

	Urząd Gminy Stalno	Data wydania:	29.04.2011
	Załącznik nr 12 do Polityki Bezpieczeństwa Urzędu Gminy Stalno	Ilość stron:	Strona 84 z 89
		Wydanie:	pierwsze

- dotykać i przemieszczać przedmiotu.

Po przybyciu Policji, kierownictwo akcji przekazywane jest policjantowi, który od tego czasu jest dowódcą prowadzonej akcji. Pracownicy Urzędu ściśle wykonują polecenie wydawane przez kierującego akcją.

W przypadku **otrzymania lub znalezienia budzącej podejrzania przesyłki w żadnym przypadku nie należy jej otwierać.**

Jeśli przesyłka została już otwarta i zawiera jakąkolwiek podejrzaną substancję w różnej postaci (płynnej, proszkowej) należy:

- nie ulegać panice,
- unikać bezpośredniego kontaktu z innymi osobami,
- nie dotykać lub przemieszczać przesyłki,
- nie wąchać zawartości przesyłki,
- pozamykać okna i drzwi w pomieszczeniu celem wstrzymania ruchu powietrza.

Powiadomiony o powyższym fakcie Kierownik komórki organizacyjnej podejmuje działania zabezpieczające miejsce informując jednocześnie kierownictwo Urzędu.

O powyższej sytuacji należy natychmiast powiadomić Policję, Straż Pożarną, placówkę służby zdrowia. Po przybyciu na miejsce służb specjalistycznych kierownictwo akcji przekazane jest funkcjonariuszowi Straży Pożarnej lub Policji.

W przypadku **otrzymania przez pracownika telefonicznej informacji o podłożonej na terenie obiektu Urzędu paczce z zawartością materiałów wybuchowych, substancji biologicznych lub chemicznych** należy:

- nie ulegać panice,
- rozmowę prowadzić spokojnie i uprzejmie,
- udając trudności ze zrozumieniem osoby telefonującej, jak najdłużej przeciągać rozmowę, celem uzyskania jak najwięcej informacji o odgłosach dochodzących z miejsca dzwoniącego
- starać się uświadomić dzwoniącemu czy wziął pod uwagę możliwość spowodowania w wyniku zamachu, śmierci lub choroby wielu niewinnych osób, w tym i dzieci,
- dążyć do uzyskania jak najwięcej informacji o dzwoniącym i jego motywie działania,

	Urząd Gminy Stalno	Data wydania:	29.04.2011
	Załącznik nr 12 do Polityki Bezpieczeństwa Urzędu Gminy Stalno	Ilość stron:	Strona 85 z 89
		Wydanie:	pierwsze

- starać się wciągnąć dzwoniącego w rozmowę, która umożliwi wykonanie następnych czynności
- prowadzić rozmowę z osobą informującą odpowiadając na pytania przy pomocy „Formularza prowadzonej rozmowy z osobą informującą” stanowiącym załącznik do niniejszego dokumentu.

Powiadomiony o powyższym fakcie Kierownik komórki organizacyjnej informuje kierownictwo Urzędu.

O powyższej sytuacji należy natychmiast powiadomić Policję, Straż Pożarną, placówka służby zdrowia.

W przypadku zaistnienia wymienionych powyżej sytuacji **każdy pracownik jest zobowiązany powiadomić natychmiast swojego bezpośredniego przełożonego.**

	Urząd Gminy Stalno	Data wydania:	29.04.2011
	Załącznik nr 12 do Polityki Bezpieczeństwa Urzędu Gminy Stalno	Ilość stron:	Strona 86 z 89
		Wydanie:	pierwsze

Załącznik
do Procedury awaryjnej nr 6
dot. sytuacji wystąpienia zagrożenia
terrorystycznego

FORMULARZ PROWADZONEJ ROZMOWY **Z OSOBĄ INFORMUJĄCĄ O PODŁOŻONYM ŁADUNKU**

Informacja dla prowadzących rozmowę.

1. Wypełniając formularz, należy właściwe informacje podkreślić lub wpisać w miejsc zaznaczone.
2. Formularz należy wypełniać w trakcie rozmowy lub bezpośrednio po jej zakończeniu.

Kiedy ładunek zaczął lub zacznie działać?

Odp.:

.....

Gdzie znajduje się ładunek?

Odp.:

.....

Co zawiera ładunek?

Odp.:

.....

Jak wygląda?

Odp.:

.....

W którym konkretnie miejscu jest on umieszczony?

Odp.:

.....

	Urząd Gminy Stolno	Data wydania:	29.04.2011
	Załącznik nr 12 do Polityki Bezpieczeństwa Urzędu Gminy Stolno	Ilość stron:	Strona 87 z 89
		Wydanie:	pierwsze

Dlaczego podłożył(a) Pan (Pani) ładunek?

Odp.:

.....

Skąd Pan (Pani) telefonuje?

Odp.:

.....

Gdzie Pan (Pani) w tej chwili się znajduje?

Odp.:

.....

Czy mogę Panu (Pani) w czymś pomóc?

Odp.:

.....

Czy chce się Pan (Pani) z kimś skontaktować?

Odp.:

.....

Czy jest Pan (Pani) konstruktorem ładunku?

Odp.:

.....

Proszę podać swoje nazwisko i adres?

Odp.:

.....

Inne pytania uzależnione od konkretnej sytuacji, które nasuną się w trakcie prowadzonej rozmowy.

Pytanie

	Urząd Gminy Stolno	Data wydania:	29.04.2011
	Załącznik nr 12 do Polityki Bezpieczeństwa Urzędu Gminy Stolno	Ilość stron:	Strona 88 z 89
		Wydanie:	pierwsze

Odp.:

.....

.....

Pytanie

Odp.:

.....

.....

Dane personalne osoby przyjmującej wymienioną informację telefoniczną:

.....

Czas przyjęcia informacji:

Cechy charakterystyczne prowadzonej rozmowy

Opis głosu rozmówcy (z jaką znaną osobą utożsamiasz głos rozmówcy)

.....

.....

Głos należał do osoby będącej: ...kobietą, mężczyzną, dzieckiem^{*)}

Głos należał do osoby w wieku: młodym, średnim, starszym^{*)}

W jakim wieku w przybliżeniu mogła być osoba dzwoniąca?

Akcent rozmówcy: cudzoziemski, miejscowy (gwara, sztucznie zmieniany)

.....

.....

Ton głosu: niski, wysoki, głośny, cichy, szybki, wolny, ciepły, chrapliwy, jękający się, zniekształcony, bełkotliwy, sepleniący, nosowy^{*)}, inny

.....

Charakterystyczna wymowa którejś z głosek

	Urząd Gminy Stolno	Data wydania:	29.04.2011
	Załącznik nr 12 do Polityki Bezpieczeństwa Urzędu Gminy Stolno	Ilość stron:	Strona 89 z 89
		Wydanie:	pierwsze

Inne cechy charakterystyczne głosu

.....

Tło akustyczne np. cisza, jakieś dźwięki

Dźwięki w tle (odgłosy dochodzące z miejsca przebywania rozmówcy) np. ulica, fabryka, biuro, dworzec autobusowy lub kolejowy, głosy ludzkie, winda,^{*)}

- głosy zwierząt, (jakich?).....

- muzyka (jakiego rodzaju)

Zachowanie się dzwoniącego: spokojne, wesołe, rozsądne, rozgniewane, desperackie, aroganckie, nieracjonalne^{*)}, inne

.....

.....

.....

Wpisać dokładną treść rozmowy:

.....

.....

Inne uwagi przyjmującego informację telefoniczną:

.....

.....

Kogo powiadomiono o informacji

.....

.....

.....
data i podpis przyjmującego informację

^{*)} zaznaczyć właściwą cechę

	Urząd Gminy Stolno	Data wydania:	29.04.2011
	Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych Załącznik nr 2 do Zarządzenia Nr 35/2011 z dnia 29.04.2011 r.	Ilość stron:	Strona 1 z 48
		Wydanie:	pierwsze

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

Urzędu Gminy Stolno

Stolno 2011

	Urząd Gminy Stolno	Data wydania:	29.04.2011
	Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych	Ilość stron:	Strona 2 z 48
	Załącznik nr 2 do Zarządzenia Nr/2011 z dnia	Wydanie:	pierwsze

SPIS TREŚCI

2.	Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.	3
2.1	Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym	15
2.2	Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem.	18
2.3	Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu.	21
2.4	Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.	27
2.5	Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe.	31
2.6	Sposób, miejsce i okres przechowywania kopii zapasowych.	33
2.7	Sposób, miejsce i okres przechowywania dokumentacji papierowej.	34
2.8	Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia.	35
2.9	Zasady i sposób odnotowywania w systemie informacji o udostępnieniu danych osobowych.	38
2.10	Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.	40
2.11	Instrukcja korzystania z systemu teleinformatycznego.	42
2.12	Sposób, zakres i tryb udostępniania danych zgromadzonych w rejestrach publicznych prowadzonych w Urzędzie Gminy Stolno	44
3.	Oświadczenie o zapoznaniu się dokumentacją /wzór/	47
4.	Dziennik zmian	48

	Urząd Gminy Stolno	Data wydania:	29.04.2011
	Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych	Ilość stron:	Strona 3 z 48
	Załącznik nr 2 do Zarządzenia Nr/2011 z dnia	Wydanie:	pierwsze

WPROWADZENIE

Nowelizacja przepisów ochrony danych osobowych w 2004 roku spowodowała wprowadzenie nowych unormowań prawnych regulujących przedmiotowe zagadnienie w zakresie dokumentacji związanej z zarządzaniem systemem informatycznym.

