Zarządzenie Nr 21/2016
Wójta Gminy Zadzim
z dnia 31.03.2016

w sprawie wprowadzenia do użytku służbowego polityki bezpieczeństwa zbiorów danych osobowych prowadzonych w Urzędzie Gminy w Zadzimiu

Na podstawie art. 36 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2015 r. poz. 2135 ze zm.) oraz § 5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100 poz. 1024) zarządza się co następuje:

§ 1. Wprowadza się do użytku służbowego „Politykę bezpieczeństwa zbiorów danych osobowych prowadzonych w Urzędzie Gminy w Zadzimiu" stanowiącą załącznik do zarządzenia.

§ 2. 1. Zobowiązuje się pracowników przetwarzających dane osobowe do przestrzegania przepisów dokumentów, o których mowa w § 1.

2. Zobowiązuje się pracowników przetwarzających dane osobowe do sprawowania nadzoru nad ich ochroną oraz współpracy z Administratorem Bezpieczeństwa Informacji w tym zakresie.

3. Zobowiązuje się wszystkich pracowników posiadających upoważnienie do przetwarzania danych osobowych , nadane przez administratora danych, do bezwzględnego przestrzegania podanych w niniejszym opracowaniu reguł i zasad tworzących politykę bezpieczeństwa.

§ 3. Traci moc Zarządzenie nr 190/VI/2014 Wójta Gminy Zadzim z dnia 7 lutego 2014 r.

§ 4. Zarządzenie wchodzi w życie z dniem podpisania

Wójt Gminy Zadzim

/-/Krzysztof Woźniak

URZĄD GMINY ZADZIM

ZATWIERDZAM:

POLITYKA BEZPIECZEŃSTWA

ZBIORÓW DANYCH OSOBOWYCH PROWADZONYCH

W URZĘDZIE GMINY ZADZIM

POZIOM WYSOKI

Marzec 2016

1. Wprowadzenie

Celem dokumentu, nazywanego dalej polityką bezpieczeństwa jest określenie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, w szczególności przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, zgodnie z art. 36 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz.U. z 2015 r. poz. 2135 ze zm.), zwanej dalej ustawą.

1.1 Zakres dokumentu polityka bezpieczeństwa

Zasady ochrony danych osobowych dotyczą systemów informatycznych oraz zbiorów tradycyjnych, w których przetwarzane są dane osobowe a administratorem danych (czyli osobą decydującą o celach i środkach przetwarzania danych) jest Wójt Gminy Zadzim. Zasady ochrony określone w niniejszym dokumencie obowiązują od dnia jego zatwierdzenia.

Polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym są to minimalne zasady ochrony danych osobowych opracowane na podstawie wytycznych i wskazówek Generalnego Inspektora Ochrony Danych Osobowych. Na polecenie administratora danych niniejszy dokument może być zmieniany i uzupełniany, w sposób nie skutkujący zmniejszeniem stopnia ochrony danych.

Zasady ochrony zawarte w niniejszej polityce bezpieczeństwa dotyczą zbiorów osobowych, przetwarzanych formie papierowej oraz w następujących systemach informatycznych:

PŁATNIK – Program do komunikacji z ZUS

GOMIG-ODPADY – Program do zarządzania systemem gospodarki odpadami

SELWIN – System ewidencji ludności

USC – System ewidencyjny Urzędu Stanu Cywilnego (akty: urodzenia, zgonu, małżeństwa)

SWDO – system wydawania dowodów osobistych

WODA – System rozliczania opłat za zużycie wody

SIO – System informacji oświatowej

HOMENET – System przelewów elektronicznych

U.I. INFO-SYSTEM – System rozliczeniowy/podatkowy, w skład którego wchodzą następujące moduły:

- **PODATKI** – Moduł podatkowy
- **KSZOB** – Księgowość i Zobowiązania
- **AUTA** – Moduł podatku od środków transportowych

KADRY I PŁACE	– Moduł Kadrowo Płacowy
KASA	– Moduł Kasowy
BUDŻET	– Moduł Budżetu Gminy
EGZEKUCJE	– Moduł Egzekucji i tytułów wykonawczych

1.2 Podstawa prawna

Dokumenty: Polityka bezpieczeństwa przetwarzania danych osobowych oraz Instrukcja Zarządzania Systemem informatycznym w Urzędzie Gminy Zadzim służą do ochrony przetwarzania danych osobowych i zostały opracowane na podstawie niniejszych aktów prawnych:

1) konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997r. (Dz.U. z 1997r. Nr 78, poz. 483 ze zm.);

2) ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tj. Dz.U. z 2015 r. poz. 2135 ze zm.);

3) rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024);

4) rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (tj. Dz.U. z 2016 r. poz. 113);

5) rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz. U. 2015, poz. 719);

6) rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz. U. 2015 poz. 745).

1.3 Słownik pojęć

Ilekroć w niniejszym dokumencie jest mowa o:

1) **Urzędzie** – należy przez to rozumieć Urząd Gminy Zadzim;

2) **Generalnym Inspektorze Ochrony Danych Osobowych**, zwanym dalej „GIODO” – należy przez to rozumieć organ do spraw ochrony danych osobowych;

3) **ustawie** – rozumie się przez to ustawę z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tj. Dz.U. z 2015 r. poz. 2135 ze zm.), zwaną dalej „ustawą”;

4) **danych osobowych** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą do zidentyfikowania jest osoba, której tożsamość można

określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny, jeden lub kilka specyficznych czynników określających jej cechy.
Do danych osobowych zalicza się więc nie tylko imię, nazwisko i adres, ale również przypisane jej numery, dane o cechach fizjologicznych, umysłowych, ekonomicznych, kulturowych i społecznych.
5) **danych wrażliwych** – dane o pochodzeniu rasowym lub etnicznym, poglądach politycznych, przekonaniach religijnych lub filozoficznych, przynależności wyznaniowej, partyjnej lub związkowej, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.
6) **przetwarzaniu danych** – operacje wykonywane na danych osobowych, tj. zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie.
7) **zbiorze danych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
8) **systemie informatycznym** – zespół współpracujących ze sobą urządzeń, programów, aplikacji, procedur wew. przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
9) **zabezpieczeniu danych w systemie informatycznym** – wdrożenie i eksploatacja stosowanych środków technicznych i organizacyjnych zapewniających ochronę danych osobowych przed ich nieuprawnioną modyfikacją, zniszczeniem, dostępem, ujawnieniem lub utratą.
10) **usuwaniu danych osobowych** – zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby której dotyczą.
11) **Administratorze danych osobowych** („ADO") – organ, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych osobowych. Funkcje Administratora danych osobowych w Urzędzie Gminy Zadzim pełni Wójt Gminy
12) **Administratorze bezpieczeństwa informacji** („ABI") - wyznaczona przez Administratora danych osobowych osoba - pracownik Urzędu - nadzorująca stosowanie środków technicznych i organizacyjnych przetwarzanych danych osobowych, odpowiednich do zagrożeń oraz kategorii danych objętych ochroną.
13) **Administratorze systemów Informatycznych** („ASI") – wyznaczony przez Administratora danych osobowych osoba lub zewnętrzny podmiot odpowiedzialny za stosowanie technicznych i organizacyjnych środków ochrony danych osobowych w Urzędzie
14) **Osobie upoważnionej** – osoba posiadające wydane przez Administratora danych osobowych upoważnienie do przetwarzania danych osobowych w Urzędzie
15) **użytkowniku systemu** – należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym Urzędu. Użytkownikiem może być pracownik Urzędu, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilnoprawnej, także osoba odbywająca praktykę lub staż w Urzędzie.
16) **identyfikatorze użytkownika** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.

17) **hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie upoważnionej do pracy w systemie informatycznym. Hasło powinno zawierać minimum 8 znaków.
18) **uwierzytelnianie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.
19) **sieci lokalnej** (LAN) – należy przez to rozumieć połączenie systemów informatycznych wyłącznie dla własnych jej potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych;
20) **sieci rozległej – publicznej** (WAN) – należy przez to rozumieć sieć publiczną w rozumieniu ustawy „prawo telekomunikacyjne".

1.4 Cel przetwarzania danych osobowych

Podstawy prawne przetwarzania danych osobowych w zbiorach prowadzonych w Urzędzie Gminy Zadzim wyszczególnione są w Rejestrze zbiorów danych osobowych w Urzędzie Gminy Zadzim, który stanowi załącznik nr 3 do niniejszego dokumentu.

1.5 Cel opracowania polityki bezpieczeństwa

Celem opracowania polityki bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy Zadzim jest określenie zasad ochrony, a w szczególności ochrony przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną a także przetwarzaniem z naruszeniem ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych.
Załącznikiem nr 1 do niniejszego dokumentu jest instrukcja zarządzania systemami przetwarzającymi dane osobowe w Urzędzie Gminy Zadzim określająca zasady ochrony danych osobowych podczas eksploatacji systemu informatycznego i stanowi jego integralną całość.

1.6 Lokalizacja systemów informatycznych oraz zbiorów danych osobowych

Dane osobowe przetwarzane są w budynku Urzędu Gminy Zadzim zlokalizowanego Zadzim 44, 99-232 Zadzim
Załącznik nr 2 zawiera wykaz pomieszczeń oraz systemy zabezpieczeń zbiorów danych osobowych wraz ze wskazaniem zbiorów których dotyczą. Załącznik Nr 2 opracowywany jest przez inspektora bezpieczeństwa informacji lub inną, wyznaczoną przez administratora danych, osobę.

1.7 Podmioty odpowiedzialne za eksploatację systemów informatycznych

Generalny nadzór nad realizacją zadań ochrony danych osobowych sprawuje Wójt Gminy Zadzim jako Administrator Danych Osobowych (ADO)
Administratorem systemów informatycznych (ASI) jest – Informatyk Urzędu Gminy Zadzim.
Administratorem bezpieczeństwa informacji jest (ABI) – Sekretarz Gminy Zadzim.

1.8 Użytkownicy systemu

Wszyscy użytkownicy systemów informatycznych, wymienionych w pkt 1.1 mają dostęp do danych osobowych jedynie w zakresie niezbędnym do realizacji zadań służbowych. Przed uzyskaniem dostępu do danych osobowych użytkownicy są szkoleni w zakresie wykonywania czynności zapewniających ochronę danych osobowych oraz dokumentów polityki bezpieczeństwa i instrukcji.

W ich zakresach czynności na zajmowanym stanowisku wpisane jest zobowiązanie do zapewnienia poufności danych osobowych oraz zobowiązanie do wykorzystywania danych osobowych, jedynie w celach służbowych.

Wyróżnia się trzy grupy użytkowników: użytkowników końcowych, administratorów systemów informatycznych i administratorów bezpieczeństwa informacji.

Użytkownicy końcowi systemu mają dostęp do danych osobowych jedynie w zakresie niezbędnym do realizacji zadań służbowych. Szczegółowe zadania użytkowników obejmują:

- przestrzeganie zasad ochrony danych osobowych określonych w niniejszym dokumencie i instrukcji zarządzania systemem informatycznym, o której mowa w pkt 1.5, oraz innych dokumentach eksploatacyjnych systemu,
- przetwarzanie danych osobowych zgodne z celami przetwarzania,
- informowanie administratora systemu informatycznego o wszelkich zauważonych nieprawidłowościach skutkujących obniżeniem poziomu ochrony danych osobowych,
- zapewnianie poufności danych osobowych, do których uzyskuje dostęp w systemie informatycznym.

Administrator systemu informatycznego ma dostęp do danych osobowych jedynie w zakresie niezbędnym do realizacji zadań administrowania systemem informatycznym. Szczegółowe zadania administratora obejmują:

- przestrzeganie zasad ochrony danych osobowych określonych w niniejszym dokumencie i instrukcji zarządzania systemem informatycznym, o których mowa w 1.5, oraz innych dokumentach eksploatacyjnych systemu,
- zapewnianie prawidłowej eksploatacji systemu, zgodnej z celami przetwarzania danych osobowych,
- zapewnienie ochrony nośników zawierających kopie zbiorów osobowych,
- informowanie administratora danych o wszelkich zauważonych nieprawidłowościach skutkujących obniżeniem poziomu ochrony danych osobowych,
- wyjaśnianie wspólnie z administratorem bezpieczeństwa informacji wszystkich zgłoszonych nieprawidłowości oraz incydentów,
- zapewnienie prowadzenia ewidencji użytkowników systemu,
- szkolenie użytkowników systemu w zakresie procedur zapewniających ochronę danych osobowych,
- zapewnianie poufności danych osobowych, do których uzyskuje dostęp w związku z czynnościami administracyjnymi systemie informatycznym.

