Zarządzenie Nr 120. 2 .2014
Wójta Gminy Jasienica
z dnia. 23. stycznia. 2014 r.

w sprawie wprowadzenia „Polityki bezpieczeństwa informacji" w Urzędzie Gminy Jasienica.

Na podstawie art. 36 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz §3 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. Nr 100, poz. 1024), zarządzam co następuje:

§ 1.

Wprowadzam „Politykę bezpieczeństwa informacji", która stanowi załącznik do niniejszego zarządzenia.

§ 2.

Zobowiązuję pracowników Urzędu Gminy Jasienica do stosowania zasad określonych w „Polityce bezpieczeństwa informacji"

§ 3.

Nadzór nad wykonaniem zarządzenia powierzam Sekretarzowi Gminy Jasienica.

§ 4.

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT
mgr inż. Janusz Pierzyna

Załącznik do Zarządzenia nr .....
Wójta Gminy Jasienica
z dnia.....

Polityka Bezpieczeństwa Informacji
w
Urzędzie Gminy Jasienica

Spis załączników:

Metryka dokumentu:

Nazwa dokumentu:	Polityka Bezpieczeństwa Informacji w Urzędzie Gminy Jasienica
Właściciel:	Urząd Gminy Jasienica
Odbiorca:	Pracownicy Urzędu Gminy Jasienica
Wersja:	1.0.2013
Data utworzenia:	13.09.2013
Liczba stron:	43
Data ostatniej modyfikacji:	27.12.2013

Wprowadzenie

Polityka Bezpieczeństwa Informacji w Urzędzie Gminy Jasienica, zwana dalej „polityką bezpieczeństwa" została stworzona z myślą o ochronie danych osobowych przetwarzanych w Urzędzie Gminy Jasienica, w wersji papierowej (kartoteki, skorowidze, księgi, wykazy i inne zbiory ewidencyjne) a przede wszystkim w systemie informatycznym. Jest dokumentem wewnętrznym wydanym przez Wójta Gminy Jasienica przeznaczonym dla pracowników pracujących przy przetwarzaniu danych osobowych.

Potrzeba opracowania niniejszego dokumentu wynika z ustawy z dnia 29 sierpnia 1997 r. **o ochronie danych osobowych** (tj. Dz. U. z 2002 r. Nr 101, poz. 926 z pózn. zm.) 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** (Dz. U. Nr 100, poz 1024 z pózn. zm.)

Przetwarzanie danych osobowych w Urzędzie Gminy Jasienica jest niezbędne do:

1. Wypełniania statutowych obowiązków Urzędu Gminy oraz zadań własnych wynikających z przepisów prawa.
2. Gromadzenia ofert pracy i przeprowadzania procesu naboru.
3. Prowadzenia dokumentów związanych z zatrudnieniem i wynagradzaniem pracowników.

Dokument ten opisuje wymagane zasady postępowania podczas codziennej pracy jak również w momencie wystąpienia sytuacji zagrożenia bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych. Zapoznaje pracowników z możliwymi zdarzeniami naruszającymi ochronę danych osobowych tj.: utrata danych, zniszczenie danych, niezamierzone pomyłki pracowników itp. i wskazuje prawidłowe zachowanie w w/w sytuacjach.

Polityka bezpieczeństwa zwraca również uwagę na konsekwencje, jakie mogą ponieść pracownicy niestosujący się do zasad określonych w niniejszym dokumencie, w tym konsekwencji dyscyplinarnych w przypadku naruszenia bezpieczeństwa danych osobowych.

Będąc świadomym ważności przetwarzanych danych osobowych w Urzędzie Gminy Jasienica, kierownictwo Urzędu zobowiązuje się do dołożenia wszelkich starań, aby zapewnić ich bezpieczeństwo przez zastosowanie odpowiednich środków technicznych i organizacyjnych jak również przez zabezpieczenie na ich ochronę odpowiednich środków finansowych.

Rozdział 1 Podstawa prawna

1. Opracowanie Polityki Bezpieczeństwa Informacji w Urzędzie Gminy Jasienica wynika z:
   1.1 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz. U. z 2002 r. Nr 101, poz. 926 z pózn. zm.)
   1.1 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 (Dz. U. Nr 100, poz 1024)
2. Niniejszy dokument oparty jest również na zapisach Polskiej Normy PN ISO IEC 27001

Rozdział 2 Podstawowe definicje

1. **Urząd** – należy przez to rozumieć Urząd Gminy Jasienica.
2. **Ustawa** – należy przez to rozumieć ustawę o z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz. U. z 2002 r. Nr 101, poz. 926 z pózn. zm.).
3. **Rozporządzenie** – należy przez to rozumieć 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 (Dz. U. Nr 100, poz 1024)
4. **Norma** – Polska Norma PN ISO IEC 27001.
5. **Administrator danych osobowych - (ADO)** należy przez to rozumieć Wójta Gminy Jasienica. Pojęcie to definiuje art. **7 ust. 4 ustawy**.
6. **Administrator bezpieczeństwa informacji – (ABI)** należy przez to rozumieć osobę wyznaczoną przez Wójta Gminy Jasienica odpowiedzialną za przestrzeganie zasad ochrony danych osobowych określonych w niniejszym dokumencie oraz wymagań dotyczących ochrony danych osobowych wynikających z odrębnych przepisów. Jest to osoba odpowiedzialna za ochronę danych osobowych. Pojęcie to definiuje art. **36 ust. 3** ustawy.
7. **Administrator systemu informatycznego – (ASI)** należy przez to rozumieć osobę odpowiedzialną za poprawne funkcjonowanie, konserwację oraz wdrażanie **technicznych zabezpieczeń** systemów informatycznych, w których przetwarzane są dane osobowe.
8. **Dane osobowe** – są wszelkie informacje dotyczące osoby zidentyfikowanej lub możliwej do zidentyfikowania. Za dane osobowe uważamy imię, nazwisko, pesel, adres, cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Pojęcie to definiuje **art. 6 ust. 1** ustawy.
9. **Dane wrażliwe** – to dane dotyczące stanu zdrowia, nałogów, skazań, orzeczeń o ukaraniu, mandatów karnych ujawniających pochodzenie rasowe, etniczne, poglądy

polityczne, przekonania religijne lub filozoficzne. Pojęcie to definiuje **art. 27 ust. 1** ustawy.

