WÓJT GMINY
Godziesze Wielkie

ZARZĄDZENIE nr 146/2016
WÓJTA GMINY GODZIESZE WIELKIE
z dnia 04 stycznia 2016 roku

w sprawie wprowadzenia i wdrożenia do stosowania Polityki bezpieczeństwa danych osobowych oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

Na podstawie art. 31 oraz art. 33 ust. 3 w związku z art. 11a ust. 1 pkt 2 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t. j. w Dz. U. z 2015 r. poz. 1515 ze 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, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024), **zarządzam co następuje**:

§ 1. Wprowadza się do użytku służbowego „Politykę bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Godziesze Wielkie" stanowiącą załącznik nr 1 do niniejszego zarządzenia oraz „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Godziesze Wielkie", stanowiącą załącznik nr 2 do zarządzenia.

§ 2. Zobowiązuje się wszystkich pracowników Urzędu Gminy Godziesze Wielkie oraz strony trzecie świadczące usługi na rzecz Urzędu Gminy Godziesze Wielkie do przestrzegania przepisów zawartych w dokumentach, o których mowa w § 1.

§ 3. Nadzór nad wykonaniem zarządzenia powierzam Sekretarzowi Gminy oraz upoważnionemu pracownikowi na stanowisku Informatyka.

§ 4. Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT GMINY
Józef Podłużny

WÓJT GMINY
Godziesze Wielkie

Załącznik Nr 1
do Zarządzenia Nr 146/2016
Wójta Gminy Godziesze Wielkie
z dnia 04 stycznia 2016 roku

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH W URZĘDZIE GMINY GODZIESZE WIELKIE

SPIS TREŚCI

ZAŁĄCZNIKI

Załącznik nr 1. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w których przetwarzane są dane osobowe

Załącznik nr 2. Wykaz zbiorów danych osobowych wraz nazwą systemu służącego do ich przetwarzania oraz zakresem informacji i powiązania między nimi

Załącznik nr 3. Lista osób upoważnionych do pobierania kluczy do pomieszczeń, w których przetwarzane są dane osobowe – wzór

Załącznik nr 4. Raport z naruszenia bezpieczeństwa danych osobowych w Urzędzie Gminy Godziesze Wielkie

WPROWADZENIE

Niniejszy dokument opisuje reguły dotyczące bezpieczeństwa przetwarzania danych osobowych w sposób tradycyjny oraz w systemach informatycznych w Urzędzie Gminy Godziesze Wielkie. Opisane reguły określają granice dopuszczalnego zachowania wszystkich pracowników biorących udział w przetwarzaniu danych osobowych w urzędzie.
Potrzeba jego opracowania wynika z ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2014r. poz. 1182 ze zm.) oraz z § 3 i § 4 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).

DOKUMENTY POWIĄZANE

Instrukcja zarządzania systemem informatycznym służącymi do przetwarzania danych osobowych w Urzędzie Gminy Godziesze Wielkie.

DEFINICJE

- 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.
- Administrator Danych Osobowych – Wójt Gminy Godziesze Wielkie.
- System informatyczny - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
- Stacja robocza – stacjonarny lub przenośny komputer wchodzący w skład systemu informatycznego umożliwiający użytkownikom systemu dostęp do danych osobowych znajdujących się w systemie.
- Bezpieczeństwo systemu informatycznego - wdrożone przez Administratora Danych Osobowych środki organizacyjne i techniczne w celu zabezpieczenia oraz ochrony danych przed dostępem, modyfikacją, ujawnieniem, pozyskaniem lub zniszczeniem.
- Przetwarzanie danych osobowych - wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie.
- Osoba upoważniona - osoba posiadająca upoważnienie wydane przez Administratora Danych Osobowych i dopuszczona do przetwarzania danych osobowych w zakresie wskazanym w upoważnieniu.
- Użytkownik systemu - osoba posiadająca uprawnienia umożliwiające dostęp do systemu informatycznego, w którym są przetwarzane dane osobowe.
- Ustawa - ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.
- Rozporządzenie - rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

ZAKRES STOSOWANIA

W zakresie podmiotowym, Polityka bezpieczeństwa obowiązuje wszystkich pracowników Urzędu Gminy Godziesze Wielkie oraz inne osoby mające dostęp do danych osobowych, w tym stażystów, praktykantów, osoby zatrudnione na umowę zlecenia lub umowę o dzieło.

Politykę bezpieczeństwa stosuje się do danych osobowych przetwarzanych w sposób tradycyjny (na papierze) oraz w systemach informatycznych, danych zapisanych na zewnętrznych nośnikach informacji i informacji dotyczących bezpieczeństwa przetwarzania danych osobowych, w szczególności dotyczących wdrożonych zabezpieczeń technicznych i organizacyjnych.
Realizacja postanowień tego dokumentu ma zapewnić ochronę danych osobowych, właściwą ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa systemów oraz zapewnić właściwy tryb działania w celu przywrócenia bezpieczeństwa danych przetwarzanych w systemach informatycznych Urzędu.

ODPOWIEDZIALNOŚĆ

1. Administrator Danych Osobowych - decyduje o celach i środkach przetwarzania danych. Administrator Danych Osobowych jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę danych przetwarzanych w sposób tradycyjny oraz w systemach informatycznych Urzędu, a w szczególności:
   1) zabezpiecza dane przed ich udostępnieniem osobom nieupoważnionym,
   2) zapobiega przed pobraniem danych przez osobę nieuprawnioną,
   3) zapobiega zmianie, utracie, uszkodzeniu lub zniszczeniu danych,
   4) zapewnia przetwarzanie danych zgodnie z obowiązującymi przepisami prawa.
2. Upoważniony przez Administratora Danych Osobowych pracownik zatrudniony na stanowisku Informatyka:
   1) przeprowadza sprawdzenie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowuje w tym zakresie sprawozdania dla Administratora Danych Osobowych,
   2) nadzoruje opracowanie i aktualizowanie dokumentacji związanej z ochroną danych osobowych, oraz przestrzegania zasad w niej określonych'
   3) zapewnia zapoznanie osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
   4) nadzoruje wdrożenie stosownych środków organizacyjnych, technicznych i fizycznych w celu ochrony przetwarzania danych osobowych,
   5) nadzoruje i kontroluje zabezpieczenia systemów informatycznych służących do przetwarzania danych osobowych i osób przy nim zatrudnionych,
   6) monitoruje fizyczne zabezpieczenia danych osobowych oraz miejsc, w których są gromadzone i przetwarzane,
   7) prowadzi dokumentację opisującą zastosowaną politykę bezpieczeństwa danych osobowych,
   8) podejmuje stosowne działania w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych

