

ZARZĄDZENIE Nr 35/2011

**Wójta Gminy Stolno
z dnia 29.04.2011 r.**

w sprawie wprowadzenia dokumentacji przetwarzania danych osobowych w Urzędzie Gminy Stolno

Działając na podstawie art. 36 § 2 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.) oraz § 3 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024) zarządzam, co następuje:

§ 1

Wprowadzam dokumentację dot. bezpieczeństwa ochrony danych osobowych przetwarzanych w Urzędzie, na którą składa się:

1. **Polityka Bezpieczeństwa Urzędu Gminy Stolno** - załącznik nr 1
2. **Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Stolno** - załącznik nr 2.

§ 2

Wdrożenie dokumentacji wskazanej w §1 powierzam Administratorowi Bezpieczeństwa Informacji, który sprawuje nadzór nad całością prawidłowej realizacji przepisów z zakresu bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy Stolno.

§ 3

Wszystkich pracowników Urzędu Gminy zobowiązuję do zapoznania się z dokumentacją wymienioną w §1 i ścisłego przestrzegania realizacji jej treści na każdym stanowisku służbowym oraz podpisania **Oświadczenia** wg wzoru stanowiącego załącznik nr 3 do niniejszego Zarządzenia.

§ 4

Pracownik Stanowiska do spraw obywatelskich i organizacyjnych Urzędu Gminy Stolno, dokument wymieniony w § 3 załączy do teczki personalnej pracowników.

§ 5

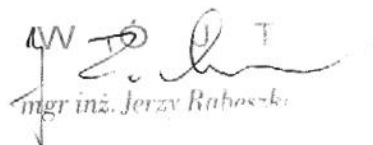
Wdrożenie dokumentacji wskazanej w §1 następuje w oparciu o harmonogram stanowiący załącznik nr 4 do niniejszego zarządzenia.

§ 6

Uchyla się §1, §2 i §5 zarządzenia Wójta Gminy Stolno z dnia 29 czerwca 2009r. w sprawie polityki bezpieczeństwa w zakresie ochrony danych osobowych w Urzędzie Gminy Stolno.

§ 7

Zarządzenie wchodzi w życie z dniem podpisania.


mgr inż. Jerzy Raboski

	Urząd Gminy Stolno	Data wydania:	29.04.2011
	Polityka Bezpieczeństwa Załącznik nr 1 do Zarządzenia Nr 35/2011 z dnia 29.04.2011 r.	Ilość stron:	Strona 1 z 89
		Wydanie:	pierwsze

POLITYKA BEZPIECZEŃSTWA

Urzędu Gminy Stolno

Stolno 2011

	Urząd Gminy Stolno	Data wydania:	29.04.2011
	Polityka Bezpieczeństwa Załącznik nr 1 do Zarządzenia Nr 35/2011 Wójta Gminy Stolno z dnia 29.04.2011 r.	Ilość stron:	Strona 2 z 89
		Wydanie:	pierwsze

SPIS TREŚCI

1.	Polityka Bezpieczeństwa Urzędu Gminy Stolno	3
1.1	Instrukcja w sprawie ochrony danych osobowych.	17
1.2	Instrukcja postępowania w sytuacji naruszenia systemu ochrony danych osobowych.	21
1.2.1	Raport z naruszenia bezpieczeństwa systemu informatycznego.	28
1.3	Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe.	30
1.4	Wykaz zbiorów danych osobowych.	32
1.5	Wykaz zbiorów danych osobowych zarejestrowanych w GODO.	33
1.6	Zgłoszenie zbioru danych do rejestracji GODO /wzór/	34
1.7	Rejestr upoważnień do przetwarzania danych osobowych.	40
1.8	Rejestr udostępnień danych osobowych.	42
1.9	Opis struktury zbiorów danych.	43
1.10	Sposób przepływu danych pomiędzy poszczególnymi systemami.	44
1.11	Wymagania bezpieczeństwa dotyczące rozwoju systemów i aplikacji.	45
1.12	Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych	48
1.13	Procedury awaryjne.	

	Urząd Gminy Stolno	Data wydania:	29.04.2011
	Polityka Bezpieczeństwa Załącznik nr 1 do Zarządzenia Nr 35/2011 Wójta Gminy Stolno z dnia 29.04.2011 r.	Ilość stron:	Strona 3 z 89
		Wydanie:	pierwsze

WPROWADZENIE

„Każdy ma prawo do ochrony dotyczących go danych osobowych”

***Art. 1. 1. Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych
(tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.)***

Powyższe stwierdzenie ujęte w treści cytowanego przepisu zostało przeniesione z założeń wyrażonych w art. 51 Konstytucji RP¹⁾ będących konsekwencją art. 47 Konstytucji RP zapewniającego każdemu obywatelowi *prawo do prywatności*.

Dla przestrzegania nienaruszalności powyższego prawa, zachowania poufności danych oraz zapewniania wysokiego poziomu bezpieczeństwa danych, zarówno w ujęciu technicznym jak i organizacyjnym w Urzędzie Gminy Stolno stosuje się politykę bezpieczeństwa przetwarzanych danych.

Wymiernym aspektem prowadzonej polityki bezpieczeństwa, jest dokument zwany „Polityka bezpieczeństwa” będący formalnym zestawem zgodnym z obowiązującym prawem, procedur i unormowań oraz praktycznych doświadczeń regulujących zasady, sposób zarządzania i postępowania, którym muszą podporządkować się zarówno pracownicy Urzędu jak i właściwe strony zewnętrzne dla osiągnięcia i zapewnienia odpowiednio wysokiego poziomu bezpieczeństwa ochrony przetwarzanych danych osobowych. Podjęte i wdrożone w Urzędzie Gminy Stolno przedsięwzięcia zmierzające do ochrony powierzonych przez obywateli swoich danych osobowych dotyczą całościowego ich zabezpieczenia na każdym stanowisku pracy, niezależnie czy są przetwarzane tradycyjnie czy w systemie informatycznym.

¹ Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. z dnia 16 lipca 1997 r. Nr 78, poz. 483; sprost. z 2001 r. Dz. U. Nr 28, poz. 319).

Art. 47. Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym

Art. 51. 1. Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby.

2. Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym.

3. Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa.

	Urząd Gminy Stolno	Data wydania:	29.04.2011
	Polityka Bezpieczeństwa Załącznik nr 1 do Zarządzenia Nr 35/2011 Wójta Gminy Stolno z dnia 29.04.2011 r.	Ilość stron:	Strona 4 z 89
		Wydanie:	pierwsze

Dokument określa, jakie zasoby (aktywa) Urzędu są chronione i jakim mogą podlegać rodzajom zagrożeniom, które w konsekwencji mogą spowodować nieobliczalne w skutkach szkody dla całego systemu i Urzędu. Dla uniknięcia takich sytuacji w instrukcjach przedstawiono, z jakimi zagrożeniami pracownicy Urzędu mogą mieć do czynienia, jak postępować, aby zapobiec wystąpieniu zagrożeń z winy pracownika a gdy już takowe wystąpią, jak w takich sytuacjach postępować.

Opisane reguły określają granice dopuszczalnego zachowania wszystkich osób mających dostęp do zasobów technologicznych i informacyjnych oraz systemów wspomagających pracę Urzędu. Odpowiednie zabezpieczenia na wysokim poziomie, ochrona przetwarzanych danych oraz niezawodność funkcjonowania systemu służącego do przetwarzania danych są podstawowym wymogiem stawianym przez kierownictwo Urzędu. Dokument zwraca również uwagę na konsekwencje, jakie mogą ponosić osoby przekraczające określone granice oraz procedury postępowania dla zapobiegania lub minimalizowania skutków zagrożeń.

