Polityka Bezpieczeństwa Ochrony Danych Osobowych

w Urzędzie Gminy w Cielądzu

Wersja 1		Pieczęć firmowa: WÓJT GMINY CIELĄDZ powiat rawski, woj. łódzkie	
Opracował:	**Data:**	**Zatwierdził:**	**Data:**
Sylwester Krawczyk - Sekretarz Gminy	14.04.2016 r.	WÓJT mgr Paweł Królak	.

1. Wstęp

Celem Polityki Bezpieczeństwa jest zapewnienie ochrony DANYCH OSOBOWYCH przetwarzanych przez URZĄD GMINY W CIELĄDZU przed wszelakiego rodzaju zagrożeniami, tak wewnętrznymi jak i zewnętrznymi, świadomymi lub nieświadomymi.

Polityka określa obowiązki administratora danych w zakresie zabezpieczenia danych osobowych, o których mowa w § 36 Ustawy o Ochronie Danych Osobowych.

Polityka określa reguły dotyczące procedur zapewnienia bezpieczeństwa danych osobowych w postaci papierowej oraz zawartych w systemach informatycznych w URZĘDZIE GMINY W CIELĄDZU.

Jako załącznik do niniejszej polityki opracowano i wdrożono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwaną dalej „Instrukcją zarządzania systemem informatycznym ochrony danych osobowych". Określa ona sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem zapewnienia ich bezpieczeństwa.

Polityka została opracowana zgodnie z wymogami określonymi w § 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).

Polityka obowiązuje wszystkich pracowników URZĘDU GMINY W CIELĄDZU oraz dostawców, podmioty współpracujące na zasadzie umów, mające jakikolwiek kontakt z danymi osobowymi objętymi ochroną.

Ochrona danych osobowych jest realizowana poprzez: zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz przez użytkowników.

Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:

1. poufność danych - rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom,
2. integralność danych - rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
3. rozliczalność danych - rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie,
4. integralność systemu rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej.

Za przestrzeganie zasad ochrony i bezpieczeństwa danych w komórkach organizacyjnych odpowiedzialni są kierownicy tych komórek.

Niniejszy dokument jest zgodny z następującymi aktami prawnymi:

1. ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883 z późn. zm.),
2. oraz aktów wykonawczych wydanych na podstawie ww. ustaw.

2. Definicje

Przez użyte w Polityce określenia należy rozumieć:

1. Polityka - rozumie się przez to Politykę bezpieczeństwa ochrony danych osobowych w URZĘDZIE GMINY W CIELĄDZU.
2. Administrator Danych Osobowych - URZĄD GMINY W CIELĄDZU REPREZENTOWANY PRZEZ WÓJTA GMINY CIELĄDZ, decydujący o celach i środkach przetwarzania danych osobowych;
3. Administrator Bezpieczeństwa Informacji (ABI) – pracownik URZĘDU GMINY W CIELĄDZU, wyznaczony przez WÓJTA GMINY CIELĄDZ, odpowiedzialny za organizację ochrony danych osobowych.
4. Kierownik – dyrektor, naczelnik, kierownik albo inna osoba pełniąca funkcje kierownicze jednostki bądź komórki organizacyjnej URZĘDU GMINY W CIELĄDZU;
5. Ustawa - rozumie się przez to ustawę z dnia 29.sierpnia.1997 r. o ochronie danych osobowych (Dz.U. z 1997 r.Nr 133, poz.883)
6. Rozporządzenie – rozumie się przez to rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 1998 r. Nr 80, poz. 521)
7. Dane osobowe (dane) - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
8. Zbiór danych - zestaw danych osobowych posiadający określoną strukturę, prowadzony w/g określonych kryteriów oraz celów np. zbiór klientów URZĘDU GMINY W CIELĄDZU, zbiór osób przekazujących swoje oferty pracy, zbiór pracowników URZĘDU GMINY W CIELĄDZU;
9. Usuwanie danych – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację , która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
10. Zgoda osoby, której dane dotyczą - rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści,
11. Baza danych osobowych - zbiór uporządkowanych powiązanych ze sobą tematycznie danych zapisanych np. w pamięci zewnętrznej komputera. Baza danych jest złożona z elementów o określonej strukturze - rekordów lub obiektów, w których są zapisane dane osobowe;
12. Przetwarzanie danych - wykonywanie jakichkolwiek operacji na danych osobowych, np. zbieranie, utrwalanie, opracowywanie, udostępnianie, zmienianie, usuwanie;
13. System informatyczny (system) zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
14. Administrator systemu - osoba nadzorująca pracę systemu informatycznego oraz wykonująca w nim czynności wymagające specjalnych uprawnień;
15. Użytkownik - pracownik URZĘDU GMINY W CIELĄDZU posiadający uprawnienia do pracy w systemie informatycznym zgodnie z zakresem obowiązków służbowych;
16. Zabezpieczenie systemu informatycznego należy przez to rozumieć wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą,
17. Nośnik komputerowy (wymienny) nośnik służący do zapisu i przechowywania informacji, np. taśmy, dyskietki, dyski twarde;