Administrator bezpieczeństwa informacji ma dostęp do danych osobowych jedynie w zakresie niezbędnym do realizacji zadań związanych z wyjaśnieniem incydentów, czynnościami kontrolnymi oraz realizacją wniosków osób, których dane dotyczą. Szczegółowe zadania administratora bezpieczeństwa informacji obejmują:

- wyjaśnianie wspólnie z administratorem systemu informatycznego wszystkich zgłoszonych nieprawidłowości oraz incydentów,
- uzupełnianie i modyfikowanie polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym,
- kontrolowanie systemów informatycznych w zakresie zapewnienia ochrony danych osobowych,
- przedstawianie administratorowi danych wniosków w zakresie ochrony danych osobowych, uzgodnionych z administratorem systemu informatycznego.

1.9 Odnośniki do stosowanych standardów bezpieczeństwa

Wszystkie rozwiązania systemu ochrony danych osobowych są zgodne z podstawowymi standardami bezpieczeństwa teleinformatycznego, w tym z normami Polskiego Komitetu Normalizacyjnego:

- PN-I-13335: Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów teleinformatycznych,
- PN-I-2000 – Zabezpieczenia w systemach informatycznych –Terminologia.
- PN-ISO/IEC 17799 Technika Informatyczna. Praktyczne zasady zarządzania bezpieczeństwem informacji.

2. Zagrożenia dla systemu informatycznego

Biorąc pod uwagę wymienione standardy bezpieczeństwa teleinformatycznego oraz wytyczne w zakresie polityki bezpieczeństwa opublikowane przez Generalnego Inspektora Ochrony Danych Osobowych podstawowe zagrożenia dla danych osobowych przetwarzanych w systemie informatycznym to: utrata poufności, dostępności, integralności, oraz rozliczalności.

Poufność to zapewnienie, aby tylko uprawniona osoba posiadała dostęp do danych osobowych w zakresie wymaganym realizowanymi zadaniami. W związku z tym zagrożenia w zakresie poufności obejmują:

- Nieuprawniony dostęp do obszarów i pomieszczeń, w których zlokalizowane są zasoby systemu informatycznego służącego do przetwarzania danych osobowych,
- Ujawnienie haseł dostępu do systemu informatycznego,

- Nieuprawnione udostępnienie informacji przez osobę uzyskującą dostęp do danych osobowych systemu informatycznego,
- Nieuprawnione przeniesienie informacji na inny nośnik elektroniczny lub papierowy,
- Utrata nośnika zawierającego dane osobowe,
- Podszycie się pod osobę posiadającą uprawnienia użytkownika systemu informatycznego.

Dostępność to zapewnienie, aby użytkownik systemu informatycznego posiadał możliwość pracy na stanowisku komputerowym zgodnie z założonymi wymaganiami ochrony. Zagrożenia w zakresie dostępności obejmują:

- Brak możliwości przetwarzania danych osobowych spowodowany brakiem dostępu do pomieszczeń, w których zainstalowane są zasoby systemu informatycznego,
- Awaria sprzętu lub systemu informatycznego,
- Zakłócenia w zasilaniu systemu informatycznego,
- Brak dostępu do haseł systemu informatycznego,
- Klęska żywiołowa.

Integralność, to zapewnienie, aby wszelkie operacje wykonywane na danych osobowych przetwarzanych w systemie informatycznym były skutkiem świadomych i zaplanowanych działań użytkowników systemu. Zagrożenia w zakresie integralności obejmują:

- Brak kontroli nad operacjami wykonywanymi na danych osobowych przez użytkowników systemów informatycznych,
- Nieuprawnione przetwarzanie danych osobowych,
- Nieuprawniony dostęp do danych osobowych,
- Błędy sprzętu i systemu informatycznego.

Rozliczalność, to zapewnienie aby czynności wykonywane przez użytkowników systemów informatycznych były rejestrowane w celu uniemożliwienia wyparcia się przez osoby wykonujące czynności na danych osobowych. Zagrożenia w systemie informatycznym obejmują:

- Brak kontroli nad czynnościami wykonywanymi w systemie informatycznym służącym do przetwarzania danych osobowych,
- Nieaktualne listy osób uprawnionych do przetwarzania danych osobowych w systemie informatycznym,
- Brak poufności haseł dostępu do systemu informatycznego,
- Brak ochrony fizycznej stanowisk dostępu do danych osobowych,
- Braki w dokumentacji eksploatacyjnej systemu, w tym dokumentowania zmian systemu.

3. Definicja wymagań bezpieczeństwa danych osobowych przetwarzanych w: Urzędzie Gminy Zadzim

Bezpieczeństwo danych osobowych wymaga spełnienia następujących wymagań ochrony:

- zabezpieczenia przed nieuprawnionym dostępem do pomieszczeń, w których zainstalowane są zasoby systemu informatycznego, oraz przechowywane są dane osobowe.
- zabezpieczenia przed nieuprawnionym dostępem do nośników elektronicznych zawierających dane osobowe,
- zabezpieczenia przed nieuprawnionym dostępem do wydruków z danymi osobowymi,
- zapewnienia dostępności użytkowników do danych osobowych zgodnie z systemami uprawnień,
- zapewnienia możliwości kontroli dostępu do zasobów systemu komputerowego oraz wykonywanych w nim czynności,
- zapewnienia bieżącej aktualizacji listy osób uprawnionych do pracy w systemie informatycznym, odpowiednio do zadań służbowych
- zapewnienia kontroli w zakresie: Kto? Kiedy? Co?
- zapewnienia przetwarzania danych osobowych zgodnie z celem prowadzenia zbioru w Urzędzie.

Powyższe wymagania bezpieczeństwa danych osobowych są realizowane poprzez:

1. Do przetwarzania danych osobowych w Urzędzie mogą być dopuszczone wyłącznie osoby posiadające upoważnienie wydane przez Administratora Danych Osobowych (wzór upoważnienia stanowi **załącznik nr 1 do Instrukcji zarządzania systemami przetwarzającymi dane osobowe w urzędzie Gminy Zadzim**),
2. Zapewnienie, aby listy osób uprawnionych były na bieżąco aktualizowane, zgodnie ze zmianami kadrowymi,
3. Zapewnienie, aby systemy informatyczne zapewniały prowadzenie kontroli operacji wykonywanych na danych osobowych,
4. Zapewnienie, aby tylko osoby przeszkolone przetwarzały dane osobowe,
5. Zapewnienie, aby każdy użytkownik systemu informatycznego miał dostęp jedynie do danych osobowych, w związku realizowaniem celu przetwarzania,
6. Zapewnienie, aby kopie zbiorów osobowych i inne zasoby systemu informatycznego były niedostępne dla osób nieuprawnionych,
7. Zapewnienie, aby pomieszczenia, w których zlokalizowane są stanowiska umożliwiające dostęp do danych osobowych, były chronione przed dostępem osób nieuprawnionych,
8. Zapewnienie, aby komputery, na których przetwarzane są dane osobowe były podłączane do lokalnej sieci zasilającej lub lokalnego zasilacza awaryjnego ups.

4. Architektura zbiorów osobowych

4.1 Ewidencja i struktura zbiorów danych osobowych

- Obowiązek rejestracji zbiorów jest jednym z podstawowych obowiązków, jakie nakłada na Administratora danych osobowych ustawa o ochronie danych osobowych.
- Zgodnie z art. 40 ustawy Administrator danych osobowych jest zobowiązany zgłosić zbiór danych osobowych do rejestracji, której dokonuje Generalny Inspektorat Ochrony Danych Osobowych w celu przetwarzania tych danych, z wyjątkiem zbiorów, które z mocy ustawy o ochronie danych osobowych nie podlegają obowiązkowi rejestracji.
- Zgodnie z art. 43, ust. 1a ustawy o ochronie danych osobowych Administrator danych osobowych powołał Administratora Bezpieczeństwa Informacji i zgłosił go Generalnemu Inspektorowi Danych Osobowych do rejestracji, w związku z czym Administrator danych osobowych nie podlega obowiązkowi rejestracji do GIODO zbiorów danych osobowych wykorzystywanych w Urzędzie z wyjątkiem zbiorów danych osobowych zawierających informacje o których mowa w art. 27 ust. 1 ustawy o ochronie danych osobowych tj. zbiorów danych osobowych zawierających dane wrażliwe.
- Administrator bezpieczeństwa informacji prowadzi w Urzędzie jawny rejestr zbiorów danych osobowych (załącznik nr 3 do niniejszego dokumentu) przetwarzanych przez administratora danych, z wyjątkiem zbiorów o których mowa w art. 43 ust. 1, zawierający nazwy zbioru oraz informacje, o których mowa w art. 41 ust. 1 pkt 2-4a i 7.

Administrator bezpieczeństwa informacji w ramach prowadzenia rejestru:

1) wpisuje zbiór danych do rejestru przed rozpoczęciem przetwarzania w zbiorze danych;

2) aktualizuje informacje dotyczące zbioru danych w rejestrze – w przypadku zmiany informacji objętych wpisem;

3) wykreśla zbiór danych z rejestru – w przypadku zaprzestania przetwarzania w nim danych osobowych;

4) udostępnia rejestr do przeglądania.

4.2 Opis środowiska przetwarzania zbiorów danych osobowych

Zbiory osobowe w systemach informatycznych przetwarzane są w środowisku systemu operacyjnego WINDOWS XP SP3, Windows 7. Wszystkie programy (z wyjątkiem programu SELWIN patrz pkt 4.3) zainstalowane są na stanowiskach komputerowych podłączonych do wewnętrznej sieci LAN z dostępem do Internetu.

4.3 Opis przepływów danych pomiędzy systemami określonymi w pkt 1.1 oraz systemami zewnętrznymi

W przypadku programu PŁATNIK, wytworzone za pomocą tego programu dokumenty przesyłane są drogą elektroniczną (poprzez siec Internet) bezpośrednio do ZUS.

W przypadku programu SELWIN aplikacja zainstalowana jest na stanowisku znajdującym się w wydzielonej sieci administrowanej przez MSW i jest „aplikacją wspierającą" System Rejestrów Państwowych „Źródło". Wszelkie zmiany danych osób z terenu Gminy Zadzim w SRP „Źródło" przesyłane są do aplikacji wspierającej – SELWIN przy pomocy modułu subskrypcji, który aktualizuje bazę danych programu SELWIN w oparciu o dane z SRP Źródło. Transmisja odbywa się poprzez wydzieloną sieć i jest zabezpieczona certyfikatem wystawionym przez MSW.

W przypadku programu SIO, wytworzone za pomocą tego programu dokumenty przesyłane są drogą elektroniczną (poprzez siec Internet) do serwera centralnego nadzorowanego przez MEN.

W przypadku programu GOMIG – Odpady istnieje integracja z modułem KSZOB (Księgowość Zobowiązań) programu U.I. INFO-SYSTEM, dzięki której dane kont wymiarowych wraz z wyliczonymi stawkami opłat automatycznie zapisują się w bazie danych programu księgowego.

