczenia biurowe w których zlokalizowane są stacje robocze
   c) Pomieszczenia w których zlokalizowane SA zbiory nieinformatyczne
3. Przebywanie wewnątrz obszarów o których mowa w ust. 2, osób nieuprawnionych do przetwarzania danych jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania tych danych lub za zgodą Właściciela zasobów danych osobowych
4. Budynki lub pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane podczas nieobecności osób upoważnionych do przetwarzania danych osobowych, w sposób ograniczający możliwość dostępu do nich osobom nieupoważnionym.
5. Przetwarzanie danych osobowych jest zakazane w pomieszczeniach, w których wykonywane są przez osoby trzecie prace techniczne.
6. Wymagany przez rozporządzenie wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe (zwany dalej „obszarem przetwarzania") stanowi załącznik nr 1 do niniejszego dokumentu.

§ 17. Wykaz zbiorów danych osobowych

1. Gmina Lipno – reprezentowana przez Wójta Gminy jest administratorem danych osobowych wymienionych w „Wykazie zbiorów danych osobowych" prowadzonych przez Administratora Bezpieczeństwa Informacji.
2. Wymagany przez rozporządzenie wykaz zbiorów danych osobowych, stanowi załącznik nr 2 do niniejszego dokumentu.

§ 18. Opis struktury zbiorów danych

1. Opisy struktury zbiorów danych osobowych prowadzi Administrator Systemu Informatycznego.
2. Zakresy danych osobowych przetwarzanych w poszczególnych zbiorach osobowych są ustalane w oparciu o strukturę zbiorów danych osobowych prowadzonych w systemach informatycznych oraz powiązania pól informacyjnych utworzonych w tych systemach
3. Wymagany przez rozporządzenie opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi stanowi załącznik nr 3 do niniejszego dokumentu.

§ 19. Sposób przepływu danych pomiędzy poszczególnymi systemami

1. Administrator Systemów Informatycznych, prowadzi dokumentację systemów informatycznych, zawierający opisy współpracy pomiędzy różnymi systemami informatycznymi oraz sposób przepływu danych pomiędzy systemami, w których te dane są przetwarzane.
2. Wymagany przez rozporządzenie sposób przepływu danych pomiędzy poszczególnymi systemami, stanowi załącznik nr 4 do niniejszego dokumentu.

§ 20. Wymagane przez rozporządzenie określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych stanowi załącznik nr 5 do niniejszego dokumentu.

§ 21. Osoby, które przetwarzają w jednostce organizacyjnej dane osobowe, muszą posiadać pisemne upoważnienie do przetwarzania danych nadane przez Administratora Danych Osobowych (załącznik nr 6 do niniejszego dokumentu).

§ 22. Każda osoba posiadająca upoważnienie do przetwarzania danych osobowych posiada swój identyfikator oraz hasło, pozwalające na zalogowanie się do systemu informatycznego, w którym przetwarzane są dane osobowe. Techniczne wymagania, jakie musi spełniać hasło, określone zostały w części II § 2 Instrukcji Zarządzania Systemem Informatycznym.

§ 23. W przypadku konieczności dostępu do obszaru przetwarzania osób, nieposiadających upoważnienia, o jakim mowa w części I § 9 ust. 3 pkt. c (załącznik nr 6 do niniejszego dokumentu), które muszą dokonać doraźnych prac o charakterze serwisowym lub innym, podpisują oni oświadczenie o zachowaniu poufności (załącznik nr 7 do niniejszego dokumentu), chyba że czynności odbywają się pod nadzorem osoby upoważnionej do przetwarzania danych.

§ 24. W przypadku otrzymania wniosku o udostępnienie danych osobowych od osoby, której one dotyczą, administrator danych w ciągu 30 dni informuje daną osobę o przysługujących jej prawach oraz udziela informacji na piśmie zgodnie z art. 32 ust. 1 pkt. 1-5a.

§ 25. W przypadku zbierania danych osobowych od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę, bezpośrednio po utrwaleniu zebranych danych o:

1. adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna – o miejscu zamieszkania oraz imieniu i nazwisku,
2. celu zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych
3. źródle danych,
4. prawie dostępu do treści swoich danych oraz ich poprawiania,
5. uprawnieniach wynikających z art. 32 ust. 1 pkt. 7 i 8 ustawy,

Część III – Postanowienia końcowe

§ 26. Nieprzestrzeganie zasad ochrony danych osobowych grozi odpowiedzialnością karną wynikającą z art. 49-54a ustawy o ochronie danych osobowych.

§ 27. W sprawach nieuregulowanych niniejszym dokumentem, znajdują zastosowanie przepisy ustawy o ochronie danych osobowych oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

§ 28. Niniejszy dokument wchodzi w życie z dniem podpisania.

Wykaz załączników:

1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe
2. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych
3. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi
4. Sposób przepływu danych pomiędzy poszczególnymi systemami
5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych
6. Upoważnienie do przetwarzania danych osobowych
7. Oświadczenie o zachowaniu poufności danych osobowych
8. Ewidencję osób upoważnionych do przetwarzania danych osobowych
9. Wykaz podmiotów, którym udostępniono dane osobowe
10. Wykaz podmiotów, z którymi zawarto umowy powierzenia przetwarzania danych osobowych
11. Wykaz osób, którym udostępniono dane osobowe

Załącznik nr 1 do Polityki Bezpieczeństwa

L.p.	Lokalizacja – adres	Precyzyjne określenie pomieszczenia	Dział/osoba użytkująca pomieszczenie	Zabezpieczenie pomieszczenia