Jednym z nowych unormowań prawnych wydanych na podstawie ustawy¹ jest rozporządzenie MSWiA z dnia 29 kwietnia 2004 roku² regulujące kwestie opracowania dokumentacji związanej z bezpieczeństwem przetwarzania danych osobowych, warunkami technicznymi, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Zgodnie z treścią powyższego aktu prawa wykonawczego jednym z wymogów, jaki został wskazany w treści § 3, jest opracowanie w formie pisemnej *Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych*, której wdrożenie do stosowania w Urzędzie jest obowiązkiem Administratora danych.

Niniejsza *Instrukcja* jest obowiązującym dokumentem zawierającym procedury oraz wytyczne niezbędne do prawidłowego zarządzania systemem informatycznym przy pomocy, którego przetwarzane są dane osobowe w Urzędzie Gminy Stolno. Dokument zawiera także informacje o systemie informatycznym oraz procedury i zasady podjęte w Urzędzie dla zapewnienia poufności, integralności i bezpieczeństwa przetwarzanych danych osobowych, które muszą być przestrzegane przez wszystkie osoby w Urzędzie zgodnie z posiadanymi uprawnieniami i zakresem obowiązków.

¹ Ustawa z dnia 22 stycznia 2004 roku o zmianie ustawy o ochronie danych osobowych oraz ustawy o wynagrodzeniu osób zajmujących kierownicze stanowiska państwowe (Dz. U. Nr 33, poz.285) wprowadziła z dniem 1 maja 2004 roku nowelizację Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 roku (tekst jednolity. Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.) dostosowując obowiązujące w RP przepisy prawne do obowiązujących w krajach Unii Europejskiej.

² Rozporządzenia MSWiA z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).

	Urząd Gminy Stolno	Data wydania:	29.04.2011
	Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych Załącznik nr 2 do Zarządzenia Nr/2011 z dnia	Ilość stron:	Strona 4 z 48
		Wydanie:	pierwsze

DEFINICJE I OKREŚLENIE POJĘĆ UŻYTYCH W DOKUMENCIE

Ilekoć w niniejszym dokumencie – *Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych* 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 Gminy Stolno jest nim informatyk obsługujący system informatyczny Urzędu Gminy.

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).

³ Tamże

	Urząd Gminy Stolno	Data wydania:	29.04.2011
	Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych Załącznik nr 2 do Zarządzenia Nr/2011 z dnia	Ilość stron:	Strona 5 z 48
		Wydanie:	pierwsze

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

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.

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
	Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych	Ilość stron:	Strona 6 z 48
	Załącznik nr 2 do Zarządzenia Nr/2011 z dnia	Wydanie:	pierwsze

(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, z którym Urząd podpisał umowę o dzieło lub umowę zlecenia.

Przetwarzanie danych osobowych – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmniejszanie, 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.

	Urząd Gminy Stalno	Data wydania:	29.04.2011
	Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych Załącznik nr 2 do Zarządzenia Nr/2011 z dnia	Ilość stron:	Strona 7 z 48
		Wydanie:	pierwsze

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

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) wcześniejsz 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 Stalno	Data wydania:	29.04.2011
	Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych	Ilość stron:	Strona 8 z 48
	Załącznik nr 2 do Zarządzenia Nr/2011 z dnia	Wydanie:	pierwsze

ROZDZIAŁ I

ADMINISTRATOR DANYCH

1. Administrator danych wprowadza „*Instrukcję...*” i upoważnia Administratora Bezpieczeństwa Informacji do nadzorowania wdrożenia sposobu administrowania i zarządzania środkami informatycznymi wspomagającymi procesy przetwarzania informacji stanowiących dane osobowe w rozumieniu ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych⁸.
2. Administrator danych stwarza właściwe warunki organizacyjno-techniczne gwarantujące bezpieczeństwo systemów informatycznych⁹ w Urzędzie, w szczególności:
 - a) w przypadku systemów informatycznych służących do przetwarzania danych w zakresie:
 - lokalizacji pomieszczeń, w których przetwarzane są dane osobowe,
 - lokalizacji pomieszczeń, w których przechowywane są kopie awaryjne zbiorów danych osobowych,
 - instalowania krat i systemów alarmowych adekwatnych do zagrożenia systemów informatycznych,
 - zakupu niszczarek do dokumentów
 - zakupu szaf metalowych do przechowywania kopii zapasowych danych osobowych z systemów informatycznych.
 - b) zabezpiecza budynki oraz pomieszczenia, w których przetwarzane są dane osobowe w systemach informatycznych przed dostępem osób niepowołanych, a w szczególności:

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

	Urząd Gminy Stolno	Data wydania:	29.04.2011
	Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych Załącznik nr 2 do Zarządzenia Nr/2011 z dnia	Ilość stron:	Strona 9 z 48
		Wydanie:	pierwsze

- wprowadza i nadzoruje bieżącą aktualizację listy osób upoważnionych do pobierania kluczy do pomieszczeń, w których przetwarzane są dane osobowe,
- wprowadza ewidencję osób pobierających klucze do pomieszczeń, w których przetwarzane są dane osobowe zawierającą m.in. czas pobierania i zdawania kluczy w budynku, w którym przetwarzane są dane osobowe w systemach informatycznych,
- określa tryb pobytu osób sprzątających pomieszczenia, w których przetwarzane są dane osobowe w systemach informatycznych uwzględniający specyfikę obiektu.

	Urząd Gminy Stalno	Data wydania:	29.04.2011
	Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych	Ilość stron:	Strona 10 z 48
	Załącznik nr 2 do Zarządzenia Nr/2011 z dnia	Wydanie:	pierwsze

ROZDZIAŁ II

ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI

1. Administrator Bezpieczeństwa Informacji odpowiada za korygowanie niniejszej „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych” w przypadku uzasadnionych zmian w przepisach prawnych dotyczących przetwarzania danych osobowych w systemach informatycznych, jak również zmian organizacyjno-funkcjonalnych zachodzących w Urzędzie Gminy Stalno.
2. Administrator Bezpieczeństwa Informacji:
 - a) czuwa nad wdrażaniem niniejszej „Instrukcji...” w systemach informatycznych Urzędu, w których przetwarzane są dane osobowe oraz dba o bieżącą aktualizację stosownie do zmieniających się technologii informatycznych oraz zagrożeń bezpieczeństwa systemów informatycznych w obiekcie Urzędu Gminy,
 - b) określa strategię zabezpieczania systemów informatycznych w obiekcie Urzędu,
 - c) sprawuje nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych,
 - d) sprawuje nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe,
 - e) identyfikuje i analizuje zagrożenia oraz ryzyko, na które narażone może być przetwarzanie danych osobowych w systemach informatycznych Urzędu,
 - f) określa potrzeby w zakresie zabezpieczenia systemów informatycznych, w których przetwarzane są dane osobowe,
 - g) sprawuje osobisty nadzór lub za pośrednictwem pisemnie upoważnionej osoby, nad bezpieczeństwem danych zawartych w komputerach przenośnych, dyskach wymiennych, w których przetwarzane są dane osobowe,
 - h) monitoruje działanie zabezpieczeń wdrożonych w celu ochrony danych osobowych w systemach informatycznych,

	Urząd Gminy Stalno	Data wydania:	29.04.2011
	Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych Załącznik nr 2 do Zarządzenia Nr/2011 z dnia	Ilość stron:	Strona 11 z 48
		Wydanie:	pierwsze

- i) sprawuje nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane oraz kontrolę dostępu do danych,
 - j) zgłasza potrzeby w zakresie zmiany w konfiguracji sprzętu lub oprogramowania mających wpływ na bezpieczeństwo systemu komputerowego,
 - k) sprawuje nadzór nad systemem komunikacji w sieci komputerowej oraz nad przesyłaniem danych za pośrednictwem urządzeń teletransmisyjnych,
 - l) określa zasady i ewidencję wykonywania czynności serwisowych w systemach informatycznych w celu wyeliminowania:
 - a) możliwości wykonania kopii danych osobowych przez osoby nieupoważnione,
 - b) przemieszczania urządzeń komputerowych i ich części służących do przetwarzania danych osobowych poza obszar objęty ochroną,
 - c) podmiany elementów sprzętu komputerowego lub oprogramowania na inny, który zawiera cechy ukryte.
3. Administrator Bezpieczeństwa Informacji publikuje zatwierdzony dokument i nadzoruje, aby wszyscy pracownicy Urzędu zapoznali się z niniejszą „Instrukcją...”

	Urząd Gminy Stalno	Data wydania:	29.04.2011
	Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych Załącznik nr 2 do Zarządzenia Nr/2011 z dnia	Ilość stron:	Strona 12 z 48
		Wydanie:	pierwsze

ROZDZIAŁ III

ADMINISTRATOR SYSTEMU INFORMATYCZNEGO

Administrator Systemu Informatycznego dla zapewnienia bezpieczeństwa systemów informatycznych Urzędu Gminy Stalno:

- a) dokonuje wyboru lub migracji do technologii minimalizującej zagrożenie uzyskania dostępu do sieci osobom nieupoważnionym,
- b) zgłasza potrzebę zakupu oprogramowania umożliwiającego rejestrowanie identyfikatorów i czas logowania użytkowników sieci,
- c) nadzoruje proces monitorowania sieci pod kątem zabezpieczenia przed dostępem osób nieupoważnionych,
- d) dokonuje zakupu pamięci masowych, streamerów oraz innych urządzeń i nośników umożliwiających wykonywanie kopii zapasowych danych osobowych w systemach informatycznych,
- e) zgłasza potrzebę zakupu systemów operacyjnych, oprogramowania antywirusowego oraz systemów kryptograficznych podnoszących bezpieczeństwo danych osobowych, gwarantujących spełnienie wymogów określonych ustawą,
- f) dokonuje właściwego prowadzenia i zabezpieczenia okablowania sieci komputerowej służącej do przetwarzania danych osobowych w systemach informatycznych w celu wyeliminowania zagrożeń.