9) analizuje sytuacje, okoliczności i przyczyny, które doprowadziły do naruszenia ochrony danych osobowych oraz przygotowuje i przedstawia Administratorowi Danych Osobowych zalecenia i rekomendacje dotyczące eliminacji ryzyk ich ponownego wystąpienia,
10) odpowiada za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych służących do przetwarzania danych osobowych oraz prowadzenie dokumentacji wynikającej z Instrukcji Zarządzania Systemami Informatycznymi.

3. Osoby upoważnione do przetwarzania danych osobowych są zobowiązane do:
   1) znajomości, zrozumienia i stosowania w możliwie największym zakresie wszelkich dostępnych środków ochrony danych osobowych oraz uniemożliwienia osobom nieuprawnionym dostępu do swojej stacji roboczej,
   2) przetwarzania danych osobowych zgodnie z obowiązującymi przepisami prawa oraz przyjętymi regulacjami,
   3) postępowania zgodnie z ustalonymi regulacjami wewnętrznymi dotyczącymi przetwarzania danych osobowych,
   4) zachowania w tajemnicy danych osobowych oraz informacji o sposobach ich zabezpieczenia,
   5) ochrony danych osobowych oraz środków przetwarzających dane osobowe przed nieuprawnionym dostępem, ujawnianiem, modyfikacją, zniszczeniem lub zniekształceniem,
   6) informowanie o wszelkich podejrzeniach naruszenia lub zauważonych naruszeniach oraz słabościach systemu przetwarzającego dane osobowe Informatyka Urzędu.

Rozdział 1
ZABEZPIECZENIE DANYCH OSOBOWYCH

1. Administratorem Danych Osobowych gromadzonych i przetwarzanych w sposób tradycyjny i w systemach informatycznych Urzędu jest Wójt Gminy Godziesze Wielkie.
2. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w których przetwarzane są dane osobowe prowadzony jest i aktualizowany przez upoważnionego przez Administratora Danych Osobowych pracownika na stanowisku Informatyka zgodnie ze wzorem stanowiącym załącznik nr 1 do niniejszego dokumentu.
3. Wykaz zbiorów danych osobowych przetwarzanych w Urzędzie wraz z nazwą systemu służącego do ich przetwarzania oraz zakresem przetwarzanych informacji i powiązania między nimi prowadzony i aktualizowany jest przez upoważnionego przez Administratora Danych Osobowych pracownika na stanowisku Informatyka według wzoru stanowiącego załącznik nr 2 do niniejszego dokumentu.
4. Dokument przedstawiający graficznie sposób przepływu danych pomiędzy poszczególnymi systemami prowadzony i aktualizowany jest przez upoważnionego przez Administratora Danych Osobowych pracownika na stanowisku Informatyka
5. Tworzenie nowego bądź modyfikacja struktury lub zakresu danych istniejącego zbioru podlega obowiązkowi zgłoszenia Administratorowi Danych Osobowych za pośrednictwem upoważnionego przez Administratora Danych Osobowych pracownika na stanowisku Informatyka. Obowiązek spoczywa na osobie tworzącej lub modyfikującej zbiór danych osobowych.
6. Jeżeli zbiór wymaga zgłoszenia do GIODO, zgłoszenie dotyczące rejestracji lub modyfikacji zarejestrowanego zbioru danych osobowych przygotowuje upoważnionego przez Administratora Danych Osobowych pracownika na stanowisku Informatyka wspólnie z użytkownikiem zbioru i przedkłada je Administratorowi Danych Osobowych.
7. Techniczną ochronę danych i ich przetwarzania realizuje się poprzez:
   1) przetwarzanie danych osobowych w wydzielonych pomieszczeniach,
   2) zabezpieczenie pomieszczeń, o których mowa w pkt. 1, przed nieuprawnionym dostępem:
      - klucze do pomieszczeń, w których następuje przetwarzanie danych osobowych wydawane są tylko osobom upoważnionym do przetwarzania danych w tych pomieszczeniach zgodnie z listą osób upoważnionych do pobierania kluczy do pomieszczeń, w których przetwarzane są dane osobowe – wzór stanowi załącznik nr 3, listę aktualizuje Sekretarz Gminy,
      - klucze nie są wynoszone po zakończeniu pracy poza miejsca przeznaczone do ich przechowywania,
      - pomieszczenia, w których odbywa się przetwarzanie danych osobowych znajdują się pod ścisłym nadzorem pracujących w nim osób upoważnionych do przetwarzania danych,
      - pomieszczenia, w których odbywa się przetwarzanie danych osobowych są zamykane w czasie chwilowej nieobecności pracownika w pomieszczeniu jak i po zakończeniu pracy, a klucze nie są pozostawiane w zamku drzwi,
   3) przechowywanie w zamykanych szafach wydruków i nośników elektronicznych zawierających dane osobowe,

4) niszczenie za pomocą niszczarek niepotrzebnych wydruków lub innych dokumentów,
5) zabezpieczenie dostępu do komputerów, na których jest prowadzone przetwarzanie danych przez wprowadzenie systemu logowania zgodnie z przyjętymi procedurami nadawania uprawnień do systemu informatycznego, określonymi w Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych,
6) systematyczne wykonywanie kopi bezpieczeństwa danych na nośnikach zewnętrznych przechowywanych w sejfach lub szafach metalowych,
7) zastosowanie zasilaczy UPS do zasilania awaryjnego serwerów, urządzeń dostępowych,
8) aktywowanie na wszystkich stacjach roboczych ochrony antywirusowej,
9) stosowanie zapory ogniowej (firewall) na ruterach dostępowych zabezpieczającej sieci przed atakiem z zewnątrz i filtrującej dostęp do sieci WAN poprzez blokowanie niektórych usług,
10) umieszczenie większości urządzeń znajdujących się w serwerowniach w szafach serwerowych i sieciowych oraz wyposażanie pomieszczeń serwerowni w urządzenia zapewniające właściwą temperaturę i wilgotność,