WÓJT
Jacek Karmiński

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

L.p.	Nazwa zbioru danych osobowych	Podlega rejestracji u GIODO (TAK/NIE) Podstawa prawna	Cel przetwarzania	Nazwa systemu, ewidencji lub aplikacji, w której przetwarzane są dane osobowe

WÓJT
Jacek Karmiński

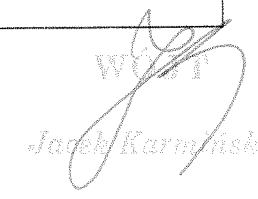
OPIS STRUKTURY ZBIORÓW DANYCH WSKAZUJĄCY ZAWARTOŚĆ POSZCZEGÓLNYCH PÓL INFORMACYJNYCH I POWIĄZANIA MIĘDZY NIMI

L.p.	Nazwa zbioru danych osobowych	Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi			Uwagi

WÓJT
Jacek Parmiński

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

L.p.	Nazwa zbioru danych osobowych	Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi			Uwagi
1.	Rejestr wniosków o informacje adresowe				
2.	Księgi stanu cywilnego				
3.	Dowody osobiste				
4.	Rejestr przedpoborowych				
5.	Lista poborowych				
6.	Ewidencja osób w zakresie powszechnej samoobrony				
7.	Ewidencja osób w formacjach OC				
8.	Akcja kurierska				
9.	Zaświadczenia podatkowe				
10.	Windykacja należności podatkowych				
11.	Świadectwa miejsca pochodzenia zwierząt				
12.	Księgowość użytkowników wieczystych				
13.	Księgowość podatku od posiadania psów i od środków transportowych				
14.	Zmiana miejscowego planu zagospodarowania przestrzennego				



L.p.	Nazwa zbioru danych osobowych	Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi			Uwagi
15.	Decyzje o rozgraniczeniu nieruchomości				
16.	Decyzje o warunkach zabudowy i zagospodarowania terenu				
17.	Gospodarowanie gminnym zasobem nieruchomości				
18.	Wnioski o wpisy i wyrysy z tekstu planu				
19.	Zamówienia publiczne				
20.	Zezwolenia na zajęcia pasa drogi				
21.	Zezwolenia na sprzedaż napojów alkoholowych				
22.	Zezwolenia na usunięcie drzew i krzewów				
23.	Zezwolenia na utrzymanie psów				
24.	Decyzje na świadczenie usług komunalnych				
25.	Decyzje w sprawie zastosowania ulg podatkowych				
26	Oznaczenie nieruchomości numerem				
27.	Pozwolenia na budowę				
28.	Windykacja należności budżetowych				
29.	Akta konkursu na stanowisko dyrektora GOK				
30.	Akta konkursu na dyrektora szkoły				
31.	Dokumentacja wypadków przy pracy				

L.p.	Nazwa zbioru danych osobowych	Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi			Uwagi
32.	Ewidencja ludności				
33.	Wieczyste użytkowanie gruntów				
34.	Wymiar należności podatkowych				
35.	Najem lokali mieszkalnych				
36.	Wnioski o nadanie medalu za zasługi dla obronności kraju				
37.	Wnioski o nadanie medalu za długoletnie pożycie małżeńskie				
38.	Wnioski o nadanie odznaki za zasługi dla oświaty				
39.	Skargi i wnioski				
40.	Sprawy dotyczące utrzymania czystości i porządku				
41.	Informacje o wyrobach zawierających azbest				
42.	Oświadczenia majątkowe radnych				
43.	Sołtysi				
44	Obowiązek szkolny i nauki				
45.	Transport dzieci oraz młodzieży				
46.	Pomoc materialna				
47.	Zmiana imion i nazwisk				
48.	Ochrona środowiska				

WÓJT
Jacek Kwiatkowski

SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY POSZCZEGÓLNYMI SYSTEMAMI

L.p.	Nazwa zbioru danych osobowych	Nazwa systemu, ewidencji lub aplikacji, w której przetwarzane są dane osobowe	Sposób przepływu danych pomiędzy poszczególnymi systemami

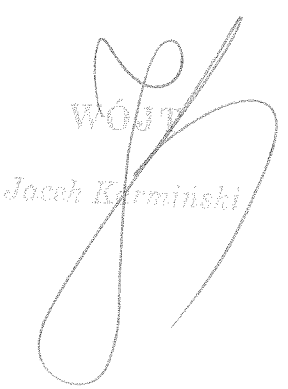
WÓJT
Jacek Kowalski

OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH NIEZBĘDNYCH DO ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH.

Zgodnie z § 4 pkt. 5 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r.(Dz. U. z 2004 r. Nr 100 poz. 1024):

1. Administrator Danych Osobowych zapewnia zastosowanie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności, rozliczalności i ciągłości przetwarzanych danych.
2. ASI wraz z wyznaczonymi Użytkownikami przeprowadzają okresową analizę ryzyka dla systemu i na tej podstawie przedstawiają Administratorowi Danych propozycje dotyczące zastosowania środków technicznych i organizacyjnych (środków ochrony), celem zapewnienia właściwej ochrony przetwarzanych danych.
3. Określenia poziomu bezpieczeństwa systemu informatycznego dokonuje ASI.
4. Zastosowane środki ochrony (techniczne i organizacyjne) powinny być adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych.
5. Środki ochrony, zastosowane przez ASI dla zapewnienia poufności, integralności, rozliczalnościi ciągłości przetwarzanych danych, obejmują:
   a) środki ochrony fizycznej (np. drzwi ochronne, firma ochroniarska, monitoring);
      - Zabezpieczenie fizyczne opisane jest w załączniku nr 1. „Wykaz pomieszczeń przetwarzane są dane osobowe".
      - Urządzenia służące do przetwarzania danych osobowych umieszczone są w zamykanych pomieszczeniach,
      - Obszar, w którym przetwarzane są dane osobowe, poza godzinami pracy, chroniony jest czujnikami ruchu,
      - Zbiory danych osobowych przechowywane są w szafach z zamkiem patentowym.
      - Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.
   b) środki techniczne (np. firewall, antywirus, podtrzymanie zasilania UPS);
      - Zastosowano urządzenia typu UPS chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania,
      - Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła,
      - Zastosowano systemowe mechanizmy wymuszające okresową zmianę haseł,
      - Zastosowano środki ochrony przed szkodliwym oprogramowaniem (ESET NOD32 Anitvirus4),
      - Na styku sieci urzędu z internetem zastosowano sprzętowy firewall do ochrony dostępu do lokalnej sieci komputerowej,
      - Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego,
      - Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe,
   c) środki organizacyjne (np. utworzenie Instrukcji zarządzania systemem informatycznym);
      - ✓ sporządzono i wdrożono Politykę bezpieczeństwa;
      - ✓ sporządzono i wdrożono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Lipno
      - ✓ wyznaczono ABI i ASI