	Urząd Gminy Stolno	Data wydania:	29.04.2011
	Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych Załącznik nr 2 do Zarządzenia Nr/2011 z dnia	Ilość stron:	Strona 13 z 48
		Wydanie:	pierwsze

ROZDZIAŁ IV

POSTANOWIENIA OGÓLNE

1. Wszyscy pracownicy, którzy zostali zapoznani z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych, potwierdzają ten fakt podpisaniem *Oświadczenia* wg wzoru, który jest załącznikiem 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.
2. Pracownik Stanowiska d/s. obywatelskich i organizacyjnych Urzędu Gminy Stolno podpisane przez pracownika „*Oświadczenie*” przechowuje w jego aktach personalnych.

	Urząd Gminy Stolno	Data wydania:	29.04.2011
	Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych Załącznik nr 2 do Zarządzenia Nr/2011 z dnia	Ilość stron:	Strona 14 z 48
		Wydanie:	pierwsze

**WYKAZ ZAŁĄCZNIKÓW DO INSTRUKCJI ZARZĄDZANIA SYSTEMEM
INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH**

Instrukcja zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Urzędzie Gminy Stolno określa:

załącznik nr 1	Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym
załącznik nr 2	Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem.
załącznik nr 3	Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu.
załącznik nr 4	Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.
załącznik nr 5	Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe.
załącznik nr 6	Sposób, miejsce i okres przechowywania kopii zapasowych.
załącznik nr 7	Sposób, miejsce i okres przechowywania dokumentacji papierowej.
załącznik nr 8	Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia MSWiA z dnia 29 kwietnia 2004 roku.
załącznik nr 9	Sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4 rozporządzenia MSWiA z dnia 29 kwietnia 2004 roku. Zasady i sposób odnotowywania w systemie informacji o udostępnieniu danych osobowych.
załącznik nr 10	Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.
załącznik nr 11	Instrukcja korzystania z systemu teleinformatycznego.
załącznik nr 12	Sposób, zakres i tryb udostępniania danych zgromadzonych w rejestrach publicznych prowadzonych w Urzędzie Gminy Stolno

	Urząd Gminy Stolno	Data wydania:	29.04.2011
	Załącznik nr 1 do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych.	Ilość stron:	Strona 15 z 48
		Wydanie:	pierwsze

PROCEDURY nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym		
INSTRUKACJA ADMINISTRACYJNO - TECHNICZNA		
1.	Numer	1
2.	Wersja	01
3.	Odwołania do innych dokumentów	
4.	Status	Obowiązująca
5.	Data wygaśnięcia	
6.	Pracownik wdrażający	Administrator Systemu Informatycznego
7.	Zatwierdzający procedurę	Wójt
8.	Lista dystrybucyjna	Kierownicy komórek organizacyjnych, Administrator Bezpieczeństwa Informacji, Użytkownicy systemu informatycznego na samodzielnych stanowiskach pracy.

1. Dostęp do danych osobowych jest możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.
2. Każdy użytkownik uprawniony do wykonywania prac w systemie informatycznym posiada własne konto, do którego ma przydzielone hasło.
3. Po wykonaniu rutynowych czynności przez pracownika, zajmującego się sprawami kadrowymi Urzędu Gminy, Administrator Systemu Informatycznego nadaje nowemu pracownikowi login składający się z pierwszej litery imienia i nazwiska, pisanych razem (bez polskich znaków diakrytycznych) oraz hasło startowe. Gdy wymaga tego sytuacja, w celu uniknięcia duplikowania się identyfikatora, nazwa użytkownika rozbudowana jest dodatkowo o drugą literę imienia.
4. W szczególnych przypadkach identyfikator może być skonstruowany wg innego klucza.
5. Każdy użytkownik systemu informatycznego w Urzędzie otrzymuje konto określone przez

unikalny identyfikator, jednoznacznie identyfikujący go w systemie.

6. Przyznawanie uprawnień odbywa się na zasadzie przynależności do konkretnych grup. Na wniosek Kierownika komórki organizacyjnej (w zależności od sytuacji wypełniane są określone *Karty* wg załącznika do *Procedur Administracyjno – Technicznych*) następuje modyfikacja, zablokowanie lub deaktywacja konta użytkownika. Administrator Systemu Informatycznego jest informowany o konieczności dokonania zmian w kontach użytkowników przez ich bezpośrednich przełożonych. W szczególności dotyczy to takich przypadków jak: wygaśnięcie umowy o pracę, dłuższa nieobecność pracownika, zmiana zakresu obowiązków itp. Wszelkie zmiany zostaną wprowadzone przez Administratora Systemu Informatycznego niezwłocznie po otrzymaniu właściwie wypełnionego wniosku.
7. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.
8. Identyfikator użytkownika (login) za pomocą, którego system informatyczny identyfikuje daną osobę wraz z przydzielonymi jej uprawnieniami bądź ograniczeniami nadawany jest tylko raz.
9. Wszyscy pracownicy Urzędu przetwarzający dane w systemach informatycznych posiadają własne konto. W miarę potrzeby dokonywana jest modyfikacja uprawnień poszczególnych pracowników przez Administratora Systemu Informatycznego.
10. Każdy użytkownik systemu informatycznego Urzędu otrzymuje przypisane do identyfikatora prawa (bądź ograniczenia) dostępu do zasobów systemu, takich jak: drukarki, przestrzeń dyskowa na serwerach, baz danych, kasowania bądź dodawania plików w katalogach, wielkości dostępnej przestrzeni dyskowej, możliwości logowania z konkretnych stacji roboczych itp.
11. Pracownik zobowiązany jest dokonać samodzielnie zmiany hasła w określonym czasie, uwzględniając przy tym wymaganą złożoność. Każdorazowo tak zmienione hasło pracownik zobowiązany jest zapisać i przekazać do ABI w zaklejonej kopercie, który prowadzi rejestr i chroni powierzone hasła.
12. ABI czuwa nad tym by dysponować zawsze aktualnym i obowiązującym w danej chwili kompletem haseł systemowych.

13. Konto bez ograniczeń może posiadać jedynie Administrator Systemu Informatycznego wraz z osobą zastępującą – jeśli została wyznaczona oraz osoby bezpośrednio wyznaczone przez Wójta Gminy.
14. Administrator Systemu Informatycznego unieważnia hasła i blokuje konta użytkowników.
15. Za realizację procedur oraz rejestrowanie i wyrejestrowanie pracownika Urzędu w systemie informatycznym odpowiedzialny jest Administrator Systemu Informatycznego, który sprawuje nadzór nad systemem informatycznym.
16. W przypadku długotrwałej nieobecności Administratora Systemu Informatycznego jego czynności wykonuje osoba powołana na zastępstwo przez Administratora danych.

	Urząd Gminy Stalno	Data wydania:	29.04.2011
	Załącznik nr 2 do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych.	Ilość stron:	Strona 18 z 48
		Wydanie:	pierwsze

Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem		
INSTRUKACJA ADMINISTRACYJNO - TECHNICZNA		
1.	Numer	2
2.	Wersja	01
3.	Odwołania do innych dokumentów	
4.	Status	Obowiązująca
5.	Data wygaśnięcia	
6.	Pracownik wdrażający	Administrator Systemu Informatycznego
7.	Zatwierdzający procedurę	Wójt
8.	Lista dystrybucyjna	Kierownicy komórek organizacyjnych, Administrator Bezpieczeństwa Informacji, Użytkownicy systemu informatycznego na samodzielnych stanowiskach

I. HASŁO DOSTĘPU

1. Hasło dostępu jest to kombinacja małych i dużych liter, cyfr i znaków specjalnych, służąca do weryfikacji tożsamości osoby dokonującej uwierzytelnienia w systemie za pomocą określonego identyfikatora użytkownika (loginu). Hasło przydzielone przez Administratora Systemu Informatycznego w momencie zakładania nowego konta nazywane jest hasłem startowym (początkowym).
2. Za wygenerowanie hasła startowego dla użytkownika odpowiada Administrator Systemu Informatycznego.
3. Po otrzymaniu od Kierownika komórki organizacyjnej prawidłowo wypełnionego wniosku (*Karta zgłoszenia do systemu wg załącznika nr 1 Procedur Administracyjno-Technicznych*) Administrator Systemu Informatycznego dokonuje założenia nowego konta z nadanym hasłem startowym (początkowym) wg informacji zawartych we wniosku.