3. Zadania ABI

Do najważniejszych obowiązków Administratora Bezpieczeństwa Informacji należy:

1. organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami ustawy o ochronie danych osobowych,
2. zapewnienie przetwarzania danych zgodnie z uregulowaniami niniejszej polityki,
3. wydawanie i anulowanie upoważnień do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład dla osób przetwarzających dane osobowe,
4. prowadzenie „Rejestru osób zatrudnionych przy przetwarzaniu danych osobowych",
5. prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych,
6. nadzór nad bezpieczeństwem danych osobowych,
7. kontrola działań komórek organizacyjnych pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych,
8. inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych w URZĘDZIE GMINY W CIELĄDZU.

Administrator Bezpieczeństwa Informacji ma prawo :

1. wstępu do pomieszczeń w których zlokalizowane są zbiory danych i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z ustawą,
2. żądać złożenia pisemnych lub ustnych wyjaśnień w zakresie niezbędnym do ustalenia stanu faktycznego,
3. żądać okazania dokumentów i wszelkich danych mających bezpośredni związek z problematyką kontroli,
4. żądać udostępnienia do kontroli urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych.

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

Szczegółowe rozmieszczenie zbiorów dokumentacji papierowej i elektronicznej, zawierającej dane osobowe, opisane jest w Załączniku A „Wykaz zbiorów danych osobowych".

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

Wykaz zbiorów danych osobowych w postaci dokumentacji papierowej i elektronicznej wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, opisany jest w Załączniku A „Wykaz zbiorów danych osobowych".

6. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych

Struktura zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych oraz informacja o programach komputerowych stosowanych do ich przetwarzania opisane są w Załączniku A „Wykaz zbiorów danych osobowych".

7. Sposób przepływu danych pomiędzy poszczególnymi systemami

System A	System B	Kierunek przepływu danych osobowych	Sposób przesyłania danych osobowych
Program Płace	Program Płatnik	Jednokierunkowo z programu „A" do Programu „B"	Automatycznie przez plik wymiany
Program Podatki	Program GOMIG	Dwukierunkowo	Automatycznie poprzez współdzielony dostęp do pliku bazy danych

8. Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

A. Środki ochrony fizycznej.

1. Podstawowe zabezpieczenia fizyczne opisane są w Załączniku A „Wykaz zbiorów danych osobowych".
2. Przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych.
3. Przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych.

4. Kopie zapasowe/archiwalne zbiorów danych osobowych w formie papierowej przechowywane są w zamkniętej niemetalowej szafie, lub w zamkniętej szafie metalowej (nie antywłamaniowej).