8. Organizacyjne środki ochrony danych osobowych i ich przetwarzania obejmują:
   1) zapoznanie każdej osoby upoważnionej z przepisami dotyczącymi ochrony danych osobowych, przed dopuszczeniem jej do pracy przy ich przetwarzaniu,
   2) przeszkolenie użytkowników systemu w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochroną danych osobowych oraz zabezpieczeniem pomieszczeń,
   3) zdefiniowanie procedur postępowania w przypadku naruszenia ochrony danych osobowych,
   4) szczególne zabezpieczenie pomieszczenia serwerowni, do którego dostęp posiadają jedynie osoby upoważnione,
9. Do przetwarzania danych osobowych, dopuszczone są wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych, wydane przez Administratora Danych Osobowych. Upoważnienia są wydawane indywidualnie przed rozpoczęciem przetwarzania danych osobowych przez Administratora Danych Osobowych.
10. W celu upoważnienia do przetwarzania danych osobowych Sekretarz Gminy lub upoważnionego przez Administratora Danych Osobowych pracownika na stanowisku Informatyka zapoznaje nowego użytkownika z Polityką bezpieczeństwa, Instrukcją zarządzania systemem informatycznym, Ustawą i Rozporządzeniem.
11. Upoważniony przez Administratora Danych Osobowych pracownik na stanowisku Informatyka prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych zgodnie ze wzorem stanowiącym załącznik do Instrukcji zarzadzania systemem informatycznym w Urzędzie Gminy Godziesze Wielkie. Ewidencja osób upoważnionych do ich przetwarzania, zawiera m.in.:
    a) imię i nazwisko osoby upoważnionej,
    b) datę nadania i ustania
    c) zakres upoważnienia do przetwarzania danych osobowych,
    d) identyfikator, jeśli dane są przetwarzane w systemie informatycznym.
12. Wszyscy użytkownicy podlegają okresowym szkoleniom, stosownie do potrzeb wynikających ze zmian w systemie informatycznym (wymiana sprzętu na nowszej

generacji, zmiana oprogramowania) oraz w związku ze zmianą przepisów o ochronie danych osobowych lub zmianą wewnętrznych regulacji.

13. Bezpieczeństwo usług zewnętrznych:
    1) Wymagania bezpieczeństwa przetwarzania danych osobowych, zakres usług oraz poziom ich dostarczenia należy każdorazowo określić w umowie świadczenia usług.
    2) Należy również zapewnić, aby użytkownicy nie będący pracownikami Urzędu Gminy Godziesze Wielkie stosowali te same zasady bezpieczeństwa przetwarzania danych osobowych co użytkownicy będący pracownikami.
14. Niezależnie od niniejszych ustaleń mają zastosowanie wszelkie inne regulaminy i instrukcje dotyczące bezpieczeństwa.

Rozdział 2
KONTROLA PRZESTRZEGANIA ZASAD ZABEZPIECZENIA DANYCH OSOBOWYCH

1. Upoważniony przez Administratora Danych Osobowych pracownik na stanowisku Informatyka odpowiada za zapewnienie przestrzegania zasad ochrony danych osobowych wynikający z ustawy o ochronie danych osobowych, zasad ustanowionych w niniejszym dokumencie oraz instrukcji zarządzana systemami informatycznymi.
2. Każdy pracownik Urzędu Gminy Godziesze Wielkie jest zobowiązany poddać się kontroli stanowiska pracy wynikającej z ochrony danych osobowych prowadzanej przez upoważnionego przez Administratora Danych Osobowych pracownika na stanowisku Informatyka oraz udostępnić niezbędne informacje mające wpływ na bezpieczeństwo danych.
3. Z przeprowadzonej kontroli sporządzane jest sprawozdanie, które przekazywane jest do Administratora Danych Osobowych.

Rozdział 3
ZASADY UDOSTĘPNIENIA DANYCH OSOBOWYCH.

1. Dane osobowe gromadzone i przetwarzane w Urzędzie mogą być udostępniane wyłącznie podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa oraz osobom uprawnionym na podstawie umotywowanego wniosku o udostępnienie danych osobowych.
2. Decyzję o udostępnieniu danych osobowych podejmuje Administrator Danych Osobowych lub Sekretarz Gminy.
3. Po otrzymaniu zgody od Administratora Danych Osobowych lub Sekretarza Gminy dane do udostępnienia przygotowuje użytkownik danych osobowych. Użytkownik jest zobowiązany do odnotowania w systemie informatycznym informacji o odbiorcach, którym dane zostały udostępnione, dacie i zakresie tego udostępnienia.
4. Bez względu na formę udostępniania danych należy zachować ich poufność i integralność. Udostępnienie danych osobowych nie może być realizowane drogą telefoniczną ani inną uniemożliwiającą ustalenie tożsamości osoby uzyskującej dostęp do danych.

Rozdziale 4
POSTEPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOSBOWYCH

1. Każdy użytkownik, który stwierdza lub podejrzewa naruszenie ochrony danych w systemie informatycznym, zobowiązany jest niezwłocznie poinformować o tym upoważnionego przez Administratora Danych Osobowych pracownika na stanowisku Informatyka.
2. Do czasu przybycia upoważnionego przez Administratora Danych Osobowych pracownika na stanowisku Informatyka na miejsce naruszenia lub ujawnienia naruszenia ochrony danych osobowych, należy:
   1) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców naruszenia,
   2) rozważyć wstrzymanie bieżącej pracy na komputerze w celu zabezpieczenia miejsca zdarzenia,
   3) zaniechać, o ile to możliwe, dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić jego udokumentowanie i analizę,
   4) udokumentować wstępnie zaistniałe naruszenie,
   5) nie opuszczać, bez uzasadnionej potrzeby, miejsca zdarzenia do czasu przybycia upoważnionego przez Administratora Danych Osobowych pracownika na stanowisku Informatyka,
3. Po przybyciu na miejsce naruszenia lub ujawnienia naruszenia ochrony danych osobowych upoważnionego przez Administratora Danych Osobowych pracownika na stanowisku Informatyka:
   1) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania;
   2) może żądać wyjaśnień dotyczących zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
   3) dokonuje zabezpieczenia systemu informatycznego przed dalszym rozprzestrzenianiem się skutków naruszenia,

4) podejmuje odpowiednie kroki w celu powstrzymania lub ograniczenia dostępu osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów naruszenia,
5) o zaistniałym naruszeniu informuje Administratora Danych Osobowych.