10. **Zbiór danych osobowych** – należy przez to rozumieć każdy zestaw danych osobowych, który posiada strukturę a wyszukiwanie w nim jest możliwe według określonych kryteriów np.: pesel, imię, adres itp. Zbiór danych może mieć strukturę rozproszoną lub być podzielony funkcjonalnie. Pojęcie to definiuje **art. 7 ust. 1** ustawy.
11. **Przetwarzanie danych** – należy przez to rozumieć wszelkie operacje, jakie są wykonywane na danych osobowych tj.: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie a zwłaszcza te, które wykonuje się w systemach informatycznych. Pojęcie to definiuje art.**7 ust 2** ustawy.
12. **Polityka bezpieczeństwa Informacji** - należy przez to rozumieć niniejszy dokument zawierający zestaw reguł, których należy przestrzegać, aby zapewnić wymagany poziom bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy Jasienica.
13. **Instrukcja zarządzania systemem informatycznym** – to wewnętrzny dokument eksploatacyjny regulujący i opisujący zasady oraz procedury pracy, zarządzania i administrowania systemem informatycznym Urzędu Gminy Jasienica.
14. **System informatyczny** - należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych. Pojęcie to definiuje **art. 7 ust 2a** ustawy.
15. **Hasło** – należy przez to rozumieć ciąg znaków literowych, cyfrowych lub znaków specjalnych znanych jedynie osobie uprawnionej do pracy w systemie informatycznym, par.2 pkt.3 rozporządzenia.
16. **Identyfikator użytkownika** – należy przez to rozumieć ciąg znaków literowych, cyfrowych, za pomocą, których możliwe jest zidentyfikowanie użytkownika w systemie informatycznym. Pojęcie to definiuje **par. 2 pkt. 2** rozporządzenia.
17. **Rozliczalność** – należy przez to rozumieć właściwość, która umożliwia przypisanie działań w systemie informatycznym danemu podmiotowi. Pojęcie to definiuje **par. 2 pkt. 7** rozporządzenia.
18. **Integralność danych** – należy przez to rozumieć właściwość, która zapewnia, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany. Pojęcie to definiuje **par. 2 pkt. 8** rozporządzenia.
19. **Poufność danych** - należy przez to rozumieć właściwość, która zapewnia, że dane nie są udostępniane nieupoważnionym podmiotom. Pojęcie to definiuje **par. 2 pkt. 10** rozporządzenia.

Rozdział 3 Obowiązki osób odpowiedzialnych za przetwarzanie danych osobowych.

1. **Administrator Danych Osobowych**, którym jest Wójt zarządzeniem wyznacza Administratora Bezpieczeństwa Informacji (**art. 36 ust. 3 ustawy),** oraz przekazuje mu obowiązki związane z ochroną danych osobowych. Druk wyznaczenia ABI i przekazania mu obowiązków stanowi załącznik nr 1 do niniejszego dokumentu.
2. Administrator Danych Osobowych jest zobowiązany do:
    a. Ochrony interesów osób, których dane są przetwarzane w Urzędzie poprzez przetwarzanie tych danych zgodnie z prawem (art. 26 ust.1 ustawy).
    b. Zastosowania środków technicznych i organizacyjnych w celu zapewnienia bezpieczeństwa przetwarzanych danych w Urzędzie (art. 36 ust.1 ustawy).
    c. Zgłoszenia zbiorów danych osobowych będących w posiadaniu Urzędu do rejestracji Generalnemu Inspektorowi (art. 40 ustawy).
    d. Zgłaszania każdej zmiany w zbiorach danych osobowych w terminie do 30 dni od dnia dokonania zmiany (art. 41 pkt. 2 ustawy).
    e. Nadanie pisemnego upoważnienia do przetwarzania danych osobowych osobom pracującym przy przetwarzaniu danych osobowych zarówno w tradycyjnej formie jak i w systemie informatycznym (art. 37 ustawy). Wzór upoważnienia stanowi załącznik nr 3 Instrukcji zarządzania.
    f. Prowadzenia ewidencji osób, którym nadał upoważnienie do przetwarzania danych osobowych (art. 39 ustawy). Wykaz wydanych upoważnień stanowi załącznik nr 2 do niniejszego dokumentu.
    g. Nadzoru nad spełnieniem obowiązku informacyjnego wynikającego z art. 24 ustawy przez pracowników.

3. **Administrator Bezpieczeństwa Informacji** jest zobowiązany do:
    a. Przejęcia obowiązków Administratora Danych Osobowych.
    b. Nadzoru nad przestrzeganiem zasad ochrony danych osobowych określonych w niniejszym dokumencie przez pracowników urzędu dopuszczonych do przetwarzania danych osobowych, poprzez okresowe przeprowadzanie kontroli tych pracowników.
    c. Przeprowadzenia kontroli co najmniej raz w roku oraz sporządzania raportu pokontrolnego. Wzór dokumentu służącego do przeprowadzenia kontroli stanowi załącznik nr 3 do niniejszego dokumentu. Raport pokontrolny ma za zadanie ocenę stanu bezpieczeństwa danych osobowych, wskazanie słabych punktów zabezpieczenia oraz sposobów ich wzmocnienia. Wzór raportu pokontrolnego stanowi załącznik nr 4 do niniejszego dokumentu.
    d. Przedłożenia raportu pokontrolnego Administratorowi Danych Osobowych.
    e. Kontrola sposobu przechowywania i archiwizacji dokumentów zawierających dane osobowe pod względem prawidłowego zabezpieczenia takich dokumentów.
    f. Udział w czynnościach kontrolnych przeprowadzanych przez uprawnionych do kontroli Inspektorów GIODO.

g. Ciągłego aktualizowania polityki bezpieczeństwa i dostosowywania jej do zmieniających się zagrożeń i standardów zabezpieczeń tak, aby była skuteczna i zawsze aktualna.
h. Opracowania i wdrożenia systemu wewnętrznego szkolenia z zakresu niniejszego dokumentu oraz przepisów i ustaw dotyczących ochrony danych osobowych dla pracowników Urzędu.
i. Informowania pracowników o dokonanych zmianach, nowych zasadach postępowania i nowych zagrożeniach bezpieczeństwa informacji w formie ustnej lub pisemnej.
j. Instruowania pracowników w razie stwierdzenia nieprawidłowości w wykonywanych czynnościach z zakresu ochrony danych osobowych.
k. Aktualizacji wykazu wydanych upoważnień.

4. **Administrator systemu informatycznego** jest zobowiązany do:
   a. Nadzoru nad poprawnym funkcjonowaniem systemów informatycznych w Urzędzie.
   b. Wdrażania nowych zabezpieczeń informatycznych chroniących zasoby systemu Urzędu przed niepowołanym dostępem z zewnątrz oraz uaktualniania istniejących zabezpieczeń w postaci programów antywirusowych.
   c. Poinformowania ABI o planowaniu wdrożenia nowych rozwiązań technologicznych.
   d. Nadzór nad konserwacją sprzętu informatycznego.
   e. Nadzór nad naprawami, konserwacją i likwidacją urządzeń komputerowych oraz nośników danych, na których są zapisane dane osobowe.
   f. Nadzór nad tworzeniem kopii zapasowych oraz nad ich przechowywaniem.
5. **Kierownicy poszczególnych referatów** Urzędu są zobowiązani do:
   a. Współpracy z Administratorem Bezpieczeństwa Informacji w zakresie ochrony danych osobowych.
   b. Nadzoru nad przestrzeganiem zasad Polityki Bezpieczeństwa oraz Instrukcji zarządzania systemem informatycznym przez podległych im pracowników.
   c. Informowania Administratora Bezpieczeństwa Informacji o potrzebie stworzenia nowego zbioru podlegającego rejestracji, zmian w zbiorach lub likwidacji zbiorów celem zgłoszenia tego faktu w GIODO. Zgłoszenie nowego zbioru/ zmian w zbiorze powinno nastąpić poprzez wypełnienie załącznika nr 5 niniejszego dokumentu. (Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych).
   d. Informowania Administratora Bezpieczeństwa Informacji o potrzebie stworzenia zbioru zawierającego dane wrażliwe przed rozpoczęciem zbierania takich danych.

e. Informowania Administratora Bezpieczeństwa Informacji o zatrudnieniu nowego pracownika, zmianie zakresu obowiązków pracownika. Wzór wniosku o nadanie/ zmianę/ odebranie uprawnień w systemie informatycznym stanowi załącznik nr 2 do Instrukcji Zarządzania Systemem Informatycznym.