B. Środki sprzętowe, informatyczne i telekomunikacyjne.

1. Pomieszczenia, w którym przetwarzane są dane osobowe zabezpieczone są przed skutkami pożaru za pomocą wolnostojącej gaśnicy.
2. Dokumenty zawierające dane osobowe, po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.
3. Co najmniej jedno urządzenie systemu informatycznego służącego do przetwarzania danych osobowych połączone jest z siecią publiczną (dla poziomu bezpieczeństwa podwyższonego i wysokiego).
4. Lokalizacja urządzeń komputerowych (komputerów typu PC, terminali, drukarek) uniemożliwia osobom niepowołanym dostęp do nich oraz wgląd do danych wyświetlanych na monitorach komputerowych.
5. Komputery przenośne, wykorzystywane do przetwarzania danych osobowych, po zakończonej pracy są przechowywane w warunkach zapewniających ich bezpieczeństwo.
6. System operacyjny zapewnia odpowiednie restrykcje w zakresie dostępu do danych i aplikacji.
7. Uniemożliwiono użytkownikom systemu informatycznego, w którym przetwarzane są dane osobowe wykonywania kopii tych danych.
8. Zastosowano urządzenia typu UPS chroniące system informatyczny służący do przetwarzania danych osobowych przed awarią zasilania.
9. Zastosowano system replikacji danych na dwóch niezależnych dyskach twardych na komputerze głównym w celu ochrony danych osobowych.
10. Zastosowano szyfrowanie danych osobowych dla wszystkich baz danych w postaci elektronicznej.

C. Środki ochrony w ramach oprogramowania systemu.

1. Dostęp do zbioru danych osobowych przetwarzanych za pomocą komputera zabezpieczony jest za pomocą hasła BIOS.
2. Zastosowano system operacyjny pozwalający na określenie odpowiednich praw dostępu do zasobów informatycznych dla poszczególnych użytkowników systemu informatycznego.
3. W systemie operacyjnym zastosowano mechanizm wymuszający okresową zmianę haseł.
4. Serwery obsługujące bazę danych oraz stanowiska komputerowe służące do przetwarzania danych osobowych dostępne są wyłącznie po przeprowadzeniu prawidłowego procesu autoryzacji (system użytkowników i haseł, ograniczenie dostępu do poziomu poleceń systemowych lub zakaz wykonywania poleceń systemowych).
5. Zapewniono rejestrację czasu nieudanych logowań do systemu przetwarzającego dane osobowe.
6. Zastosowano system rejestracji dostępu do zbioru danych osobowych.
7. Na serwerze zastosowano oprogramowanie umożliwiające wykonanie kopii zapasowych zbiorów danych osobowych.
8. Zastosowano oprogramowanie zabezpieczające przed nieuprawnionym dostępem do systemu informatycznego.

D. Środki ochrony w ramach narzędzi baz danych i innych narzędzi programowych.

1. Dostęp do zbioru danych osobowych zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
2. Dostęp do zbioru danych osobowych zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem karty mikroprocesorowej (program PŁATNIK).
3. Zastosowano mechanizm umożliwiający rejestrację identyfikatora użytkownika wprowadzającego dane osobowe.
4. Wykorzystano środki pozwalające na rejestrację dokonanych zmian w zbiorze danych osobowych.
5. Zastosowano środki umożliwiające określenie praw dostępu do zbioru danych osobowych.
6. Zastosowano identyfikator i hasło dostępu do danych na poziomie aplikacji.
7. Dla każdego użytkownika systemu jest ustalony odrębny identyfikator.
8. Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych.

E. Środki ochrony w ramach systemu użytkowego.

1. Zastosowano zabezpieczone hasłem wygaszanie ekranu w przypadku dłuższej nieaktywności użytkownika.
2. Zastosowano blokadę klawiatury, w przypadku dłuższej nieaktywności użytkownika.
3. Zastosowano działający w „tle" program antywirusowy na komputerach użytkowników.