4. Po wyczerpaniu niezbędnych środków doraźnych, upoważnionego przez Administratora Danych Osobowych pracownika na stanowisku Informatyka zasięga niezbędnych opinii i proponuje działania mające na celu usunięcie naruszenia i jego skutków oraz ustosunkowuje się do kwestii ewentualnego odtworzenia danych z kopii zapasowej i terminu wznowienia przetwarzania danych.
5. Upoważniony przez Administratora Danych Osobowych pracownik na stanowisku Informatyka dokumentuje zaistniały przypadek naruszenia oraz sporządza raport z naruszenia bezpieczeństwa danych osobowych w Urzędzie Gminy Godziesze Wielkie– wzór stanowi załącznik nr 4 do niniejszej polityki, który zawiera w szczególności:
   1) wskazanie osoby powiadamiającej o naruszeniu oraz innych osób, które złożyły wyjaśnienia w związku z naruszeniem,
   2) określenie dokładnego czasu i miejsca naruszenia oraz powiadomienia o naruszeniu;
   3) określenie rodzaju naruszenia i okoliczności mu towarzyszących,
   4) wyszczególnienie uwzględnionych przesłanek wyboru metody postępowania i opis podjętego działania,
   5) wstępną ocenę przyczyn wystąpienia naruszenia,
   6) ocenę przeprowadzonego postępowania wyjaśniającego i działań podjętych w celu usunięcia naruszenia i jego skutków.
6. Upoważniony przez Administratora Danych Osobowych pracownik na stanowisku Informatyka przekazuje raport do Administratora Danych Osobowych w terminie 7 dni od daty zdarzenia.
7. Po przywróceniu prawidłowego funkcjonowania systemu informatycznego, upoważniony przez Administratora Danych Osobowych pracownik na stanowisku Informatyka przeprowadza szczegółową analizę w celu określenia przyczyn naruszenia ochrony danych osobowych lub podejrzenia takiego naruszenia oraz podejmuje kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.

Rozdział 5
POSTANOWIENIA KOŃCOWE

1. Wobec osoby, która w przypadku naruszenia ochrony danych osobowych lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, wszczyna się postępowanie dyscyplinarne.
2. W kwestiach nieuregulowanych w niniejszym dokumencie a dotyczących bezpieczeństwa danych osobowych w Urzędzie Gminy Godziesze Wielkie decyzje na wniosek zainteresowanego wydaje Administrator Danych Osobowych.

WÓJT GMINY
Józef Podłużny

Załącznik Nr 1
do Polityki bezpieczeństwa
przetwarzania danych osobowych
w Urzędzie Gminy Godziesze
Wielkie

Wykaz budynków, pomieszczeń, części pomieszczeń tworzących obszary, w których przetwarzane są dane osobowe

Określenie budynków i pomieszczeń tworzących obszar, w których przetwarzane są dane osobowe, powinno obejmować zarówno miejsca, w których wykonuje się operacje na danych osobowych (wpisuje, modyfikuje, kopiuje), jak również miejsca, gdzie przechowuje się wszelkie nośniki informacji, zawierające dane osobowe (szafy z dokumentacją papierową, szafy zawierające komputerowe nośniki informacji z kopiami zapasowymi danych, stacje komputerowe, serwery i inne urządzenia komputerowe, jak np. macierze dyskowe, na których dane osobowe są przetwarzane na bieżąco).

Lp.	Budynek, dokładny adres	Pomieszczenie	Osoba nadzorująca zabezpieczenie obszaru	Umowa najmu/ współpracy
1.				
2.				

.....
data aktualizacji i podpis

Załącznik Nr 2
do Polityki bezpieczeństwa
przetwarzania danych osobowych
w Urzędzie Gminy Godziesze Wielkie

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych oraz opis struktury zbiorów danych osobowych wskazujących zawartość poszczególnych pól informacyjnych i powiązań między nimi

Lp.	Nazwa zbioru oraz Administrator[1]	Cel przetwarzania Podstawa prawna	Miejsca agregacji ----- System przetwarzania	← OPIS STRUKTURY ZBIORÓW → Zakres danych	Powiązania między zbiorami
1.					
2.					
3.					
4.					
5.					
6.					

[1] Administrator - tylko w przypadku systemu w formie elektronicznej a w przypadku tradycyjnego, osoba odpowiedzialna za zbiór.

Załącznik Nr 3
do Polityki bezpieczeństwa
przetwarzania danych osobowych
w Urzędzie Gminy Godziesze
Wielkie

Lista osób upoważnionych do pobierania kluczy do pomieszczeń, w których przetwarzane są dane osobowe

Lp.	Imię i Nazwisko osoby upoważnionej	Nr pomieszczenia	Data ustania upoważnienia

Załącznik Nr 4
do Polityki bezpieczeństwa
przetwarzania danych osobowych
w Urzędzie Gminy Godziesze
Wielkie

Raport z naruszenia bezpieczeństwa danych osobowych w Urzędzie Gminy Godziesze Wielkie

1. Data: ..... r., godzina: .....
   (dd.mm.rrrr) (00:00)

2. Osoba powiadamiająca o zaistniałym zdarzeniu: .....
.....
.....
(imię, nazwisko, stanowisko służbowe, nazwa użytkownika- jeśli występuje)

3. Lokalizacja zdarzenia:
.....
(np. nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:
.....
.....
.....

5. Podjęte działania:
.....
.....
.....

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

7. Postępowanie wyjaśniające:
.....
.....
.....

.....
(data i podpis
upoważnionego przez Administratora Danych Osobowych
pracownika na stanowisku Informatyka)

WÓJT GMINY
Godziesze Wielkie

Załącznik Nr 2
do Zarządzenia Nr 146/2016
Wójta Gminy Godziesze Wielkie
z dnia 04 stycznia 2016 roku

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYMI DO PRZETWARZANIA DANYCH OSOBOWYCH W URZĘDZIE GMINY GODZIESZE WIELKIE

SPIS TREŚCI

ZAŁĄCZNIKI

PODSTAWA PRAWNA

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz. U. 2014 r. poz.1182 ze zm.) oraz Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, póz. 1024 ze zm.)