Dokument „*Polityka bezpieczeństwa*” jest poddawany regularnemu przeglądowi przez Administratora Bezpieczeństwa Informacji, a w przypadku istotnych zmian jest dokonywana aktualizacja jego treści, aby zapewnić jego przydatność, adekwatność i skuteczność²⁾ w działalności Urzędu.

Niniejszy dokument został zatwierdzony przez Wójta Gminy Stolno i jest udostępniany wszystkim pracownikom Urzędu oraz właściwym stronom zewnętrznym w celu przestrzegania zawartych w nim wytycznych.

Każdy nowo przyjęty pracownik podlega obowiązkowi zapoznania się z niniejszym dokumentem opisującym prowadzoną politykę bezpieczeństwa przetwarzanych danych osobowych w Urzędzie.

² PN-ISO/IEC 27001:2007 Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji - Wymagania. s. 20

	Urząd Gminy Stolno	Data wydania:	29.04.2011
	Polityka Bezpieczeństwa Załącznik nr 1 do Zarządzenia Nr 35/2011 Wójta Gminy Stolno z dnia 29.04.2011 r.	Ilość stron:	Strona 5 z 89
		Wydanie:	pierwsze

DEFINICJE I OKREŚLENIE POJĘĆ UŻYTYCH W DOKUMENCIE

Ilekoć w niniejszym dokumencie - *Polityka Bezpieczeństwa* oraz jego załącznikach użyto określenia:

Administrator Bezpieczeństwa Informacji (ABI) – należy przez to rozumieć osobę wyznaczoną przez Administratora danych, która odpowiedzialna jest za bezpieczeństwo przetwarzanych danych w Urzędzie.

Administrator danych – należy rozumieć przez to organ, jednostkę organizacyjną, podmiot lub osobę decydującą o celach i środkach przetwarzania danych osobowych. W tekście niniejszego dokumentu określa Wójt Gminy Stolno.

Administrator Systemu Informatycznego – rozumie się przez to osobę powołaną do zarządzania oprogramowaniem i siecią informatyczną Urzędu. Z uwagi na specyfikę Urzędu jest nim informatyk obsługujący system informatyczny Urzędu.

Aplikacja systemowa – specjalistyczne oprogramowanie dedykowane dla danej komórki organizacyjnej lub spełniające określone funkcje użytkowe.

Dostępność – oznacza właściwość, że przetwarzane dane osobowe są dostępne i użyteczne na żądanie upoważnionego podmiotu³⁾.

(czyli ochrona przed ich chwilową lub trwałą utratą)

GIODO – Generalny Inspektor Ochrony Danych Osobowych.

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

Kierownictwo Urzędu – należy przez to rozumieć osobę nadzorującą pracę Urzędu Gminy Stolno (Wójt, Sekretarz Gminy, Skarbnik)

Kierownik komórki organizacyjnej - należy przez to rozumieć osobę nadzorującą pracę komórki organizacyjnej Urzędu Gminy Stolno, a także osobę upoważnioną do wykonywania jej zadań.

³ Tamże

	Urząd Gminy Stolno	Data wydania:	29.04.2011
	Polityka Bezpieczeństwa Załącznik nr 1 do Zarządzenia Nr 35/2011 Wójta Gminy Stolno z dnia 29.04.2011 r.	Ilość stron:	Strona 6 z 89
		Wydanie:	pierwsze

Komórka organizacyjna – należy przez to rozumieć wydzieloną organizacyjnie część Urzędu. W strukturze organizacyjnej Urzędu jest nią Referat, samodzielne Stanowisko.

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

Integralność danych – oznacza właściwość zapewniającą, że dane osobowe przetwarzane w Urzędzie nie zostaną zmienione lub zniszczone w sposób nieautoryzowany⁴.

(czyli ochrona przed celową lub przypadkową modyfikacją danych osobowych)

Odbiorcy danych - rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:

- a) osoby, której dane dotyczą,
- b) osoby upoważnionej do przetwarzania danych,
- c) przedstawiciela, o którym mowa w art. 31a,
- d) podmiotu, o którym mowa w art. 31,
- e) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

Państwie trzecim - rozumie się przez to państwo nienależące do Europejskiego Obszaru Gospodarczego⁵.

Poufność danych – oznacza właściwość zapewniającą, że dane osobowe nie są udostępniane lub ujawniane nieupoważnionym osobom lub podmiotom⁶.

(czyli ochrona przed kradzieżą danych osobowych)

Pracownik - osoba, z którą Urząd nawiązał stosunek pracy na podstawie umowy o pracę, praktykant i stażysta odbywający praktykę lub staż, również z którym Urząd podpisał umowę o dzieło lub umowę zlecenia.

⁴ Tamże

⁵ Europejski Obszar Gospodarczy tworzą państwa członkowskie Unii Europejskiej oraz trzy państwa członkowskie tworzące Europejskie Stowarzyszenie Wolnego Handlu (Islandia, Lichtenstein i Norwegia), które dostosowały część swojego ustawodawstwa do prawa Wspólnot Europejskich i wobec tego są traktowane jak państwa członkowskie Unii Europejskiej.

⁶ Tamże

	Urząd Gminy Stolno	Data wydania:	29.04.2011
	Polityka Bezpieczeństwa Załącznik nr 1 do Zarządzenia Nr 35/2011 Wójta Gminy Stolno z dnia 29.04.2011 r.	Ilość stron:	Strona 7 z 89
		Wydanie:	pierwsze

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

Rejestr Zbiorów - rejestr zbiorów danych osobowych przetwarzanych w Urzędzie.

Rejestr Upoważnień – rejestr wydanych i wycofanych *Upoważnień do przetwarzania danych osobowych*.

Rozliczalność — rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

Sieć informatyczna – to należy rozumieć organizacyjne i techniczne połączenie systemu informatycznego.

System informatyczny – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

Teletransmisja — rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej.

Urząd – należy przez to rozumieć Urząd Gminy Stolno.

Usuwanie danych – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,

Uwierzytelnianie — rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

Użytkownik - pracownik Urzędu Gminy Stolno, posiadający uprawnienia do pracy w systemie informatycznym zgodnie z zakresem obowiązków służbowych.

Zabezpieczenie danych w Systemie informatycznym – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.

	Urząd Gminy Stolno	Data wydania:	29.04.2011
	Polityka Bezpieczeństwa	Ilość stron:	Strona 8 z 89
	Załącznik nr 1 do Zarządzenia Nr 35/2011 Wójta Gminy Stolno z dnia 29.04.2011 r.	Wydanie:	pierwsze

Zasoby (aktywa) – oznacza wszystko, co ma wartość dla Urzędu⁷.

Zbiór danych – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie, czy zautomatyzowany, czy niezautomatyzowany (manualny, tradycyjny). Zbiorem danych będą m.in. ręczne zbiory ewidencyjne, akta (teczki, kartoteki) osobowe, a także znormalizowane materiały w postaci formularzy, kwestionariusze, z wyjątkiem akt nieposiadających żadnego strukturalnego układu danych osobowych.