G. Środki organizacyjne.

1. Wyznaczono administratora bezpieczeństwa informacji. Administrator danych osobowych również sam nadzoruje przestrzeganie zasad ochrony przetwarzanych danych osobowych.
2. Opracowano i wdrożono Politykę bezpieczeństwa ochrony danych osobowych i Instrukcję zarządzania systemem informatycznym ochrony danych osobowych.
3. Wdrożono odpowiedni podział obowiązków i kontroli dostępu.
4. Do danych osobowych mają dostęp jedynie osoby posiadające upoważnienie nadane przez Administratora Danych Osobowych.
5. Administrator Bezpieczeństwa Informacji prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych.
6. Wprowadzono mechanizmy autoryzacji odpowiednio zabezpieczone przed dostępem osób trzecich.
7. Wprowadzono procedury alarmowe i informacyjne.
8. Osoby upoważnione do przetwarzania danych osobowych przed dopuszczeniem do tych danych są szkolone w zakresie obwiązujących przepisów o ochronie danych osobowych, procedur przetwarzania danych oraz informowane o podstawowych zagrożeniach związanych z przetwarzaniem danych osobowych. Osoby te są zobowiązane do podpisania stosownego oświadczenia.
9. Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane są do zachowania ich w tajemnicy.
10. Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym.
11. Tymczasowe wydruki z danymi osobowymi są po ustaniu ich przydatności niszczone w niszczarce.
12. Korespondencja w zakresie procedur kadrowo-płacowych prowadzona jest za pomocą listów poleconych.
13. Zapewniono klauzulę poufności z wszystkimi podmiotami zewnętrznymi mającymi dostęp do danych osobowych Urzędu.

14. Zapewnia się bezpieczne przechowywanie lub niszczenie uszkodzonych nośników zawierających dane osobowe (np. dysk twardy), szczególnie, gdy sprzęt, w którym zamontowany jest dany nośnik przekazywany jest do naprawy do firmy zewnętrznej.

9. Instrukcja alarmowa (postępowania w przypadku naruszenia ochrony danych osobowych).

9.1. Zdarzenia zagrażające bezpieczeństwu danych osobowych

Do zdarzeń zagrażających bezpieczeństwu danych osobowych należą:

1. próby naruszenia ochrony danych:
   - z zewnątrz – włamania do systemu, podsłuch, kradzież danych,
   - z wewnątrz – nieumyślna lub celowa modyfikacja danych, kradzież danych,
2. programy destrukcyjne:
   - wirusy,
   - konie trojańskie,
   - makra,
   - bomby logiczne,
3. awarie sprzętu lub uszkodzenie oprogramowania,
4. zabór sprzętu lub nośników z ważnymi danymi,
5. inne skutkujące utratą danych osobowych, bądź wejściem w ich posiadanie osób nieuprawnionych,
6. usiłowanie zakłócenia działania systemu informatycznego,

9.2. Procedura postępowania w przypadkach naruszenia bezpieczeństwa danych osobowych

1. W przypadku stwierdzenia faktu nieuprawnionego przetwarzania, ujawnienia lub nienależytego zabezpieczenia przed osobami nieuprawnionymi danych osobowych, jak również stwierdzenia istnienia przesłanek wskazujących na prawdopodobieństwo naruszenia ochrony danych osobowych, każdy pracownik URZĘDU GMINY W CIELĄDZU zobowiązany jest poinformować o zdarzeniu ASI a ten w uzasadnionych przypadkach ABI.
2. W sytuacji, określonej w pkt. 1, Administrator Bezpieczeństwa Informacji prowadzi postępowanie wyjaśniające w toku, którego:
   - ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały,
   - ustala osoby odpowiedzialne za naruszenie,
   - podejmuje działania w kierunku ograniczenia szkód oraz przeciwdziałania podobnym przypadkom w przyszłości,
   - sporządza pisemną notatkę z przeprowadzonego postępowania.
3. Administrator Bezpieczeństwa Informacji powiadamia o wynikach postępowania wyjaśniającego WÓJTA GMINY CIELĄDZ.
4. W przypadku zaistnienia zdarzenia, określonego w ust. 1, decyzje dyscyplinarne w stosunku do winnych oraz w sprawie wniosku o pociągnięcie ich do odpowiedzialności karnej podejmuje WÓJT z własnej inicjatywy lub na wniosek ABI.