- ✓ do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez administratora danych
- ✓ Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych,
- ✓ Osoby zatrudnione przy przetwarzaniu danych osobowych zobowiązane zostały do zachowania ich w tajemnicy,
- ✓ przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych;
- ✓ przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych
- ✓ dokumenty i nośniki informacji zawierające dane osobowe, które podlegają zniszczeniu, neutralizuje się za pomocą urządzeń do tego przeznaczonych lub dokonując takiej ich modyfikacji, która nie pozwoli na odtworzenie ich treści, aby po dokonaniu usunięcia danych niemożliwa była identyfikacja osób.



Załącznik nr 6 do Polityki Bezpieczeństwa

Data nadania upoważnienia: .....

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 37 ustawy z dnia 29.08.1997r. o ochronie danych osobowych (Dz. U. 2016 poz. 922 z późn. zm.)

1. Upoważniam Panią/Pana .....
   zatrudnioną/-ego na stanowisku .....
   w Urzędzie Gminy Lipno do dostępu zbiorów danych osobowych w celu ich przetwarzania zgodnie z zajmowanym stanowiskiem

2. Identyfikator/Login: .....

3. Upoważnienie wygasa z chwilą ustania Pana/Pani zatrudnienia w Urzędzie Gminy Lipno.

Wystawił: .....
(podpis Administratora Danych Osobowych)

4. Osoba upoważniona do przetwarzania danych, objętych zakresem, o którym mowa wyżej, jest zobowiązana do zachowania ich w tajemnicy, również po ustaniu zatrudnienia oraz zachowania w tajemnicy informacji o ich zabezpieczeniu.

Data i podpis osoby upoważnionej: .....

Wykonano w 3 egzemplarzach
1. Osoba upoważniona
2. Kadry
3. ABI

OŚWIADCZENIE O ZACHOWANIU POUFNOŚCI DANYCH OSOBOWYCH

Zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których mam, lub będę miał/-a dostęp w związku z wykonywaniem jakichkolwiek czynności na rzecz Urzędu Gminy Lipno.

Zobowiązuję się przestrzegać wszelkich procedur obowiązujących w wyżej wymienionej jednostce organizacyjnej dotyczących ochrony danych osobowych – w szczególności określonych w Polityce Bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym.

Oświadczam, że zapoznałem/-am się z przepisami dotyczącymi ochrony danych osobowych, w tym z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz. U. z 2016 poz. 922 z późn. zm.), w tym z zasadami odpowiedzialności karnej określonymi w rozdziale 8 wyżej wymienionej ustawy.

.....
(data i podpis osoby oświadczającej)

Wójt
Jacek Kwaśniński

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

L.p.	Imię i nazwisko	Stanowisko/komórka organizacyjna	**Zakres** *(określenie, do jakich zbiorów dana osoba ma dostęp, zgodnie z załącznikiem numer 2 do Polityki Bezpieczeństwa)*	Data nadania upoważnienia	Data ustania upoważnienia	Identyfikator/ Login w danym systemie informatycznym

WYKAZ PODMIOTÓW, KTÓRYM UDOSTĘPNIONO DANE OSOBOWE

L.p.	**Imię i Nazwisko/Nazwa zbioru** *(możliwie najpełniejszy opis osoby, której dane zostały udostępnione lub całego zbioru)*	**Data udostępnienia**	**Nazwa podmiotu, któremu udostępniono dane** *(np. upoważniony organ, instytucja lub inny, który wykazał uprawnienie do udostępnienia mu danych)*	**Cel udostępnienia** *(podstawa prawna/numer umowy)*	**Zakres udostępnionych danych** *(jakie dane zostały udostępnione)*	**Rodzaj zbioru/zasobu i jego lokalizacja** *(np. papierowy wydruk, dane w formie elektronicznej)*

Wójt
Jacek Karwicki

WYKAZ PODMIOTÓW Z KTÓRYMI ZAWARTO UMOWY POWIERZENIA PRZETWARZANIA OSOBOWYCH

L.p.	Nazwa podmiotu, któremu powierzono dane	Data powierzenia	Cel powierzenia oraz numer umowy powierzenia	Zakres powierzonych danych *(jakie dane zostały powierzone)*	Określenie zbioru/zasobu

Wójt
Jacek Jarmiński

WYKAZ OSÓB, KTÓRYM UDOSTĘPNIONO DANE OSOBOWE

L.p.	Imię i nazwisko osoby, której dane są udostępniane	Data udostępnienia	Rodzaj zbioru/zasobu i jego lokalizacja *(np. papierowy wydruk danych zawartych w określonym zbiorze)*

Wójt
Jacek Kamiński

ZATWIERDZAM"
Administrator Danych
Wójt
Jacek Kwaśniński
.....