Zgłoszenie – należy rozumieć czynność związaną z przesłaniem informacji, (za pośrednictwem poczty elektronicznej lub poczty tradycyjnej), Generalnemu Inspektorowi Ochrony Danych Osobowych, w związku z rejestracją lub zmianą (aktualizacją) we wcześniej zarejestrowanym zbiorze danych osobowych.

⁷ PN-I-13335-1:1999 Technika informatyczna - Wytyczne do zarządzania bezpieczeństwem systemów informatycznych - Pojęcia i modele bezpieczeństwa systemów informatycznych. s. 6 i następne.

	Urząd Gminy Stolno	Data wydania:	29.04.2011
	Polityka Bezpieczeństwa Załącznik nr 1 do Zarządzenia Nr 35/2011 Wójta Gminy Stolno z dnia 29.04.2011 r.	Ilość stron:	Strona 9 z 89
		Wydanie:	pierwsze

ROZDZIAŁ I

OCHRONA DANYCH OSOBOWYCH

1. Administratorem danych zawartych i przetwarzanych w systemach manualnych i informatycznych Urzędu Gminy Stolno jest Wójt.
2. Zgodnie z uprawnieniem wynikającym z art. 36 ust. 3 ustawy⁸⁾ Wójt Gminy, Zarządzeniem Nr 35/2011 z dnia 29.04.2011 roku wyznaczył Administratora Bezpieczeństwa Informacji (w skrócie ABI) w Urzędzie Gminy Stolno, odpowiedzialnego za nadzorowanie przestrzegania zasad ochrony i bezpieczeństwa przetwarzanych danych osobowych w Urzędzie.
3. Administrator danych jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających odpowiedni poziom bezpieczeństwa ochrony przetwarzanych danych w systemach manualnych i informatycznych Urzędu, a w szczególności:
 - a) zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym,
 - b) zapobiegać przed zabraniem danych przez osobę nieuprawnioną,
 - c) zapobiegać przetwarzaniu danych z naruszeniem ustawy⁹⁾ oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych.
4. Do zastosowanych środków technicznych zapewniających bezpieczeństwa przetwarzanych danych należy:
 - a) przetwarzanie danych osobowych w odpowiednio zabezpieczonych pomieszczeniach,
 - b) monitorowanie obiektu za pośrednictwem czujników ruchu pracujących w paśmie

⁸⁾ Ustawa z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. Nr 101, poz.926, Dz. U. Nr 153, poz.1271; zm. z 2004 r. Dz. U. Nr 25, poz. 219, Dz. U. Nr 33, poz. 285; zm. z 2006 r. Dz. U. Nr 104, poz. 708, Dz. U. Nr 104, poz.711; zm. z 2007 r. Dz. U. Nr 165, poz.1170, Dz. U. Nr 176, poz.1238; zm. z 2010 r. Dz. U. Nr 41, poz. 233)

⁹⁾ patrz przypis nr 7

	Urząd Gminy Stolno	Data wydania:	29.04.2011
	Polityka Bezpieczeństwa Załącznik nr 1 do Zarządzenia Nr 35/2011 Wójta Gminy Stolno z dnia 29.04.2011 r.	Ilość stron:	Strona 10 z 89
		Wydanie:	pierwsze

podczerwieni oraz kamer na zewnątrz obiektu z rejestracją obrazu,

- c) szczególne zabezpieczenie kluczowych urządzeń infrastruktury informatycznej Urzędu (serwery, switchy, firewalle) poprzez zastosowanie zaawansowanego systemu kontroli dostępu oraz zalecanego systemu ochrony przeciwpożarowej dla urządzeń elektronicznych,
- d) podłączenie urządzeń infrastruktury informatycznej do systemu podtrzymywania zasilania,
- e) wyposażenie pomieszczeń w szafy metalowe lub meblowe zamykane na zamki, w których po zakończonej pracy przechowywane są wszystkie zbiory w postaci papierowej tzn. kartotek, skorowidzów, spisów, wykazów itp., dające gwarancję bezpieczeństwa tej dokumentacji,
- f) obowiązek sporządzania kopii awaryjnych i przechowywanie ich w metalowej szafie w bezpiecznym pomieszczeniu poza pomieszczeniem serwerowni,
- g) dokumenty papierowe zawierające dane osobowe niszczone są przy pomocy niszczarki o co najmniej 3-im stopniu utajenia według Normy DIN 32757¹⁰⁾.

5. Do zastosowanych środków organizacyjnych zapewniających ochronę przetwarzanych danych należy:

- a) zapoznanie każdej osoby z przepisami dotyczącymi ochrony danych osobowych oraz z treścią niniejszego dokumentu przed dopuszczeniem jej do pracy przy przetwarzaniu danych osobowych,
- b) przeszkolenie osób, o których mowa w pkt. a), w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochroną danych osobowych,
- c) uniemożliwienie pracy w zakresie przetwarzania danych osobowych osobom

¹⁰⁾ DIN (skrót: Deutsches Institut für Normung) Niemiecki Instytut Normalizacyjny.

Niemiecka norma przemysłowa DIN (pomimo, iż norma ta nie jest oficjalnie uznawana na terytorium RP to została przyjęta za pewien wzór, a wszystkie na świecie urządzenia do niszczenia dokumentów produkowane są tak aby spełniały wymagania powyższej normy) w zakresie charakterystyki poziomów bezpieczeństwa (stopni utajnienia) reguluje wielkość mechanicznie zniszczonych papierowych nośników danych. Norma DIN 32757 określa 6 stopni bezpieczeństwa w zależności od wielkości ścinka, jaki powstaje w procesie niszczenia. Im wyższy stopień bezpieczeństwa tym mniejsze prawdopodobieństwo odczytania zniszczonych danych.

Wszelkie dokumenty poufne, do których należy zaliczyć dane i dokumentację osobową muszą być niszczone w niszczarkach o 3 stopniu utajnienia, natomiast wszelkie błędnie sporządzone kopie, bądź wydruki komputerowe można niszczyć niszczarką o 2 stopniu utajnienia.

	Urząd Gminy Stolno	Data wydania:	29.04.2011
	Polityka Bezpieczeństwa Załącznik nr 1 do Zarządzenia Nr 35/2011 Wójta Gminy Stolno z dnia 29.04.2011 r.	Ilość stron:	Strona 11 z 89
		Wydanie:	pierwsze

nie posiadających imiennego upoważnienia Administratora danych,

- d) ewidencja dostępu do pomieszczeń, w których są przetwarzane dane osobowe, polegająca na monitorowaniu otwierania i zamykania pomieszczeń,
- e) nie pozostawianie pomieszczeń niezabezpieczonych bez nadzoru pracownika w czasie godzin pracy,
- f) przyjęcie polityki „czystego biurka” w odniesieniu do dokumentów papierowych i nośników informacji zawierających dane osobowe oraz polityki „czystego ekranu” dla urządzeń do przetwarzania danych, celem ograniczenia wystąpienia ryzyka nieuprawnionego dostępu, utraty bądź uszkodzenia informacji zarówno w czasie normalnych godzin pracy jak i poza nimi,
- g) opracowanie i wdrożenie instrukcji postępowania dla ochrony przed zniszczeniami powstałymi na skutek pożaru, wybuchu, zalanie, niepokojów społecznych i innych form naturalnych lub spowodowanych przez człowieka katastrof.