4. W Urzędzie Gminy Stolno obowiązuje forma pisemna przydzielania hasła.
5. Po otrzymaniu hasła startowego każdy użytkownik zobowiązany jest do zmiany hasła przy pierwszym zalogowaniu się do systemu.
6. Każdy użytkownik jest poinformowany o wymaganej złożoności i wymuszonej niepowtarzalności hasła.
7. Hasło składa się, z co najmniej 8-miu znaków, stanowiących kombinację małych i wielkich liter oraz cyfr oraz znaków specjalnych.
8. Użytkownik obowiązany jest chronić swoje hasło oraz dokładać wszelkiej staranności w celu utrzymania hasła w tajemnicy. W szczególności niedopuszczalne jest zapisywanie hasła w ogólnodostępnych miejscach, w okolicy komputera itp.
9. Zabronione jest, aby użytkownik po otrzymaniu identyfikatora i hasła przechowywał je w miejscu, z którego może zaistnieć możliwość przeczytania przez inne osoby.
10. W Urzędzie Gminy Stolno jest zakaz przekazywania hasła przez inne osoby niż wymienione w pkt. 2 i za pośrednictwem niezabezpieczonej poczty elektronicznej.

II. ZMIANA HASŁA

1. Użytkownik zmienia hasło samodzielnie.
2. Aby zmienić hasło do systemu należy użyć kombinacji klawiszy „*Control – Alt –Delete*” i na wyświetlonym oknie wybrać dialogowym wybrać „Zmień hasło”.
3. W kolejnym etapie należy podać odpowiednio: stare hasło oraz dwa razy nowe (uwzględniając restrykcje dotyczące hasła dostępu).
4. Następnie należy potwierdzić zmiany klawiszem „OK”.
5. Po pomyślnej zmianie hasła należy zrestartować komputer, a następnie zalogować się ponownie przy użyciu nowego hasła.
6. Niespełnienie tego wymogu może skutkować automatycznym zablokowaniem konta, gdyż

propagacja nowego hasła następuje dopiero po ponownym zalogowaniu.

III. HASŁO ADMINISTRATORA SYSTEMU INFORMATYCZNEGO

1. Kluczowe hasła infrastruktury teleinformatycznej takie jak hasło użytkownika „Administrator” przechowywane są przez Administratora Bezpieczeństwa Informacji w zaklejonych kopertach w szafie metalowej.
2. Po awaryjnym użyciu w/w hasło musi zostać zmienione i ponownie umieszczone w zapieczętowanej kopercie.
3. Administrator Bezpieczeństwa Informacji odnotowuje fakt i powód otwarcia koperty z hasłem użytkownika.

	Urząd Gminy Stalno	Data wydania:	29.04.2011
	Załącznik nr 3 do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych.	Ilość stron:	Strona 21 z 48
		Wydanie:	pierwsze

Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu		
INSTRUKACJA ADMINISTRACYJNO - TECHNICZNA		
1.	Numer	3
2.	Wersja	01
3.	Odwołania do innych dokumentów	
4.	Status	Obowiązująca
5.	Data wygaśnięcia	
6.	Pracownik wdrażający	Administrator Systemu Informatycznego
7.	Zatwierdzający procedurę	Wójt
8.	Lista dystrybucyjna	Kierownicy komórek organizacyjnych, Administrator Bezpieczeństwa Informacji, Użytkownicy systemu informatycznego na samodzielnych stanowiskach pracy.

PROCEDURA UŻYTKOWNIKA		
1.	Numer	3.1
2.	Wersja	01
3.	Okoliczności stosowania procedury	<u>Rozpoczęcie pracy w systemie</u>
4.	Odwolania do innych dokumentów	
5.	Status	Obowiązująca
6.	Data wygaśnięcia	
7.	Pracownik wdrażający	Administrator Systemu Informatycznego
8.	Zatwierdzający procedurę	Wójt
9.	Lista dystrybucyjna	Kierownicy komórek organizacyjnych, Administrator Bezpieczeństwa Informacji, Użytkownicy systemu informatycznego.

1. Czynności w zakresie rozpoczęcia pracy każdy pracownik wykonuje osobiście i samodzielnie.
2. W celu rozpoczęcia pracy w systemie konieczne jest włączenia komputera (w razie konieczności podanie hasła BIOS),
3. Po włączeniu komputera i zgłoszeniu się okna logowania użytkownik jest zobowiązany wcisnąć kombinację klawiszy „Control – Alt – Delete”. Ma to na celu wyeliminowanie ewentualnego oprogramowania przechwytyującego hasło użytkownika.
4. Następnie w oknie logowania w odpowiednich polach należy wpisać swój identyfikator (jeśli wpisany domyślnie login jest niewłaściwy) oraz hasło. W oknie logowania domyślnie pojawia się nazwa ostatnio zalogowanego użytkownika. W trakcie wpisywania hasła na ekranie pojawiają się gwiazdki -- ma to zapobiec ewentualnemu podejrzeniu hasła przez osoby niepowołane. Po poprawnym wprowadzeniu informacje te należy potwierdzić poprzez wciśnięcie klawisza „Enter” (lub wciśnięcie klawisza „OK.” za pomocą lewego przycisku myszy). Następnym w/w czynności jest zalogowanie do systemu i uzyskanie możliwości normalnej w nim pracy.
5. Rozpoczęcie pracy użytkownika jest równoznaczne z wprowadzeniem identyfikatora i hasła pozwalającego na zalogowanie się użytkownika do systemu.
6. Użytkownik zobowiązany jest do wprowadzania identyfikatora i hasła w sposób zmniejszający ryzyko podejrzenia przez osoby trzecie.
7. Użytkownik może logować się do aplikacji tylko i wyłącznie przy wykorzystaniu swojego identyfikatora i hasła.
8. Po pozytywnym przejściu procedury uwierzytelnienia użytkownik uzyskuje dostęp do

systemu.

9. Czynności w zakresie rozpoczęcia pracy każdy pracownik wykonuje osobiście i samodzielnie.
10. Dostęp do danych przetwarzanych w danym zbiorze ma tylko pracownik, który je przetwarza oraz Administrator Systemu Informatycznego.
11. Ekrany monitorów na stanowiskach, na których przetwarza się dane osobowe, ustawiane są w sposób uniemożliwiający osobom nieupoważnionym dostęp do wyświetlanych informacji.

W przypadku wystąpienia sytuacji podejrzenia naruszenia bezpieczeństwa systemu objawiającej się brakiem możliwości zalogowania się użytkownika na jego konto, bądź w przypadku stwierdzenia fizycznej ingerencji w przetwarzane dane lub użytkowane narzędzia programowe lub sprzętowe, każdy pracownik-użytkownik ma obowiązek zgłoszenia tego faktu Administratorowi Systemu Informatycznego, który sprawdza wszystkie okoliczności danej sytuacji. Administrator Bezpieczeństwa Informacji rejestruje przypadki naruszenia bezpieczeństwa systemu informatycznego.

PROCEDURA UŻYTKOWNIKA		
1.	Numer	3.2
2.	Wersja	01
3.	Okoliczności stosowania procedury	<u>Zawieszenie pracy w systemie</u>
4.	Odwołania do innych dokumentów	
5.	Status	Obowiązująca
6.	Data wprowadzenia	
7.	Pracownik wdrażający	Administrator Systemu Informatycznego
8.	Zatwierdzający procedurę	Wójt
9.	Lista dystrybucyjna	Kierownicy komórek organizacyjnych, Administrator Bezpieczeństwa Informacji, Użytkownicy systemu informatycznego.

1. Każdorazowe oddalenie się pracownika od stanowiska komputerowego w czasie pracy musi być poprzedzone zablokowaniem stacji, na której przetwarzane są dane tak, aby na ekranie monitora nie były wyświetlane dane osobowe.
2. W przypadku tymczasowego zawieszenia pracy w sytuacji, kiedy wgląd w ekran monitora mogą mieć osoby niepowołane, użytkownik obowiązany jest zablokować stację roboczą. W tym celu należy wcisnąć kombinację klawiszy „Control – Alt – Delete” i w oknie wybrać klawisz „Zablokuj komputer”. Tę samą czynność można wykonać naciskając jednocześnie klawisz „z logo firmy Microsoft” oraz klawisz „L”. Niezależnie od tego po 10 minutach bezczynności system sam uruchamia wygaszacz ekranu, powodując automatyczne zablokowanie stacji roboczej.
3. W celu wznowienia pracy użytkownik musi wprowadzić swoje indywidualne hasło.
4. Aby uniknąć utraty danych spowodowanej awarią zasilania wskazane jest, aby użytkownik, który planuje zawieszenie pracy na dłużej wylogował się z systemu, zapisując uprzednio wprowadzone dane.
5. Czynności w zakresie zawieszenia pracy każdy pracownik wykonuje osobiście i samodzielnie.
6. W przypadku opuszczenia pokoju, w którym nie pozostaje żaden pracownik, należy pomieszczenie zamknąć w sposób uniemożliwiający dostęp osobom nieuprawnionym.

PROCEDURA UŻYTKOWNIKA		
1.	Numer	3.3
2.	Wersja	01
3.	Okoliczności stosowania procedury	<u>Zakończenie pracy w systemie</u>
4.	Odwołania do innych dokumentów	
5.	Status	Obowiązująca
6.	Data wygaśnięcia	
7.	Pracownik wdrażający	Administrator Systemu Informatycznego
8.	Zatwierdzający procedurę	Wójt
9.	Lista dystrybucyjna	Kierownicy komórek organizacyjnych, Administrator Bezpieczeństwa Informacji, Użytkownicy systemu informatycznego.