5. Udostępnianie danych

Najważniejsze przesłanki i zasady udostępniania danych:

a) nie jest istotne czy udostępnianie danych ma charakter odpłatny czy nie, aby czynność była uznana za udostępnianie;

b) nie ma znaczenia (ujmując problem technicznie) czy udostępnianie następuje w formie przekazu ustnego, pisemnego, za pomocą powszechnych środków przekazu lub poprzez sieć komputerową itd.;

c) udostępnianie danych osobowych osobom lub podmiotom uprawnionym do ich otrzymania odbywa się na mocy przepisów prawa;

d) dane osobowe z wyłączeniem danych wrażliwych mogą być udostępniane w oparciu o przepisy prawa, jeżeli osoba wnioskująca w sposób wiarygodny uzasadni potrzebę posiadania tych danych, a ich udostępnienie nie naruszy praw i wolności osób których dane dotyczą,

e) dane osobowe udostępnia się na pisemny, umotywowany wniosek, chyba że przepis innej ustawy stanowi inaczej. Wniosek powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazać ich zakres i przeznaczenie.

f) udostępnione dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

6. Powierzenie przetwarzania danych osobowych

W przypadku konieczności przetwarzania danych osobowych przez odrębne podmioty świadczące usługi dla Administratora danych osobowych może on powierzyć ich przetwarzanie, w drodze umowy zawartej na piśmie, pod następującymi warunkami:

a) pisemna umowa powinna być zawarta niezależnie od posiadanej umowy określającej relacje obu stron;

b) podmiot, któremu powierzono przetwarzanie danych, może przetwarzać je wyłącznie w zakresie i celu przewidzianych w umowie;

c) podmiot, któremu powierzono przetwarzanie danych, jest obowiązany przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające zbiór danych, o których mowa w art. 36-39 ustawy.

d) W zakresie przestrzegania tych przepisów podmiot ponosi odpowiedzialność jak administrator danych.

e) Odpowiedzialność za przestrzeganie przepisów niniejszej ustawy spoczywa na Administratorze danych osobowych, co nie wyłącza odpowiedzialności podmiotu, który zawarł umowę, za przetwarzanie danych niezgodne z tą umową.

7. Definicja środków zabezpieczających

W Urzędzie Gminy Zadzim należy stosować następujące kategorie środków zabezpieczeń danych osobowych:

a) zabezpieczenia fizyczne:

- całodobowy monitoring budynku Urzędu Gminy
- pomieszczenia zamykane na klucz;
- szafy z zamkami.

b) zabezpieczenia procesów przetwarzania danych w dokumentacji papierowej:

- przetwarzanie danych osobowych następuje w wyznaczonych pomieszczeniach,
- przetwarzanie danych osobowych następuje przez wyznaczone do tego celu osoby.
- dokumenty zawierające dane osobowe zbędne do prowadzenia dalszych działań i które nie podlegają, archiwizacji są niezwłocznie niszczone w sposób uniemożliwiający ich odczytanie.

d) zabezpieczenia informatyczne.

- hasła dostępu do systemu operacyjnego
- hasła dostępu do aplikacji służących do przetwarzania danych osobowych

c) zabezpieczenia organizacyjne:

– osobami bezpośrednio odpowiedzialnymi za bezpieczeństwo danych są: użytkownicy, lokalni administratorzy danych, Administrator Sieci Informatycznych (ASI), Administrator Bezpieczeństwa Informacji (ABI);

– Administrator Bezpieczeństwa Informacji, Administrator sieci informatycznych, lokalni administratorzy danych osobowych na bieżąco kontrolują z należytą starannością, zgodnie z aktualnie obowiązującą w tym zakresie wiedzą i z obowiązującymi procedurami, pracę pracowników odpowiedzialnych za przetwarzanie danych osobowych oraz systemu informatycznego.

8. Kontrola dostępu do danych osobowych

W celu kontroli dostępu użytkowników do danych osobowych na poziomie bazy danych użytkownikom końcowym nadaje się indywidualne identyfikatory i hasła dostępu. Zakres przydzielonych uprawnień dostępu do danych wynika z realizowanych zadań służbowych

8.1 Kontrola dostępu do systemu komputerowego

W celu kontroli dostępu użytkowników do danych osobowych zakłada się, że na komputerach zainstalowany jest system operacyjny umożliwiający separację poszczególnych jego użytkowników, aby posiadali oni dostęp do danych osobowych wg zasady wiedzy uzasadnionej. Hasła dostępu są znane tylko ich właścicielom. Parametry użytkownika automatycznie wymuszają zmianę haseł po upływie terminu ważności hasła jeśli jest to możliwe.
Zakres przydzielonych uprawnień dostępu do danych wynika z realizowanych zadań służbowych. Systemy operacyjne muszą być tak skonfigurowane aby rejestrować wszystkie logowania i próby logowania do systemu.

8.2 Zasady korzystania z haseł przez użytkowników systemów

Hasło użytkownika jest podstawowym elementem ochrony danych osobowych przetwarzanych w systemach baz danych osobowych.
Hasła administratorów systemu nie muszą być oznaczane klauzulą tajności. Muszą być jednak chronione w zamkniętych i opieczętowanych kopertach. Szczegółowe zasady tworzenia haseł opisane są w instrukcji zarządzania systemem informatycznym.
Wszyscy użytkownicy przestrzegają następujących zasad ochrony haseł:

1. Użytkownik hasła odpowiada za nieuprawnione ujawnienie swojego hasła.
2. Użytkownik przechowuje swoje hasło w sposób uniemożliwiający zapoznanie się z nim przez inne osoby.
3. W sytuacji gdy zachodzi podejrzenie ujawnienia hasła, użytkownik jest zobowiązany do natychmiastowej jego zmiany lub w przypadku niemożliwości zmiany, do zwrócenia się do administratora o zmianę hasła.
4. Hasła zawierają minimum 6 znaków dla użytkowników systemu oraz 8 znaków dla administratora.
5. BIOS jest zabezpieczony hasłem.

Wyżej wymienione zasady ochrony haseł dostępu opisane są w instrukcji. Fakt zapoznania się z tymi zasadami poświadczany jest własnoręcznym podpisem użytkownika systemu.

8.3 Usuwanie kont użytkowników systemów baz danych

Usuwanie kont użytkowników końcowych lub zmiana uprawnień realizowana jest niezwłocznie na polecenie administratora danych lub kierownika komórki. Czynności te wykonuje administrator systemu informatycznego.

9. Zabezpieczenie systemu informatycznego przed oprogramowaniem złośliwym lub penetrującym

Błędy w poprawnym działaniu urządzeń i oprogramowania, w których przetwarzane są dane osobowe powoduje oprogramowanie szkodliwe tj., wirusy, robaki, konie trojańskie i itp. W celu wyeliminowania negatywnych skutków ww. oprogramowania w zakresie poufności, dostępności, integralności i rozliczalności zaleca się instalowanie oprogramowania antywirusowego na wszystkich komputerach, na których przetwarzane są dane osobowe. Aktualizacja baz wirusów winna być wykonywana automatycznie lub nie rzadziej jak raz w miesiącu w przypadku stanowisk bez dostępu do sieci Internet . Ponadto oprogramowanie antywirusowe jest tak skonfigurowane aby każdy nośnik wkładany do komputera był sprawdzany na obecność złośliwego oprogramowania.

10. Zarządzanie incydentami bezpieczeństwa

Administrator systemu informatycznego na bieżąco monitoruje poprawność działania poszczególnych komponentów systemu przy pomocy narzędzi administratora systemu operacyjnego i bazy danych.

Użytkownik ma obowiązek zgłaszania wszystkich zauważonych nieprawidłowości, które mogą skutkować obniżeniem stopnia ochrony danych osobowych. Administrator systemu informatycznego wspólnie z administratorem bezpieczeństwa informacji wyjaśniają przyczyny i proponują rozwiązania eliminujące nieprawidłowości. Odpowiednio modyfikowane są procedury zawarte w instrukcji zarządzania systemem informatycznym oraz jeżeli to niezbędne niniejsza polityka bezpieczeństwa. Administrator danych powiadamiany jest każdorazowo w przypadku uzasadnionego podejrzenia naruszenia poufności, dostępności, integralności i rozliczalności danych osobowych przetwarzanych w systemie informatycznym. Szczegółowy procedury postępowania w przypadku wystąpienia incydentu bezpieczeństwa opisuje dokument pn „Procedura alarmowa – Ochrona danych osobowych w Urzędzie Gminy Zadzim”, który stanowi załącznik nr 4 do niniejszej polityki.

11. Procedury zarządzania systemem informatycznym

Szczegółowe zadania ochrony danych osobowych realizowane są podczas codziennej eksploatacji systemu informatycznego. Zawarte są one w procedurach zarządzania systemami informatycznymi, służącym do przetwarzania danych osobowych. Wszystkie procedury tworzą instrukcję zarządzania, o której mowa w pkt 1.5. Obejmuje ona:

- Procedury nadawania uprawnień do pracy w systemie informatycznym;
- Procedury określające zasady rejestracji użytkowników
- Procedury przydziału i zmiany haseł;
- Procedury użytkowania (rozpoczęcia, zawieszenia i zakończenia pracy w systemie):

  Specyfikacja czynności jakie musi użytkownik wykonać aby włączyć się do pracy w systemie, przerwać na chwilę pracę w systemie, zakończyć pracę w systemie oraz czynności, które winny być podjęte, w przypadku stwierdzenia ingerencji w dane osobowe lub inne zasoby systemu;
- Procedury tworzenia kopii zapasowych:

  Należy wskazać metody (przyrostowa lub całościowa) i częstotliwość tworzenie kopii zapasowych, określić co będzie kopiowane i na jaki nośnik; zasady rotacji nośników oraz czas użytkowania nośników, procedury likwidacji nośników. Należy określić sposób i czas przechowywania nośników. Należy wskazać pomieszczenia, w których nośniki elektroniczne są przechowywane.
- Procedura bezpiecznej transmisji;
- Procedura bezpieczeństwa urządzeń;
- Procedury kontroli dostępu do danych osobowych i bezpieczeństwa:

  Opis sposobów odnotowywania w systemie informatycznym informacji o udostępnieniach (osobom uzyskującym dostęp do systemu informatycznego).
- Procedura zarządzania konfiguracją;
- Procedury ochrony antywirusowej;
- Procedury utrzymania ciągłości działania;
- Procedura rozliczenia zadań.

12. Szkolenia

Dla zapewnienia odpowiedniego poziomu bezpieczeństwa systemu informatycznego wprowadzone są następujące obowiązkowe szkolenia:

- Wszyscy użytkownicy systemów informatycznych służących do przetwarzania danych osobowych obowiązkowo zapoznają się dokumentem niniejszej polityki bezpieczeństwa. Zrozumienie zawartych w niej zasad poświadczają swoim podpisem na karcie zapoznania z dokumentacją ochrony danych osobowych, która stanowi załącznik nr 5 do niniejszej polityki.
- Administratorzy systemów informatycznych, w których przetwarzane są dane osobowe, szkolą użytkowników w zakresie poprawnej pracy, w tym procedur systemu informatycznego, przed rozpoczęciem przez nich pracy z danymi osobowymi. Użytkownicy podpisują oświadczenie o zapoznaniu się i zrozumieniu procedur zawartych w instrukcji zarządzania systemem.
- Osoby odpowiedzialne za realizację zadań ochrony danych osobowych w Urzędzie zapewniają ogólne szkolenie w zakresie przepisów ustawy i aktów wykonawczych, dotyczących ochrony danych osobowych.

Załącznik nr 1
do Polityki Bezpieczeństwa Zbiorów Danych Osobowych
Prowadzonych w Urzędzie Gminy Zadzim

URZĄD GMINY ZADZIM

ZATWIERDZAM:

INSTRUKCJA ZARZĄDZANIA SYSTEMAMI PRZETWARZAJĄCYMI DANE OSOBOWE

W URZĘDZIE GMINY ZADZIM

Marzec 2016

Spis treści

1. Wprowadzenie

Wszystkie rozdziały niniejszego dokumentu tworzą instrukcję określającą sposób zarządzania systemami informatycznymi, służącymi do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji.

Wszystkie systemy przetwarzania danych osobowych oraz ich charakterystyka i metody zabezpieczeń wymienione zostały w załączniku nr 2 do Polityki Bezpieczeństwa Zbiorów Danych Osobowych w Urzędzie Gminy Zadzim – **Wykaz pomieszczeń i systemów zabezpieczeń.**

W przypadku modułów programu U.I. Info-System oraz programu Gomig-Odpady bazy danych znajdują się na serwerze, który umieszczony jest w pomieszczeniu serwerowym w pokoju nr …..... Dostęp do serwera możliwy jest wyłącznie poprzez sieć lokalną z ograniczonego zakresu adresów IP oraz zabezpieczony hasłem. Dla pozostałych systemów przetwarzania danych osobowych bazy danych znajdują się na lokalnych komputerach użytkowników.