6. **Pracownicy posiadający upoważnienie do przetwarzania danych osobowych** są zobowiązani do:
   a. Zachowania w tajemnicy informacji o przetwarzanych danych osobowych oraz o stosowanych w Urzędzie środkach zabezpieczeń, **art. 39 ust. 2** nawet po wygaśnięciu stosunku pracy.
   b. Spełnienia obowiązku informacyjnego w przypadku zbierania danych osobowych od osoby, której one dotyczą poprzez poinformowanie tej osoby o:
      - pełnej nazwie i adresie siedziby Urzędu
        celu zbierania danych,
      - prawie dostępu do treści swoich danych oraz ich poprawiania,
      - dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.
   c. Obowiązek informacyjny można spełnić poprzez ustne przekazanie w/w informacji, wywieszenie tych informacji w dobrze widocznym miejscu w pomieszczeniu obsługującym petentów Urzędu lub poprzez umieszczenie informacji na ankiecie, którą wypełnia petent.
   d. Odbycia wewnętrznego szkolenia z zakresu niniejszego dokumentu oraz przepisów i ustaw dotyczących ochrony danych osobowych w celu podwyższenia standardów bezpieczeństwa.
   e. Sumiennego i rzetelnego wykonywania prac związanych z przetwarzaniem danych osobowych w celu uniknięcia sytuacji zagrożenia bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych.
   f. Podporządkowania się poleceniom administratora bezpieczeństwa informacji, administratora systemów informatycznych oraz kierownika referatu w zakresie ochrony danych osobowych.
   g. Podpisanie oświadczenia o dopuszczeniu do przetwarzania danych osobowych.
   h. Zgłaszania nieprawidłowości w działaniu systemów informatycznych Administratorowi tych systemów.
   i. Pracownicy mający w posiadaniu notebooki, pendrive'y, telefony komórkowe są zobowiązani do zachowania szczególnej ostrożności ze względu na możliwość kradzieży, zagubienia lub zniszczenia posiadanych danych osobowych.
   j. Pracownicy posiadający sprzęt przenośny (notebooki, pendrive'y, telefony komórkowe) są zobowiązani do podpisania umowy powierzenia sprzętu. Umowa powinna być przechowywana w aktach osobowych pracowników. Wzór oświadczenia o powierzeniu mienia stanowi załącznik nr 6 niniejszego dokumentu.

k. Odpowiedzialność za powierzone mienie przekazuje się pracownikowi.

7. **Pracownicy nieposiadający uprawnienia do przetwarzania danych osobowych** są zobowiązani do:
   a. Zgłoszenia Administratorowi Bezpieczeństwa Informacji o występujących nieprawidłowościach występujących przy przetwarzaniu danych osobowych w momencie, gdy takie nieprawidłowości zauważą (nie wyłączony komputer po zakończeniu pracy, pozostawione dokumenty na biurku).
   b. Niezwłocznego zgłoszenia Administratorowi Bezpieczeństwa Informacji faktu zauważenia dokumentów z danymi osobowymi poza obszarem przetwarzania danych osobowych.
8. **Zasady naboru na wolne stanowiska**
   a. Przygotowanie ogłoszenia o naborze zgodnie z ustawą z dnia 21 listopada 2008 roku o pracownikach samorządowych oraz z zarządzeniem Wójta Gminy Jasienica Nr 0152/38/2005 w sprawie „Regulaminu naboru na wolne stanowiska urzędnicze w tym na Kierownicze stanowiska urzędnicze w Urzędzie Gminy Jasienica"
   b. Powołanie Komisji rekrutacyjnej
   c. Rozpatrywanie dokumentów przez Komisję Rekrutacyjną:
      - W przypadku podania przez kandydata w dokumentach rekrutacyjnych danych wrażliwych w rozumieniu ustawy o ochronie danych osobowych art. 27 pkt.1 nie dopuszcza się dalszego rozpatrywania takich dokumentów.
      - Do rozpatrywania dokumentów zawierające dane wrażliwe Kandydat musi wyrazić zgodę na przetwarzanie danych wrażliwych. W przypadku braku takiej zgody Komisja rekrutacyjna jest zobowiązana takie dokumenty zniszczyć.
   d. Po osiągnięciu celu rekrutacji, czyli wyłonieniu kandydata i zakończeniu procesu rekrutacji dokumenty pozostałych kandydatów zawierające dane osobowe powinny być trwale zniszczone w niszczarce w obecności Komisji rekrutacyjnej.
   e. Aplikacja złożona drogą mailową nie zostanie dopuszczona do procesu naboru.
9. **Zasady umieszczania informacji w Biuletynie Informacji Publicznej.**

Pracownik odpowiedzialny za umieszczanie informacji w BIP jest zobowiązany do umieszczenia na stronie tylko części A oświadczenia majątkowego. Nie umieszczamy części B, która zawiera dane osobowe osób składających oświadczenie.

Rozdział 4 Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe.

Wykaz pomieszczeń, w których przetwarzane są dane osobowe w tradycyjnej formie oraz za pomocą systemów informatycznych zawiera załącznik nr 7 niniejszego dokumentu.

Rozdział 5

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.

Wykaz zbiorów danych osobowych zawiera załącznik nr 8 niniejszego dokumentu.

Rozdział 6 Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi.

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi zawiera załącznik nr 9 niniejszego dokumentu.

Rozdział 7 Sposób przepływu danych pomiędzy poszczególnymi systemami.

Opis sposobu przepływu danych pomiędzy poszczególnymi systemami zawiera załącznik nr 10 niniejszego dokumentu.

Rozdział 8 Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Aby zapewnić bezpieczeństwo danych osobowych przetwarzanych w Urzędzie Gminy Jasienica zastosowano odpowiednie środki techniczne i organizacyjne. Zastosowane środki według ustawy mają zapewnić przetwarzanym danym poufność, integralność i rozliczalność, czyli takie własności, które mają na celu uniemożliwienie dostępu do danych nieupoważnionym osobom.

1. Zasady dostępu do pomieszczeń znajdujących się w strefie przetwarzania danych osobowych zawiera załącznik nr 11 niniejszego dokumentu.