ZAKRES STOSOWANIA

1. Instrukcja zarządzania systemem informatycznym Urzędu Gminy Godziesze Wielkie zwana dalej instrukcją, opisuje sposoby nadawania uprawnień użytkownikom, określa sposób pracy we wszystkich systemach informatycznych, procedury zarządzania oraz czynności mające wpływ na zapewnienie bezpieczeństwa systemów informatycznych Urzędu Gminy Godziesze Wielkie.
2. Niniejsza instrukcja realizuje „Politykę bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Godziesze Wielkie".

DEFINICJE

1. Ilekroć w niniejszym dokumencie jest mowa o:
   - Urzędzie - należy przez to rozumieć Urząd Gminy Godziesze Wielkie
   - Administratorze Danych Osobowych – oznacza to Wójta Gminy Godziesze Wielkie,
   - Użytkowniku systemu - należy przez to rozumieć osobę posiadającą uprawnienia umożliwiające dostęp do systemu informatycznego, w którym są przetwarzane dane osobowe,
   - Osobie upoważnionej - należy przez to rozumieć osobę posiadającą upoważnienie, wydane przez Administratora Danych Osobowych, do przetwarzania danych osobowych w systemie informatycznym w zakresie wskazanym w upoważnieniu
   - Sieci lokalnej - należy przez to rozumieć połączenie systemów informatycznych Urzędu wyłącznie dla własnych potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych,
   - Sieci rozległej - należy przez to rozumieć sieć publiczną w rozumieniu ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. 2014 poz. 243 ze zm.).

PROCEDURY NADAWANIA I ZMIANY UPRAWNIEŃ W SYSTEMACH INFORMATYCZNYCH SŁUŻĄCYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Do przetwarzania danych osobowych, dopuszczone są wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych, wydane przez Administratora Danych Osobowych w toku następującej procedury:
   1) upoważnienia są wydawane indywidualnie przed rozpoczęciem przetwarzania danych osobowych przez Administratora Danych Osobowych,
   2) w celu upoważnienia do przetwarzania danych osobowych Sekretarz Gminy lub upoważniony przez Administratora Danych Osobowych pracownik na stanowisku Informatyka zapoznaje nowego użytkownika z Polityką bezpieczeństwa, Instrukcją zarządzania systemem informatycznym, Ustawą i Rozporządzeniem,
   3) zapoznanie się z powyższymi regulacjami użytkownik potwierdza własnoręcznym podpisem na oświadczeniu, którego wzór stanowi załącznik nr 1 niniejszego dokumentu,
   4) Sekretarz przedkłada Administratorowi Danych Osobowych do akceptacji upoważnienie do przetwarzania danych osobowych, w którym określa dane użytkownika wraz z wyszczególnieniem zbioru danych i zakresu czynności dla każdego z nich oddzielnie np. odczyt, wprowadzanie, modyfikacja, usuwanie (wzór upoważnienia stanowi załącznik nr 2),
   5) Administrator Danych Osobowych wystawia formalne upoważnienie do przetwarzania danych osobowych,
   6) Upoważniony przez Administratora Danych Osobowych pracownik na stanowisku Informatyka prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych zgodnie ze wzorem stanowiącym załącznik nr 3 do niniejszej Polityki Bezpieczeństwa,
   7) zgodnie z wydanym upoważnieniem pracownik na stanowisku Informatyka nadaje prawa dostępu do zasobów (unikalny login i hasło umożliwiające dostęp do wszystkich systemów i aplikacji w zakresie wskazanym w upoważnieniu),
   8) przekazuje nadany login (identyfikator) wraz ze wskazaniem systemu oraz szkoli użytkownika w zakresie bezpiecznej obsługi urządzeń i programów,
   9) Oświadczenia i upoważnienia pracowników przechowywane są w aktach osobowych.
2. Przełożeni osób upoważnionych do przetwarzania danych osobowych odpowiadają za natychmiastowe zgłoszenie do upoważnionego przez Administratora Danych Osobowych pracownika na stanowisku Informatyka oraz Sekretarza Gminy osób, które utraciły uprawnienia lub dostęp do danych osobowych.
3. Modyfikacja upoważnienia do przetwarzania danych osobowych i uprawnień do systemu informatycznego przetwarzającego dane osobowe podlega analogicznej procedurze jak przy jego nadawaniu.
4. Do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych, mogą zostać dopuszczone również osoby, którym

udzielono upoważnień do przetwarzania danych osobowych na podstawie porozumień – umów zawartych w sprawie powierzenia przetwarzania danych osobowych.

5. W systemie informatycznym stosuje się uwierzytelnianie dwustopniowe: na poziomie dostępu do komputera oraz dostępu do aplikacji.
6. Hasła ustanowione podczas przyznawania uprawnień przez Informatyka należy zmienić na indywidualne podczas pierwszego logowania się w systemie.
7. Pracownik ma prawo do wykonywania tylko tych czynności, do których posiada uprawnienia oraz ponosi pełną odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu.
8. Identyfikator osoby, która utraciła upoważnienie do przetwarzania danych osobowych lub uprawnienia dostępu do systemu informatycznego należy niezwłocznie zablokować i nie należy go nadawać innym użytkownikom.