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

w URZĘDZIE GMINY LIPNO

Wersja 1.0

I – Część ogólna

§ 1 Zgodnie z art. 39a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 1997 Nr 133 poz. 883) oraz z § 3 ust. 1 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024), ustanawia się „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych".

§ 2 Ilekroć w niniejszym dokumencie jest mowa o:
Administrator danych – rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, o której mowa w art.. 3 ustawy, decydującej o celach i środkach przetwarzania danych osobowych.

Administrator bezpieczeństwa informacji /ABI/ – należy przez to rozumieć Administratora Bezpieczeństwa Informatycznego w rozumieniu § 3 niniejszej części. Jest to osoba 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.

Administrator systemów informatycznych – należy przez to rozumieć Administratora Systemu Informatycznego (ASO) w rozumieniu § 3 niniejszej części. Jest to 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.

Bezpieczeństwo przetwarzania danych osobowych – zachowanie integralności, poufności i rozliczalności danych osobowych ; ponadto należy brać pod uwagę inne cechy, w szczególności dostępność, niezawodność.

GIODO – Generalny Inspektor Ochrony Danych Osobowych.

Integralność danych – właściwość zapewniająca, dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,

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.

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

Rozliczalność – jest to właściwość zapewniająca ,że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

Przetwarzanie danych osobowych – są to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te które wykonuje się w systemie informatycznym.

Ustawa – Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 roku (tj. Dz. U. z 2016 roku poz. 922 z późn. zm.).

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. z 2004r. poz.1024).

Urząd – Urząd Gminy Lipno.

Użytkownik systemu –należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym w drodze upoważnienia, o jakim mowa w części III § 13 pkt. 1, Polityki Bezpieczeństwa.

Identyfikatorze użytkownika – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.

Haśle – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znanych jedynie osobie uprawnionej do pracy w systemie informatycznym.

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

System informatyczny – jest to zespół współpracujących urządzeń , programów, procedur przetwarzania informacji i oraz narzędzi programowych zastosowanych w celu przetwarzania danych.

Sieci telekomunikacyjnej – rozumie się przez to sieć telekomunikacyjną w rozumieniu art.2 pkt. 23 ustawy z dnia 21 lipca 2000r – prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852, z późn. zm.)

Sieci publicznej – rozumie się p[rzez to sieć publiczną w rozumieniu art. 2 pkt. 22 ustawy z dnia 21 lipca 2000r. – Prawo telekomunikacyjne.

Teletransmisji – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej zestawienia zakresu i treści przetwarzanych danych.

Raporcie – rozumie się przez to przygotowane przez system informatyczny

Zbiór danych – jest to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego , czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

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 nie elektronicznej, poza systemem informatycznym, w szczególności w formie kartoteki, skorowidza, księgi ,wykazu a także w każdej innej formie w postaci zbioru.

Instrukcji – należy przez to rozumieć niniejszy dokument

Polityce Bezpieczeństwa – należy przez to rozumieć przyjęty do stosowania w jednostce organizacyjnej dokument zatytułowany: „Polityka Bezpieczeństwa w Urzędzie Gminy Lipno."

§ 3. Administratora Systemów Informatycznych (ASI) wyznacza Administrator Danych Osobowych, któremu wydaje się pisemne upoważnienie wg wzoru stanowiącego załącznik nr 1 do niniejszego dokumentu. ASI jest zobowiązany do podpisania oświadczenia, stanowiącego załącznik nr 6 do Polityki Bezpieczeństwa.

§ 4 Administrator Systemów Informatycznych (ASI) jest odpowiedzialny za przestrzeganie zasad bezpieczeństwa przetwarzania danych osobowych w zakresie systemu informatycznego służącego do tego celu.

1. Do kompetencji Administratora Systemów Informatycznych należy:
   a) Zabezpieczenie systemów przetwarzania danych osobowych zgłoszonych ASI, w zależności od kategorii przetwarzanych w tym systemie danych
   b) Zapewnienie poufności, integralności, dostępności i rozliczalności danych przetwarzanych w systemach informatycznych
2. Do obowiązku Administratora Systemów Informatycznych należy:
   a) Bieżący nadzór oraz zapewnienie optymalnej ciągłości działania systemu informatycznego w tym opracowanie procedur określających zarządzanie systemem informatycznym przetwarzającym dane osobowe
   b) Reagowanie bez zbędnej zwłoki, w przypadku naruszenia bądź powstania zagrożenia bezpieczeństwa danych osobowych
   c) Przeciwdziałanie próbom naruszenia bezpieczeństwa danych osobowych
   d) Analizę raportów wszystkich zdarzeń w tym incydentów związanych z bezpieczeństwem systemów przetwarzania danych
   e) Zapewnienie wszystkich wdrażanych systemów przetwarzania danych osobowych z Ustawą oraz niniejsza Polityką bezpieczeństwa i Instrukcją zarządzania systemem Informatycznym w Urzędzie Gminy Lipno
   f) Instalację i konfigurację oprogramowania i sprzętu typu „stand - alone", sieciowego i serwerowego używanego do przetwarzania danych osobowych
   g) Konfigurację i administrację oprogramowaniem systemowym i sieciowym zabezpieczającym dane osobowe przed nieupoważnionym dostępem
   h) Nadzór nad czynnościami związanymi ze sprawdzaniem systemu pod kątem obecności szkodliwego oprogramowania
   i) Nadzór nad systemem komunikacji w sieci komputerowej oraz przesyłaniem danych za pośrednictwem urządzeń teletransmisji

j) Nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe
k) Świadczenie pomocy technicznej w ramach oprogramowania a także serwis sprzętu komputerowego będącego na stanie Urzędu Gminy Lipno, służącego do przetwarzania danych osobowych
l) Diagnozowanie i usuwanie awarii sprzętu komputerowego oraz realizacje umów z firmami świadczącymi usługi pogwarancyjnego sprzętu komputerowego
m) Wykonywanie i zarządzanie kopiami awaryjnymi oprogramowania systemowego (w tym danych osobowych oraz zasobów umożliwiających ich przetwarzanie) i sieciowego
n) Nadzór nad wdrażaniem i zarządzaniem aplikacjami (przeglądanie, nadawanie, i odbieranie uprawnień użytkownikom, itp.), w których przetwarzane są dane osobowe
o) Zatwierdzanie wniosków zgłoszeń do rejestracji zbiorów danych osobowych w części E i F
p) Umożliwienie przeprowadzenia kontroli systemu informatycznego przez służby Biura Generalnego Inspektora Ochrony Danych Osobowych

§ 5 W Urzędzie Gminy system informatyczny służący do przetwarzania danych osobowych jest połączony z siecią Internet, w związku z powyższym wprowadza się wysoki poziom bezpieczeństwa.

II – Część szczegółowa

Urząd Gminy Lipno	Instrukcja Zarządzania Systemem Informatycznym	*Nr / wersja procedury*
Tytuł procedury: **Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym**		1/1.0

Przedmiot i cel:
Celem procedury jest zapewnienie kontroli dopuszczeniem do przetwarzania danych wyłącznie osób posiadające upoważnienie nadane przez administratora danych, który jest zobowiązany do zapewnienia kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.

Osoby realizujące:
Administrator Danych Osobowych,
Administrator Bezpieczeństwa Informacji,
Administrator Systemu Informatycznego,
Właściciel zasobów (Kierownik referatu),
Użytkownik systemu (pracownik).

Dokumenty związane z procedurą:
Polityka Bezpieczeństwa w Urzędzie Gminy Lipno,
Instrukcja Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych w Urzędzie Gminy Lipno

Wprowadzenie:
Administrator Danych Osobowych jest odpowiedzialny za przetwarzanie i ochronę danych osobowych zgodnie z przepisami prawa, w tym wprowadzenie do stosowania procedur postępowania zapewniających prawidłowe przetwarzanie danych osobowych, rozumiane jako ochronę danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zmianą lub zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem Ustawy oraz utratą, uszkodzeniem lub zniszczeniem.

Opis procedury:
1. Użytkownik zamierzający przetwarzać dane osobowe, po uzyskaniu upoważnienia stanowiącego załącznik nr 6 do Polityki Bezpieczeństwa, występuje do przełożonego – kierownika referatu (właściciela zasobów) o nadanie identyfikatora (loginu) i hasła w celu umożliwienia wykonywania przetwarzania danych osobowych w systemie informatycznym. ASI na wniosek właściciela zasobów zobowiązany jest niezwłocznie przydzielić użytkownikowi identyfikator i tymczasowe hasło dostępowe. Podanie użytkownikowi hasła musi nastąpić w sposób umożliwiający zapoznanie się z nim przez osoby trzecie.
   Tymczasowe hasło ustanowione podczas przyznania uprawnień przez ASI użytkownik musi zmienić na indywidualne podczas pierwszego logowania się w systemie.
2. W przypadku wygaśnięcia przesłanek uprawniających użytkownika do przetwarzania danych osobowych, na wniosek kierownika referatu (właściciela zasobu) ASI niezwłocznie wyrejestrowuje z systemu informatycznego identyfikator (login) użytkownika oraz unieważnia hasło. ASI zobowiązany jest do dopełnienia czynności uniemożliwiających ponowne wykorzystanie identyfikatora użytkownika, którego uprawnienia wygasły.
3. ABI zobowiązany jest do prowadzenia rejestru użytkowników i ich uprawnień w systemie informatycznym.

Nr rozdziału w dokumencie	*Ilość stron:*	*Data wprowadzenia procedury*	*Data wycofania procedury*
Część III § 21	1	15.10.2016r.	

Urząd Gminy Lipno	Instrukcja Zarządzania Systemem Informatycznym	*Nr / wersja procedury*
Tytuł procedury: **Stosowane metody i środki uwierzytelniania, oraz procedury związane z ich zarządzaniem i użytkowaniem**		2/1.0

Przedmiot i cel:
W systemie informatycznym służącym do przetwarzania danych osobowych stosuje się mechanizmy kontroli dostępu do tych danych. Dostęp jest możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia

Osoby realizujące:
Administrator Bezpieczeństwa Informacji,
Administrator Systemu Informatycznego,
Właściciel zasobów (Kierownik referatu),
Użytkownik systemu (pracownik).

Dokumenty związane z procedurą:
Polityka Bezpieczeństwa w Urzędzie Gminy Lipno,
Instrukcja Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych w Urzędzie Gminy Lipno

Wprowadzenie:
Identyfikatory i hasła są sposobem zagwarantowania rozliczalności, poufności i integralności przetwarzanych danych osobowych w systemach informatycznych. Służą do weryfikowania tożsamości użytkownika, uzyskania dostępu do określonych zasobów, kont uprzywilejowanych lub uruchamiania określonych funkcji.