2. Procedurę zarządzania kluczami w budynku Urzędu Gminy Jasienica zawiera załącznik nr 12 niniejszego dokumentu.
    a. Wzór wykazu osób pobierających i zdających klucze stanowi załącznik nr 13 niniejszego dokumentu.
    b. Wykaz osób upoważnionych do pobierania kluczy do pomieszczeń w strefie przetwarzania danych osobowych stanowi załącznik nr 14.
    c. Wykaz osób posiadających klucze do budynku Urzędu Gminy oraz do stref alarmowych stanowi załącznik nr 15.
3. Procedurę postępowania z danymi osobowymi zawiera załącznik nr 16 niniejszego dokumentu.
4. Procedurę zarządzania hasłami zawiera Instrukcja zarządzania.
5. Zgodnie z art. 31 ustawy należy podpisać umowę powierzenia danych z każdym podmiotem, któremu Urząd Gminy Jasienica powierza dane. Umowa powierzenia danych powinna być jednym z wymogów podczas realizowania przetargów z podmiotami, którym powierzane są dane osobowe.
6. Formy zabezpieczeń przed nieautoryzowanym dostępem do baz danych Urzędu stanowi załącznik nr 17 niniejszego dokumentu.
7. Formy zabezpieczeń przed nieautoryzowanym dostępem do baz danych Urzędu poprzez Internet stanowi załącznik nr 18.
8. Formy zabezpieczeń przed utratą danych osobowych w wyniku awarii stanowi załącznik nr 19.

Rozdział 8 Procedura postępowania w przypadku wykrycia naruszenia ochrony danych osobowych.

Niniejsza procedura określa sposób postępowania pracowników w momencie stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych w przypadku systemu informatycznego lub tradycyjnego zbioru danych. Opis procedury stanowi załącznik nr 20.

Rozdział 9 Konsekwencje niestosowania się do Polityki Bezpieczeństwa.

Konsekwencje niestosowania się do zasad określonych w niniejszym dokumencie zostały opisane w załączniku nr 21.

WÓJT
mgr inż. Janusz Pierzyna

WÓJT GMINY JASIENICA
43-385 JASIENICA 159

Załącznik nr 1
do Polityki Bezpieczeństwa Informacji
w Urzędzie Gminy Jasienica

Zarządzenie Nr 120.
Wójta Gminy Jasienica
z dnia .....

w sprawie: wyznaczenia Administratora Bezpieczeństwa Informacji w Urzędzie Gminy Jasienica

Na podstawie art. 36 ust. 3 ustawy dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002r. Nr 101, poz. 926 z późn. zm.)

zarządzam:

§1

Wyznaczyć Pana/Panią .....(Imię i Nazwisko) ....., ... (nazwa zajmowanego stanowiska) w Urzędzie Gminy Jasienica na Administratora Bezpieczeństwa Informacji w Urzędzie.

§2

Zadaniem Administratora Bezpieczeństwa Informacji jest nadzór nad przestrzeganiem zasad ochrony danych osobowych w Urzędzie Gminy Jasienica.

§3

Wykonanie zarządzenia powierzyć Sekretarz Gminy.

§4

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT
mgr inż. Janusz Pierzyna

Załącznik nr 2
do Polityki Bezpieczeństwa Informacji
w Urzędzie Gminy Jasienica

Wykaz wydanych upoważnień do przetwarzania danych osobowych:

Lp:	Imię:	Nazwisko:	Numer upoważnienia:	Data nadania upoważnienia:	Identyfikator w systemie informatycznym:	Zakres upoważnienia:	Data ustania upoważnienia	Podpis ABI/ASI

WÓJT
mgr inż. Janusz Pleszyna

WÓJT GMINY JASIENICA
43-385 JASIENICA 159

Załącznik nr 3
do Polityki Bezpieczeństwa Informacji
w Urzędzie Gminy Jasienica

Raport nr /2012 z przeprowadzonej kontroli w dniu: .....

Dane pracownika kontrolowanego:		
Imię:		
Nazwisko:		
Referat:		
Nr pokoju:		
Obszary kontrolowania:	Tak	Nie
Czy pracownik zachowuje zasadę czystego biurka?		
Czy pracownik zachowuje zasadę czystego ekranu?		
Czy błędne wydruki są niszczone w odpowiedni sposób za pomocą niszczarki?		
Czy dokumenty z danymi osobowymi są przechowywane w zamykanych na klucz szafach?		
Czy pomieszczenie będące w strefie przetwarzania danych osobowych jest zamykane na klucz przez ostatnią wychodzącą osobę?		
Czy komputer jest blokowany za pomocą klawiszy ctrl+alt+delete w momencie odejścia pracownika ze stanowiska pracy?		
Czy pracownik posiada upoważnienie do przetwarzania danych osobowych?		
Uwagi:		

.....
Data i podpis
Administratora Bezpieczeństwa Informacji

WÓJT
mgr inż. Janusz Pietrzyna

Jasienica, dnia: .....

Raport pokontrolny nr.....
oceniający stan zabezpieczenia danych osobowych w Urzędzie Gminy Jasienica

1. Termin przeprowadzonej kontroli:
   .....
   .....
2. Wnioski z przeprowadzonej kontroli.
   .....
   .....
   .....
3. Czy kontrola wykazała słabe punkty w ochronie danych osobowych?
   .....
   .....
   .....
4. Aby zapewnić właściwe zabezpieczenie należy wprowadzić zmiany w środkach:
   a. organizacyjnych:
      .....
      .....
   b. technicznych:
      .....
      .....

Tabela kosztów:

	Zapotrzebowanie:	Kwota:	Miejsce przeznaczenia:
Środki techniczne:	Np.:Szafa metalowa		
Środki organizacyjne:	Np.:Szkolenie ABI		

.....

Podpis ABI

.....

Podpis ADO

WÓJT
mgr inż. Janusz Pierzyna

ZGŁOSZENIE ZBIORU DANYCH DO REJESTRACJI GENERALNEMU INSPEKTOROWI OCHRONY

DANYCH OSOBOWYCH

* ☐ – zgłoszenie zbioru na podstawie art. 40 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 i Nr 153, poz. 1271 oraz z 2004 r. Nr 25, poz. 219 i Nr 33, poz. 285),

* ☐ – zgłoszenie zmian na podstawie art. 41 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

* ☐ – zgłoszenie zbioru, w którym będą przetwarzane dane określone w art. 27 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

Nr .....

Wnoszę o wpisanie zbioru danych osobowych o nazwie:

.....
do Rejestru Zbiorów Danych Osobowych.

Część B. Charakterystyka administratora danych

1. Wnioskodawca (administrator danych):

.....

.....

(nazwa administratora danych i adres jego siedziby lub nazwisko, imię i adres miejsca zamieszkania wnioskodawcy oraz nr REGON)

2. Przedstawiciel Wnioskodawcy, o którym mowa w art. 31a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych:

.....

.....

(nazwa przedstawiciela administratora danych i adres jego siedziby lub nazwisko, imię i adres miejsca zamieszkania)

3. Powierzenie przetwarzania danych osobowych:

* ☐ – administrator danych powierzył w drodze umowy zawartej na piśmie przetwarzanie danych innemu podmiotowi (art. 31 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych).

* ☐ – administrator danych przewiduje powierzenie przetwarzania danych innemu

W przypadku powierzenia przetwarzania danych innemu podmiotowi podaj nazwę i adres siedziby lub nazwisko, imię i adres miejsca zamieszkania podmiotu, któremu powierzono przetwarzanie danych osobowych:

.....