9.3. Procedura postępowania w przypadkach zagrożeń (stwierdzenia słabości systemu)

1. W przypadku jakiejkolwiek nieprawidłowości w działaniu systemu, uszkodzenia lub podejrzenia o uszkodzenie sprzętu, oprogramowania lub danych należy bezzwłocznie powiadomić ASI, który zawiadamia ABI.

2. W przypadku włamania lub podejrzenia o włamanie do systemu administrator danego systemu podejmuje działania w celu zabezpieczenia systemu i danych:
   - zmienia hasła administracyjne,
   - określa rodzaj i sposób włamania,
   - podejmuje działania w celu uniemożliwienia ponownego włamania tego samego typu,
   - szacuje straty w systemie,
   - przywraca stan systemu sprzed włamania.
3. W przypadku uszkodzenia sprzętu lub programów z danymi administrator danego systemu podejmuje działania w celu:

- określenia przyczyny uszkodzenia,
- oszacowania strat wynikłych z w w uszkodzenia,
- naprawy uszkodzeń, a w szczególności naprawy sprzętu, ponownego zainstalowania danego programu, odtworzenie jego pełnej konfiguracji oraz wczytania danych z ostatniej kopii zapasowej.

4. W przypadku uszkodzenia danych administrator systemu podejmuje następujące działania:

- ustala przyczynę uszkodzenia danych,
- określa wielkość i jakość uszkodzonych danych,
- podejmuje działania w celu odtworzenia danych z ostatniej kopii zapasowej.

5. W przypadku stwierdzenia nieprawidłowości w funkcjonowaniu sieci telekomunikacyjnej każdy użytkownik zobowiązany jest niezwłocznie powiadomić administratora sieci, który podejmuje działania w celu ustalenia przyczyn zaistniałej sytuacji oraz wyeliminowania nieprawidłowości.

W przypadku zidentyfikowania osób odpowiedzialnych za wystąpienie któregoś ze zdarzeń zagrażających bezpieczeństwu danych administrator danego systemu zobowiązany jest powiadomić Administratora Bezpieczeństwa Informacji, a ten WÓJTA.

10. Procedura działań korygujących i zapobiegawczych

1. Celem procedury jest uporządkowanie i przedstawienie czynności związanych z: inicjowaniem oraz realizacją działań korygujących i zapobiegawczych wynikających z zaistnienia incydentów bezpieczeństwa lub słabości systemu ochrony danych osobowych.
2. Procedura działań korygujących i zapobiegawczych obejmuje wszystkie te procesy, w których incydenty bezpieczeństwa, zagrożenia lub słabości systemu ochrony danych osobowych mogą wpłynąć na zgodność z wymaganiami ustawy o ochronie danych osobowych, jak również na poprawne funkcjonowanie systemu ochrony danych osobowych.
3. Osobą odpowiedzialną za nadzór nad procedurą jest Administrator Bezpieczeństwa Informacji. Przy czym czynności związane z realizacją poszczególnych zadań/ zabezpieczeń wykonuje osoba odpowiedzialna a zatwierdza WÓJT.

Definicje

1. Niezgodność – niespełnienie wymagania, czyli potrzeby lub oczekiwania, które zostało ustalone, przyjęte zwyczajowo lub jest obowiązkowe.
2. Incydent - naruszenie bezpieczeństwa informacji ze względu na poufność, dostępność i integralność.
3. Zagrożenie – potencjalna możliwość wystąpienia incydentu.
4. Słabość systemu – zdarzenie, stan rzeczy zwiększający ryzyko wystąpienia incydentu.

5. Działanie korygujące – jest to działanie przeprowadzane w celu wyeliminowania przyczyny wykrytej niezgodności / incydentu lub innej niepożądanej sytuacji.
6. Działanie zapobiegawcze – jest to działanie, które należy przedsięwziąć, aby wyeliminować przyczyny potencjalnej niezgodności/incydentu lub innej potencjalnej sytuacji niepożądanej.
7. Korekcja – działanie w celu wyeliminowania wykrytej niezgodności lub incydentu.
8. Kontrola (Audit) – systematyczny, niezależny i udokumentowany proces oceny skuteczności systemu ochrony danych osobowych, na podstawie określonych kryteriów, wymagań, polityk i procedur.