Opis procedury:

1. Mając na uwadze zagwarantowanie wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych oraz zagwarantowanie użytkownikom pełnej rozliczalności wykonywanych przez nich operacji w systemach informatycznych, wszyscy użytkownicy przy uwierzytelnianiu do systemów informatycznych powinni stosować się do poniższych zasad:
   a) Użytkownik systemu powinien posiadać unikalny identyfikator do swojego osobistego użytku
   b) Hasła tworzone przez użytkownika stanowią tajemnicę służbową, znaną wyłącznie temu użytkownikowi
   c) Użytkownik ponosi pełną odpowiedzialność za utworzenie hasła dostępu oraz jego przechowywanie
   d) Hasła nie mogą być ujawniane lub przekazywane komukolwiek, bez względu na okoliczności i utrzymywane w tajemnicy nawet po upływie ich ważności.
   e) Użytkownik nie powinien przechowywać haseł w widocznych miejscach, nie powinien umieszczać haseł w żadnych automatycznych procesach logowania (skryptach, makrach lub pod klawiszami funkcyjnymi)
   f) hasło składa się, z co najmniej 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne
   g) osobą odpowiedzialną za przydział identyfikatora i pierwszego hasła jest informatyk
   h) użytkownik, po pierwszym zalogowaniu się do systemu jest zobowiązany do zmiany hasła, jest również zobowiązany do zmiany hasła, co każde 60 dni – (dotyczy to tylko systemu Windows)
   i) Użytkownicy są odpowiedzialni za wszelkie działania w systemach informatycznych prowadzone z użyciem ich identyfikatora i hasła.

Nr rozdziału w dokumencie	*Ilość stron:*	*Data wprowadzenia procedury*	*Data wycofania procedury*
Część III § 22	1	15.10.2016r.	

Urząd Gminy Lipno	Instrukcja Zarządzania Systemem Informatycznym	*Nr / wersja procedury*
Tytuł procedury: **Rozpoczęcie, zawieszenie i zakończenie pracy przeznaczone dla użytkowników systemu**		3/1.0

Przedmiot i cel:
Celem procedury jest zabezpieczenie danych osobowych przed nieuprawnionym dostępem i utratą poufności w sytuacji, gdy użytkownik rozpoczyna, przerywa lub kończy pracę w systemie informatycznym przetwarzającym dane osobowe.

Osoby realizujące:
Właściciel zasobów (Kierownik referatu),
Użytkownik systemu (pracownik).

Dokumenty związane z procedurą:
Polityka Bezpieczeństwa w Urzędzie Gminy Lipno,
Instrukcja Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych w Urzędzie Gminy Lipno

Wprowadzenie:
W celu osiągnięcia i utrzymania wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych konieczne jest zaangażowanie każdego pracownika w zakresie ochrony danych osobowych.

Opis procedury:

1. Przed przystąpieniem do pracy z systemem, użytkownik zobowiązany jest dokonać sprawdzenia stanu urządzeń informatycznych oraz oględzin swojego stanowiska pracy, ze zwróceniem szczególnej uwagi, czy nie zaszły okoliczności wskazujące na naruszenie ochrony danych osobowych.
2. W przypadku stwierdzenia bądź podejrzenia, iż miało miejsce naruszenie ochrony danych osobowych, użytkownik systemu zobowiązany jest niezwłocznie poinformować o tym fakcie ASI, który niezwłocznie podejmuje czynności zmierzające do ustalenia przyczyn naruszeń zasad bezpieczeństwa i stosuje środki uniemożliwiające ich naruszanie w przyszłości.
3. Rozpoczynając prace na komputerze użytkownik loguje się do systemu.
4. Przed opuszczeniem stanowiska pracy użytkownik obowiązany jest zablokować swoją stację roboczą poprzez wciśnięcie klawiszy „Windows + L" i wybranie opcji „zablokuj stację roboczą".Kończąc prace użytkownik zobowiązany jest do wylogowania się z systemu informatycznego i zabezpieczenie stanowiska pracy, w szczególności wszelkiej dokumentacji i wydruków.

Nr rozdziału w dokumencie	*Ilość stron:*	*Data wprowadzenia procedury*	*Data wycofania procedury*
Część III § 13	1	15.10.2016r.	

Urząd Gminy Lipno	Instrukcja Zarządzania Systemem Informatycznym	*Nr / wersja procedury*
Tytuł procedury: **Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania**		4/1.0

Przedmiot i cel:
Celem procedury jest zabezpieczenie danych osobowych podczas przetwarzanie danych osobowych w systemach informatycznych *(operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te które wykonuje się w systemie informatycznym).*

Osoby realizujące:
Administrator Systemu Informatycznego,

Dokumenty związane z procedurą:
Polityka Bezpieczeństwa w Urzędzie Gminy Lipno,
Instrukcja Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych w Urzędzie Gminy Lipno

Wprowadzenie:
W celu osiągnięcia i utrzymania wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych konieczne jest tworzenie kopii zapasowych tych baz..

Opis procedury:
Kopie zapasowe wykonywane są na koniec każdego dnia roboczego z wykorzystaniem odpowiednio skonfigurowanych zasobów sieciowych Urzędu Gminy.

Backup baz danych - Robione automatycznie przez serwer.
Kopie dzienne - Codziennie od poniedziałku do piątku.
Kopie tygodniowe - W każdą sobotę.
Kopie miesięczne - W pierwszą niedziele miesiąca.
W przypadku awarii jesteśmy wstanie odzyskać nawet kopie z 12 miesięcy wstecz z zachowaniem harmonogramu powyżej

Backup pozostałych danych z serwera - Robione automatycznie przez serwer
Kopie dzienne - Codziennie od poniedziałku do piątku (dyski sieciowe i profile użytkownika)
W przypadku awarii jesteśmy wstanie odzyskać pięć ostatnich kopii

Backup danych użytkowników.
Użytkownik dane które mają być archiwizowane zobowiązany jest trzymać na „Pulpicie" lub „Moich dokumentach". Dane te przy wyłączaniu komputera kopiują się na serwer.
Jest to tzw. usługa profili mobilnych, Backup danych na serwerze jest robiony codziennie od poniedziałku do piątku. W przypadku awarii jesteśmy wstanie odzyskać pięć ostatnich kopii.