Niniejsza instrukcja jest zbiorem obowiązujących procedur i stanowi uzupełnienie dokumentu „POLITYKA BEZPIECZEŃSTWA ZBIORÓW DANYCH OSOBOWYCH PROWADZONYCH W URZĘDZIE GMINY ZADZIM".

Żadne odstępstwa lub poprawki do niniejszego dokumentu, powodujące obniżenie zaprojektowanego w nim poziomu bezpieczeństwa nie są dozwolone, dopóki nie zostaną zatwierdzone przez administratora bezpieczeństwa informacji.

2. Opis systemu

	Instrukcja Zarządzania Systemem Przetwarzającym Dane Osobowe	Data wprowadzenia: - - 2016 r.
OPIS SYSTEMU		Ilość stron: 1

Na stanowiskach komputerowych zainstalowane są wyłącznie systemy operacyjne, które zapewniają możliwość nadawania indywidualnych uprawnień użytkownikom do określonych zasobów komputera oraz rejestrują fakt pracy (zalogowania) w systemie każdego użytkownika.
BIOS komputera musi być zabezpieczony hasłem.
Jeżeli istnieje możliwość zabezpieczenia aplikacji przetwarzającej dane osobowe hasłem, należy je założyć. Hasło takie powinno być zmieniane co 30 dni. Zbiory osobowe przetwarzane są w środowisku systemu operacyjnego Windows XP SP3 oraz Windows 7

Parametry konfiguracyjne:
- zasady blokady kont: błędnie wprowadzone hasło nie pozwala uruchomić komputera
  błędnie wprowadzone hasło nie pozwala uruchomić programu
- zasady prowadzenia inspekcji: rejestrowane logi użytkowników
- opcje zabezpieczeń: hasło dostępowe wymuszone co 30 dni

Przetwarzanie danych osobowych na komputerach przenośnych (typu notebook) jest możliwe pod warunkiem zachowania szczególnej ostrożności podczas jego transportu, użytkowania i przechowywania. Komputer przenośny powinien pozostawać pod stałym nadzorem osoby, która nim dysponuje. Wynoszenie komputera przenośnego poza pomieszczenia Urzędu dozwolone jest za zgodą administratora danych.

3. Nadawanie uprawnień

	Instrukcja Zarządzania Systemem Przetwarzającym Dane Osobowe	Data wprowadzenia: - - 2016 r.
PROCEDURA NADAWANIA UPRAWNIEŃ DO PRACY W SYSTEMIE INFORMATYCZNYM		**Ilość stron: 1**

1) W przypadku przyjęcia do pracy nowego pracownika, którego zakres obowiązków obejmować będzie przetwarzanie danych osobowych, Administrator danych wydaje upoważnienie do przetwarzania danych osobowych, którego treść stanowi załącznik nr 1 do niniejszej instrukcji;

2) Pracownik, któremu administrator danych udzieli upoważnienia, jest zobowiązany do podpisania oświadczenia, którego treść stanowi załącznik nr 2 do niniejszej instrukcji;

3) Nadanie/zmiana/odebranie uprawnień w systemie informatycznym następuje na wniosek bezpośredniego przełożonego, który wypełnia formularz, w oparciu o wzór stanowiący załącznik nr 3 a następnie przekazuje go administratorowi bezpieczeństwa informacji do akceptacji i administratorowi systemu informatycznego do realizacji;

4) Przepisy pkt 1, 2, 3, 5, 6 stosuje się odpowiednio do stażystów oraz praktykantów odbywających staż lub praktyki w Urzędzie;

5) W przypadku zmiany stanowiska przez pracownika, bądź zakresu obowiązków pracowniczych, bezpośredni przełożony i osoba zatrudniona na samodzielnym stanowisku pracy zobowiązani są bezzwłocznie powiadomić Administratora Danych o zaistniałej sytuacji;

6) Rozwiązanie stosunku pracy równoznaczne jest z unieważnieniem upoważnienia wymienionego w pkt. 1;

7) Ewidencję pracowników upoważnionych do przetwarzania danych prowadzi Administrator Bezpieczeństwa Informacji;

8) Wzór ewidencji pracowników upoważnionych do przetwarzania danych oraz ich uprawnień w systemie informatycznym określa załącznik nr 4 do niniejszej instrukcji.

4. Zasady rejestracji użytkowników

	Instrukcja Zarządzania Systemem Przetwarzającym Dane Osobowe	Data wprowadzenia: - - 2016 r.
PROCEDURA OKREŚLAJĄCA ZASADY REJESTRACJI UŻYTKOWNIKÓW		Ilość stron: 1

Hasło użytkownika jest podstawowym elementem ochrony komputerowych zasobów użytkownika uprawnionego do przetwarzania danych osobowych w systemie informatycznym. Hasło dostępu do konta użytkownika musi być przez użytkownika zapamiętane. Hasła administratorów systemu nie muszą być oznaczone klauzulą tajności. Muszą być jednak chronione. Powinny być przechowywane w zamkniętej i zaplombowanej kopercie u ASI.

Wszyscy użytkownicy przestrzegają następujących zasad ochrony haseł:

- Użytkownik hasła odpowiada za nieuprawnione ujawnienie swojego hasła;
- Użytkownik przechowuje swoje hasło w sposób uniemożliwiający zapoznanie się z nim przez inne osoby;
- W sytuacji gdy zachodzi podejrzenie ujawnienia hasła, użytkownik jest zobowiązany do natychmiastowej jego zmiany lub w przypadku niemożności zmiany, do zwrócenia się do administratora z zmianę hasła;
- Hasła zawierają minimum 6 znaków dla użytkowników systemu oraz 8 znaków dla administratora;
- BIOS jest zabezpieczony hasłem.

Za prawidłowe użytkowanie stanowiska komputerowego systemu odpowiada użytkownik stanowiska, administrator bezpieczeństwa informacji oraz kierownik komórki organizacyjnej.

5. Zasady przydziału i zmiany haseł

	Instrukcja Zarządzania Systemem Przetwarzającym Dane Osobowe	Data wprowadzenia: - - 2016 r.
PROCEDURA OKREŚLAJĄCA ZASADY PRZYDZIAŁU I ZMIANY HASEŁ		Ilość stron: 1

Hasła zabezpieczające przed nieautoryzowanym uruchomieniem komputera są przekazywane i ustalane w formie ustnej.

Częstotliwość zmiany haseł:

1) do programów przetwarzających dane osobowe - co 30 dni automatycznie, chyba, że funkcja taka nie jest zaimplementowana w programie, wtedy zmiana następuje ręcznie, lub w przypadku naruszenia bezpieczeństwa, chyba, że odrębne przepisy wymagają ważności hasła przez określony czas;

2) do systemu operacyjnego - co 30 dni automatycznie, chyba że funkcja taka nie jest zaimplementowana w systemie, wtedy zmiana następuje ręcznie, lub w przypadku naruszenia bezpieczeństwa, chyba że odrębne przepisy wymagają ważności hasła przez określony czas;

Przyjmuje się następujące zasady haseł:

- hasła muszą spełniać wymagania co do złożoności
- maksymalny okres ważności hasła - 30 dni
- minimalna długość hasła użytkownika - 6 znaków
- minimalna długość hasła administratora - 8 znaków
- minimalny okres ważności hasła - 15 dni
- ilość obowiązkowych wytworzonych historii haseł - 5 szt.

6. Procedura użytkowania systemu

	Instrukcja Zarządzania Systemem Przetwarzającym Dane Osobowe	Data wprowadzenia: - - 2016 r.
PROCEDURA ROZPOCZYNANIA, ZAWIESZANIA I KOŃCZENIA PRACY W SYSTEMIE		**Ilość stron: 1**

Użytkownik chcąc uruchomić komputer zobowiązany jest podłączyć go do sieci zasilającej i wcisnąć przycisk „POWER" na obudowie komputera. Następnie po uruchomieniu komputera zobowiązany jest podać swoje unikatowe hasło, które wymusza system przy uruchomieniu komputera. Po wprowadzeniu znanego tylko przez niego hasła następuje uruchomienie na jednostce komputerowej systemu operacyjnego. W przypadku tymczasowego zaprzestania pracy na skutek chwilowego opuszczenia stanowiska pracy użytkownik zobowiązany jest do wylogowania się z programu. Dodatkowym zabezpieczeniem jest ustawienie w konfiguracji komputera wygaszacza ekranu, który aktywuje się po okresie 5 minut i dezaktywuje w momencie ponownego powrotu użytkownika do pracy i podaniu hasła zabezpieczającego. Po zakończeniu pracy w programie użytkownik zobowiązany jest do wylogowania się z programu.

W przypadku stwierdzenia podejrzenia naruszenia bezpieczeństwa systemu (tj. stwierdzenia fizycznej ingerencji w przetwarzane dane lub użytkowane narzędzia programowe lub sprzętowe) użytkownik zgłasza ten fakt Administratorowi Systemów Informatycznych UG Zadzim, ten zaś w uzasadnionym przypadku powiadamia Administratora Bezpieczeństwa Informacji a następnie Administratora Danych.

7. Procedura tworzenia kopii zapasowych

	Instrukcja Zarządzania Systemem Przetwarzającym Dane Osobowe	Data wprowadzenia: - - 2016 r.
PROCEDURA TWORZENIA KOPII ZAPASOWEJ		**Ilość stron: 1**

Kopie bezpieczeństwa systemów wykonywane są w cyklu dwutygodniowym i miesięcznym:

1) W cyklu dwutygodniowym wykonuje się kopie:

— programów finansowo-księgowych

— system ewidencji ludności;

— programów podatkowych.

2) W cyklu miesięcznym wykonuje się kopie:

— programów płacowo-kadrowych, ZUS

— innych zbiorów danych osobowych

Kopie wykonuje się na trwałych nośnikach takich jak taśmy, płyty CD, płyty DVD i ewidencjonuje wg wzoru który określa załącznik nr 5 do niniejszej instrukcji.

Kopie bezpieczeństwa są sprawdzane automatycznie pod względem poprawności zapisu danych.

Kopie bezpieczeństwa należy okresowo sprawdzać pod kątem ich przydatności do odtworzenia danych w przypadku awarii systemu.

Wykonanie kopii nie jest obowiązkowe, jeżeli w danym okresie nie wykonano zapisu zmieniającego bazę danych.

Nośniki uszkodzone i nieprzydatne niszczy się komisyjnie i sporządza protokół zniszczenia wg wzoru który określa załącznik nr 6 do niniejszej instrukcji.

8. Procedura bezpiecznej transmisji

	Instrukcja Zarządzania Systemem Przetwarzającym Dane Osobowe	Data wprowadzenia: - - 2016 r.
PROCEDURA BEZPIECZNEJ TRANSMISJI		**Ilość stron: 1**

Jeżeli stanowiska komputerowe przetwarzające dane osobowe pracują w sieci lokalnej, wszystkie kable logiczne tworzące tą sieć powinny przebiegać w obrębie strefy kontrolowanej przez Urząd.

W przypadku programu Płatnik transmisja danych z ZUS odbywa się szyfrowanym kanałem komunikacji poprzez sieć Internet, a za bezpieczeństwo transmisji odpowiedzialna jest aplikacja Płatnik.

W przypadku programu SELWIN aplikacja zainstalowana jest na stanowisku znajdującym się w wydzielonej sieci administrowanej przez MSW i jest „aplikacją wspierającą" System Rejestrów Państwowych „Źródło". Wszelkie zmiany danych osób z terenu Gminy Zadzim w SRP „Źródło" przesyłane są do aplikacji wspierającej – SELWIN przy pomocy modułu subskrypcji, który aktualizuje bazę danych programu SELWIN w oparciu o dane z SRP Źródło. Transmisja odbywa się poprzez wydzieloną sieć i jest zabezpieczona certyfikatem wystawionym przez MSW.

Dla systemu Gomig-Odpady dopuszcza się eksport danych do pliku office (xls, csv, ods), a następnie zabezpieczenie tego pliku min. 8 znakowym hasłem. W tej formie plik z danymi może zostać przekazany drogą elektroniczną podmiotowi realizującemu obowiązek odbioru odpadów z Gminy Zadzim.