.....

..... * ☐ *ew. cd. w załączniku nr*

4. Podstawa prawna upoważniająca do prowadzenia zbioru danych:

* ☐ – zgoda osoby, której dane dotyczą, na przetwarzanie danych jej dotyczących,

* ☐ – przetwarzanie jest niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa

.....

.....

..... * ☐ *ew. cd. w załączniku nr*

* ☐ – przetwarzanie jest konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą,

* ☐ – przetwarzanie jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego – jeśli TAK, to opisz te zadania:

.....

.....

..... * ☐ *ew. cd. w załączniku nr*

* ☐ – przetwarzanie jest niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

Część C. Cel przetwarzania danych, opis kategorii osób, których dane dotyczą, oraz zakres przetwarzanych danych

5. Cel przetwarzania danych w zbiorze:

.....

.....

..... * ☐ *ew. cd. w załączniku nr*

6. Opis kategorii osób, których dane dotyczą:

.....

.....

7. Zakres przetwarzanych w zbiorze danych o osobach:

* ☐ – nazwiska i imiona,
* ☐ – imiona rodziców,
* ☐ – data urodzenia,
* ☐ – miejsce urodzenia,
* ☐ – adres zamieszkania lub pobytu,
* ☐ – numer ewidencyjny PESEL,
* ☐ – Numer Identyfikacji Podatkowej,
* ☐ – miejsce pracy,
* ☐ – zawód,
* ☐ – wykształcenie,
* ☐ – seria i numer dowodu osobistego,
* ☐ – numer telefonu.

8. Inne dane osobowe, oprócz wymienionych w pkt 7, przetwarzane w zbiorze – *należy podać jakie*:

.....

.....

..... * ☐ *ew. cd. w załączniku nr*

9. Dane przetwarzane w zbiorze:

a) ujawniają bezpośrednio lub w kontekście:

* ☐ – pochodzenie rasowe,
* ☐ – przynależność partyjną,

* ☐ – pochodzenie etniczne,
* ☐ – poglądy polityczne,
* ☐ – przekonania religijne,
* ☐ – przekonania filozoficzne,
* ☐ – przynależność wyznaniową,
* ☐ – przynależność związkową,
* ☐ – stan zdrowia,
* ☐ – kod genetyczny,
* ☐ – nałogi,
* ☐ – życie seksualne,

b) dotyczą:

* ☐ – skazań,
* ☐ – mandatów karnych,
* ☐ – orzeczeń o ukaraniu,
* ☐ – innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym

Jeśli nie zakreślono żadnej odpowiedzi, należy przejść od razu do pkt 11.

10. Podstawa prawna przetwarzania danych wskazanych w pkt 9:

* ☐ – osoby, których dane dotyczą, będą wyrażać na to zgodę na piśmie,
* ☐ – przepis szczególny innej ustawy zezwala na przetwarzanie bez zgody osoby, której dane dotyczą, jej danych osobowych – jeśli TAK, to podaj odniesienie do przepisu tej ustawy:

....

....

....

.... * ☐ *ew. cd. w załączniku nr*

* ☐ – przetwarzanie danych jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby, gdy osoba, której dane dotyczą, nie jest fizycznie lub prawnie zdolna do wyrażenia zgody, do czasu ustanowienia opiekuna prawnego lub
* ☐ – przetwarzanie jest niezbędne do wykonania statutowych zadań kościoła, innego związku wyznaniowego, stowarzyszenia, fundacji lub innej niezarobkowej organizacji lub instytucji o celach politycznych, naukowych, religijnych, filozoficznych lub związkowych, a przetwarzanie danych dotyczy wyłącznie członków tej organizacji lub instytucji albo osób utrzymujących z nią stałe kontakty w związku z jej działalnością i zapewnione są pełne gwarancje ochrony przetwarzanych danych – jeśli TAK, to podaj

....

....

.... * ☐ *ew. cd. w załączniku nr*

* ☐ – przetwarzanie dotyczy danych, które są niezbędne do dochodzenia praw przed sądem,
* ☐ – przetwarzanie jest niezbędne do wykonania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych jest określony w ustawie,
* ☐ – przetwarzanie jest prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych i są stworzone pełne gwarancje ochrony danych osobowych,
* ☐ – przetwarzanie dotyczy danych, które zostały podane do wiadomości publicznej przez osobę, której dane dotyczą,

* ☐ – przetwarzanie jest niezbędne do prowadzenia badań naukowych, w tym do przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego, a publikowanie wyników badań naukowych uniemożliwia identyfikację osób, których dane zostały przetworzone,

* ☐ – przetwarzanie danych jest prowadzone przez stronę w celu realizacji praw i obowiązków wynikających z orzeczenia wydanego w postępowaniu sądowym lub

Część D. Sposób zbierania oraz udostępniania danych

11. Sposób zbierania danych do zbioru:

* ☐ – od osób, których dotyczą,

* ☐ – z innych źródeł niż osoba, której dane dotyczą,

12. Sposób udostępniania danych ze zbioru:

* ☐ – podmiotom innym niż upoważniona na podstawie przepisów prawa,

13. Odbiorcy lub kategorie odbiorców, którym dane mogą być przekazywane – należy *podać nazwę i adres siedziby lub nazwisko, imię i adres miejsca zamieszkania podmiotu, któremu dane mogą być przekazywane:*

.....

.....

.....

..... * ☐ *ew. cd. w załączniku nr*

14. Informacja dotycząca ewentualnego przekazywania danych do państwa trzeciego – *podaj nazwę państwa:*

.....

.....

..... * ☐ *ew. cd. w załączniku nr*

Część E. Opis środków technicznych i organizacyjnych zastosowanych

w celach określonych w art. 36–39 ustawy z dnia 29 sierpnia 1997 r.

15. Zbiór danych osobowych będzie przetwarzany:

a) * ☐ – centralnie

* ☐ – w architekturze rozproszonej

b) * ☐ – wyłącznie w postaci papierowej

* ☐ – z użyciem systemu informatycznego

c) * ☐ – z użyciem co najmniej jednego urządzenia systemu informatycznego służącego do przetwarzania danych osobowych połączonego z siecią publiczną (np. Internetem).

* ☐ – bez użycia żadnego z urządzeń systemu informatycznego służącego do przetwarzania danych osobowych połączonego z siecią publiczną (np. Internetem),

16. Zostały spełnione wymogi określone w art. 36–39 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[1)]:

a) * ☐ – został wyznaczony administrator bezpieczeństwa informacji nadzorujący przestrzeganie zasad ochrony przetwarzania danych osobowych,

* ☐ – administrator danych sam wykonuje czynności administratora bezpieczeństwa informacji,

b) * ☐ – do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez administratora danych,

c) * ☐ – prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych.

d) * ☐ – została opracowana i wdrożona polityka bezpieczeństwa.

e) * ☐ – została opracowana i wdrożona instrukcja zarządzania systemem

f) Inne środki, oprócz wymienionych w pkt. a – e, zastosowane w celu zabezpieczenia danych:

.....