1. W celu zakończenia pracy w systemie użytkownik obowiązany jest wylogować się z systemu i wyłączyć komputer.
2. Czynności te są wykonywane automatycznie kolejno po sobie i wymagają wyboru pozycji „Zamknij system” z Menu Start (na monitorze w lewym dolnym rogu).
3. Uprzednio należy zamknąć wszystkie otwarte aplikacje i dokumenty.
4. Niespełnienie tego wymogu grozi utratą niezapisanych informacji, zaś niezamknięte sesje aplikacji sieciowych mogą wywołać niestabilność ich pracy a w konsekwencji zawieszenie systemu.
5. W systemach Microsoft Windows 2000, Microsoft Windows XP oraz Microsoft Windows VISTA i Microsoft Windows 7 następuje automatyczne wyłączenie komputera.
6. Wyłączenia komputera należy dokonać nie później niż o godzinie zakończenia pracy Urzędu. W razie konieczności dłuższej pracy w systemie użytkownik jest obowiązany o tym fakcie poinformować Administratora Bezpieczeństwa Informacji lub Administratora Systemu Informatycznego.
7. Czynności w zakresie zakończenia pracy każdy pracownik wykonuje osobiście i samoczynnie.
8. Po skończonej pracy użytkownik ma obowiązek zamknięcia aplikacji oraz systemu w sposób uniemożliwiający ponowne uruchomienie bez procedury logowania.
9. Zakończenie pracy użytkownika jest równoznaczne z jego wylogowaniem się z systemu informatycznego, a następnie wyłączeniem stacji komputerowej.
10. Zabronione jest pozostawianie stanowiska komputerowego z uruchomionym systemem lub programem bez kontroli pracownika.

11. Każdy użytkownik poinstruowany jest o konieczności wykonania operacji wyrejestrowania się z systemu informatycznego przed wyłączeniem stacji komputerowej oraz o czynnościach, jakie w tym celu powinien wykonać.

W przypadku wystąpienia sytuacji podejrzenia naruszenia bezpieczeństwa systemu objawiającej się brakiem możliwości zalogowania się użytkownika na jego konto, bądź w przypadku stwierdzenia fizycznej ingerencji w przetwarzane dane lub użytkowane narzędzia programowe lub sprzętowe, każdy pracownik-użytkownik ma obowiązek zgłoszenia tego faktu Administratorowi Systemu Informatycznego, który sprawdza wszystkie okoliczności danej sytuacji. W przypadku potwierdzenia naruszenia bezpieczeństwa systemu natychmiast powiadamiany jest Administrator Bezpieczeństwa Informacji.

	Urząd Gminy Stolno	Data wydania:	29.04.2011
	Załącznik nr 4 do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych.	Ilość stron:	Strona 27 z 48
		Wydanie:	pierwsze

PROCEDURY tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania		
INSTRUKACJA ADMINISTRACYJNO - TECHNICZNA		
1.	Numer	4
2.	Wersja	01
3.	Odwołania do innych dokumentów	
4.	Status	Obowiązująca
5.	Data wygaśnięcia	
6.	Pracownik wdrażający	Administrator Systemu Informatycznego
7.	Zatwierdzający procedurę	Wójt
8.	Lista dystrybucyjna	Kierownicy komórek organizacyjnych, Administrator Bezpieczeństwa Informacji, Użytkownicy systemu informatycznego na samodzielnych stanowiskach pracy

I. TWORZENIE KOPII ZAPASOWYCH

1. Proces sporządzania kopii zapasowych zbiorów i oprogramowania, służącego do ich przetwarzania, umożliwiającym ich odtworzenie jest jedną z form zapewnienia bezpieczeństwa przetwarzanych danych osobowych.
2. Administrator Bezpieczeństwa Informacji:
 - określa częstotliwość tworzenia kopii,
 - określa techniczny sposób tworzenia kopii (sprzęt, oprogramowanie),
 - ponosi odpowiedzialność za okresowe testowanie odtwarzania danych z kopii zapasowych,
 - koordynuje proces odtwarzania danych w trybie awaryjnym,
 - zabezpiecza sprzęt używany do procesów odtworzeniowych,
 - zabezpiecza nośniki przeznaczone do tworzenia kopii zapasowych,

- ponosi odpowiedzialność za właściwe tworzenie dokumentacji i prowadzenie ewidencji tworzonych kopii zapasowych.
3. Kopie zapasowe baz danych oraz aplikacji znajdujących się na serwerze wykonuje Administrator Systemu Informatycznego.
 4. Wszelkie zbiory danych oraz programy służące do ich przetwarzania podlegają cyklicznym procesom archiwizacji i backupowania (sporządzania kopii zapasowych), przy czym odpowiednio:
 - a) serwer Fujitsu Siemens Primergy TX150 S5, który stanowi podstawowy serwer bazodanowy dla oprogramowania RADIX backupowany jest 5 razy w tygodniu, w systemie poniedziałek-czwartek na płyty DVD RW a w każdy piątek na płyty DVD+R.
 - b) wszystkie backupy realizowane są przy użyciu wbudowanych w system mechanizmów oraz mechanizmów silników bazodanowych,
 - c) dane mniejszej wagi np. foldery domowe użytkowników są archiwizowane w zależności od potrzeb,
 - d) programy narzędziowe, których odtworzenie w bieżącej konfiguracji wymagałoby znacznych nakładów czasowych są archiwizowane tuż po każdorazowej modyfikacji.
 5. Tworzone kopie zapasowe gromadzone są w postaci spakowanej na dysku twardym, a następnie umieszczone na nośniku wymiennym.
 6. Codzienna kopia bezpieczeństwa nie jest tworzona na pojedynczych stanowiskach komputerowych.
 7. Kopie bezpieczeństwa dokumentów tekstowych oraz arkuszy kalkulacyjnych zapisanych lokalnie wykonują sami użytkownicy.
 8. Nośniki zawierające dane osobowe winny być w sposób jednoznaczny oznaczone poprzez określenie rodzaju przechowywanych danych, daty sporządzenia oraz nazwiska wykonującego.
 9. Nośnik kopii zapasowej powinien posiadać unikalną nazwę, związaną bezpośrednio z cyklem wykonywania (kopia dzienna, tygodniowa, miesięczna) oraz datą sporządzenia w przypadku

nośników jednorazowego użytku.

10. Kopie nośników danych osobowych zarówno w postaci elektronicznej, jak i papierowej są zabezpieczone przed dostępem osób nieuprawnionych, modyfikacją i zniszczeniem.
11. Nadzór nad wykonywaniem kopii zapasowych ich weryfikacją i poprawnością sprawuje Administrator Bezpieczeństwa Informacji.

II. USUWANIE KOPII ZAPASOWYCH I DANYCH OSOBOWYCH Z NIEWYMIENNYCH NOŚNIKÓW INFORMACJI.

1. Likwidacja nośników zawierających kopie zapasowe danych, po ich wycofaniu na skutek utraty przydatności lub w przypadku uszkodzenia dokonywana jest poprzez np. fizyczne zniszczenie lub demagnetyzację. Natomiast w przypadku dysków zawierających dane osobowe i przeznaczonych do likwidacji, bezpowrotnie pozbawia się danych przez zerowanie dysku, a gdy nie jest to możliwe poprzez uszkodzenie w sposób uniemożliwiający ich odczytanie.
2. Pozbawione danych nośniki powinny zostać przekazane do nadzorowanej utylizacji uprawnionemu podmiotowi.
3. Każdorazowo sporządza się protokół zniszczenia nośników.
4. Niepotrzebne wydruki zawierające dane osobowe są rozdrabniane w niszczarce do dokumentów, co najmniej 3 klasy utajnienia.
5. Czynność wymieniona w pkt. 1 wykonywana jest przez Administratora Systemu Informatycznego lub przez wskazaną przez niego osobę jest zgodna z wymogami zawartymi w pkt. VI ppkt 1 załącznika do rozporządzenia MSWiA z dnia 29 kwietnia 2004 roku¹.
6. W razie konieczności wykonania naprawy stacji roboczej lub serwera zawierających dane osobowe przez podmioty trzecie naprawa taka winna być wykonana pod nadzorem.

¹ Rozporządzenie 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. Nr 100, poz. 1024)

7. Jeśli natomiast niemożliwe jest przeprowadzenie napraw pod nadzorem, należy przed przekazaniem sprzętu wymontować nośnik, który zawiera bądź zawierał dane osobowe.

III. OKRESY UŻYTKOWANIA NOŚNIKÓW WIELOKROTNIEGO ZAPISU.

1. w przypadku płyt CD/DVD wielokrotnego zapisu – 12 miesięcy
2. w przypadku taśm – 12 miesięcy

	Urząd Gminy Stalno	Data wydania:	29.04.2011
	Załącznik nr 5 do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych.	Ilość stron:	Strona 31 z 48
		Wydanie:	pierwsze

Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe		
INSTRUKACJA ADMINISTRACYJNO - TECHNICZNA		
1.	Numer	5
2.	Wersja	01
3.	Odwołania do innych dokumentów	
4.	Status	Obowiązująca
5.	Data wygaśnięcia	
6.	Pracownik wdrażający	Administrator Systemu Informatycznego
7.	Zatwierdzający procedurę	Wójt
8.	Lista dystrybucyjna	Kierownicy komórek organizacyjnych, Administrator Bezpieczeństwa Informacji, Użytkownicy systemu informatycznego na samodzielnych stanowiskach pracy

1. Wszystkie istotne dla Urzędu dane przechowywane są na serwerach i dyskach poszczególnych stacji lokalnych.
2. Zakazuje się przetwarzania danych osobowych na zewnętrznych nośnikach magnetycznych, optycznych i innych oraz ich przesyłania pocztą elektroniczną bez uprzedniego zaszyfrowania.
3. Każdy użytkownik nośnika magnetycznego, optycznego lub innego, na którym miałyby być przetwarzane dane osobowe zobowiązany jest do jego zewidencjonowania u Administratora Bezpieczeństwa Informacji.
4. Na nośnikach, o których mowa w pkt. 3, dopuszczalne jest przetwarzanie jedynie jednostkowych danych osobowych.
5. Nośniki magnetyczne z zaszyfrowanymi jednostkowymi danymi osobowymi są na czas ich użyteczności przechowywane w zamkniętych na klucz szafach, a po wykorzystaniu dane na nich zawarte są trwale usuwane lub nośniki te są niszczone.