W wyjątkowych przypadkach (np. awaria) dopuszcza się wysyłkę baz danych do producenta oprogramowania celem usunięcia usterek i nieprawidłowości. W takiej sytuacji Administrator Systemu Informatycznego przed wysłaniem bazy danych obligatoryjnie sporządza i archiwizuje jej kopię zapasową, a następnie kompresuje ją do formatu ZIP lub RAR z opcją zabezpieczenia min. 8 znakowym hasłem.

Wszystkie przypadki udostępniania danych osobowych ewidencjonuje się wg wzoru który określa załącznik nr 7 do niniejszej instrukcji.

9. Procedura bezpieczeństwa urządzeń

	Instrukcja Zarządzania Systemem Przetwarzającym Dane Osobowe	Data wprowadzenia: - - 2016 r.
PROCEDURA BEZPIECZEŃSTWA URZĄDZEŃ		**Ilość stron: 1**

Wszelkie czynności związane z konserwacją, naprawą i wymianą sprzętu lub oprogramowania wchodzącego w skład stanowiska komputerowego organizuje i nadzoruje wyznaczony imiennie administrator systemu.
Bezpośrednie czynności konserwujące i naprawcze mogą być wykonywane wyłącznie przez administratora systemu a w przypadku konieczności skorzystania z serwisu zewnętrznego czynności te mogą być wykonywane wyłącznie przez podmioty autoryzowane przez producenta sprzętu/oprogramowania informatycznego pod osobistym nadzorem administratora.

W przypadku konieczności oddania sprzętu do naprawy zewnętrznej, obowiązkiem administratora jest dopilnować aby zostały wymontowane z komputera wszystkie dyski twarde HDD (oraz inne nieulotne nośniki zamontowane na stałe, w pamięci których mogą być przechowywane dane osobowe), które administrator zabezpiecza przed nieuprawnionym dostępem.

10. Procedura kontroli dostępu i bezpieczeństwa

	Instrukcja Zarządzania Systemem Przetwarzającym Dane Osobowe	**Data wprowadzenia: - - 2016 r.**
PROCEDURA KONTROLI DOSTĘPU I BEZPIECZEŃSTWA		**Ilość stron: 1**

Uprawnienia użytkowników identyfikują mechanizmy zainstalowanego systemu operacyjnego pod kontrolą, którego przetwarzane są dane osobowe.

Jeżeli zachodzi taka konieczność należy stosować dodatkowe urządzenia uwierzytelniające użytkownika w postaci innych dostępnych na rynku identyfikatorów.

11. Procedura ochrony antywirusowej

	Instrukcja Zarządzania Systemem Przetwarzającym Dane Osobowe	Data wprowadzenia: - - 2016 r.
PROCEDURA OCHRONY ANTYWIRUSOWEJ		Ilość stron: 1

Na każdym komputerze przetwarzającym dane osobowe musi być zainstalowane oprogramowanie antywirusowe zabezpieczające zasoby komputera przed oprogramowaniem złośliwym.

kontrola oprogramowania (pliki systemowe, pliki z danymi)

Nawet w przypadku braku zgłoszeń od użytkowników, administrator raz w roku sprawdza wszystkie zasoby komputerowe na obecność wirusa.

kontrola nośników zewnętrznych

Administrator systemu tak konfiguruje oprogramowanie antywirusowe, żeby każdy nośnik komputerowy wkładany do napędu był natychmiast sprawdzany na zawartość złośliwego oprogramowania.

postępowanie w przypadku wykrycia wirusa lub innego szkodliwego oprogramowania

W przypadku wykrycia przez oprogramowanie „wirusa komputerowego" należy zaprzestać eksploatacji systemu i natychmiast powiadomić administratora systemu, który podejmuje odpowiednie działania diagnostyczne i naprawcze.

12. Procedura zarządzania konfiguracją

	Instrukcja Zarządzania Systemem Przetwarzającym Dane Osobowe	Data wprowadzenia: - - 2016r.
PROCEDURA ZARZĄDZANIA KONFIGURACJĄ		**Ilość stron: 1**

Wszelkie prace związane z konfiguracją systemu, wprowadzaniem zmian, wykonywaniem przeglądów stanowisk i oprogramowania wykonywane są przez wyznaczonego Administratora Systemów Informatycznych (ASI), uprawnionych pracowników Ministerstwa właściwego ds. przetwarzania danych w danym zbiorze lub uprawnionych pracowników firm dostarczających oprogramowanie do przetwarzania danych.

W przypadku wątpliwości ASI uzgadnia decyzję z Administratorem Danych Osobowych.

13. Procedura utrzymania ciągłości działania

	Instrukcja Zarządzania Systemem Przetwarzającym Dane Osobowe	Data wprowadzenia: - - 2016 r.
PROCEDURA UTRZYMANIA CIĄGŁOŚCI DZIAŁANIA		Ilość stron: 1

Żeby zapewnić ciągłość działania systemu przetwarzającego dane osobowe zaleca się zasilać stanowiska systemu z gwarantowanej sieci energetycznej, a tam gdzie brak takiej sieci wyposażyć stanowisko w zasilacz awaryjny UPS umożliwiający podtrzymanie zasilania energetycznego na czas niezbędny do zamknięcia systemu i wyłączenia stanowiska.

Administrator na bieżąco monitoruje poprawność działania poszczególnych komputerów lub sieci przetwarzającej dane osobowe przy pomocy narzędzi administratora systemu operacyjnego.
Użytkownik systemu zgłasza awarie lub inne zauważone problemy administratorowi systemu.

Po wstępnym zdiagnozowaniu systemu, administrator podejmuje odpowiednie działania celem wyeliminowania nieprawidłowości lub gdy stwierdzi brak możliwości naprawy powiadamia bezpośredniego przełożonego.

14. Procedura rozliczenia zadań

	Instrukcja Zarządzania Systemem Przetwarzającym Dane Osobowe	Data wprowadzenia: - - 2016 r.
PROCEDURA ROZLICZENIA ZADAŃ		Ilość stron: 1

Zaleca się, żeby administrator systemu, raz w miesiącu dokonywał przeglądu stanowiska komputerowego podczas którego, sprawdza ustawienia konfiguracyjne systemu oraz logi systemowe.

Jeżeli administrator przeglądając logi systemowe zauważy nieprawidłowości w zakresie naruszenia bezpieczeństwa systemu , archiwizuje log za dany okres do czasu pełnego wyjaśnienia incydentu.

W nazwie archiwizowanego logu powinna zawierać się data archiwizacji lub okresu, który log obejmuje.

W przypadku nie stwierdzenia w kontrolowanym okresie wystąpienia jakichkolwiek nieprawidłowości administrator czyści logi bez ich archiwizacji.

Opracowano na podstawie:

„Wskazówek dotyczących sposobu opracowania instrukcji określającej sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji" opublikowanych przez GIODO.

Załącznik nr 1
do Instrukcji Zarządzania Systemami
Przetwarzającymi Dane Osobowe

Zadzim, dn. ….....

Znak: ….....

Pan/Pani

….....

….....
(stanowisko)

UPOWAŻNIENIE
do przetwarzania danych osobowych

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tj. Dz.U. z 2015 r. poz. 2135 ze zm.), w związku z wykonywaniem zadań na stanowisku …..... upoważniam Pana/Panią do przetwarzania danych osobowych zawartych w zbiorze / zbiorach:

….....

….....

Niniejsze upoważnienie obejmuje przetwarzanie danych osobowych w formie tradycyjnej (papierowej) oraz w systemach informatycznych. Upoważnienie wygasa automatycznie w przypadku zmiany stanowiska pracy lub ustania zatrudnienia.

Zgodnie z art. 39 ust. 2 ustawy, upoważniona do przetwarzania danych osoba zobowiązana jest do zachowania w tajemnicy dane osobowe zawarte w wyżej wymienionych zbiorach oraz informacje o ich zabezpieczeniu również po ustaniu zatrudnienia.

Wykonano w 3 Egz.

1. Osoba upoważniona
2. ABI (a/a)
3. Pracownik ds. kadr

Załącznik nr 2
do Instrukcji Zarządzania Systemami
Przetwarzającymi Dane Osobowe

Zadzim, dn ….....

….....
(imię i nazwisko)

OŚWIADCZENIE

Oświadczam, iż zostałem(am) zapoznany(a) z przepisami dotyczącymi ochrony danych osobowych, w szczególności z ustawą z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tj. Dz.U. z 2015 r. poz. 2135 ze zm.), wydanych na jej podstawie aktów wykonawczych oraz wprowadzonych i wdrożonych do stosowania przez Administratora Danych Osobowych „Polityki bezpieczeństwa danych osobowych" oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych".

Zobowiązuję się do:
- nieujawniania danych osobowych nieuprawnionym osobom lub instytucjom w jakiejkolwiek formie bez zgody Pracodawcy;
- przestrzegania zapisów zawartych w wyżej wymienionych dokumentach;
- korzystania z oprogramowania wyłącznie w związku z wykonywaniem obowiązków pracowniczych;
- wykorzystywania jedynie legalnego oprogramowania pochodzącego od Pracodawcy;
nie podejmowania prób samodzielnego instalowania oprogramowania pochodzącego z innych źródeł;
- wnoszenia, wynoszenia i użytkowania przenośnych nośników danych wyłącznie za wiedzą i zgodą Pracodawcy;
- należytej dbałości o powierzone sprzęt i oprogramowanie;
- korzystanie z produktów w wersjach ewaluacyjnych, testowych lub w jakikolwiek inny sposób ograniczony umowami licencyjnymi może być użytkowane zgodnie z ich przeznaczeniem, wyłącznie za zgodą pracodawcy.

Naruszenie przez Pracownika jego podstawowych obowiązków pracowniczych w zakresie wskazanym powyżej, będzie stanowić podstawę do podjęcia przez Pracodawcę przysługujących mu środków prawnych, a w szczególności, może stanowić przyczynę uzasadniającą wypowiedzenie przez Pracodawcę umowy o pracę lub rozwiązanie przez Pracodawcę tejże umowy, bez wypowiedzenia z winy pracownika, zgodnie z przepisami ustawy z dnia 26 czerwca 1974 r. Kodeks Pracy (tj. Dz.U. z 2014 r. poz. 1502 ze zm.).

….....
(podpis pracownika)

Otrzymują:
1. Pracownik
2. ABI
3. Podinspektor ds. oświaty i kadr (do akt osobowych)

Załącznik nr 3
do Instrukcji Zarządzania Systemami
Przetwarzającymi Dane Osobowe

ZLECENIE

nadania / zmiany / anulowania zakresu uprawnień użytkownika w systemie informatycznym

☐ Nowy użytkownik	☐ Modyfikacja uprawnień	☐ Odebranie uprawnień

Imię i nazwisko użytkownika	
Miejsce przetwarzania/pokój:	**Stanowisko:**

Opis zakresu uprawnień użytkownika w systemie informatycznym
P – przeglądanie i drukowanie danych
Z – zmiana danych
D – dopisywanie danych
U – usuwanie danych
A – administracja użytkownikami systemu

Uprawnienia / Programy	**P**	**Z**	**D**	**U**	**A**
Gomig-Odpady					
Woda					
Płatnik					
USC					
SelWin					
Moduły Programu Info-System					
Podatki					
KSZOB					
Auta					
Kadry i płace					
Kasa					
Budżet					
Przelewy					
Egzekucje					

….....
(data i podpis bezpośredniego przełożonego)

….....
(data i podpis ABI)

….....
(data i podpis ASI)

Załącznik nr 4
do Instrukcji Zarządzania Systemami
Przetwarzającymi Dane Osobowe

REJESTR UŻYTKOWNIKÓW I ICH UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM

Lp.	Nazwa zbioru danych	Nazwisko i imię użytkownika	Nazwa aplikacji	Identyfikator	Rodzaj uprawnień *	Data rejestracji	Data Wyrejestrowania	Uwagi

* - Skróty stosowane do określenia uprawnień
P – Przeglądanie danych na ekranie i drukowanie danych
Z – Zmiana danych
D – Dopisywanie danych
U – Usuwanie danych
A – Administracja użytkownikami systemu

Dane aktualne na dzień: .....