.....

..... * ☐ *ew. cd. w załączniku nr*

Część F. Informacja o sposobie wypełnienia warunków technicznych i organizacyjnych, o których mowa w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie doku–mentacji 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)

17. Zastosowano środki bezpieczeństwa na poziomie:

* ☐ – podstawowym,

* ☐ – podwyższonym,

* ☐ – wysokim.

.....

(data, podpis i pieczęć wnioskodawcy)

Objaśnienia:

* W przypadku odpowiedzi twierdzącej należy zakreślić kwadrat lilerą „X".

1) Administrator danych prowadzący zbiór w systemie tradycyjnym (papierowym) zobowiązany jest do zastosowariia środków określonych w pkt 15 ppkt a – d, a w przypadku prowadzenia zbioru w systemie informatycznym, ponadto środka określonego w pkt 16 ppkt e.

2) Należy wskazać odpowiedni poziom bezpieczeństwa określony w § 6 ww. rozporządzenia (UWAGA! Dotyczy wyłącznie administratorów przetwarzających dane w systemie informatycznym);

– jeżeli wnioskodawca przetwarza dane wymienione w pkt 9 zgłoszenia, należy zastosować środki bezpieczeństwa przynajmniej na poziomie podwyższonym;

– w przypadku gdy przynajmniej jedno urządzenie systemu informatycznego służącego do przetwarzania danych osobowych połączone jest z siecią publiczną należy stosować środki

– w pozostałych przypadkach wystarczające jest zastosowanie środków bezpieczeństwa na poziomie podstawowym.

WÓJT mgr inż. Janusz Pierzyna

Jasienica, dnia .....

.....
Imię Nazwisko

.....
Stanowisko

OŚWIADCZENIE

Oświadczam niniejszym, że jestem świadoma/y odpowiedzialności materialnej na podstawie art. 114 kodeksu pracy z tytułu zajmowanego stanowiska pracy w Urzędzie Gminy Jasienica. Równocześnie oświadczam, iż przyjmuję odpowiedzialność materialną stosownie do treści przepisów art. 124 kodeksu pracy za poniższy sprzęt:

Dane powierzonego sprzętu:	
Nazwa sprzętu:	
Data zakupu:	
Nr inwentarzowy:	
Nr seryjny:	

.....
Podpis pracownika

WÓJT
mgr inż. Janusz Pierzyna

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

1. Wykaz pomieszczeń, w których przetwarzane są dane osobowe za pomocą systemów informatycznych.

Lp:	Lokalizacja:	Nr pokoju:
1.	Parter	
2.	I piętro	
3.	II piętro	

Wszystkie pomieszczenia znajdujące się w wykazie zlokalizowane są w budynku Urzędu Gminy Jasienica w Jasienicy 159, 43-385 Jasienica.

2. Wykaz pomieszczeń, w których przetwarzane są dane osobowe w tradycyjnej formie:

Lp:	Lokalizacja:	Nr pokoju:
1.	Parter	
2.	I piętro	
3.	II piętro	

3. Archiwum Urzędu Gminy Jasienica znajduje się w pokoju nr .....

WÓJT GMINY JASIENICA
43-385 JASIENICA 159

Załącznik nr 8
do Polityki Bezpieczeństwa Informacji
w Urzędzie Gminy Jasienica

Dane osobowe w Urzędzie Gminy Jasienica są przetwarzane w następujących zbiorach (bazach):

Nazwa zbioru (bazy) danych	Programy pracujące na zbiorze (bazie) danych	Opis programu	Nazwa adres firmy dostarczającej oprogramowanie	Data usunięcia aplikacji	Uwagi

Dane osobowe w Urzędzie Gminy Jasienica są przetwarzane w następujących zbiorach informatycznych:

Lp.	Nazwa zbioru (opis)	Miejsce zbioru	Program do przetwarzania danych	Opis zbioru

Dane osobowe w Urzędzie Gminy Jasienica są przetwarzane w następujących zbiorach tradycyjnych:

Lp.	Nazwa zbioru	Miejsce zbioru	Nazwa referatu:	Opis zbioru

Załącznik nr 9
do Polityki Bezpieczeństwa Informacji
w Urzędzie Gminy Jasienica

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi.

Lp.	Określenie zakresu danych (nazwa tablicy)	Nazwa identyfikatora powiązania z innym, określonym zakresem danych	Wykaz danych wchodzących w określony zakres danych.	Systemy aktualizujące zapisy w tabeli

Jasienica, dnia:.....

Załącznik nr 10
do Polityki Bezpieczeństwa Informacji
w Urzędzie Gminy Jasienica

1. Sposób przepływu danych pomiędzy poszczególnymi systemami

WÓJT
mgr inż. Janusz Pierzyna

Załącznik nr 11

do Polityki Bezpieczeństwa Informacji

w Urzędzie Gminy Jasienica

Ustalenie zasad dostępu do pomieszczeń znajdujących się w strefie przetwarzania danych osobowych

- Dostęp do pomieszczeń, gdzie są przetwarzane dane osobowe mogą mieć tylko osoby upoważnione do przetwarzania danych osobowych. Dostęp do tych pomieszczeń jest możliwy tylko w godzinach pracy urzędu. W przypadku konieczności pracy w innych godzinach jest to możliwe jedynie za zgodą przełożonego.
- Siedziba Gminy, w której zlokalizowane są zbiory danych osobowych, jest nadzorowana przez pracowników ochrony poza godzinami pracy urzędu.
- Osoby nieupoważnione do przetwarzania danych osobowych oraz petenci mogą przebywać w pomieszczeniu tylko i wyłącznie w obecności osoby upoważnionej do przetwarzania danych osobowych.
- Wszystkie pomieszczenia, w których przetwarza się dane osobowe są zamykane na klucz, w przypadku opuszczenia pomieszczenia przez ostatnią osobę upoważnioną do przetwarzania danych osobowych - także w godzinach pracy.
- Osoby wykonujące pracę poza godzinami otwarcia - dotyczy to ekip sprzątających urząd, pracowników ochrony, oraz ekip budowlanych wykonujących prace remontowe lub inne prace np.: konserwacyjne – powinny posiadać pisemne zezwolenie na wykonywanie w/w prac. Zezwolenie wydaje Wójt Gminy Jasienica.

Procedura zarządzania kluczami w budynku Urzędu Gminy Jasienica.

- W celu zapewnienia rozliczalności dostępu do pomieszczeń wchodzących w skład strefy przetwarzania danych osobowych wprowadza się wykaz osób pobierających klucze.
- Uprawniony do pobrania klucza pracownik jest zobowiązany do wpisania się do wykazu pobranych kluczy przy pobieraniu i zdawaniu klucza na portierni.
- Klucze do poszczególnych pomieszczeń mają prawo pobierać osoby do tego upoważnione.