Nr rozdziału w dokumencie	*Ilość stron:*	*Data wprowadzenia procedury*	*Data wycofania procedury*
Część III § 13	1	15.10.2016r.	

Urząd Gminy Lipno	Instrukcja Zarządzania Systemem Informatycznym	*Nr / wersja procedury*
Tytuł procedury: **Sposób, miejsce i okres przechowywania kopii zapasowych**		5/1.0

Przedmiot i cel:
Celem procedury jest zabezpieczenie danych osobowych przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem.

Osoby realizujące:
Administrator Systemu Informatycznego

Dokumenty związane z procedurą:
Polityka Bezpieczeństwa w Urzędzie Gminy Lipno,
Instrukcja Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych w Urzędzie Gminy Lipno

Wprowadzenie:
Kopie zapasowe przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem.

Opis procedury:
Sposób, miejsce i okres przechowywania

1. Elektronicznych nośników informacji
   a) Sprzęt komputerowy, na którego dyskach twardych zawarte są dane osobowe, przechowywany jest w obszarze przetwarzania danych osobowych, w pomieszczeniach zabezpieczonych zgodnie z załącznikiem nr 1 do Polityki Bezpieczeństwa.
2. Kopii zapasowych o których mowa w § 4
   a) Kopie zapasowe przechowywane są w „serwerowni" pomieszczeniu nr 11 i12 na pierwszym piętrze.
3. Kopie zapasowe usuwa się niezwłocznie po ustaniu ich użyteczności.

Nr rozdziału w dokumencie	*Ilość stron:*	*Data wprowadzenia procedury*	*Data wycofania procedury*
Część III § 13	1	15.10.2016r.	

Urząd Gminy Lipno	Instrukcja Zarządzania Systemem Informatycznym	*Nr / wersja procedury*
Tytuł procedury: **Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt. III ppkt 1 załącznika do rozporządzenia**		6/1.0

Przedmiot i cel:
Celem procedury jest zabezpieczenie systemu informatycznego do przetwarzania danych przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do niego.

Osoby realizujące:
Administrator Systemu Informatycznego

Dokumenty związane z procedurą:
Polityka Bezpieczeństwa w Urzędzie Gminy Lipno,
Instrukcja Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych w Urzędzie Gminy Lipno

Wprowadzenie:
System informatyczny służący do przetwarzania danych osobowych zabezpiecza się , w szczególności przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego.

Opis procedury:
System informatyczny służący do przetwarzania danych osobowych zabezpieczony jest oprogramowaniem antywirusowym „ESET NOD32 Antivirus ". Użytkownikom nie wolno otwierać na komputerach, na których odbywa się przetwarzanie danych osobowych, plików pochodzących z niewiadomego źródła bez zgody ASI

1. Za wdrożenie i korzystanie z oprogramowania antywirusowego, określonego w pkt. 1, oraz oprogramowania firewall, odpowiada ASI.

Nr rozdziału w dokumencie	*Ilość stron:*	*Data wprowadzenia procedury*	*Data wycofania procedury*
Część III § 13	1	15.10.2016r.	

Urząd Gminy Lipno	Instrukcja Zarządzania Systemem Informatycznym	*Nr / wersja procedury*
Tytuł procedury: **Sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt. 4**		7/1.0

Przedmiot i cel:
Celem procedury jest zagwarantowanie praw wynikających z ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tj. Dz. U. z 2016 r., poz.922 z późn. zm.)

1. *Art. 1.1 Każdy ma prawo do ochrony dotyczących go danych osobowych.*
2. *Art. 1.2 Przetwarzanie danych osobowych może mieć miejsce ze względu na dobro publiczne, dobro osoby, której dane dotyczą, lub dobro osób trzecich w zakresie i trybie określonym ustawą.*

Osoby realizujące:
Właściciel zasobów (Kierownik referatu),
Użytkownik systemu (pracownik).

Dokumenty związane z procedurą:
Polityka Bezpieczeństwa w Urzędzie Gminy Lipno,
Instrukcja Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych w Urzędzie Gminy Lipno

Wprowadzenie:
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 ich na piśmie- system ten zapewnia odnotowanie informacji o odbiorcach, *(z wyłączeniem osób, których dane dotyczą, osób posiadających upoważnienie do przetwarzania danych, przedstawiciela, którym mowa w art.31a ustawy, podmiotu o którym mowa w art. 31 ustawy, organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem)* którym dane osobowe zostały udostępnione, i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych.

Opis procedury:

1. Odnotowanie informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia *(z wyłączeniem osób, których dane dotyczą, osób posiadających upoważnienie do przetwarzania danych, przedstawiciela, którym mowa w art.31a ustawy, podmiotu o którym mowa w art. 31 ustawy, organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem),* odbywa się poprzez zapisanie tej informacji w utworzonym na dysku komputera pliku dotyczącym danej osoby, zgodnie z zasadą że:
2. Dla każdej osoby, której dane są przetwarzane, system informatyczny służący do przetwarzania danych osobowych *(z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie)* zapewnia odnotowanie:
   a) daty pierwszego wprowadzenia danych do systemu *(automatycznie)*
   b) identyfikatora użytkownika wprowadzającego dane osobowe do systemu *(automatycznie)*
   c) źródła danych *(jedynie w przypadku zbierania danych nie od osoby, której dotyczą)*
   d) informacji o odbiorcach w rozumieniu art. 7 pkt 6 ustawy o ochronie danych osobowych
   e) sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 ustawy o ochronie danych osobowych
3. Dla każdej osoby, której dane osobowe są przetwarzane system informatyczny, zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w pkt. 2 lit. a-e, tj.
   a) daty pierwszego wprowadzenia danych do systemu,
   b) identyfikatora użytkownika wprowadzającego dane osobowe do systemu,
   c) źródła danych *(jedynie w przypadku zbierania danych nie od osoby, której dotyczą)*
   d) informacji o odbiorcach w rozumieniu art. 7 pkt 6 ustawy o ochronie danych osobowych
   e) sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 ustawy o ochronie danych osobowych

Nr rozdziału w dokumencie	*Ilość stron:*	*Data wprowadzenia procedury*	*Data wycofania procedury*
Część III § 13	1	15.10.2016r.	