Data i podpis ABI:.....

Załącznik nr 5
do Instrukcji Zarządzania Systemami
Przetwarzającymi Dane Osobowe

REJESTR NOŚNIKÓW KOMPUTEROWYCH ZAWIERAJĄCYCH WAŻNE DANE

Oznaczenie nośnika	**Data wpisania w rejestr**	**Opis nośnika**	**Miejsce przechowywania nośnika**	**Podpis użytkownika**	**Uwagi**

Oznaczenie nośnika:
Symbol placówki / symbol nośnika / kolejny nr nośnika (np. UGZm-DVD-1; UGZm-CD-2)

Przykładowe symbole nośników
CD – Płyta CD
DVD – Płyta DVD
D – Dyskietka
P – Pendrive
HDD – Dysk twardy
DDS – Taśma DDS

Załącznik nr 6
do Instrukcji Zarządzania Systemami
Przetwarzającymi Dane Osobowe

ZATWIERDZAM

Protokół nr ….....
zniszczenia uszkodzonych nośników komputerowych
w Urzędzie Gminy Zadzim

Dnia …..... komisja powołana przez ….....
(data) (imię, nazwisko i stanowisko osoby powołującej komisję)

w składzie:

1. Przewodniczący: ….....

2. Członkowie: ….....

….....

dokonała trwałego zniszczenia nośników komputerowych:

Lp	Nazwa	Nr ewidencyjny	Sposób zniszczenia	Uwagi

Dokonanie ww czynności zostaje potwierdzone własnoręcznymi podpisami komisji:

….....

….....

….....

Załącznik nr 7
do Instrukcji Zarządzania Systemami
Przetwarzającymi Dane Osobowe

EWIDENCJA UDOSTĘPNIANIA DANYCH OSOBOWYCH

Lp.	Data udostępnienia danych	Podmiot, któremu udostępniono dane (nazwa. adres)	Podstawa prawna udostępnienia danych	Zakres udostępnionych danych	Podpis pracownika

Załącznik nr 2
do Polityki Bezpieczeństwa Zbiorów Danych Osobowych
Prowadzonych w Urzędzie Gminy Zadzim

WYKAZ POMIESZCZEŃ I SYSTEMÓW ZABEZPIECZEŃ

Legenda:
1* - zwyczajowa lub własna, np. dane kadrowe, dane płacowe
2* - (SQL) – silnik bazy danych, (F) – Firebird, (MDB) – plik bazy danych MS Access, (O) – office, (P) – dokumenty papierowe
3* - (H) – hasło dostępowe, (SZ) – szyfrowanie transmisji, (WS) – wydzielona fizycznie sieć, (EKD) – elektroniczna karta dostępowa
4* - (S) – serwerownia, (L) – lokalizacja programu – pokój użytkownika
5* - (U) – pomieszczenie osób przetwarzających dane, (K) – Miejsce przechowywania kopii bezpieczeństwa
6* - (K) – kraty w oknach, (W) – wzmocnione drzwi, (ZP) – zamki patentowe, (SM) – szafa metalowa, (ZS) – zamykana szafa drewniana, (SA) system alarmowy

L.p	Nazwa zbioru danych 1*	Forma danych / Rodzaj bazy danych 2*	Zabezpieczenie informatyczne 3*	Bazę danych chroni UPS (TAK/NIE)	Program służący do przetwarzania baz danych	Czy dane osobowe przekazywane są poza Urząd (TAK/NIE)	Lokalizacja bazy danych 4*	Lokalizacja programu do przetwarzania danych lub zbioru danych w wersji papierowej	Funkcja lokalizacji 5*	Zabezpieczenia fizyczne 6*
1										
2										
...										

Dane aktualne na dzień: .....

Data i podpis ABI:.....

REJEST ZBIORÓW DANYCH OSOBOWYCH W URZĘDZIE GMINY ZADZIM

l.p.	nazwa zbioru	Historia zmian w rejestrze	Data wykonanej czynności (wpis, aktualizacja, wykreślenie, zbioru danych)	Oznaczenie administratora danych i adres jego siedziby lub miejsca zamieszkania oraz numer identyfikacyjny rejestru podmiotów gospodarki narodowej, jeżeli został mu nadany;	Oznaczenie przedstawiciela administratora danych, o którym mowa w art. 31a ustawy, i adres jego siedziby lub miejsca zamieszkania – w przypadku wyznaczenia takiego podmiotu;	Oznaczenie podmiotu, któremu powierzono przetwarzanie danych ze zbioru na podstawie art. 31 ustawy, i adres jego siedziby lub miejsca zamieszkania – w przypadku powierzenia przetwarzania danych temu podmiotowi;	Podstawa prawna upoważniająca do prowadzenia zbioru danych	Cel przetwarzania danych w zbiorze	Opis kategorii osób, których dane są przetwarzane w zbiorze;	Zakres danych przetwarzanych w zbiorze	Sposób zbierania danych do zbioru, w szczególności informacja, czy dane do zbioru są zbierane od osób, których dotyczą, czy z innych źródeł niż osoba, której dane dotyczą;	Sposób udostępniania danych ze zbioru, w szczególności informacja, czy dane ze zbioru są udostępniane innym podmiotom niż upoważnione na podstawie przepisów prawa;	Oznaczenie odbiorcy danych lub kategorii odbiorców, którym dane mogą być przekazywane	Informacja dotycząca ewentualnego przekazywania danych do państwa trzeciego
1.														
1.1		np.aktualizacja zbioru												

METRYKA ZMIAN W REJESTRZE ZBIORÓW			
l.p.	data wprowadzenia zmian w rejestrze zbiorów danych osobowych	Rodzaj wprowadzonych zmian (wpis zbioru danych osobowych do rejestru, aktualizacja zbioru danych osobowych, wykreślenie zbioru danych osobowych z rejestru)	imię i nazwisko osoby wprowadzającej zmiany w rejestrze
1.			
2.			
3.			

Załącznik nr 4
do Polityki Bezpieczeństwa Zbiorów Danych Osobowych
Prowadzonych w Urzędzie Gminy Zadzim

URZĄD GMINY ZADZIM

ZATWIERDZAM:

Procedura alarmowa
Ochrona danych osobowych w Urzędzie Gminy Zadzim

Marzec 2016

Spis treści:

1. Wstęp

Administrator Danych Osobowych w Urzędzie Gminy Zadzim w celu pełnej kontroli oraz zapobiegania możliwym zagrożeniom związanym z ochroną danych osobowych na podstawie art. 36 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz.U. z 2015 r. poz. 2135 ze zm.) wprowadza dokument o nazwie **„Procedura Alarmowa”**. Zapisy tego dokumentu obowiązują wszystkich pracowników Urzędu Gminy Zadzim, którzy przetwarzają dane osobowe w systemach informatycznych i w wersji papierowej.

Z niniejszym dokumentem powinni zapoznać się wszyscy pracownicy, a w szczególności:

1. kierownicy referatów i pracownicy z samodzielnych stanowisk pracy,
2. osoby upoważnione do przetwarzania danych osobowych w zbiorach i bazach danych,
3. obsługa informatyczna Urzędu Gminy.

Niniejsze procedury są rozszerzeniem dokumentu pn. **POLITYKA BEZPIECZEŃSTWA ZBIORÓW DANYCH OSOBOWYCH PROWADZONYCH W URZĘDZIE GMINY ZADZIM**

Za rozpowszechnienie dokumentu i umożliwienie zapoznania się z nim przez wszystkich pracowników odpowiedzialny jest Administrator Bezpieczeństwa Informacji.

Podstawa prawna:

1) Ustawa z dn. 29.08.1997 r. o ochronie danych osobowych (tj. Dz.U. z 2015 r. poz. 2135 ze zm.),

2)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 (Dz.U. 2008 Nr 229, poz. 1536),

3) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 22 kwietnia 2004 r. w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz.U. 2004 Nr 94, poz. 923),

4) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29.04.2004 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. 2004 Nr 100, poz. 1024).

2. Podstawowe definicje i pojęcia

ADO - Administrator Danych Osobowych – Wójt Gminy Zadzim

ABI - osoba wyznaczona przez Administratora Danych Osobowych do pełnienia funkcji Administratora Bezpieczeństwa Informacji.

ASI - osoba wyznaczona przez Administratora Danych Osobowych do pełnienia funkcji Administratora Systemu Informatycznego Urzędu Gminy Zadzim.

Użytkownik danych – każdy pracownik, który wykonując czynności służbowe, przetwarza dane osobowe, tzn. wykonuje na nich operacje takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, usuwanie;

Osoba upoważniona – osoba posiadająca upoważnienie wydane przez ADO lub osobę uprawnioną przez niego i dopuszczona jako użytkownik do przetwarzania danych osobowych w systemie informatycznym w zakresie wskazanym w upoważnieniu.

Osoba uprawniona – osoba posiadająca upoważnienie wydane przez ABI do wykonywania w jego imieniu określonych czynności.

Uchybienie - świadome lub nieświadome działania zmierzające do zagrożenia, wskutek których może dojść do utraty danych osobowych, kradzieży danych osobowych lub uszkodzenia nośników danych.

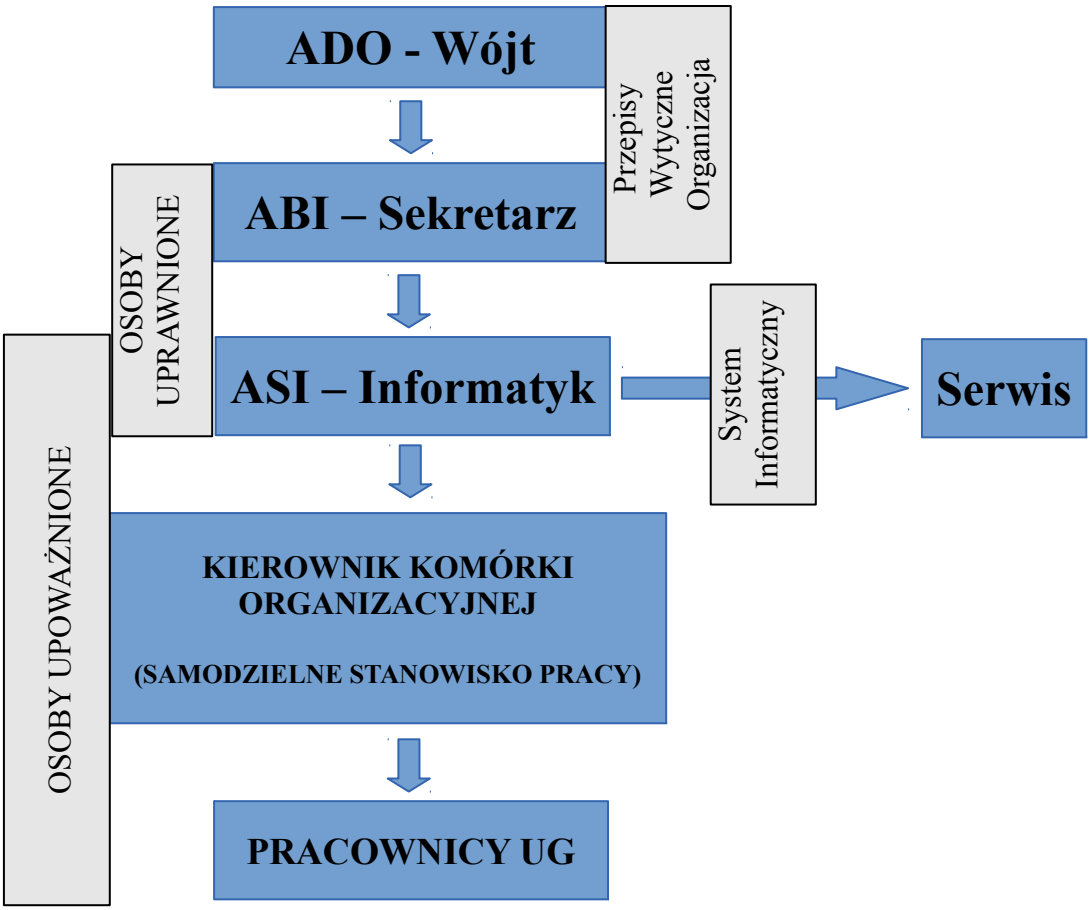
Zagrożenie - świadome lub nieświadome działania, wskutek których doszło do utraty danych osobowych, kradzieży danych osobowych lub uszkodzenia nośników danych.