6. Niezależnie od niniejszych zasad opisanych w dokumencie „*Polityka Bezpieczeństwa*” w zakresie bezpieczeństwa mają zastosowanie wszelkie wewnętrzne regulaminy lub instrukcje dotyczące bezpieczeństwa ludzi i zasobów informacyjnych oraz indywidualne zakresy zadań osób zatrudnionych przy przetwarzaniu danych osobowych w określonym systemie. Dokumenty te nie mogą być sprzeczne z regulacjami określonymi w „*Polityce Bezpieczeństwa*”.

7. Prawidłowość realizacji przepisów w zakresie ochrony danych osobowych przetwarzanych w Urzędzie określa „*Instrukcja w sprawie ochrony danych osobowych*” stanowiąca załącznik nr 1 do niniejszego dokumentu.

	Urząd Gminy Stolno	Data wydania:	29.04.2011
	Polityka Bezpieczeństwa	Ilość stron:	Strona 12 z 89
	Załącznik nr 1 do Zarządzenia Nr 35/2011 Wójta Gminy Stolno z dnia 29.04.2011 r.	Wydanie:	pierwsze

ROZDZIAŁ II

ZDARZENIA NARUSZAJĄCE OCHRONĘ DANYCH OSOBOWYCH

Rozpatrując zagadnienie bezpieczeństwa przetwarzanych danych w Urzędzie nie można pominąć zagrożeń mogących negatywnie wpłynąć na zasoby Urzędu powodując poważne straty. Zagrożenia mogą mieć swoje źródło w naturalnych przyczynach lub w działaniach ludzi (pracownikach Urzędu lub petentach), które mogą być przypadkowe lub umyślne. Zagrożenia można podzielić na:

1. Zagrożenia ludzkie

- a. **rozmyślne** (np.: modyfikacja danych, włamanie do systemu, złośliwy kod, kradzież itp.).

W wyniku takiego działania może dojść do zniszczenia danych i zakłócenia ciągłości pracy systemu.

Następuje naruszenie poufności i integralności danych.

- b. **przypadkowe** (np.: niezamierzone pomyłki i pominięcia, nieprawidłowe skierowanie czy skasowanie pliku - popełnione przez administratorów i operatorów, przerwy w zasilaniu).

Działania te mogą prowadzić do utraty integralności danych.

2. Zagrożenia techniczne (np.: błędy w działającym oprogramowaniu, wadliwa praca urządzeń sprzętowych, itp.).

Może dojść do zakłócenia ciągłości pracy systemu lub utraty danych.

3. Zagrożenia środowiskowe (np.: trzęsienie ziemi, powódź, pożar, piorun - wyładowania atmosferyczne).

Sytuacje takie powodują zniszczenia i uszkodzenia infrastruktury technicznej systemu, ciągłość systemu zostaje zakłócona.

Naruszona zostaje integralność danych i integralność systemu.

W przypadku naruszenia systemu ochrony danych osobowych w Urzędzie, każdy pracownik Urzędu zobowiązany jest do stosowania zapisów postanowień *Instrukcji postępowania w przypadku naruszenia systemu ochrony danych osobowych* stanowiącej załącznik nr 2.

	Urząd Gminy Stolno	Data wydania:	29.04.2011
	Polityka Bezpieczeństwa Załącznik nr 1 do Zarządzenia Nr 35/2011 Wójta Gminy Stolno z dnia 29.04.2011 r.	Ilość stron:	Strona 13 z 89
		Wydanie:	pierwsze

ROZDZIAŁ III

KONTROLA PRZESTRZEGANIA ZASAD ZABEZPIECZENIA DANYCH OSOBOWYCH

1. Administrator danych przeprowadza nie rzadziej niż raz na dwa lata przeglądy systemu zarządzania bezpieczeństwem informacji¹¹⁾ i sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych wynikających z Ustawy o ochronie danych osobowych¹²⁾ oraz zasad ustanowionych w niniejszym dokumencie.
2. Zadania wymienione w ust. 1 Administrator danych wykonuje za pośrednictwem Administratora Bezpieczeństwa Informacji (ABI).
3. Administrator Bezpieczeństwa Informacji sporządza i przedstawia Wójtowi nie rzadziej niż raz w roku raport dotyczący stanu bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy.
4. Raport, o którym mowa w pkt. 3 powinien zawierać wnioski i propozycje dotyczące spraw bezpieczeństwa, w tym:
 - a) wskazania niedociągnięć lub zaniedbań,
 - b) dokonania koniecznych zabezpieczeń oraz niezbędnych doposażeń,
 - c) wprowadzenia nowych lub znowelizowaniu istniejących w Urzędzie procedur działania,
 - d) sposób podnoszenia wiedzy w zakresie bezpieczeństwa danych osobowych przez pracowników,
 - e) sposób prowadzenia dzienników systemów.

¹¹⁾ PN-ISO/IEC 27001:2007 Technika ... op. cit.

¹²⁾ patrz przypis 3

	Urząd Gminy Stolno	Data wydania:	29.04.2011
	Polityka Bezpieczeństwa Załącznik nr 1 do Zarządzenia Nr 35/2011 Wójta Gminy Stolno z dnia 29.04.2011 r.	Ilość stron:	Strona 14 z 89
		Wydanie:	pierwsze

ROZDZIAŁ IV

POSTANOWIENIA KOŃCOWE

1. Przypadki, nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu będą potraktowane jako ciężkie naruszenie obowiązków pracowniczych. Wobec osoby, która w przypadku naruszenia bezpieczeństwa danych 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, będzie wdrożony formalny proces postępowania dyscyplinarnego.
2. Osoby, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych, potwierdzają ten fakt poprzez podpisanie *Oświadczenia* wg wzoru stanowiącego załącznik nr 3 do Zarządzenia Nr 35/2011 Wójta Gminy Stolno z dnia 29.04.2011 roku wprowadzającego dokumentację przetwarzania danych osobowych w Urzędzie Gminy Stolno. *Oświadczenia* takie przechowywane są w aktach personalnych pracownika.
3. Orzeczona kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych¹³⁾ oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
4. Wszystkie regulacje dotyczące systemów informatycznych określone w „*Polityce Bezpieczeństwa*” dotyczą również przetwarzania danych osobowych w bazach prowadzonych w każdej innej formie.

¹³⁾ patrz przypis 3

	Urząd Gminy Stolno	Data wydania:	29.04.2011
	Polityka Bezpieczeństwa Załącznik nr 1 do Zarządzenia Nr 35/2011 Wójta Gminy Stolno z dnia 29.04.2011 r.	Ilość stron:	Strona 15 z 89
		Wydanie:	pierwsze

5. Wdrożenie „*Polityki Bezpieczeństwa*” odbywa się na podstawie planu opracowanego przez ABI, który zawiera w szczególności:

- zakres, sposób i czas zapoznania się pracowników z „*Polityką Bezpieczeństwa*”,
- terminarz szkoleń z zakresu wprowadzanych procedur,
- terminarz szkoleń stanowiskowych,
- terminarz wprowadzenia do stosowania poszczególnych elementów „*Polityki Bezpieczeństwa*”,
- termin kontroli stosowania wszystkich postanowień wprowadzonych „*Polityką Bezpieczeństwa*”,
- sprawdzenie funkcjonowania procedur poprzez symulację jednego z zagrożeń określonych w „*Instrukcji postępowania w sytuacji naruszenia systemu ochrony danych osobowych*” stanowiącej załącznik nr 2 do niniejszego dokumentu,
- analizę zgodności innych wewnętrznych aktów prawa z „*Polityką Bezpieczeństwa*”, a w przypadku stwierdzonych niezgodności - harmonogram dostosowania ich postanowień do wymogów „*Polityki Bezpieczeństwa*”,
- zestawienie zawierające potrzeby w zakresie dostosowania struktury organizacyjnej oraz stosowanego sprzętu i oprogramowania.