Wykaz osób pobierających i zdających klucze do pomieszczeń wchodzących w skład strefy przetwarzania danych osobowych:

Imię i Nazwisko	Nr pokoju	Data pobrania klucza	Godzina pobrania klucza	Podpis	Data zdania klucza	Godzina zdania klucza	Podpis

WÓJT
mgr inż. Janusz Pierzyna

Załącznik nr 14
do Polityki Bezpieczeństwa Informacji
w Urzędzie Gminy Jasienica

Wykaz osób upoważnionych do pobierania kluczy do pomieszczeń w strefie przetwarzania danych osobowych:

Imię:	Nazwisko:	Upoważnienie do pobierania kluczy do pokoju nr:	Podpis osoby posiadającej klucze	Podpis ABI

WÓJT GMINY JASIENICA
43-385 JASIENICA 159

Załącznik nr 15
do Polityki Bezpieczeństwa Informacji
w Urzędzie Gminy Jasienica

Wykaz osób posiadających klucze do budynku Urzędu Gminy.

Imię i Nazwisko	Data odbioru klucza:	Podpis osoby posiadającej klucz	Podpis ABI

WÓJT
mgr inż. Janusz Pierzyna

Procedura postępowania z danymi osobowymi:

- Dostęp do danych osobowych mogą mieć tylko pracownicy posiadający pisemne zezwolenie od Administratora danych osobowych – Wójta Urzędu Gminy Jasienica.
- Zabrania się wynoszenia danych osobowych zapisanych w formie tradycyjnej (papierowej) lub elektronicznej (pamięć flash, płyta CD, DVD, dyskietka lub inne nośniki danych) poza obszar przetwarzania danych osobowych.
- Aby zwiększyć bezpieczeństwo danych osobowych każdą osobę upoważnioną do ich przetwarzania obowiązuje szkolenie z zakresu ochrony danych osobowych, zapoznanie z Polityką bezpieczeństwa oraz Instrukcją zarządzania systemem informatycznym.
- Pracownicy posiadający upoważnienie do przetwarzania danych osobowych zobowiązani są do przestrzegania zasady „czystego biurka". Na biurku mogą się znajdować tylko te dokumenty, nad którymi pracownik aktualnie pracuje. Po skończonej pracy wszystkie dokumenty powinny być schowane w szafkach.
- Pracownicy posiadający upoważnienie do przetwarzania danych osobowych zobowiązani są do przestrzegania zasady „czystego ekranu". Podczas pracy pracownicy powinni mieć otwarte tylko te aplikacje, które są niezbędne do wykonania obowiązków służbowych.
- Pracownicy zobowiązani są do niszczenia w niszczarkach nieaktualnych lub błędnych wydruków zawierających dane osobowe. Nie dopuszcza się innej formy niszczenia takich dokumentów.
- W celu ograniczenia możliwości nieuprawnionego podglądu i dostępu do danych osobowych przez petentów należy wyraźnie odznaczyć „strefę petenta" od strefy przetwarzania danych osobowych poprzez zastosowanie np.: lady odgradzającej obie strefy.
- Dokumenty zawierające dane osobowe oraz nośniki zawierające takie dane po skończonej pracy powinny być przechowywane w zamykanych na klucz meblach biurowych, a tam, gdzie jest to możliwe - w szafach metalowych lub pancernych; klucze od szafek należy zabezpieczyć przed dostępem osób nieupoważnionych do przetwarzania danych osobowych.

WÓJT
mgr inż. Janusz Pleszyna

Formy zabezpieczeń przed nieautoryzowanym dostępem do baz danych Gminy:

- Udostępnianie użytkownikowi zasobów sieci zawierających dane osobowe (programów i baz danych) przez administratora systemu informatycznego następuje na podstawie wniosku przełożonego załącznik nr 2 Instrukcji zarządzania.
- Użytkownik jest identyfikowany w systemie informatycznym poprzez zastosowanie uwierzytelnienia.
- Każdemu użytkownikowi systemu zostaje przydzielony indywidualny identyfikator i hasło w celu zapewnienia rozliczalności, poufności i integralności danych. System rejestruje również czas logowania i rodzaj wprowadzonych przez użytkownika danych.
- Aby spełnić zabezpieczenia na poziomie podstawowym, co 30 dni następuje wymuszenie zmiany hasła dostępu do systemu informatycznego.
- Aby zabezpieczyć system przed niepożądanymi awariami pracownicy posiadają konta z ograniczonymi uprawnieniami.
- Dostęp do centrum przetwarzania danych (serwerowni) mają tylko pracownicy upoważnieni. Serwerownia musi być zabezpieczona alarmem.
- Stosowanie programu antywirusowego na komputerach ze środowiskiem operacyjnym MS Windows.
- Automatyczne wygaszanie ekranu i blokowanie nieużywanego komputera po upływie 20 minut.
- Blokowanie nieużywanego komputera przez pracownika w momencie wyjścia z pomieszczenia.

WÓJT
mgr inż. Janusz Pierzyna

Formy zabezpieczeń przed nieautoryzowanym dostępem do baz danych Urzędu poprzez Internet:

- logiczne oddzielenie sieci wewnętrznej LAN od sieci zewnętrznej, uniemożliwiające uzyskanie połączenia z bazą danych spoza systemu informatycznego, jak również uzyskanie dostępu z systemu do sieci rozległej Internet,
- zastosowanie dwóch poziomów zabezpieczenia sieci:
  - pierwszy poziom ochrony stanowi lokalna brama sieciowa z zainstalowanym systemem typu firewall - **z funkcją analizy charakteru ruchu sieciowego** - uniemożliwiającym nawiązanie połączenia z chronionymi komputerami oraz blokującym ruch o charakterze niepożądanym lub takim, który może zostać uznany za szkodliwy,
  - drugi poziom zabezpieczeń stanowią listy dostępu do serwerów baz danych z określonych adresów i puli adresowej.

WÓJT
mgr inż. Mirosław Pierzyna

Formy zabezpieczeń przed utratą danych osobowych w wyniku awarii:

- odrębne zasilanie sprzętu komputerowego,
- ochrona serwerów przed zanikiem zasilania poprzez stosowanie zasilaczy zapasowych UPS oraz agregatu prądotwórczego,
- ochrona przed utratą zgromadzonych danych poprzez cykliczne wykonywanie kopii zapasowych, z których, w przypadku awarii, odtwarzane są dane i system operacyjny,
- w celu zapewnienia bezpieczeństwa danych wykonywane są dzienne i tygodniowe kopie zapasowe,
- kopie zapasowe powinny być przechowywane w sejfie ognioodpornym w innym pomieszczeniu niż centrum przetwarzania danych,
- ochrona przed awarią podsystemu dyskowego poprzez używanie macierzy dyskowych,
- zapewnienie właściwej temperatury i wilgotności powietrza dla pracy sprzętu komputerowego, poprzez zastosowanie redundantnych klimatyzatorów,
- zastosowanie ochrony przeciwpożarowej poprzez umieszczenie w serwerowni gaśnic, okresowo kontrolowanych przez specjalistę,
- zwiększenie niezawodności serwerów i urządzeń sieciowych poprzez logiczne rozmieszczenie ich w szafach serwerowych,
- aby zapewnić stabilne parametry zasilania dla sprzętu komputerowego zastosowano dedykowaną sieć elektryczną. Do zasilania w/w sprzętu zastosowano specjalne gniazda dedykowane z tzw. kluczem tak, aby żaden inny odbiornik elektryczny poza wyznaczonymi nie mógł być do niej przyłączony,
- użytkownikom nie wolno na własną rękę podpinać, wypinać urządzeń końcowych (komputera, terminala, drukarki) z dedykowanych gniazd elektrycznych (czerwony kolor). W/w czynności mogą być wykonane tylko i wyłącznie przez administratora sieci lub upoważnionego pracownika

WÓJT
mgr inż. Janusz Pierzyna

Procedura postępowania w przypadku wykrycia naruszenia ochrony danych osobowych.