Opis czynności

1. ABI oraz ASI są odpowiedzialni za analizę incydentów bezpieczeństwa, zagrożeń lub słabości systemu ochrony danych osobowych. Typowymi źródłami informacji o incydentach, zagrożeniach lub słabościach są:
- Zgłoszenia od pracowników
- Alarmy z systemów informatycznych
- Analizy incydentów
- Wyniki auditów kontroli.
2. Gdy ABI stwierdzi konieczność podjęcia działań korygujących lub zapobiegawczych, określa:
- Źródło powstania incydentu/zagrożenia lub słabości
- Zakres działań korygujących lub zapobiegawczych
- Termin realizacji
- Osobę odpowiedzialną.
3. ABI jest odpowiedzialny za nadzór nad poprawnością i terminowością wdrażanych działań korygujących lub zapobiegawczych.
4. Po przeprowadzeniu działań korygujących lub zapobiegawczych, ABI jest zobowiązany do oceny efektywności ich zastosowania.

11. Kontrola systemu ochrony danych osobowych i przegląd zarządzania

1. Celem procedury jest uporządkowanie i przedstawienie czynności związanych z: kontrolą stanu bezpieczeństwa danych osobowych oraz okresową oceną Systemu Ochrony Danych Osobowych
2. Procedura obejmuje wszystkie procesy organizacji, gdzie przestrzeganie zasad ochrony danych osobowych jest wymagane.
3. Do kontroli stanu ochrony danych osobowych w URZĘDZIE GMINY W CIELĄDZU upoważnieni są:
- WÓJT GMINY CIELĄDZ lub osoby przez niego upoważnione,
- Administrator Bezpieczeństwa Informacji,
- Administrator Systemu Informatycznego.
4. Raz w roku kontroli (auditowi) podlegają wszystkie systemy informatyczne przetwarzające dane osobowe oraz zabezpieczenia fizyczne i bezpieczeństwo osobowe.
5. Administrator Bezpieczeństwa Informacji przygotowuje plan kontroli uwzględniając zakres oraz potrzebne zasoby fizyczne, czasowe i osobowe.
6. Kontroli podlega warstwa sprzętowa, systemy operacyjne oraz aplikacje, realizacja zabezpieczeń przez pracowników Urzędu i przestrzeganie polityki bezpieczeństwa.
7. Po dokonanej kontroli Administrator Bezpieczeństwa Informacji przygotowuje raport poauditowy, którego jeden egzemplarz przekazuje kierownikowi kontrolowanej

jednostki lub komórki organizacyjnej. Na jego podstawie informuje WÓJTA o konieczności podjęcia właściwych działań korygujących i doskonalących.

12. Postanowienia końcowe

1. „Polityka Bezpieczeństwa" jest dokumentem wewnętrznym i nie może być udostępniania osobom postronnym w żadnej formie.
2. Kierownicy komórek organizacyjnych są obowiązani zapoznać z treścią „Polityki bezpieczeństwa" każdego użytkownika.
3. Użytkownik zobowiązany jest złożyć oświadczenie o tym, iż został zaznajomiony z przepisami ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz instrukcjami wdrożonymi przez Administratora Danych Osobowych, a także o zobowiązaniu się do ich przestrzegania.
4. Oświadczenie potwierdzające zaznajomienie użytkownika z przepisami ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz instrukcjami obowiązującymi u Administratora Danych, a także o zobowiązaniu się do ich przestrzegania, przechowywane jest w aktach osobowych pracownika.
   - Przypadki, nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia, nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie dyscyplinarne.
   - Kara dyscyplinarna, orzeczona wobec osoby uchylającej się od powiadomienia, nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926) oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
   - Wszystkie regulacje dotyczące systemów informatycznych określone w Polityce Bezpieczeństwa dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiejkolwiek innej formie.
5. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej „Polityce".
6. W sprawach nieuregulowanych w niniejszej „Polityce bezpieczeństwa" mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r., o ochronie danych osobowych (tj. Dz.U. z 2002r., Nr 101, poz. 926 ze zm.) oraz wydanych na jej podstawie aktów wykonawczych.