Urząd Gminy Lipno	Instrukcja Zarządzania Systemem Informatycznym	*Nr / wersja procedury*
Tytuł procedury: **Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych:**		8/1.0

Przedmiot i cel:
Administrator danych jest zobowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę danych osobowych odpowiednia do zagrożeń oraz kategorii danych objętych ochroną.
Osoby realizujące:
Właściciel zasobów (Kierownik referatu),
Użytkownik systemu (pracownik).
Dokumenty związane z procedurą:
Polityka Bezpieczeństwa w Urzędzie Gminy Lipno,
Instrukcja Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych w Urzędzie Gminy Lipno
Wprowadzenie:
W celu osiągnięcia i utrzymania wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych konieczne jest zabezpieczenie danych przed ich udostępnieniem osobom nieuprawnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem..
Opis procedury:

1. Bieżących oraz okresowych przeglądów, napraw i konserwacji niewymagających angażowania zewnętrznych form serwisowych dokonuje ASI.
2. W przypadku stwierdzenia przez ASI nieprawidłowości w działaniu elementów systemu opisanych w pkt.1 niniejszego paragrafu podejmuje on niezwłocznie czynności zmierzające do przywrócenia ich prawidłowego działania.
3. Przeglądów konserwacji zbiorów danych osobowych dokonują użytkownicy, zgodnie z indywidualnymi zakresami uprawnień i odpowiedzialności.
4. Jeżeli do przywrócenia prawidłowego działania systemu niezbędna jest pomoc podmiotu zewnętrznego, wszelkie czynności na sprzęcie komputerowym dokonywane w obszarze przetwarzania danych osobowych odbywają się za wiedzą ABI przez uprawnionych przedstawicieli firm pod nadzorem ASI.
5. 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 ASI
6. Usuwanie danych osobowych utrwalonych na nośnikach elektronicznych następuje poprzez nadpisanie usuwanych informacji przez ASI w taki sposób, by nie istniała możliwość ich ponownego odczytania. W celu usunięcia danych zapisanych na elektronicznych nośnikach ASI może dokonać ich fizycznego uszkodzenia w taki sposób, by nie istniała możliwość odtworzenia zapisanych na nich danych.

Nr rozdziału w dokumencie	*Ilość stron:*	*Data wprowadzenia procedury*	*Data wycofania procedury*
CzęśćIII § 13	1	15.10.2016r.	

Urząd Gminy Lipno	Instrukcja Zarządzania Systemem Informatycznym	*Nr / wersja procedury*
Tytuł procedury: **Sposób stosowania środków zapewnienia poufności i integralności danych na urządzeniach i nośnikach przekazywanych poza obszar w którym przetwarzane są dane osobowe.**		9/1.0

Przedmiot i cel:
Administrator danych jest zobowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę danych osobowych odpowiednia do zagrożeń oraz kategorii danych objętych ochroną.

Osoby realizujące:
Właściciel zasobów (Kierownik referatu),
Użytkownik systemu (pracownik).

Dokumenty związane z procedurą:
Polityka Bezpieczeństwa w Urzędzie Gminy Lipno,
Instrukcja Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych w Urzędzie Gminy Lipno

Wprowadzenie:
W celu osiągnięcia i utrzymania wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych konieczne jest zabezpieczenie danych przed ich udostępnieniem osobom nieuprawnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem..

Opis procedury:
1. Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych osobowych, w tym dodatkowo zabezpiecza hasłem pliki lub foldery zawierające dane osobowe.
2. System informatyczny służący do przetwarzania danych osobowych jest zabezpieczony przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej poprzez stosowanie (alternatywnie a lub b, lub oba na raz):
   a) Zasilacz UPC APS Back-UPS Pro 1200BR1200G-FR. Urządzenie umożliwia automatyczne bezpieczne wyłączenie serwera.
   b) Urządzenie Synology DS216se które przechowuje kopie serwera na wypadek jego awarii.
   c) listew przepięciowych, połączonych pomiędzy siecią zasilającą a komputerami

Nr rozdziału w dokumencie	*Ilość stron:*	*Data wprowadzenia procedury*	*Data wycofania procedury*
Część III § 13	1	15.10.2016r.	

Lipno 1.10.2016r.

UPOWAŻNIENIE
DLA ADMINISTRATORA SYSTEMU INFORMATYCZNEGO (ASI)

Na podstawie części I §3 Instrukcji Zarządzania Systemem Informatycznym, z dniem 1.10.2016r wyznaczam Administratora Systemu Informatycznego (ASI), powierzając tę funkcję Danielowi Mruk.

Wójt
Jacek Kwiatkowski

.....
podpis w imieniu Administratora Danych Osobowych (ADO)

Ja, niżej podpisany, zobowiązuję się do pełnienia obowiązków Administratora Systemu Informatycznego w oparciu o przepisy wewnętrzne obowiązujące w jednostce organizacyjnej, ze szczególnym uwzględnieniem obowiązków przewidzianych w części I § 4 Instrukcji Zarządzania Systemem Informatycznym.

.....
podpis Administratora Systemu Informatycznego (ASI)