6. Zewidencjonowane przez ABI nośniki zawierające dane osobowe, po ustaniu przydatności muszą zostać zniszczone, w obecności ABI, sposób uniemożliwiający ponowne odtworzenie informacji. Cały proces musi zostać odnotowany w prowadzonym rejestrze.
7. W przypadku uszkodzenia lub zużycia nośnika zawierającego dane osobowe należy fizycznie zniszczyć nośnik poprzez np.: demagnetyzację uniemożliwiając jego nieuprawnione wykorzystania.
8. Dyski twarde z danymi osobowymi należy niszczyć zgodnie z obowiązującymi przepisami dotyczącymi gospodarki środkami trwałymi oraz wartościami niematerialnymi.
9. Nośniki magnetyczne raz użyte do przetwarzania danych osobowych nie mogą być wykorzystywane do innych celów mimo usunięcia danych i podlegają ochronie w trybie niniejszej instrukcji.
10. W przypadku posługiwania się nośnikami danych pochodzącymi od podmiotu zewnętrznego użytkownik jest zobowiązany do sprawdzenia go programem antywirusowym oraz do zarejestrowania tego nośnika u ABI.
11. Nośniki informatyczne przechowywane są w miejscach, do których dostęp mają wyłącznie osoby upoważnione do przetwarzania danych osobowych i nie mogą zostać wyniesione poza teren budynku bez zgody ABI.
12. Wynoszone wydruki i nośniki informacji muszą zostać zabezpieczone przed kradzieżą, zgubieniem lub zniszczeniem przez ich szyfrowanie.
13. Osoba użytkująca komputer przenośny, zawierający dane osobowe zachowuje wszelkie środki ostrożności podczas jego transportu, przechowywania i użytkowania poza Urzędem.
14. Przekazywanie nośników zawierających dane osobowe innemu podmiotowi może się odbyć jedynie za zgodą Administratora danych.

	Urząd Gminy Stalno	Data wydania:	29.04.2011
	Załącznik nr 6 do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych.	Ilość stron:	Strona 33 z 48
		Wydanie:	pierwsze

Sposób, miejsce i okres przechowywania kopii zapasowych		
INSTRUKACJA ADMINISTRACYJNO - TECHNICZNA		
1.	Numer	6
2.	Wersja	01
3.	Odwołania do innych dokumentów	
4.	Status	Obowiązująca
5.	Data wygaśnięcia	
6.	Pracownik wdrażający	Administrator Systemu Informatycznego
7.	Zatwierdzający procedurę	Wójt
8.	Lista dystrybucyjna	Kierownicy komórek organizacyjnych, Administrator Bezpieczeństwa Informacji, Użytkownicy systemu informatycznego na samodzielnych stanowiskach pracy

1. Zgodnie z wymogami pkt IV ppkt 4a załącznika do rozporządzenia MSWiA z dnia 29 kwietnia 2004 roku², kopie zapasowe przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem.
2. Kopie zapasowe zbiorów danych osobowych oraz oprogramowania i narzędzi programowych zastosowanych do przetwarzania danych są przechowywane w szafie metalowej.
3. Kopie zapasowe usuwa się niezwłocznie po ustaniu ich użyteczności.

² 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. Nr 100, poz. 1024)

	Urząd Gminy Stolno	Data wydania:	29.04.2011
	Załącznik nr 7 do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych.	Ilość stron:	Strona 34 z 48
		Wydanie:	pierwsze

Sposób, miejsce i okres przechowywania dokumentacji papierowej

INSTRUKACJA ADMINISTRACYJNO - TECHNICZNA		
1.	Numer	7
2.	Wersja	01
3.	Odwołania do innych dokumentów	
4.	Status	Obowiązująca
5.	Data wygaśnięcia	
6.	Pracownik wdrażający	Administrator Systemu Informatycznego
7.	Zatwierdzający procedurę	Wójt
8.	Lista dystrybucyjna	Kierownicy komórek organizacyjnych, Administrator Bezpieczeństwa Informacji, Użytkownicy systemu informatycznego na samodzielnych stanowiskach pracy.

1. Wydruki z danymi osobowymi przechowywane są w pomieszczeniach stanowiących obszar przetwarzania danych osobowych,
2. Po zakończeniu pracy przez użytkowników, wydruki są zamykane w szafach biurowych,
3. Dane osobowe zapisane w formie papierowej, nie podlegające regulacjom przepisów ustawy o narodowym zasobie archiwalnym i archiwach,³ po ich wykorzystaniu i po ustaniu ich użyteczności, należy zniszczyć w sposób uniemożliwiający ich ponowne odtworzenie /np.: przy wykorzystaniu niszczarki do dokumentów co najmniej 3 klasy utajnienia /.

³ Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (tekst jednolity Dz. U. z 2006 r. Nr 97, poz. 973; zm. z 2006 r. Dz. U. Nr 104, poz. 708, Dz. U. Nr 170, poz. 1217, Dz. U. Nr 220, poz. 1600; zm. z 2007 r. Dz. U. Nr 64, poz. 426; zm. z 2008 r. Dz. U. Nr 227, poz. 1505; zm. z 2009 r. Dz. U. Nr 39, poz. 307, Dz. U. Nr 166, poz. 1317; zm. z 2010 r. Dz. U. Nr 40, poz. 230, Dz. U. Nr 47, poz. 278, Dz. U. Nr 182, poz. 1228)

	Urząd Gminy Stolino	Data wydania:	29.04.2011
	Załącznik nr 8 do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych.	Ilość stron:	Strona 35 z 48
		Wydanie:	pierwsze

**Sposób zabezpieczenia systemu informatycznego przed
działalnością oprogramowania, o którym mowa w pkt III ppkt 1
załącznika do rozporządzenia MSWiA z dnia 29 kwietnia 2004 r.
(Dz. U. Nr 100, poz. 1024)**

INSTRUKACJA ADMINISTRACYJNO - TECHNICZNA		
1.	Numer	8
2.	Wersja	01
3.	Odwołania do innych dokumentów	
4.	Status	Obowiązująca
5.	Data wygaśnięcia	
6.	Pracownik wdrażający	Administrator Systemu Informatycznego
7.	Zatwierdzający procedurę	Wójt
8.	Lista dystrybucyjna	Kierownicy komórek organizacyjnych, Administrator Bezpieczeństwa Informacji, Użytkownicy systemu informatycznego na samodzielnych stanowiskach pracy

1. Oprogramowanie użytkowe oraz systemowe wykorzystywane w Urzędzie jest automatycznie, aktualizowane poprzez poprawki dostarczane przez producenta oprogramowania.
2. Z komputera można pobrać dane tylko w przypadku jego połączenia z siecią komputerową lub przy użyciu urządzeń wejścia-wyjścia takich jak stacje dysków, nagrywarki CD/DVD, porty USB. W przypadku próby pobrania danych przy użyciu urządzeń zewnętrznych niezbędny jest bezpośredni dostęp osoby nieuprawnionej do komputera, co jest wyeliminowane procedurą dostępu do stanowiska komputerowego. W celu ochrony danych przed ich uszkodzeniem zakazane jest instalowanie nielicencjonowanego oraz pochodzącego z niesprawdzonych źródeł oprogramowania.
3. W przypadku podłączenia stacji roboczej do sieci komputerowej oprogramowanie, które chciałoby uzyskać dostęp do systemu informatycznego może tego dokonać za pośrednictwem owej sieci bez użycia urządzeń wejścia-wyjścia. Wrogie oprogramowanie typu np. „koń trojański” może po zainstalowaniu na komputerze lokalnym próbować wysłać dane z dysku do

innego komputera. W tym przypadku zachowane są minimum te same zabezpieczenia, co w przypadku stanowisk wydzielonych, ze szczególnym uwzględnieniem bieżącej aktualizacji programu antywirusowego, systemu i aplikacji.

4. Obszar systemu informatycznego, który jest najbardziej narażony na ingerencję wirusów komputerowych tworzą stacje robocze Urzędu, do których szkodliwe oprogramowanie może przedostać się ze strony WWW, nośników danych USB, FDD, CD-R, DVD-R lub za pośrednictwem poczty elektronicznej.
5. Dla zminimalizowania skutków samoistnego zainstalowania się szkodliwego oprogramowania zostały ograniczone uprawnienia użytkowników na stacjach roboczych.
6. Sprawdzanie obecności wirusów komputerowych w systemie informatycznym oraz ich usuwanie odbywa się przy wykorzystaniu oprogramowania Kaspersky, zainstalowanego na serwerach, stacjach roboczych oraz komputerach przenośnych przez Administratora Systemu Informatycznego.
7. Oprogramowanie, o którym mowa w pkt 6, sprawuje ciągły nadzór (auto-ochrona) nad pracą systemu i jego zasobami oraz serwerami i stacjami roboczymi.
8. Niezależnie od ciągłego nadzoru, o którym mowa w pkt 7, Administrator Systemu Informatycznego nie rzadziej niż raz na kwartał na 3 wybranych losowo stanowiskach, przeprowadza kontrolę obecności wirusów komputerowych w systemie oraz jego zasobach, jak również na serwerach i stacjach roboczych.
9. Na serwerze poczty elektronicznej ochrona antywirusowa wzmocniona jest filtrem antyspamowym.
10. Do obowiązków Administratora Systemu Informatycznego należy aktualizacja oprogramowania antywirusowego oraz określenie częstotliwości automatycznych aktualizacji definicji wirusów, dokonywanych przez to oprogramowanie.
11. Użytkownik jest obowiązany zawiadomić Administratora Systemu Informatycznego o pojawiających się komunikatach, wskazujących na wystąpienie zagrożenia wywołanego szkodliwym oprogramowaniem.
12. Każdy użytkownik sieci komputerowej Urzędu został poinformowany o postępowaniu

w przypadku sygnalizowania przez oprogramowanie zabezpieczające o wykryciu wirusa.