6. Plan, o którym mowa w pkt 5 stanowi załącznik nr 4 do Zarządzenia nr 35/2011 r. Wójta Gminy Stolno z dnia 29.04.2011r.

	Urząd Gminy Stolno	Data wydania:	29.04.2011
	Polityka Bezpieczeństwa	Ilość stron:	Strona 16 z 89
	Załącznik nr 1 do Zarządzenia Nr 35/2011 Wójta Gminy Stolno z dnia 29.04.2011 r.	Wydanie:	pierwsze

WYKAZ ZAŁĄCZNIKÓW DO POLITYKI BEZPIECZEŃSTWA

załącznik nr 1	Instrukcja w sprawie ochrony danych osobowych.
załącznik nr 2	Instrukcja postępowania w sytuacji naruszenia systemu ochrony danych osobowych
załącznik nr 3	Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe
załącznik nr 4	Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych
załącznik nr 5	Wykaz zbiorów danych osobowych zarejestrowanych w GODO
załącznik nr 6	Zgłoszenie zbioru danych do rejestracji GODO /wzór/
załącznik nr 7	Rejestr upoważnień do przetwarzania danych osobowych
załącznik nr 8	Rejestr udostępnień danych osobowych
załącznik nr 9	Opis struktury zbiorów danych
załącznik nr 10	Wymagania bezpieczeństwa dotyczące rozwoju systemów i aplikacji
załącznik nr 11	Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych
załącznik nr 12	Procedury awaryjne

	Urząd Gminy Stolno	Data wydania:	29.04.2011
	Załącznik nr 1 do Polityki Bezpieczeństwa Urzędu Gminy Stolno	Ilość stron:	Strona 17 z 89
		Wydanie:	pierwsze

INSTRUKCJA

w sprawie ochrony danych osobowych

§ 1

Przetwarzanie danych osobowych pozostających w zbiorach Urzędu Gminy Stolno, służy realizacji zadań wynikających z Ustawy o samorządzie gminnym¹⁾ oraz innych zadań powierzonych.

§ 2

1. Administratorem danych w rozumieniu ustawy o ochronie danych osobowych²⁾ jest Gmina Stolno, reprezentowana przez organ wykonawczy, którym jest Wójt Gminy.
2. Zgodnie z treścią art. 36 ust. 3 ustawy³⁾, Wójt wyznacza Administratora Bezpieczeństwa Informacji, który jest odpowiedzialny za nadzorowanie przestrzegania ochrony i bezpieczeństwa przetwarzanych danych w systemach informatycznych oraz w formie papierowej w Urzędzie Gminy Stolno.

§ 3

1. Administrator Bezpieczeństwa Informacji zobowiązany jest do osobistego prowadzenia:
 - a) *Wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym*

¹⁾ Ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (tekst jednolity Dz. U z 2001 r. Nr 142, poz. 1591, zm. z 2002 r. Dz. U. Nr 23, poz. 220, Dz. U. Nr 62, poz. 558, Dz. U. Nr 113, poz. 984, Dz. U. Nr 153, poz. 1271, Dz. U. Nr 214, poz. 1806; zm. z 2003 r. Dz. U. Nr 80, poz. 717, Dz. U. Nr 162, poz. 1568; zm. z 2004 r. Dz. U. Nr 102, poz. 1055, Dz. U. Nr 116, poz. 1203, Dz. U. Nr 167, poz. 1759; zm. z 2005 r. Dz. U. Nr 172, poz. 1441, Dz. U. Nr 175, poz. 1457; zm. z 2006 r. Dz. U. Nr 7, poz. 128, Dz. U. Nr 181, poz. 1337; zm. z 2007 r. Dz. U. Nr 48, poz. 327, Dz. U. Nr 138, poz. 974, Dz. U. Nr 173, poz. 1218; zm. z 2008 r. Dz. U. Nr 180, poz. 1111, Dz. U. Nr 223, poz. 1458; zm. z 2009 r. Dz. U. Nr 52, poz. 420, Dz. U. Nr 157, poz. 1241, zm. z 2010 r. Dz. U. Nr 28, poz. 142 i 146, Dz. U. Nr 40, poz. 230, Dz. U. Nr 106, poz. 675).

²⁾ art. 7 pkt.4 - Ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926, Dz. U. Nr 153, poz. 1271; zm. z 2004 r. Dz. U. Nr 25, poz. 219, Dz. U. Nr 33, poz. 285; zm. z 2006 r. Dz. U. Nr 104, poz. 708, Dz. U. Nr 104, poz. 711; zm. z 2007 r. Dz. U. Nr 165, poz. 1170, Dz. U. Nr 176, poz. 1238; zm. z 2010 r. Dz. U. Nr 41, poz. 233)

³⁾ Ustawa z dnia 29 sierpnia 1997 roku o ochronie danych ... op. cit.

	Urząd Gminy Stalno	Data wydania:	29.04.2011
	Załącznik nr 1 do Polityki Bezpieczeństwa Urzędu Gminy Stalno	Ilość stron:	Strona 18 z 89
		Wydanie:	pierwsze

przetwarzane są dane osobowe zgodnie z załącznikiem nr 3 do Polityki Bezpieczeństwa,
Zgodnie z ustawą o ochronie danych osobowych⁴ obszar przetwarzania danych obejmuje:

- miejsca, w których wykonuje się operacje na danych osobowych,
- miejsca, gdzie przechowuje się nośniki informacji zawierające dane osobowe:
 - szafy z dokumentacją papierową,
 - szafy zawierające komputerowe nośniki informacji z kopiami zapasowymi danych,
 - stacje komputerowe,
 - serwery,
 - dyski przenośne, na których przechowywane są kopie awaryjne przetwarzanych danych,
 - elementy aktywne sieci,
 - okablowanie sieciowe,
- miejsca, gdzie gromadzone są uszkodzone komputerowe nośniki danych:
 - taśmy,
 - dyski,
 - płyty CD, DVD,
 - uszkodzone komputery,
 - inne urządzenia z nośnikami obejmującymi dane osobowe,
 - archiwum.

b) *Wykazu zbiorów danych osobowych zgodnie z załącznikiem nr 4 do Polityki Bezpieczeństwa,*

c) *Wykazu zbiorów danych osobowych zarejestrowanych w GODO zgodnie z załącznikiem nr 5 do Polityki Bezpieczeństwa,*

d) *Rejestru upoważnień do przetwarzania danych osobowych zgodnie z załącznikiem nr 7 do Polityki Bezpieczeństwa,*

⁴ patrz przypis nr 3

	Urząd Gminy Stolno	Data wydania:	29.04.2011
	Załącznik nr 1 do Polityki Bezpieczeństwa Urzędu Gminy Stolno	Ilość stron:	Strona 19 z 89
		Wydanie:	pierwsze

Obok pracowników przetwarzających dane osobowe, w związku z zatrudnieniem ich na stanowisku, na którym rutynowo w efekcie wykonywania obowiązków wynikających ze stosunku pracy dane te są przetwarzane, upoważnienia powinni otrzymać także m. in:

- osoby z kierownictwa Urzędu,
- informatyk i pracownik pełniący funkcję Administratora Bezpieczeństwa Informacji,
- osoby wykonujące pracę na podstawie umowy zlecenia lub umowy o dzieło związane z dostępem do danych osobowych przetwarzanych w Urzędzie. Szczególnie należy zwrócić uwagę na monitorowanie dostępu do tych danych w przypadku wykonywania prac wdrożeniowych, czy serwisowych systemu informatycznego,
- praktykanci, stażyści, jeżeli ich zajęcie może się wiązać z przetwarzaniem danych osobowych.

e) *Rejestru udostępnień danych osobowych zgodnie z załącznikiem nr 8 do Polityki Bezpieczeństwa.*

2. Zobowiązuje się pracownika Stanowiska d/s. obywatelskich i organizacyjnych Urzędu Gminy Stolno do uzupełniania akt osobowych pracowników zatrudnionych przy przetwarzaniu danych osobowych o *Oświadczenia*, że zapoznali się z przepisami obowiązującymi w tym zakresie.
3. Udostępnianie danych osobowych pozostających w bazach danych Urzędu do celów innych niż określone w § 1 niniejszej *Instrukcji*, odbywa się wyłącznie po uprzednim uzyskaniu zgody Wójta Gminy Stolno.

§ 4

Osoby nieprzestrzegające przepisów w zakresie ochrony danych osobowych podlegają,

	Urząd Gminy Stolno	Data wydania:	29.04.2011
	Załącznik nr 1 do Polityki Bezpieczeństwa Urzędu Gminy Stolno	Ilość stron:	Strona 20 z 89
		Wydanie:	pierwsze

niezależnie od odpowiedzialności wynikającej z Kodeksu pracy⁵⁾, sankcjom przewidzianym w rozdziale 8 Ustawy o ochronie danych osobowych⁶⁾ oraz przepisom karnym zawartych w innych przepisach szczególnych w tym zakresie.

§ 5

Instrukcja dotyczy w równym stopniu przetwarzania danych w systemach innych niż informatyczne.

⁵ Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy – (tekst jednolity Dz. U. z 1998 r. Nr 21, poz. 94; zm. z 1998 r. Dz. U. Nr 106, poz. 668, Dz. U. Nr 113, poz. 717; zm. z 1999 r. Dz. U. Nr 99, poz. 1152; zm. z 2000 r. Nr 19, poz. 239, Dz. U. Nr 43, poz. 489, Dz. U. Nr 107, poz. 1127, Dz. U. Nr 120, poz. 1268; zm. z 2001 r. Dz. U. Nr 11, poz. 84, Dz. U. Nr 28, poz. 301, Dz. U. Nr 52, poz. 538, Dz. U. Nr 99, poz. 1075, Dz. U. Nr 111, poz. 1194, Dz. U. Nr 123, poz. 1354, Dz. U. Nr 128, poz. 1405, Dz. U. Nr 154, poz. 1805; zm. z 2002 r. Dz. U. Nr 74, poz. 676, Dz. U. Nr 135, poz. 1146, Dz. U. Nr 196, poz. 1660, Dz. U. Nr 199, poz. 1673, Dz. U. Nr 200, poz. 1679; zm. z 2003 r. Dz. U. Nr 166, poz. 1608, Dz. U. Nr 213, poz. 2081; zm. z 2004 r. Dz. U. Nr 96, poz. 959, Dz. U. Nr 99, poz. 1001, Dz. U. Nr 120, poz. 1252, Dz. U. Nr 240, poz. 2407; zm. z 2005 r. Dz. U. Nr 10, poz. 71, Dz. U. Nr 68, poz. 610, Dz. U. Nr 86, poz. 732, Dz. U. Nr 167, poz. 1398; zm. z 2006 r. Dz. U. Nr 104, poz. 708 i 711, Dz. U. Nr 133, poz. 935, Dz. U. Nr 217, poz. 1587, Dz. U. Nr 221, poz. 1615; zm. z 2007 r. Dz. U. Nr 64, poz. 426, Dz. U. Nr 89, poz. 589, Dz. U. Nr 176, poz. 1239, Dz. U. Nr 181, poz. 1288, Dz. U. Nr 225, poz. 1672; zm. z 2008 r. Dz. U. Nr 93, poz. 586, Dz. U. Nr 223, poz. 1460, Dz. U. Nr 237, poz. 1654; zm. z 2009 r. Dz. U. Nr 6, poz. 33, Dz. U. Nr 56, poz. 458, Dz. U. Nr 58, poz. 485, Dz. U. Nr 98, poz. 817, Dz. U. Nr 99, poz. 825, Dz. U. Nr 115, poz. 958, Dz. U. Nr 157, poz. 1241, Dz. U. Nr 219, poz. 1704; zm. z 2010 r. Dz. U. Nr 105, poz. 655, Dz. U. Nr 135, poz. 912, Dz. U. Nr 182, poz. 1228)

⁶ Patrz przypis 3

	Urząd Gminy Stolno	Data wydania:	29.04.2011
	Załącznik nr 2 do Polityki Bezpieczeństwa Urzędu Gminy Stolno	Ilość stron:	Strona 21 z 89
		Wydanie:	pierwsze

INSTRUKCJA

postępowania w sytuacji naruszenia systemu ochrony danych osobowych

§ 1

Instrukcja jest przeznaczona dla osób zatrudnionych przy przetwarzaniu danych osobowych w Urzędzie Gminy Stolno.

§ 2

Instrukcja określa tryb postępowania w przypadku, gdy:

1. stwierdzono naruszenie zabezpieczenia systemu informatycznego lub naruszenie zabezpieczenia zbioru danych osobowych zebranych i przetwarzanych w innej formie.
2. stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej, mogą wskazywać na naruszenie zabezpieczeń tych danych.

§ 3

1. Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe to głównie:
 - a) **sytuacje losowe lub nieprzewidziane** oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.,
 - b) **niewłaściwe parametry środowiska**, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje

	Urząd Gminy Stolno	Data wydania:	29.04.2011
	Załącznik nr 2 do Polityki Bezpieczeństwa Urzędu Gminy Stolno	Ilość stron:	Strona 22 z 89
		Wydanie:	pierwsze

pochodzące od urządzeń przemysłowych,

- c) **awaria sprzętu lub oprogramowania**, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru,
- d) **pojawienie się odpowiedniego komunikatu alarmowego** od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,
- e) **jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego** wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
- f) **naruszenie lub próba naruszenia** integralności systemu lub bazy danych w tym systemie,
- g) **stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych** bez odpowiedniego upoważnienia (autoryzacji),
- h) **niedopuszczalna manipulacja** danymi osobowymi w systemie,
- i) **ujawnienie osobom nieupoważnionym** danych osobowych lub objętych tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń,
- j) **praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa** od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych - np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.,
- k) **ujawnienie istnienia nieautoryzowanych kont dostępu** do danych lub tzw. "bocznej furtki", itp.,
- l) **podmniczenie lub zniszczenie nośników z danymi** osobowymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane osobowe,
- m) **rażące naruszenie dyscypliny pracy** w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.).

	Urząd Gminy Stolno	Data wydania:	29.04.2011
	Załącznik nr 2 do Polityki Bezpieczeństwa Urzędu Gminy Stolno	Ilość stron:	Strona 23 z 89
		Wydanie:	pierwsze

2. Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydruki), kliszy, folii, zdjęciach, dyskiecie w formie niezabezpieczonej itp.