STOSOWANE METODY I ŚRODKI UWIERZYTELNIAJĄCE UŻYTKOWNIKA ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM

1. Bezpośredni dostęp do systemu informatycznego może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.
2. Hasło użytkownika powinno być zmieniane, co najmniej raz w miesiącu i jeżeli istnieje taka możliwość system powinien wymuszać zmianę hasła.
3. Identyfikator jest przypisany do użytkownika na stałe i nie należy go zmieniać ani przydzielać innemu użytkownikowi.
4. Użytkownicy są odpowiedzialni za zachowanie poufności swoich haseł.
5. Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności.
6. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie.
7. W sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, użytkownik zobowiązany jest do natychmiastowej zmiany hasła.
8. Przy wyborze hasła obowiązują następujące zasady:
   a) minimalna długość hasła - 8 znaków,
   b) zakazuje się stosować: haseł, które użytkownik stosował uprzednio w okresie minionego roku, swojej nazwy użytkownika w jakiejkolwiek formie (pisanej dużymi literami, w odwrotnym porządku, dublując każdą literę, itp.), swojego imienia, drugiego imienia, nazwiska, przezwiska, pseudonimu w jakiejkolwiek formie, imion (w szczególności imion osób z najbliższej rodziny), ogólnie dostępnych informacji o użytkowniku takich jak: numer telefonu, numer rejestracyjny samochodu, jego marka, numer dowodu osobistego, nazwa ulicy, na której mieszka lub pracuje, itp. wyrazów słownikowych, przewidywalnych sekwencji znaków z klawiatury np.: QWERTY", "12345678", itp.
   c) należy stosować hasła zawierające:
      - kombinacje liter i cyfr,
      - małe i wielkie litery

- znaki specjalne: znaki interpunkcyjne, nawiasy, symbole @, #, &, itp. o ile system informatyczny na to pozwala,

d) używane hasła powinny być łatwe do zapamiętania i wykluczać konieczność ich zapisywania oraz powinny być łatwe i szybkie do wprowadzenia, po to by trudniej było podejrzeć je osobom trzecim

9. W systemach, które posiadają opcję zapamiętania nazw użytkownika i jego hasła nie należy korzystać z tego ułatwienia.
10. Hasło Informatyka o prawach administratora powinno znajdować się w zapieczętowanej kopercie w zamykanej na klucz szafie metalowej lub sejfie, do której dostęp mają:
    - Wójt,
    - Sekretarz,
    - Informatyk.
11. Każdorazowe pobranie hasła z zapieczętowanej koperty przez osobę uprawnioną musi zostać odnotowane w ewidencji wydania dostępu do konta administracyjnego, którego wzór stanowi załącznik nr 4 do niniejszego dokumentu.
12. Po każdorazowym pobraniu hasła z zapieczętowanej koperty przez osobę uprawnioną Informatyk ma obowiązek dokonać zmiany hasła oraz aktualne hasło ponownie umieścić w zapieczętowanej kopercie. Fakt zmiany hasła z podaniem daty należy odnotować w ewidencji.

PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY W SYSTEMIE

1. Przed przystąpieniem do pracy z systemem informatycznym, użytkownik systemu 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 powiadomić o tym fakcie swojego upoważnionego przez Administratora Danych Osobowych pracownika na stanowisku Informatyka lub Sekretarza Gminy.
3. Przed rozpoczęciem pracy w systemie komputerowym należy załogować się do systemu operacyjnego przy użyciu indywidualnego identyfikatora oraz hasła.
4. Przy opuszczeniu stanowiska pracy na odległość uniemożliwiającą jego obserwację należy wykonać czynność wylogowania z systemu (zablokowania dostępu).
5. Każdy komputer powinien mieć włączony wygaszacz ekranu ustawiony na 5 min. i aktywowaną opcję żądania podania hasła przy wznowieniu pracy.
6. Osoba udostępniająca stanowisko komputerowe innemu uprawnionemu do pracy na tym stanowisku pracownikowi zobowiązana jest wykonać operację wylogowania z systemu.
7. Monitory stanowisk komputerowych, na których przetwarzane są dane osobowe, znajdujące się w pomieszczeniach, gdzie przebywają osoby, które nie posiadają upoważnień do

przetwarzania danych osobowych, należy ustawić w taki sposób, aby uniemożliwić tym osobom wgląd w dane.

8. Przebywanie osób nieuprawnionych w pomieszczeniach znajdujących się na obszarze, w którym są przetwarzane dane osobowe, jest dopuszczalne tylko w obecności osoby upoważnionej do ich przetwarzania.
9. Przed wyłączeniem komputera należy bezwzględnie zakończyć pracę uruchomionych programów i wykonać zamknięcie systemu.
10. Niedopuszczalne jest wyłączanie komputera przed zamknięciem uruchomionego oprogramowania oraz zakończeniem pracy w sieci.
11. Kończąc pracę użytkownik jest również zobowiązany do zabezpieczenia swojego stanowiska pracy, w szczególności wszelkiej dokumentacji, wydruków oraz elektronicznych nośników informacji, na których znajdują się dane osobowe i umieszczenia ich w zamykanych szafach.
12. Czas pracy przy przetwarzaniu zbiorów danych osobowych pokrywa się z czasem pracy urzędu. Praca przy przetwarzaniu zbiorów poza tymi godzinami wymaga zgody Administratora Danych Osobowych i powinna być zgłoszona Sekretarzowi.

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

1. Za systematyczne wykonywanie kopii bezpieczeństwa wszystkich systemów pracujących w Urzędzie odpowiada Informatyk.
2. Kopie bezpieczeństwa wykonywane są w zależności od ilości i częstotliwości wprowadzanych danych do systemu codzienne po zakończeniu pracy wszystkich użytkowników w sieci komputerowej lub w innych odstępach czasu ale zawsze raz w miesiącu.
3. Kopie bezpieczeństwa wykonywane są w systemie informatycznym a następnie przenoszone na opisane w przejrzysty sposób nośniki zewnętrzne (dysk przenośny).

Wykonane kopie bezpieczeństwa przechowuje się, co najmniej:

- w odniesieniu do kopii dziennych przez okres 1 miesiąca od daty ich wykonania,
- w odniesieniu do kopii miesięcznych przez okres 12 miesięcy od daty ich wykonania,
- w odniesieniu do kopii rocznych przechowuje się wszystkie kopie.