13. Użytkownicy mogą korzystać z zewnętrznych nośników danych tylko po uprzednim sprawdzeniu zawartości nośnika oprogramowaniem antywirusowym.
14. Dostęp pracowników do Internetu możliwy jest jedynie przez sieć lokalną Urzędu oraz za pomocą urządzeń stanowiących wyposażenie Urzędu Gminy i dopuszczonych do użytkowania przez ASI.
15. W sieci lokalnej z dostępem do sieci publicznej, stosuje się wszystkie wymienione zabezpieczenia odseparowując jednocześnie stosownym zabezpieczeniem logicznym lub fizycznym możliwość nieautoryzowanej transmisji danych z sieci lokalnej do sieci publicznej.
16. Zabronione jest wykorzystywanie prywatnego sprzętu i urządzeń pozwalających na dostęp do Internetu z zewnętrznych źródeł jak np. GSM.
17. Nie należy udostępniać zasobów komputera lokalnego w sieci, gdyż stanowi to kolejne potencjalne zagrożenie dla komputera i zasobów.

	Urząd Gminy Stalno	Data wydania:	29.04.2011
	Załącznik nr 9 do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych.	Ilość stron:	Strona 38 z 48
		Wydanie:	pierwsze

**Sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4
rozporządzenia MSWiA z dnia 29 kwietnia 2004 roku
Zasady i sposób odnotowywania w systemie informacji o udostępnieniu danych
osobowych**

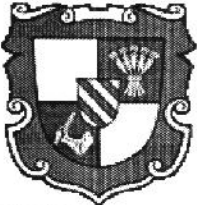
INSTRUKACJA ADMINISTRACYJNO - TECHNICZNA		
1.	Numer	9
2.	Wersja	01
3.	Odwołania do innych dokumentów	
4.	Status	Obowiązująca
5.	Data wygaśnięcia	
6.	Pracownik wdrażający	Administrator Bezpieczeństwa Informacji
7.	Zatwierdzający procedurę	Wójt
8.	Lista dystrybucyjna	Kierownicy komórek organizacyjnych, Administrator Bezpieczeństwa Informacji, Użytkownicy systemu informatycznego na samodzielnych stanowiskach pracy

1. W systemie informatycznym odnotowywane są informacje o odbiorcach danych z tego systemu.
2. Odbiorcą danych jest każdy, komu udostępnia się dane osobowe, z wyłączeniem:
 - osoby, której dane dotyczą,
 - użytkownika systemu lub innej osoby upoważnionej do przetwarzania danych osobowych w Urzędzie,
 - przedstawiciela, o którym mowa w art. 31a ustawy o ochronie danych osobowych⁴,
 - podmiotu, któremu powierzono przetwarzania danych,
 - organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

⁴ Ustawa z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity z 2002 r. Dz. U. 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) – „art. 31a. W przypadku przetwarzania danych osobowych przez podmioty mające siedzibę albo miejsce zamieszkania w państwie trzecim, administrator danych jest obowiązany wyznaczyć swojego przedstawiciela w Rzeczypospolitej Polskiej.”

3. Odnotowywane informacje obejmują:
 - data przekazania danych,
 - nazwę jednostki organizacyjnej lub imię i nazwisko osoby, której przekazano dane,
 - zakres przekazanych danych,
4. System nie zapewnia odnotowywanie informacji o udostępnieniu danych. Obowiązek ten spoczywa na użytkowniku systemu, który odnotowuje ten fakt w odpowiednio przeznaczonym polu w bazie danych.
5. Wypełnienie wspomnianego pola następuje z chwilą przekazania danych osobowych.
6. Udostępnianie danych osobowych następuje wyłącznie na pisemną prośbę odbiorcy danych w formie wniosku, o którym mowa w art. 29 ust. 3 ustawy o ochronie danych osobowych.⁵
7. Nadzór nad prawidłowym odnotowywaniem informacji o udostępnionych danych osobowych sprawuje Administrator Bezpieczeństwa Informacji.

⁵ patrz przypis 1 Ustawa op. cit. „art. 29 ust. 3. 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 wskazywać ich zakres i przeznaczenie.”

	Urząd Gminy Stolno	Data wydania:	29.04.2011
	Załącznik nr 10 do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych.	Ilość stron:	Strona 40 z 48
		Wydanie:	pierwsze

Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych

INSTRUKACJA ADMINISTRACYJNO - TECHNICZNA		
1.	Numer	10
2.	Wersja	01
3.	Odwolania do innych dokumentów	
4.	Status	Obowiązująca
5.	Data wygaśnięcia	
6.	Pracownik wdrażający	Administrator Bezpieczeństwa Informacji
7.	Zatwierdzający procedurę	Wójt
8.	Lista dystrybucyjna	Kierownicy komórek organizacyjnych, Administrator Bezpieczeństwa Informacji, Użytkownicy systemu informatycznego na samodzielnych stanowiskach pracy

1. Kontrole i testy przeprowadzane przez Administratora Bezpieczeństwa Informacji powinny obejmować zarówno dostęp do zasobów systemu, jak i profile oraz uprawnienia poszczególnych użytkowników.
2. Zapisy logów systemowych powinny być przeglądane przez Administratora Systemu Informatycznego każdorazowo po wykryciu naruszenia zasad bezpieczeństwa.
3. Konserwacja i przeglądy urządzeń tworzących system informatyczny Urzędu Gminy Stolno wykonywane są na bieżąco.
4. W Urzędzie Gminy Stolno osobami uprawnionymi do przeprowadzania przeglądów i konserwacji jest Informatyk Urzędu, a w szczególnych sytuacjach pracownik serwisu.
5. W przypadku zaistnienia potrzeby przekazania sprzętu komputerowego do naprawy przez specjalistów firmy zewnętrznej (serwisu) wykonywana jest kopia danych zapisanych na dysku, po czym następuje wymontowanie dysku z komputera.
6. W przypadku wystąpienia sytuacji, w której nie ma możliwości wymontowania dysku z urządzenia postępowanie jest prowadzone zgodnie z wymogiem określonym w punkcie VI

ppkt. 3 załącznika do rozporządzenia MSWiA z dnia 29 kwietnia 2004 roku⁶, który nakazuje, aby urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do naprawy, pozbawiać wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie, bądź też naprawiać je pod nadzorem osoby upoważnionej przez Administratora danych. Ponadto nośniki informatyczne zawierające dane osobowe przed ich przekazaniem są trwale pozbawiane zapisanych na nich informacji.

7. Przegląd programów i narzędzi programowych (np. zmiana wersji oprogramowania serwera, zmiana wersji oprogramowania na stanowisku komputerowym użytkownika, zmiana systemu operacyjnego serwera, wykonanie zmian w projekcie systemu spowodowanych koniecznością naprawy, modyfikacji czy konserwacji systemu) jest dokonywany w zależności od wystąpienia takiej potrzeby.

⁶ Rozporządzenie 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. Nr 100, poz. 1024)

	Urząd Gminy Stalno	Data wydania:	29.04.2011
	Załącznik nr 11 do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych.	Ilość stron:	Strona 42 z 48
		Wydanie:	pierwsze

Instrukcja korzystania z systemu teleinformatycznego		
INSTRUKACJA ADMINISTRACYJNO - TECHNICZNA		
1.	Numer	11
2.	Wersja	01
3.	Odwołania do innych dokumentów	
4.	Status	Obowiązująca
5.	Data wygaśnięcia	
6.	Pracownik wdrażający	Administrator Bezpieczeństwa Informacji
7.	Zatwierdzający procedurę	Wójt
8.	Lista dystrybucyjna	Kierownicy komórek organizacyjnych, Administrator Bezpieczeństwa Informacji, Użytkownicy systemu informatycznego na samodzielnych stanowiskach pracy

§ 1

Użytkownikom systemu teleinformatycznego zabrania się:

1. udostępniania hasła innym osobom oraz przechowywania go w formie pisemnej, w łatwo dostępnym miejscu,
2. samowolnego podłączania jakichkolwiek urządzeń peryferyjnych (typu: aparat cyfrowy, drukarka),
3. korzystania z prywatnych skrzynek pocztowych,
4. wykorzystywania służbowej poczty elektronicznej do celów prywatnych,
5. udostępniania stanowisk roboczych oraz istniejących w nich danych (w postaci pisemnej lub elektronicznej) osobom nieupoważnionym,
6. wykorzystania sieci komputerowej w celach innych niż wyznaczone przez Administratora danych,
7. samowolnego instalowania i użytkowania programów komputerowych (posiadających lub nie posiadających licencji),

8. trwałego lub okresowego kopiowania programów w całości lub części bez zgody administratora systemu,
9. publicznego rozpowszechniania programów komputerowych lub ich kopii dla osób postronnych,
10. przenoszenia programów komputerowych z własnego stanowiska roboczego na inne stanowiska,
11. udostępniania osobom postronnym programów komputerowych przez możliwość dostępu do sieci wewnętrznej lub Internetu,
12. używania oprogramowania w większym zakresie niż pozwala na to umowa licencyjna,
13. używania nośników udostępnianych przez osoby postronne i podejrzanych z zainfekowanie wirusem

W przypadku podejrzenia o zainfekowanie wirusem nośnika danych (dyskietki lub dysku twardego) użytkownik ma obowiązek niezwłocznie poinformować o tym Administratora danych osobowych lub inną uprawnioną osobę.