§ 4

1. Każda osoba zatrudniona w Urzędzie, która stwierdzi lub podejrzewa naruszenie zabezpieczenia ochrony danych osobowych w systemie informatycznym (lub przetwarzanych w inny sposób), powinna niezwłocznie poinformować o tym osobę zatrudnioną przy przetwarzaniu tych danych, bezpośredniego przełożonego oraz Administratora Bezpieczeństwa Informacji.
2. Osoba zatrudniona przy przetwarzaniu danych osobowych, która uzyskała informację lub sama stwierdziła naruszenie zabezpieczenia bazy danych osobowych, zobowiązana jest niezwłocznie powiadomić o tym Administratora Bezpieczeństwa Informacji.

§ 5

1. Dane osobowe zostają ujawnione, gdy stają się znane w całości lub części pozwalającej na określenie osobom nieuprawnionym tożsamości osoby, której dane dotyczą.
2. W stosunku do danych, które zostały zagubione, pozostawione bez nadzoru poza obszarem bezpieczeństwa należy przeprowadzić postępowanie wyjaśniające, czy dane osobowe należy uznać za ujawnione.

§ 6

Niezwłocznie po uzyskaniu informacji o naruszeniu danych osobowych należy podjąć działania w celu powstrzymania lub ograniczenia dostępu do danych przez osoby niepowołane, poprzez:

- a) fizyczne odłączenie urządzeń i segmentów sieci, które mogły umożliwić dostęp do bazy danych osobie nieuprawnionej,

	Urząd Gminy Stolno	Data wydania:	29.04.2011
	Załącznik nr 2 do Polityki Bezpieczeństwa Urzędu Gminy Stolno	Ilość stron:	Strona 24 z 89
		Wydanie:	pierwsze

- b) wylogowanie użytkownika podejrzanego o naruszenie zabezpieczenia ochrony danych,
- c) zmianę hasła dla konta użytkownika, poprzez które uzyskano nielegalny dostęp w celu uniknięcia ponownej próby włamania,
- d) zamknięcie i opieczętowanie urządzeń, w których przechowywane są dane osobowe w formie analogowej,
- e) podjęcie innych stosownych do zagrożenia działań.

§ 7

1. Do czasu przybycia ABI na miejsce naruszenia ochrony danych osobowych, nie należy opuszczać bez uzasadnionej potrzeby miejsca zdarzenia, oraz:
 - a) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców,
 - b) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
 - c) zaniechać, o ile to możliwe, dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,
 - d) podjąć inne działania przewidziane i określone w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących naruszeniu,
 - e) podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej,
 - f) zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku,
 - g) udokumentować wstępnie zaistniałe naruszenie,
2. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych, Administrator Bezpieczeństwa Informacji:
 - a) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy Urzędu,

	Urząd Gminy Stolno	Data wydania:	29.04.2011
	Załącznik nr 2 do Polityki Bezpieczeństwa Urzędu Gminy Stolno	Ilość stron:	Strona 25 z 89
		Wydanie:	pierwsze

- b) może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
- c) rozważa celowość i potrzebę powiadomienia o zaistniałym naruszeniu Administratora danych,
- d) nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba, ze specjalistami spoza Urzędu.

§ 8

ABI, po uzyskaniu informacji o naruszeniu danych osobowych, powinien w pierwszej kolejności:

- a) zapisać wszelkie informacje związane z danym zdarzeniem,
- b) na bieżąco wygenerować i wydrukować wszystkie możliwe dokumenty i raporty, które mogą pomóc w ustaleniu okoliczności zdarzenia,
- c) przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, zwłaszcza do określenia skali zniszczeń i metody dostępu do danych osoby niepowołanej,
- d) wyniki postępowania zabezpieczającego oraz okoliczności naruszenia bezpieczeństwa danych osobowych należy ująć w raporcie i niezwłocznie przekazać Administratorowi danych.

§ 9

- 1 Po dokonaniu czynności zabezpieczenia danych osobowych i ustaleniu przyczyn naruszenia ochrony danych osobowych należy niezwłocznie przywrócić normalny stan działania.
- 2 Administrator Bezpieczeństwa Informacji, w przypadku stwierdzenia ingerencji w system informatyczny zasięga niezbędnych opinii. W dalszej kolejności proponuje postępowanie naprawcze, w którym ustosunkowuje się do kwestii ewentualnego odtworzenia danych oraz terminu wznowienia przetwarzania danych.

	Urząd Gminy Stalno	Data wydania:	29.04.2011
	Załącznik nr 2 do Polityki Bezpieczeństwa Urzędu Gminy Stalno	Ilość stron:	Strona 26 z 89
		Wydanie:	pierwsze

- 3 Po przywróceniu integralności systemu, powinna zostać przeprowadzona szczegółowa analiza, dokonana przez zespół opiniujący (kierownictwo Urzędu, Administrator Bezpieczeństwa Informacji, Administrator Systemu Informatycznego oraz Pełnomocnik ds. Ochrony Informacji Niejawnych), w celu określenia przyczyny naruszenia ochrony danych osobowych, wskazania odpowiedzialnych oraz przedsięwzięcia kroków mających na celu wyeliminowanie podobnych zdarzeń w przyszłości.
- 4 Jeżeli przyczyną zdarzenia był błąd osoby zatrudnionej przy przetwarzaniu danych osobowych, ABI niezwłocznie zarządza przeprowadzenie dodatkowego szkolenia dla osób biorących udział przy przetwarzaniu danych osobowych. Dokumentację ze szkolenia dołącza do raportu określonego w §10.

§ 10

- 1 Po dokonaniu czynności przedstawionych powyżej ABI sporządza szczegółowy raport zawierający:
 - a) opis zdarzenia,
 - b) przyczynę jego zaistnienia,
 - c) skutki naruszenia ochrony danych osobowych,
 - d) podjęte działania i zastosowane środki,
 - e) analizę zdarzenia oraz wnioski dotyczące podjętych przedsięwzięć organizacyjnych, technicznych i kadrowych.
- 2 Raport z naruszenia bezpieczeństwa systemu informatycznego przedkładany jest niezwłocznie Administratorowi danych, który wydaje pisemne zalecenia.
- 3 We wskazanym przez Administratora danych terminie ABI przeprowadza kontrolę wydanych zaleceń.
- 4 Nie wykonanie zaleceń, traktowane będzie jako ciężkie naruszenie dyscypliny w rozumieniu art. 52 §.1 pkt.1 k.p.¹⁾, a także poniesienie odpowiedzialności karnej określonej w rozdziale 8 ustawy o ochronie danych²⁾ oraz w przepisach kodeksu karnego³⁾

¹ Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy – (tekst jednolity Dz. U. z 1998 r. Nr 21, poz. 94; : zm. z 1998 r. Dz. U. Nr 106, poz. 668, Dz. U. Nr 113, poz. 717; zm. z 1999 r. Dz. U. Nr 99, poz. 1152; zm. z 2000 r. Dz. U. Nr 19, poz. 239, Dz. U. Nr 43, poz. 489, Dz. U. Nr 107, poz. 1127, Dz. U. Nr 120, poz. 1268; zm. z 2001 r. Dz. U. Nr 11, poz. 84, Dz. U. Nr 28, poz. 301, Dz. U. Nr 52, poz. 538, Dz. U. Nr 99, poz. 1075, Dz. U. Nr 111, poz. 1194, Dz. U. Nr 123, poz. 1354,

	Urząd Gminy Stolno	Data wydania:	29.04.2011
	Załącznik nr 2 do Polityki Bezpieczeństwa Urzędu Gminy Stolno	Ilość stron:	Strona 27 z 89
		Wydanie:	pierwsze

5 Całość dokumentacji w zakresie naruszenia systemu ochrony danych osobowych przechowuje ABI.

§ 11

W zakresie nieuregulowanym niniejszą *Instrukcją*, stosuje się odpowiednie przepisy ustawy o ochronie danych osobowych⁴⁾ oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych⁵⁾.