Procedura alarmowa – sposób postępowania (rodzaj czynności) osób funkcyjnych i pracowników w sytuacji zagrożenia utraty danych osobowych przetwarzanych w Urzędzie Gminy Zadzim

3. Procedura alarmowa

Procedura alarmowa wskazuje na możliwe zagrożenia oraz definiuje „Dziennik Uchybień i Zagrożeń", związany z niewłaściwym przetwarzaniem danych osobowych lub ich wyciekiem.
Celem Procedury Alarmowej jest skatalogowanie możliwych uchybień i zagrożeń oraz opisanie procedur działania w przypadku ich wystąpienia, jak i również ograniczenie ich powstania w przyszłości.
Częścią Procedury Alarmowej jest „Dziennik Uchybień i Zagrożeń" - (załącznik nr 1), „Protokół Zagrożenia" - (załącznik nr 2), oraz „Protokół Uchybienia" - (załącznik nr 3), Dokumenty prowadzone są przez ABI w przypadku stwierdzenia naruszenia ochrony danych osobowych w Urzędzie Gminy Zadzim

Reagowanie w sytuacji powstania uchybień i zagrożenia wiąże się ze strukturą uprawnień oraz zakresem odpowiedzialności za prawidłowe przetwarzanie danych osobowych w Urzędzie Gminy Zadzim (rys. 1).



Rysunek 1
Struktura uprawnień oraz zakresu odpowiedzialności za prawidłowe przetwarzanie danych w Urzędzie Gminy Zadzim

4. Charakterystyka możliwych „Uchybień i Zagrożeń”

4.1. Uchybienia i zagrożenia nieświadome wewnętrzne i zewnętrzne

Do uchybień i zagrożeń nieświadomych wewnętrznych i zewnętrznych należą działania pracowników Urzędu Gminy lub osób nie będących pracownikami Urzędu Gminy, w następstwie których może dojść lub doszło do zniszczenia danych, wycieku danych lub naruszenia ich poufności.

W szczególności są to działania takie jak:
- niewłaściwe zabezpieczenie dostępu do pomieszczeń, w których przetwarzane są dane osobowe,
- niewłaściwe zabezpieczenie danych przetwarzanych na stanowisku pracy,
- niewłaściwe zabezpieczenie sprzętu komputerowego, włamanie do systemu,
- dopuszczenie do przetwarzania danych przez osoby nieposiadające upoważnienia,
- pomyłki informatyków, samowolna zmiana oprogramowania,
- wykorzystanie sprzętu do celów prywatnych z użyciem nie sprawdzonych nośników danych,
- brak reakcji na zagrożenia,
- kradzież danych,
- niewłaściwe przechowywanie, posługiwanie się oraz nieuprawnione udostępnianie haseł i kodów dostępu,
- pozostawienie bez opieki a w konsekwencji utrata lub kradzież sprzętu informatycznego,
- działanie wirusów i innego szkodliwego oprogramowania oraz inne działania, wskutek których dojdzie do utraty danych osobowych lub uszkodzenia nośników danych.

4.2. Uchybienia i zagrożenia umyślne wewnętrzne i zewnętrzne

Do uchybień i zagrożeń umyślnych wewnętrznych i zewnętrznych należą celowe działania pracowników Urzędu Gminy, w następstwie których może dojść lub doszło do zniszczenia danych, wycieku danych lub naruszenia ich poufności.
W szczególności są to działania takie jak:
- celowe zniszczenie sprzętu, danych osobowych lub nośników danych,
- kradzież lub utrata danych osobowych,
- dopuszczenie do przetwarzania danych przez osoby nieposiadające upoważnienia,
- nadmierne nadawanie uprawnień do dostępu do systemu i przetwarzanych danych osobowych,
- kradzież danych,
- zainfekowanie złośliwego oprogramowania,
- niewłaściwe niszczenie dokumentów,
- nie stosowanie obowiązujących procedur, brak szkolenia,
- kradzież sprzętu informatycznego,
- działanie wirusów i innego szkodliwego oprogramowania oraz inne działania, wskutek których dojdzie do utraty danych osobowych lub uszkodzenia nośników danych.

4.3. Uchybienia i zagrożenia losowe

Do uchybień i zagrożeń losowych należą sytuacje losowe, w następstwie których może dojść lub doszło do zniszczenia danych, wycieku danych lub naruszenia ich poufności.

W szczególności są to sytuacje takie jak:
- klęski żywiołowe,
- przerwy w dostawie prądu (zasilania),
- niesprawne źródła zasilania awaryjnego,
- awarie serwera i innych urządzeń wchodzących w skład systemu,
- pożar,
- zalanie wodą.

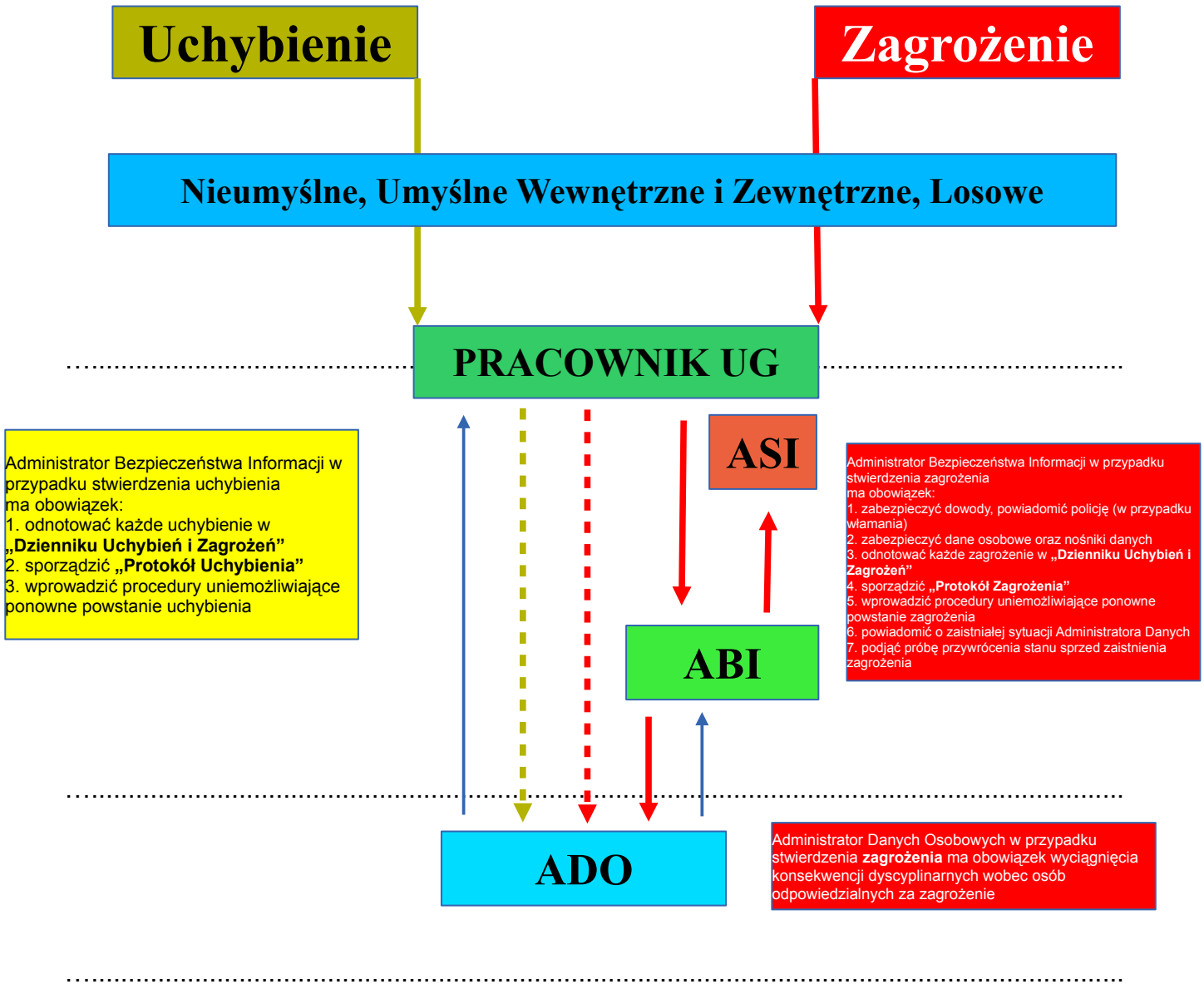
4.4. Procedura postępowania w przypadku stwierdzenia naruszenia ochrony danych osobowych.

Każdy pracownik Urzędu Gminy w Zadzimiu posiadający upoważnienie do przetwarzania danych osobowych, w przypadku stwierdzenia uchybienia lub zagrożenia ma obowiązek niezwłocznie powiadomić o tym fakcie Administratora Bezpieczeństwa Informacji lub Administratora Danych (rys 2).

Administrator Bezpieczeństwa Informacji w przypadku stwierdzenia **uchybienia** ma obowiązek:
- odnotować każde uchybienie w **„Dzienniku Uchybień i Zagrożeń”**,
- sporządzić **„Protokół Uchybienia”**,
- wprowadzić procedury uniemożliwiające ponowne powstanie uchybienia.

Administrator Bezpieczeństwa Informacji w przypadku stwierdzenia **zagrożenia** ma obowiązek:
- zabezpieczyć dowody, powiadomić policję (w przypadku włamania)
- zabezpieczyć dane osobowe oraz nośniki danych,
- odnotować każde zagrożenie w **„Dzienniku Uchybień i Zagrożeń”**
- sporządzić **„Protokół Zagrożenia”**
- wprowadzić procedury uniemożliwiające ponowne powstanie zagrożenia
- powiadomić o zaistniałej sytuacji Administratora Danych
- podjąć próbę przywrócenia stanu sprzed zaistnienia zagrożenia.

Administrator Danych Osobowych w przypadku stwierdzenia zagrożenia może wyciągnąć konsekwencje dyscyplinarne wobec osób odpowiedzialnych za zagrożenie.



Rysunek 2 Postępowanie w przypadku naruszenia ochrony danych osobowych.