Załącznik A
do polityki bezpieczeństwa

Szczegółowy wykaz zbiorów danych osobowych wraz ze wskazaniem programów

Zbiór danych	Użytkownik/ Administrator	Miejsce przechowywania	Sposób zabezpieczenia dostępu (program komputerowy/	Dodatkowe informacje	Oprogramowanie do przetwarzania NAZWA
Ewidencja ludności	Irena Grotek	Komputer klasy PC + dokumentacja	Login i hasło/ szafa zamykana na klucz	Pokój nr 19	SELWIN (Sygnity S.A.)
Zbiór wydanych i utraconych dowodów	Irena Grotek	Komputer klasy PC + dokumentacja	Login i hasło/ szafa zamykana na klucz	Pokój nr 19 / odrębna sieć	System Wydawania Dowodów Osobistych
Akta osobowe pracowników i	Agnieszka Miniak	papierowo	szafa zamykana na klucz	Sekretariat	
Zbiór danych osób przeznaczonych do	Piotr Król	Dokumentacja papierowa	dodatkowe pomieszczenie zamykane na klucz	Pokój nr 19	n/a
Zbiór danych właścicieli/użytkownik	Julianna Libera, Czarnecka Janina,	Komputer klasy PC + dokumentacja	login i hasło / szafa zamykana na klucz	Pokój nr 11/ login i hasło	EWOPIS (Geo-Bit)
Ewidencja podatników	Julianna Libera, Czarnecka Janina,	Komputer klasy PC + dokumentacja	login i hasło / szafa zamykana na klucz	Pokój nr 11/ login i hasło	Program "PODATKI" (Groszek*)
Ewidencja odbiorców wody z systemu	Julianna Libera, Czarnecka Janina,	Komputer klasy PC + dokumentacja	**brak**	Pokój nr 11/	Program WODA (Groszek)
Ewidencja księgowa podatników	Julianna Libera, Czarnecka Janina,	Komputer klasy PC + dokumentacja	login i hasło / szafa zamykana na klucz	Pokój nr 11/ login i hasło	KSZOB (Groszek)
Ewidencja danych płatników składek ZUS	Piotr Libera	Komputer klasy PC + dokumentacja	login i hasło / szafa	Pokój nr 13	PŁATNIK (Asseco)
Zbior danych osób zatrudnionych w UG	Ewelina Biernacka	Komputer klacy PC + dokumentacja	login i hasło	Pokój nr 13	PŁACE (Groszek)
Program Budżet	Gabriela Milczarska	elektronicznie	login i hasło		Budżet (GROSZEK)
Program do Gospodarki odpadami	Agnieszka Zielińska	elektronicznie oraz wydruki papierowe	szafa zamykana na klucz	Pokój nr 11	GOMiG
Rejestr wyborców	Irena Grotek	elektronicznie	login i hasło	Pokój nr 19	SELWIN (Sygnity S.A.)
Rejestr mieszkańców gminy	Irena Grotek	elektronicznie	login i hasło	Pokój nr 19	SELWIN (Sygnity S.A.)