4. Dodatkowe zabezpieczenie systemu i danych należy wykonać przed przystąpieniem do newralgicznych czynności mających wpływ na funkcjonalność oprogramowania lub zmianę struktury baz danych związanych np. z aktualizacją oprogramowania oraz zawsze na koniec roku kalendarzowego.
5. W celu sprawdzenia poprawności wykonywanych kopii należy dokonywać okresowego sprawdzenia poprawności zapisu danych (odtworzenia) oraz jego użyteczności przy odtworzeniu danych,

SPOSÓB, MIEJSCE I OKRES PRZECHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE ORAZ WYDRUKÓW

A. Elektroniczne nośniki informacji.

1. Danych osobowych w postaci elektronicznej zapisanych na nośnikach zewnętrznych nie wolno wynosić poza siedzibę Urzędu.
2. Komputery przenośne używane do gromadzenia lub przetwarzania danych osobowych można wynosić poza obszar przetwarzania danych osobowych, określony w Polityce bezpieczeństwa jedynie po uzyskaniu pisemnej zgody Administratora Danych Osobowych.
3. Wymienne elektroniczne nośniki informacji - za wyjątkiem kopii bezpieczeństwa – należy używać tylko w pokojach stanowiących obszar przetwarzania tych danych osobowych, określony w Polityce bezpieczeństwa.
4. Po zakończeniu pracy przez użytkowników systemu, wymienne elektroniczne nośniki informacji należy przechowywać w zamykanych szafkach biurowych.
5. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie.
6. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymywania danych osobowych pozbawia się wcześniej zapisu tych danych.
7. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem Informatyka.
8. Za podjęcie czynności określonych w pkt. 5-7 odpowiada Informatyk.

B. Kopie zapasowe.

1. Kopie bezpieczeństwa są przechowywane w szafie metalowej w budynku Urzędu Gminy Godziesze Wielkie
2. Dostęp do kopii opisanych w punkcie 1 ma Administratora Danych Osobowych oraz upoważniony przez Administratora Danych Osobowych pracownik na stanowisku Informatyka.

C. Wydruki.

1. W przypadku konieczności przechowywania wydruków zawierających dane osobowe należy je przechowywać w miejscu uniemożliwiającym bezpośredni dostęp osobom niepowołanym.
2. Pomieszczenie, w którym przechowywane są wydruki zawierające dane osobowe musi być należycie zabezpieczone po godzinach pracy.
3. Wydruki, które zawierają dane osobowe i są przeznaczone do zniszczenia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

ŚRODKI OCHRONY SYSTEMU PRZED ZŁOŚLIWYM OPROGRAMOWANIEM I WIRUSAMI KOMPUTEROWYMI

1. Na każdym stanowisku komputerowym zainstalowane jest oprogramowanie antywirusowe pracujące w trybie monitora.
2. Każdy e-mail wpływający do Urzędu jest sprawdzony pod kątem występowania wirusów przez monitor antywirusowy.
3. Definicje wzorców wirusów aktualizowane są na bieżąco on-line a na stacjach roboczych pozbawionych dostępu do Internetu nie rzadziej niż raz w miesiącu.
4. Zabrania się używania nośników niewiadomego pochodzenia bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje użytkownik, który nośnik zamierza użyć.
5. Zabrania się pobierania z Internetu plików niewiadomego pochodzenia. Każdy plik pobrany z Internetu musi być sprawdzony programem antywirusowym. Sprawdzenia dokonuje użytkownik, który pobiera plik.
6. Zabrania się odczytywania załączników poczty elektronicznej bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje pracownik, który otrzymał pocztę.
7. Informatyk nadzoruje automatyczne kontrole antywirusowe na wszystkich komputerach, w razie nieprzeprowadzonej kontroli uruchamia kontrolę antywirusową indywidualną na wybranym komputerze.
8. Kontrola antywirusowa przeprowadzana jest również na komputerze w przypadku zgłoszenia nieprawidłowości w jego funkcjonowaniu.
9. W przypadku wykrycia wirusów komputerowych sprawdzane jest stanowisko komputerowe, na którym wirusa wykryto oraz wszystkie posiadane przez użytkownika nośniki.

PROCEDURY WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMU

A. Przeglądy i konserwacja urządzeń.

1. Przeglądy i konserwacja urządzeń wchodzących w skład systemu informatycznego powinny być wykonywane w terminach i w zakresie określonym przez producenta sprzętu.
2. Nieprawidłowości ujawnione w trakcie działania urządzeń powinny być niezwłocznie usunięte, a ich przyczyny przeanalizowane. O fakcie zaistnienia nieprawidłowości w działaniu urządzeń należy niezwłocznie zawiadomić Informatyka.

B. Przegląd i konfiguracja programów i narzędzi programowych.

1. Konserwacja i indeksacja baz danych przeprowadzana jest zgodnie z zaleceniami twórców poszczególnych programów.

2. Po wykryciu trzech nieudanych prób, system automatycznie blokuje dostęp użytkownika do systemu.
3. Wszystkie logi opisujące pracę systemu, zameldowania i wymeldowania użytkowników oraz rejestr z systemu śledzenia wykonywanych operacji w programie należy przed usunięciem zapisać na płytę CD-R/DVD-R.

C. Rejestracja działań konserwacyjnych, awarii oraz napraw.
1. Informatyk prowadzi „Dziennik zdarzeń systemów informatycznych Urzędu Gminy Godziesze Wielkie". Wzór i zakres informacji rejestrowanych w dzienniku określony jest w załączniku nr 5.
2. Wpisów do dziennika może dokonywać wyłącznie Informatyk lub osoba go zastępująca.

D. Przeglądy i konserwacje urządzeń przez firmy zewnętrzne mogą odbywać się tylko w obecności Informatyka.

POŁĄCZENIE DO SIECI INTERNET

1. Połączenie lokalnej sieci komputerowej Urzędu Gminy Godziesze Wielkie z siecią WAN (internetem) jest realizowane wyłącznie poprzez skonfigurowaną na routerze sprzętową zaporę ogniową (firewall). Ochrona antywirusowa jest realizowana na każdym terminalu indywidualnie poprzez zainstalowane aktualne oprogramowanie antywirusowe.. Za konfigurację i optymalizację pracy zapór ogniowych na routerach oraz instalację, konfiguracje i aktualizację ochrony antywirusowej na wszystkich komputerach w sieci odpowiada Informatyk.
2. W efekcie zastosowanie zapory firewall i oprogramowania antywirusowego zapewnione jest:
   1) zabezpieczenie sieci przed atakiem z zewnątrz,
   2) filtrowanie dostępu do sieci WAN i blokowanie niektórych usług,
   3) objęcie ochroną antywirusową wszystkich danych ściąganych z Internetu na stacjach lokalnych.