1. **Naruszenie danych może być wynikiem:**
   a. zamierzonych lub niezamierzonych działań użytkowników posiadających uprawnienia do przetwarzania danych osobowych w systemach informatycznych lub tradycyjnych zbiorach,
   b. nieuprawnionych działań osób nieupoważnionych do dostępu do danych osobowych,
   c. sytuacje losowe lub szkodliwy wpływ czynników zewnętrznych na zasoby zawierające dane osobowe np.: wybuch gazu, pożar zalanie pomieszczeń, niepożądane działania ekip remontowych.

2. **Za zamierzone lub niezamierzone działania użytkowników, których wynikiem jest złamanie obowiązujących zasad ochrony danych osobowych uważa się:**
   a. dopuszczenie do przetwarzania danych osobowych pracowników bez odpowiednich upoważnień i przeszkolenia,
   b. wyniesienie danych osobowych zapisanych w formie tradycyjnej (papierowej) lub elektronicznej (pamięć flash, płyta CD, DVD, dyskietka lub inne nośniki danych) poza obszar przetwarzania danych osobowych.
   c. niszczenie dokumentów zawierających dane osobowe w inny sposób niż za pomocą niszczarki,
   d. pozostawienie danych osobowych w drukarce lub kserokopiarce,
   e. nieprzestrzeganie zasad czystego biurka i czystego ekranu,
   f. umożliwienie dostępu do danych osobowych poprzez pozostawienie dokumentów zawierających dane osobowe na biurku po zakończonej pracy,
   g. pozostawienie bez nadzoru osób nieuprawnionych w strefie przetwarzania danych osobowych,
   h. ujawnienie indywidualnego hasła do systemu lub aplikacji dziedzinowych osobom trzecim lub zapisywanie haseł na kartkach,
   i. praca na loginie i haśle innej osoby,
   j. nieuprawnione ujawnienie danych osobowych,
   k. zagubienie danych osobowych w formie tradycyjnej lub zagubienie nośników zawierających dane osobowe,
   l. niezamierzone zniszczenie lub modyfikację danych osobowych,

m. powierzenie mienia służącego do przetwarzania danych osobowych (laptopy, pendrive, telefony komórkowe itp.) bez podpisania oświadczenia o powierzeniu mienia,
n. wykonanie nieuprawnionych kopii danych osobowych,
o. niewykonanie kopii zapasowych danych osobowych,
p. niewłaściwe przechowywanie kopii zapasowych,
q. kradzież sprzętu informatycznego zawierającego dane osobowe,

3. **Za nieuprawnione działania osób nieupoważnionych do przetwarzania danych osobowych uważa się:**
   a. Próby włamania do pomieszczeń wchodzących w strefę przetwarzania danych osobowych,
   b. Próby włamania się do systemu informatycznego,
   c. Próby wyłudzenia danych osobowych przez telefon,
   d. Kradzież mienia służbowego.

4. **O możliwości nieuprawnionego działania osób nieupoważnionych do przetwarzania danych osobowych może świadczyć:**
   a. brak możliwości zalogowania się do aplikacji,
   b. zmiany w zawartości danych osobowych,
   c. inny niż zwykle wygląd aplikacji,
   d. pojawienie się niewystępujących zazwyczaj komunikatów,
   e. pojawienie się komunikatów z systemu antywirusowego o możliwości zainfekowania komputera wirusami,
   f. ślady włamania się do pomieszczenia wchodzącego w strefę ochrony danych osobowych,
   g. awaria sprzętu informatycznego,

5. W momencie wykrycia lub podejrzenia naruszenia ochrony danych osobowych należy natychmiast (ustnie lub telefonicznie) powiadomić Administratora Bezpieczeństwa Informacji lub Administratora Systemu Informatycznego. W przypadku nieobecności w/w osób należy niezwłocznie poinformować bezpośredniego przełożonego.
6. Użytkownik zgłaszający wykrycie lub podejrzenie naruszenia ochrony danych osobowych do czasu przybycia ABI lub ASI zobowiązany jest do podjęcia wszelkich działań mających na celu powstrzymanie niepożądanych skutków naruszenia poprzez:
   a. wstrzymanie pracy na komputerze, na którym wystąpiło naruszenie,
   b. zabezpieczenie wstępu do pomieszczenia, w którym nastąpiło włamanie,
   c. określenie sytuacji i czasu, w jakim zauważono naruszenie oraz podanie wszelkich informacji umożliwiających ustalenie przyczyny powstania naruszenia.

7. Administrator Bezpieczeństwa Informacji lub Administrator Systemu Informatycznego po otrzymaniu zgłoszenia od użytkownika zobowiązany jest do niezwłocznego podjęcia czynności mających na celu usunięcia zaistniałego zagrożenia. W tym celu ABI/ASI przede wszystkim powinien:
    a. dokonać oceny zaistniałego zagrożenia i stwierdzić czy w wyniku zaistniałej sytuacji rzeczywiście doszło do naruszenia ochrony danych osobowych,
    b. ocenić skalę powstałych zniszczeń,
    c. podjąć działania naprawcze umożliwiające dalszą pracę,
    d. jeżeli zniszczenia powstały w systemie informatycznym w wyniku działania osoby nieupoważnionej ASI powinien dążyć do ustalenia sposobu działania takiej osoby oraz natychmiastowej próby zablokowania dostępu do systemu,
    e. określić przyczyny powstania naruszenia danych osobowych i podjąć odpowiednie środki w celu zabezpieczenia przed podobną sytuacją w przyszłości oraz podjąć działania umożliwiające dalszą pracę.
    f. sporządzić raport z zaistniałej sytuacji zawierający:

    - imię i nazwisko osoby powiadamiającej o naruszeniu ochrony danych osobowych oraz innych zaangażowanych osób,
    - czas i miejsce naruszenia i powiadomienia,
    - rodzaj naruszenia oraz opis podjętych działań,
    - wstępną ocenę przyczyn wystąpienia naruszenia,
    - ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.

WÓJT
mgr inż. Janusz Pierzyna

Osoba upoważniona do przetwarzania danych osobowych za naruszenie obowiązków, opisanych w niniejszym dokumencie ponosi odpowiedzialność wynikającą:

- z art. 108 par. 1 Kodeksu Pracy za nieprzestrzeganie przez pracownika ustalonej organizacji i porządku w procesie pracy. Pracodawca może stosować karę upomnienia lub nagany w zależności od wagi naruszenia.
- z ustawy o ochronie danych osobowych.

WÓJT
mgr inż. Janusz [illegible]