Rejestr wniosków o wpis do CEIDG	Piotr Król	papierowo	szafa zamykana na klucz	Pokój nr 19	
Wykaz osób podlegających	Piotr Król	papierowo	szafa zamykana na klucz	Pokój nr 19	
Wykaz osób podlegających	Piotr Król	papierowo	szafa zamykana na klucz	Pokój nr 19	
Rejestr decyzji o usunięcie drzew	Magdalena Ostalska	papierowo	szafa zamykana na klucz	Pokój 13	
Zbiór danych osobowych klientów	Bogusława Kubacak, Irena Grotek	Komputer klasy PC + dokumentacja	login i hasło / szafa zamykana na klucz	Pokój USC	PB_USC (Technika IT)
Zezwolenia na sprzedaż alkoholu	Magdalena Ostalska	papierowo	szafa zamykana na klucz	Pokój 13	
Zezwolenia na usunięcie odpadów	Magdalena Ostalska	papierowo	szafa zamykana na klucz	Pokój 13	
Gospodarka gruntami	Magdalena Ostalska	papierowo	szafa zamykana na klucz	Pokój 13	
Rejestr wymiarowy	Julianna Libera, Czarnecka Janina,	papierowo	szafa zamykana na klucz	Pokój nr 11	
Kwitariusze podatkowe	Julianna Libera	papierowo	szafa zamykana na klucz	Pokój nr 11	
Rejestr umów z dyrektorami	Agnieszka Miniak	papierowo	szafa zamykana na klucz		
Zamówienia Publiczne	Konrad Grzejszczak	elektronicznie i papierowo	szafa zamykana na klucz		Program "Zamówienia Publiczne"

Pola informacyjne (imię, nazwisko...)	Podstawa przetwarzania	Cel	gdzie przekazywane jeśli TAK	
imię i nazwisko, płeć, data i	Ustawa o ewidencji ludności i dowodach	ewidencja		
	Ustawa o ewidencji ludności i dowodach	ewidencja		
imię i nazwisko, adres	ustawa o pracownikach samorzadowych	ewidencja		
imię i nazwisko, adres	za zgodą	ewidencja		
imię i nazwisko, adres	Ustawa o podatkach	ewidencja		
imię i nazwisko, adres	Ustawa o podatkach	ewidencja		
imię i nazwisko, adres	Ustawa o podatkach	ewidencja, pobór opłat		
imię i nazwisko, adres	Ustawa o podatkach	ewidencja		
imię i nazwisko, adres	Ustawa z dnia 12 marca 200	rozliczenia		
imię i nazwisko, adres, nr konta	ustawa o pracownikach samorzadowych	ewidencja		
nazwa firmy, nip, adres	za zgodą	rozliczenia		
imię i nazwisko, adres, pesel, nip	ustawa o odpadach	rozliczenia		
imię i nazwisko, data urodzenia,	Kodeks wyborczy z 27 maja 2007	ewidencja	komisje wyborcze	
imię i nazwisko, płeć, data i	Ustawa o ewidencji ludności i dowodach	ewidencja	organy administracji publicznej	

imię i nazwisko, płeć, nr dow.,	za zgodą	PRZEKSZTAŁCENIE WNIOSKÓW	do CEIDG	
imię i nazwisko, imię ojca, data i	Ustawa o powszechnym obowiązku obrony	ewidencja	Powiatowa Komisja Lekarska w Rawie Maz.	
imię i nazwisko, imię ojca,	Ustawa o powszechnym obowiązku obrony	dla celów wojskowych	Wojskowa Komenda Uzupełnień	
imię i nazwisko, adres	za zgodą	wydania decyzji		
imię i nazwisko, data i miejsce	Kodeks Rodzinno - Opiekuńczy	ewidencja	organy administracji publicznej	
imię i nazwisko, nip, adres, regon	za zgodą	w celu wydania zezwoleń	do CEIDG	
nip, regon, adres, imię i nazwisko	za zgodą	w celu wydania zezwoleń	do CEIDG	
imię i nazwisko, imiona rodziców,	za zgodą	wydania decyzji	Starostwo Powiatowe w Rawie Maz.	
imię i nazwisko, adres	Ustawa o podatkach	do celów podatkowych i		
imie i nazwisko, adres	Ustawa o podatkach	pobieranie podatków		
imię i nazwisko, adres, pesel, nip	za zgodą	realizacja projektu	Urząd Marszałkowski w Łodzi	
nazwa, adres, tel., nip, regon, imię i	ustawa o zamówieniach publicznych	prowadzenie zamówienia		