Dz. U. Nr 128, poz. 1405, Dz. U. Nr 154, poz. 1805; zm. z 2002 r. Dz. U. Nr 74, poz. 676, Dz. U. Nr 135, poz. 1146, Dz. U. Nr 196, poz. 1660, Dz. U. Nr 199, poz. 1673, Dz. U. Nr 200, poz. 1679; zm. z 2003 r. Dz. U. Nr 166, poz. 1608, Dz. U. Nr 213, poz. 2081; zm. z 2004 r. Dz. U. Nr 96, poz. 959, Dz. U. Nr 99, poz. 1001, Dz. U. Nr 120, poz. 1252, Dz. U. Nr 240, poz. 2407; zm. z 2005 r. Dz. U. Nr 10, poz. 71, Dz. U. Nr 68, poz. 610, Dz. U. Nr 86, poz. 732, Dz. U. Nr 167, poz. 1398; zm. z 2006 r. Nr 104, poz. 708 i 711, Dz. U. Nr 133, poz. 935, Dz. U. Nr 217, poz. 1587, Dz. U. Nr 221, poz. 1615; zm. z 2007 r. Dz. U. Nr 64, poz. 426, Dz. U. Nr 89, poz. 589, Dz. U. Nr 176, poz. 1239, Dz. U. Nr 181, poz. 1288, Dz. U. Nr 225, poz. 1672; zm. z 2008 r. Dz. U. Nr 93, poz. 586, Dz. U. Nr 223, poz. 1460, Dz. U. Nr 237, poz. 1654; zm. z 2009 r. Dz. U. Nr 6, poz. 33, Nr 56, poz. 458, Dz. U. Nr 58, poz. 485, Dz. U. Nr 98, poz. 817, Dz. U. Nr 99, poz. 825, Dz. U. Nr 115, poz. 958, Dz. U. Nr 157, poz. 1241, Dz. U. Nr 219, poz. 1704; zm. z 2010 r. Dz. U. Nr 105, poz. 655, Dz. U. Nr 135, poz. 912, Dz. U. Nr 182, poz. 1228)

2 Ustawa z dnia 29 sierpnia 1997 roku o ochronie danych osobowych – (tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926, Dz. U. Nr 153, poz. 1271; zm. z 2004 r. Dz. U. Nr 25, poz. 219, Dz. U. Nr 33, poz. 285; zm. z 2006 r. Dz. U. Nr 104, poz. 708, Dz. U. Nr 104, poz. 711; zm. z 2007 r. Dz. U. Nr 165, poz. 1170, Dz. U. Nr 176, poz. 1238; zm. z 2010 r. Dz. U. Nr 41, poz. 233)

3 Ustawa z dnia 6 czerwca 1997 r. Kodeks karny – (Dz. U. Nr 88, poz. 554; zm. z 1997 r. Dz. U. Nr 128, poz. 840; zm. z 1999 r. Dz. U. Nr 64, poz. 729, Dz. U. Nr 83, poz. 931; zm. z 2000 r. Dz. U. Nr 48, poz. 548, Dz. U. Nr 93, poz. 1027, Dz. U. Nr 116, poz. 1216; zm. z 2001 r. Dz. U. Nr 98, poz. 1071; zm. z 2003 r. Dz. U. Nr 111, poz. 1061, Dz. U. Nr 121, poz. 1142, Dz. U. Nr 179, poz. 1750, Dz. U. Nr 199, poz. 1935, Dz. U. Nr 228, poz. 2255; zm. z 2004 r. Dz. U. Nr 25, poz. 219, Dz. U. Nr 69, poz. 626, Dz. U. Nr 93, poz. 889, Dz. U. Nr 243, poz. 2426; zm. z 2005 r. Dz. U. Nr 86, poz. 732, Dz. U. Nr 90, poz. 757, Dz. U. Nr 132, poz. 1109, Dz. U. Nr 163, poz. 1363, Dz. U. Nr 178, poz. 1479, Dz. U. Nr 180, poz. 1493; zm. z 2006 r. Dz. U. Nr 190, poz. 1409, Dz. U. Nr 218, poz. 1592, Dz. U. Nr 226, poz. 1648; zm. z 2007 r. Dz. U. Nr 89, poz. 589, Dz. U. Nr 123, poz. 850, Dz. U. Nr 124, poz. 859, Dz. U. Nr 192, poz. 1378; zm. z 2008 r. Dz. U. Nr 90, poz. 560, Dz. U. Nr 122, poz. 782, Dz. U. Nr 171, poz. 1056, Dz. U. Nr 173, poz. 1080, Dz. U. Nr 214, poz. 1344; zm. z 2009 r. Dz. U. Nr 62, poz. 504, Dz. U. Nr 63, poz. 533, Dz. U. Nr 166, poz. 1317, Dz. U. Nr 168, poz. 1323, Dz. U. Nr 190, poz. 1474, Dz. U. Nr 201, poz. 1540, Dz. U. Nr 206, poz. 1589; zm. z 2010 r. Dz. U. Nr 7, poz. 46, Dz. U. Nr 40, poz. 227 i 229, Dz. U. Nr 98, poz. 625 i 626, Dz. U. Nr 125, poz. 842, Dz. U. Nr 127, poz. 857, Dz. U. Nr 157, poz. 1018 i 1021, Dz. U. Nr 182, poz. 1228)

4 Ustawa z dnia 29 sierpnia 1997 roku o ochronie ... op. cit.

5 Rozporządzenie MSWiA 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. Nr 100, poz. 1024)

	Urząd Gminy Stalno	Data wydania:	29.04.2011
	Załącznik do Instrukcji postępowania w sytuacji naruszenia systemu ochrony danych osobowych.	Ilość stron:	Strona 28 z 89
		Wydanie:	pierwsze

R A P O R T

z naruszenia bezpieczeństwa systemu informatycznego w Urzędzie Gminy Stalno

1. Data:.....
(dd. mm. rrrr)

Godzina:.....
(00:00)

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

.....
(Imię i nazwisko, stanowisko służbowe, nazwa użytkownika - jeśli występuje)

3. Lokalizacja zdarzenia:

.....
(np. nr pokoju, nazwa pomieszczenia)

4. Opis zdarzenia:

.....
(rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące)

5. Przyczyny wystąpienia zdarzenia:

6. Skutki naruszenia ochrony danych:

	Urząd Gminy Stalno	Data wydania:	29.04.2011
	Załącznik do Instrukcji postępowania w sytuacji naruszenia systemu ochrony danych osobowych.	Ilość stron:	Strona 29 z 89
		Wydanie:	pierwsze

7. Podjęte działania:

8. Postępowanie wyjaśniające:

(analiza zdarzenia oraz wnioski dot. przedsięwzięć organizacyjnych, technicznych, kadrowych)

data, podpis
Administratora Bezpieczeństwa Informacji