BEZPIECZNA EKSPLOATACJA SYSTEMÓW INFORMATYCZNYCH

Bezpieczna eksploatacja systemów informatycznych przetwarzających dane osobowe, zostaje zapewniona poprzez przestrzeganie następujących zasad:
1. Użytkownikom zabrania się, wprowadzania zmian do oprogramowania, sprzętu informatycznego poprzez jego samodzielne konfigurowanie i wyposażanie.
2. Użytkownikom zabrania się, umożliwiania stronom trzecim uzyskiwania nieupoważnionego dostępu do systemów informatycznych.
3. Użytkownikom nie wolno instalować nowego lub aktualizować już zainstalowanego oprogramowania.

4. Użytkownikom nie wolno korzystać z systemów informatycznych dla celów innych niż związane z wykonywaniem obowiązków służbowych.
5. Użytkownikom nie wolno korzystać z prywatnego sprzętu informatycznego, w tym oprogramowania oraz nośników pamięci.
6. Użytkownikom nie wolno podejmować prób testowania, modyfikacji i naruszenia zabezpieczeń systemów informatycznych lub jakichkolwiek działań noszących takie znamiona.

ZASADY UDOSTĘPNIENIA DANYCH OSOBOWYCH

1. Dane osobowe gromadzone i przetwarzane w Urzędzie mogą być udostępniane wyłącznie podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa oraz osobom uprawnionym na podstawie umotywowanego wniosku o udostępnienie danych osobowych.
2. Decyzję o udostępnieniu danych osobowych podejmuje Administrator Danych Osobowych lub Sekretarz Gminy.
3. Po otrzymaniu zgody od Administratora Danych Osobowych lub Sekretarza Gminy dane do udostępnienia przygotowuje użytkownik danych osobowych. Użytkownik jest zobowiązany do odnotowania w systemie informatycznym informacji o odbiorcach, którym dane zostały udostępnione, dacie i zakresie tego udostępnienia.
4. Bez względu na formę udostępniania danych należy zachować ich poufność i integralność. Udostępnienie danych osobowych nie może być realizowane drogą telefoniczną ani inną uniemożliwiającą ustalenie tożsamości osoby uzyskującej dostęp do danych.

POSTANOWIENIA KOŃCOWE

W kwestiach nieuregulowanych w niniejszym dokumencie a dotyczących bezpieczeństwa danych osobowych w Urzędzie Gminy Godziesze Wielkie decyzje na wniosek zainteresowanego wydaje Administrator Danych Osobowych.

WÓJT GMINY
Józef Podłużny

Załącznik Nr 1
do Instrukcji zarzadzania
systemami informatycznymi
w Urzędzie Gminy Godziesze
Wielkie

Godziesze Wielkie, ...

OŚWIADCZENIE

Oświadczam, iż zostałam/em zaznajomiona/y z przepisami dotyczącymi ochrony danych osobowych, w szczególności ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. j.t. z 2014r. poz. 1182), wydanych na jej podstawie aktów wykonawczych oraz wprowadzonymi i wdrożonymi do stosowania przez Administratora Danych Osobowych Polityką bezpieczeństwa w zakresie danych osobowych oraz Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Godziesze Wielkie. Jednocześnie zobowiązuję się do ich przestrzegania.

.....
(podpis osoby składającej oświadczenie)

Załącznik Nr 2
do Instrukcji zarzadzania
systemami informatycznymi
w Urzędzie Gminy Godziesze
Wielkie

Godziesze Wielkie, ...

UPOWAŻNIENIE
DO PRZETWARZANIA DANYCH OSOBOWYCH
W URZĘDZIE GMINY GODZIESZE WIELKIE

Z dniem ..... na podstawie art.37 w związku z art.31 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t. j. Dz. U. z 2014r. poz.1182), upoważniam Panią/Pana* ..... do przetwarzania danych zgromadzonych w zbiorach danych osobowych Urzędu Gminy Godziesze Wielkie w następującym zakresie:

1.....
2. ....
3.....

Upoważnienie wygasa z chwilą ustania Pan/Pana* zatrudnienia w Urzędzie Gminy Godziesze Wielkie, a ponadto może być w każdym czasie zmienione lub odwołane.

.....
Własnoręczny podpis Administratora Danych Osobowych

* niepotrzebne skreślić

Załącznik Nr 3
do Instrukcji zarzadzania
systemami informatycznymi
w Urzędzie Gminy Godziesze
Wielkie

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH W URZĘDZIE GMINY GODZIESZE WIELKIE

Lp.	Nazwisko i imię osoby upoważnionej do przetwarzania danych osobowych	Nr upoważnienia	Data wydania (modyfikacji) upoważnienia	Data utraty ważności upoważnienia	Zakres upoważnienia do przetwarzania danych osobowych	Identyfikator w systemie	System

Załącznik Nr 4
do Instrukcji zarzadzania
systemami informatycznymi
w Urzędzie Gminy Godziesze
Wielkie

EWIDENCJA WYDANIA DOSTĘPU DO KONTA ADMINISTRACYJNEGO

Lp.	Nazwa systemu informatycznego	Imię i Nazwisko osoby pobierającej dostęp do konta administracyjnego	Data pobrania	Podpis osoby pobierającej	Data zmiany hasła dostępu

Załącznik Nr 5
do Instrukcji zarzadzania
systemami informatycznymi
w Urzędzie Gminy Godziesze
Wielkie

Dziennik zawiera opisy wszelkich zdarzeń istotnych dla działania systemu informatycznego w szczególności:

- w przypadku awarii - opis awarii, przyczyna awarii, szkody wynikłe na skutek awarii, sposób usunięcia awarii, opis systemu po awarii, wnioski;
- w przypadku konserwacji systemu - opis podjętych działań, wnioski.

DZIENNIK ZDARZEŃ SYSTEMÓW INFORMATYCZNYCH URZĘDU GMINY GODZIESZE WIELKIE

Lp.	Data i godzina zdarzenia	Opis zdarzenia	Podjęte działania/ wnioski