4. Rejestr uchybień i zagrożeń oraz szczegółowa instrukcja postępowania dla osób posiadających upoważnienie do przetwarzania danych osobowych w Urzędzie Gminy

Kod uchybienia lub zagrożenia	Uchybienia i zagrożenia nieświadome, świadome wewnętrzne i zewnętrzne oraz zdarzenia losowe	Postępowanie w przypadku uchybienia lub zagrożenia
01	Pomieszczenie lub środki do przetwarzania danych osobowych pozostają bez nadzoru.	Należy zabezpieczyć dane osobowe oraz powiadomić ABI. ABI sporządza protokół uchybienia.
02	Pozostawienie niezabezpieczonych pomieszczeń, szaf w których przechowywane są dane osobowe oraz dokumentów na biurkach po zakończeniu pracy.	Należy zabezpieczyć dane osobowe, pomieszczenia i powiadomić ABI. ABI sporządza protokół uchybienia.
03	Dokumenty i nośniki elektroniczne zawierające dane osobowe nie zostały zniszczone w sposób uniemożliwiający ich odczyt, pozostawiono je koszu naśmieci lub nie odebrano wydruków z drukarek ogólnodostępnych	Należy zabezpieczyć dane osobowe, nośniki, dokumenty i powiadomić ABI. ABI sporządza protokół uchybienia.
04	Zgubiono klucze, lub wykonano kopie kluczy do pomieszczeń biurowych w których przechowuje się dane osobowe, nie zachowując obowiązującej procedury	Należy zabezpieczyć dane osobowe, pomieszczenia i powiadomić ABI. ABI sporządza protokół zagrożenia i powiadamia ADO
05	Zidentyfikowano lub wykorzystywano środek przetwarzający informacje nieznanego pochodzenia (sprzęt, nośniki) oraz wykonywanie zdalnej pracy przy pomocy komputera inny niż służbowy.	Należy zabezpieczyć dane osobowe, sprzęt i powiadomić ABI. Należy zabezpieczyć sprzęt. ABI sporządza protokół zagrożenia lub uchybienia, powiadamia ADO adekwatnie do sytuacji.
06	Niestosowanie się do wymagań dotyczących złożoności haseł, przechowywanie ich w sposób niewłaściwy lub nieuprawnione ich udostępnianie.	Należy zabezpieczyć dane osobowe, sprzęt i powiadomić ABI. ASI zmienia hasło dostępu. ABI sporządza protokół zagrożenia i powiadamia ADO.
07	Podjęto pracę w stanie zagrożenia bezpieczeństwa informacji (m. in. próba logowania za pomocą nieprawidłowego hasła) w wyniku czego zostało zablokowane konto użytkownika.	Należy zabezpieczyć dane osobowe, sprzęt i powiadomić ABI. ABI sporządza protokół zagrożenia i powiadamia ADO
08	Komputer nie jest zabezpieczony hasłem.	Należy zabezpieczyć dane osobowe oraz powiadomić ABI. ABI sporządza protokół uchybienia.
09	Stwierdzono wykorzystywanie nielegalnego lub złośliwego oprogramowania (wirusa, atak hackera) oraz narzędzi służących do obchodzenia zabezpieczeń w systemie informatycznym, próby instalacji nie zatwierdzonego oprogramowania lub zmiany konfiguracji sprzętowej oraz programowej systemów oraz stacji roboczych przez nieupoważnione osoby.	Należy zabezpieczyć dane osobowe, sprzęt i powiadomić ABI. ABI sporządza protokół zagrożenia i powiadamia ADO

10	Dostęp do danych osobowych mają osoby nieposiadające upoważnienia, pracownik nie podpisał oświadczeń	Należy uniemożliwić dostęp osób bez upoważnienia oraz powiadomić ABI. ABI sporządza protokół uchybienia.
11	Nie anulowano uprawnień pracownikowi, z którym wygasła, rozwiązano umowę o pracę, nie rozliczył się z powierzonych materiałów i środków przetwarzania informacji.	Należy zabezpieczyć dane osobowe i powiadomić ABI. ABI sporządza protokół uchybienia
12	Utrata danych osobowych w wyniku kradzieży, zagubienia, nieuprawnionego przekazania	Należy zabezpieczyć dane osobowe i powiadomić ABI. ABI sporządza protokół zagrożenia
13	Nadawanie nadmiernych uprawnień dostępu do systemów przetwarzających dane osobowe	Należy powiadomić ABI. ABI sporządza protokół uchybienia
14	Nieuprawniony dostęp do otwartych aplikacji w systemie informatycznym	Należy powiadomić ABI, który powinien sprawdzić system uwierzytelniania oraz sprawdzić czy nie doszło do kradzieży lub zniszczenia danych. ABI sporządza protokół uchybienia
15	Próba kradzieży danych osobowych poprzez zewnętrzny nośnik danych	Należy nie dopuścić do kradzieży danych i powiadomić ABI. ABI powinien zabezpieczyć nośnik danych i powiadomić ADO. ABI sporządza protokół zagrożenia i powiadamia ADO
16	Próba kradzieży danych osobowych w formie papierowej.	Należy nie dopuścić do kradzieży danych i powiadomić ABI. ABI powinien zabezpieczyć dane i powiadomić ADO. ABI sporządza protokół zagrożenia i powiadamia ADO.
17	Nieuprawniony dostęp do danych osobowych w formie papierowej.	Należy uniemożliwić dostęp osób bez upoważnienia oraz powiadomić ABI. ABI sporządza protokół uchybienia.
18	Dane osobowe przechowywane są w niezabezpieczonym pomieszczeniu	Należy powiadomić ABI. ABI powinien zabezpieczyć pomieszczenie. ABI sporządza protokół uchybienia.
19	Próba włamania do pomieszczenia/budynku, kradzieży sprzętu przetwarzającego dane osobowe.	Należy zabezpieczyć dowody i powiadomić ABI. ABI sprawdza stan uszkodzeń, zabezpiecza dowody i wzywa policję. ABI sporządza protokół zagrożenia i powiadamia ADO.
20	Działanie zewnętrznych aplikacji, wirusów, złośliwego oprogramowania	Należy zrobić audyt systemów zabezpieczeń, a w szczególności systemów antywirusowych, firewall. ABI we współpracy z ASI powinien ocenić, czy nie doszło do utraty danych osobowych i w zależności od tego sporządzić protokół uchybienia lub zagrożenia.
21	Brak aktywnego oprogramowania antywirusowego	Należy powiadomić ABI. ASI powinien zaktualizować lub nabyć oprogramowanie antywirusowe. ABI sporządza protokół uchybienia.

22	Nieuprawniona zmiana, zniszczenie lub modyfikacja danych osobowych w formie papierowej.	Należy zabezpieczyć dowody i powiadomić ABI. ABI sprawdza stan uszkodzeń, zabezpiecza dowody i powiadamia ADO. ABI sporządza protokół zagrożenia
23	Nieuprawniona zmiana, zniszczenie, uszkodzenie, (w tym sprzętu oraz nośników przetwarzających dane osobowe) lub modyfikacja danych osobowych w systemie informatycznym.	Należy zabezpieczyć dowody i powiadomić ABI. ABI sprawdza stan uszkodzeń, zabezpiecza dowody i powiadamia ADO. ABI sporządza protokół zagrożenia.
24	Awaria systemu informatycznego, uszkodzenie komputerów, nośników danych.	Należy powiadomić ABI. ASI powinien ocenić w wyniku czego doszło do zniszczenia i przywrócić dane z kopii zapasowej. ABI powiadamia ADO i sporządza protokół zagrożenia
25	Próba nieuprawnionej interwencji przy sprzęcie komputerowym.	Należy uniemożliwić dostęp osób do sprzętu komputerowego oraz powiadomić ABI. ABI sporządza protokół uchybienia
26	Utrudniona dostępność systemu informatycznego spowodowana awarią zasilania urządzeń przetwarzających informacje, obciążeniem procesora, przekroczenie dostępnych zasobów systemowych, itp	Należy zabezpieczyć dane osobowe, pomieszczenia i powiadomić ABI. ABI sporządza protokół uchybienia.
27	Błędy w obsłudze i konserwacji sprzętu komputerowego oraz przechowywaniu, eksploatacji i konserwacji oprogramowania	Należy zabezpieczyć sprzęt i oprogramowania i powiadomić ABI. ABI sporządza protokół uchybienia
28	Nie wykonywane są kopie bezpieczeństwa oraz nie weryfikuje się możliwości odtworzenia danych z kopii zapasowych.	Należy zabezpieczyć dane osobowe, pomieszczenia i powiadomić ABI. ABI sporządza protokół zagrożenia i powiadamia ADO
29	Zdarzenia losowe (pożar, zalanie, klęska żywiołowa).	Powiadomić ABI i ASI. ABI oszacowuje powstałe starty i sporządza protokół zagrożenia lub uchybienia i powiadamia ADO.

5. Załączniki

Załącznik nr 1 – Dziennik uchybień i zagrożeń
Załącznik nr 2 – Protokół zagrożenia
Załącznik nr 3 – Protokół uchybienia
Załącznik nr 4 – Sprawozdanie roczne stanu systemu ochrony danych osobowych i wzór raportu rocznego

Załącznik nr 1
do Procedury Alarmowej

DZIENNIK UCHYBIEŃ I ZAGROŻEŃ

Kod	Data i godzina zdarzenia	Rodzaj zdarzenia *(uchybienie/ zagrożenie)*	Opis zdarzenia	Skutki zdarzenia	Działania naprawcze	Podpis ABI

Załącznik nr 2
do Procedury Alarmowej

Urząd Gminy Zadzim
Zadzim 44
99-232 Zadzim

Zadzim, dnia …… 20 … r.

PROTOKÓŁ ZAGROŻENIA

Data i godzina wystąpienia zagrożenia - .....

Kod zagrożenia - .....

Opis zagrożenia

.....
.....
.....
.....
.....

Przyczyny powstania zagrożenia

.....
.....
.....
.....
.....

Zaistniałe skutki zagrożenia

.....
.....
.....
.....
.....

Podjęte działania naprawczo-zapobiegawcze

.....
.....
.....

Administrator Bezpieczeństwa Informacji

….....
Podpis

Administrator Danych Osobowych

.....
Podpis

Załącznik nr 3
do Procedury Alarmowej

Urząd Gminy Zadzim
Zadzim 44
99-232 Zadzim

Zadzim, dnia …… 20 … r.

PROTOKÓŁ UCHYBIENIA

Data i godzina wystąpienia uchybienia - .....

Kod uchybienia - .....

Opis uchybienia

.....
.....
.....
.....
.....

Przyczyny powstania uchybienia

.....
.....
.....
.....
.....

Zaistniałe skutki uchybienia

.....
.....
.....
.....
.....

Podjęte działania naprawczo-zapobiegawcze

.....
.....
.....

Administrator Bezpieczeństwa Informacji

….....
Podpis

Administrator Danych Osobowych

.....
Podpis

Załącznik nr 4
do Procedury Alarmowej

Sprawozdanie roczne stanu systemu ochrony danych osobowych – Raport roczny

W celu pełnej kontroli oraz zapobieganiu możliwym zagrożeniom związanych z ochroną danych osobowych na podstawie art. 36 ust. 1 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych Administrator Danych wdraża dokument o nazwie ”Sprawozdanie roczne stanu systemu ochrony danych osobowych”

1. Sprawozdanie roczne stanu systemu ochrony danych osobowych przeprowadzać się będzie od 2015r. raz w roku. Osoba odpowiedzialna za przygotowanie sprawozdania jest ABI. Sprawozdanie roczne przygotowuje się na podstawie dokumentu „Raport roczny”

2. Po przeprowadzeniu analizy stanu ochrony danych osobowych w porozumieniu z ASI ABI uzupełnia raport roczny i zwołuje zebranie w którym uczestniczą: ADO, ABI, ASI, kierownicy referatów

3. Podczas zebrania ASI przedstawia uczestnikom stan infrastruktury informatycznej a ABI przedstawia dziennik uchybień i zagrożeń. Na spotkaniu omawiane są procedury zabezpieczające podmiot przed sytuacjami, w których może dojść do zniszczenia danych, wycieku danych lub naruszenia ich poufności.

„Raport roczny”

Nazwa i adres podmiotu ……	Miejscowość i data ……
Zagadnienia omawiane na zebraniu	**Uwagi/wnioski**
Podsumowanie realizacji wytycznych z poprzedniego „Sprawozdania rocznego stanu systemu ochrony danych osobowych”	
Omówienie zmian procedur w systemie oraz zmian w systemie informatycznym	
Omówienie Dziennika Uchybień i Zagrożeń	
Wnioski oraz zadania do realizacji	
Uczestnicy zebrania	Podpis uczestnika
Podpis ABI	Podpis ADO

Załącznik nr 5
do Polityki Bezpieczeństwa Zbiorów Danych Osobowych
Prowadzonych w Urzędzie Gminy Zadzim

KARTA ZAPOZNANIA Z DOKUMENTACJĄ OCHRONY DANYCH OSOBOWYCH W URZĘDZIE GMINY ZADZIM

- Polityka bezpieczeństwa zbiorów danych osobowych prowadzonych w Urzędzie Gminy Zadzim
- Instrukcja zarządzania systemami informatycznymi przetwarzającymi dane osobowe w Urzędzie Gminy Zadzim
- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych

Oświadczam, iż zapoznałem/zapoznałam się z treścią powyższych dokumentów oraz rozumiem zasady i procedury w nich zawarte

Lp.	Nazwisko i imię	Data	Podpis	Lp.	Nazwisko i imię	Data	Podpis
1				23			
2				24			
3				25			
4				26			
5				27			
6				28			
7				29			
8				30			
9				31			
10				32			
11				33			
12				34			
13				35			
14				36			
15				37			
16				38			
17				39			
18				40			
19				41			
20				42			
21				43			
22				44			