§ 2

Każdy użytkownik stacji roboczej zobowiązany jest do:

1. Okresowej zmiany hasła zgodnie z polityką haseł (min. długość hasła – 8 znaków, hasło powinno być unikatowe, złożone z małych i dużych znaków oraz cyfr lub znaków specjalnych).
2. Blokowania stacji przy każdorazowym opuszczeniu stanowiska pracy.
3. Natychmiastowego poinformowania Administratora Bezpieczeństwa Informacji o każdej nieprawidłowości mogącej mieć wpływ na naruszenie bezpieczeństwa systemu teleinformatycznego.

	Urząd Gminy Stolno	Data wydania:	29.04.2011
	Załącznik nr 12 do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych.	Ilość stron:	Strona 44 z 48
		Wydanie:	pierwsze

Sposób, zakres i tryb udostępniania danych zgromadzonych w rejestrach publicznych prowadzonych w Urzędzie Gminy Stolno

INSTRUKACJA ADMINISTRACYJNO - TECHNICZNA		
1.	Numer	12
2.	Wersja	01
3.	Odwołania do innych dokumentów	
4.	Status	Obowiązująca
5.	Data wygaśnięcia	
6.	Pracownik wdrażający	Administrator Bezpieczeństwa Informacji
7.	Zatwierdzający procedurę	Wójt
8.	Lista dystrybucyjna	Kierownicy komórek organizacyjnych, Administrator Bezpieczeństwa Informacji, Użytkownicy systemu informatycznego na samodzielnych stanowiskach pracy

1. Dane zgromadzone w rejestrach publicznych prowadzonych w Urzędzie Gminy Stolno udostępnia się podmiotowi publicznemu oraz podmiotowi niebędącemu podmiotem publicznym realizującym zadania publiczne na podstawie odrębnych przepisów bądź na skutek powierzenia lub zlecenia ich realizacji przez podmiot publiczny⁷ - wyłącznie do realizacji tychże zadań publicznych.
2. Dane udostępnia Wójt Gminy Stolno na wniosek spełniający wymagania określone w § 2 ust. 2 rozporządzenia⁸ wg załączonego wzoru będącego załącznikiem do wspomnianego aktu prawnego.
3. Dane udostępnia się na warunkach, w sposób, w zakresie i w terminie określonym w przepisach, na których podstawie rejestr jest prowadzony, a jeżeli przepisy te nie określają terminu – dane udostępnia się nie później niż w ciągu 14 dni od dnia doręczenia wniosku o ich udostępnienie. Dane udostępnia się w formie papierowej lub na nośnikach

⁷ § 1 Rozporządzenia Rady Ministrów z dnia 27 września 2005 r. w sprawie sposobu, zakresu i trybu udostępniania danych zgromadzonych w rejestrze publicznym (Dz. U. Nr 205, poz. 1692).

⁸ Rozporządzenie Rady Ministrów z dnia 27 września 2005 r. op. cit.

elektronicznych (dyskietka, CD). Dane w formie elektronicznej udostępnia się w formatach: doc, rtf, xls, PDF.

4. Podmiot, któremu udostępniono dane, jest zobowiązany do ich zabezpieczenia przed dostępem osób nieupoważnionych lub nieuprawnioną zmianą ich zawartości oraz przed ich wykorzystaniem niezgodnym z celem, dla którego zostały uzyskane, odpowiada za bezpieczeństwo i integralność uzyskanych danych. W związku z tym podmiot ten jest zobowiązany posiadać zabezpieczenia techniczne i organizacyjne gwarantujące ochronę udostępnionych danych w ww. aspektach.

.....
(nazwa podmiotu ubiegającego się o udostępnienie danych zgromadzonych w rejestrze)

.....
(adres siedziby wnioskodawcy)

.....
(Nr REGON wnioskodawcy)

.....
(nazwa podmiotu, do którego jest skierowany wniosek)

WNIOSEK

o udostępnienie danych zgromadzonych w rejestrze publicznym

1.
(wskazanie zadania publicznego i podstawy prawnej jego realizacji przez podmiot ubiegający się o udostępnienia danych zgromadzonych w rejestrze, którego wykonanie wymaga udostępnienia tych danych)

.....

2.
(określenie rejestru, w którym są zgromadzone dane, które mają być udostępnione)

3.
(zakres żądanych danych i wskazanie sposobu ich udostępniania)

.....

4.
(wskazanie okresu udostępnienia danych)

..... zobowiązuję się
(nazwa podmiotu)
do wykorzystywania udostępnionych danych wyłącznie do realizacji zadania publicznego
wskazanego w pkt 1.

..... oświadczam, że spełnia
(nazwa podmiotu)
warunki zabezpieczeń technicznych i organizacyjnych niezbędnych do uzyskania dostępu
do danych zgromadzonych w rejestrze wskazanym w pkt 2.

.....
(data, podpis, pieczęć osoby reprezentującej podmiot)

	Urząd Gminy Stolno	Data wydania:	29.04.2011
	Oświadczenie Załącznik nr 3 do Zarządzenia Nr 35/2011 z dnia 29.04.2011 r.	Ilość stron:	Strona 47 z 48
		Wydanie:	pierwsze

Do teczki personalnej pracownika

.....
imię i nazwisko pracownika

OŚWIADCZENIE

Oświadczam, że zapoznałem się z treścią:

„Polityki Bezpieczeństwa” oraz „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Stolno”.

Zobowiązuję się do stosowania zasad zawartych w tym dokumencie.

Stolno, dnia..... 2011 r.

.....
podpis pracownika

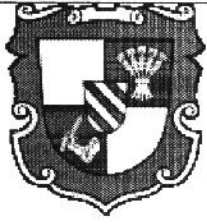
	Urząd Gminy Stalno	Data wydania:	29.04.2011
	Załącznik nr 4 do Zarządzenia Nr 35/2011 z dnia 29.04.2011 r.	Ilość stron:	Strona 1 z 2
		Wydanie:	pierwsze

HARMONOGRAM WDROŻENIA POLITYKI BEZPIECZEŃSTWA

Założenie wyjściowe: „Polityka bezpieczeństwa” zostaje podpisana przez Wójta w dniu 29.04.2011r.

1. **Do 16.05.2011r.** przekazanie wszystkim pracownikom polityki bezpieczeństwa w formie papierowej i elektronicznej.
2. **Do 24.05.2011r.** odebranie od pracowników oświadczenia, iż zapoznali się z polityką bezpieczeństwa (2 egz. Oświadczenia : 1 - teczka ABI, 2 – akta osobowe pracownika)
3. **Do 07.06.2011r.** – szkolenie dla wszystkich pracowników z zakresu wprowadzanych procedur (ze szkolenia lista obecności i protokół, pracownikom przekazać akty prawa)
4. **Do 22 czerwca 2011r.** szkolenia stanowiskowe pracowników.
5. **15-31.12.2011r.** Termin kontroli wszystkich postanowień wprowadzonych polityką
6. **01.08.2011** – Wprowadzenie załączników 1-12 do PB
7. **Wrzesień/Październik 2011r.** Przeprowadzenie symulacji na jedno z zagrożeń.
8. **Maj-lipiec 2011 r.** Analiza zgodności wewnętrznych aktów z polityką bezpieczeństwa
9. **Czerwiec 2011** – zestawienie potrzeb w zakresie dostosowania struktury organizacyjnej do polityki bezpieczeństwa
10. **Terminarz wprowadzenie do stosowania poszczególnych elementów polityki**

L.p	Nazwy poszczególnych elementów polityki bezpieczeństwa	Data wprowadzenia
1	Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym	01 lipca 2011
2	Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem.	01 lipca 2011
3	Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu.	01 lipca 2011
4	Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.	01 czerwiec 2011
5	Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe.	01 czerwiec 2011
6	Sposób, miejsce i okres przechowywania kopii zapasowych.	01 czerwiec 2011

	Urząd Gminy Stolno	Data wydania:	29.04.2011
	Załącznik nr 4 do Zarządzenia Nr 35/2011 z dnia 29.04.2011 r.	Ilość stron:	Strona 2 z 2
		Wydanie:	pierwsze

7	Sposób, miejsce i okres przechowywania dokumentacji papierowej.	01 czerwiec 2011
8	Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia MSWiA z dnia 29 kwietnia 2004 roku.	01 czerwiec 2011
9	Sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4 rozporządzenia MSWiA z dnia 29 kwietnia 2004 roku. Zasady i sposób odnotowywania w systemie informacji o udostępnieniu danych osobowych.	01 czerwca – w przypadku systemów, które takową opcję posiadają. W pozostałych przypadkach – systematycznie po wprowadzeniu takiej funkcji.
10	Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.	01 lipca 2011
11	Instrukcja korzystania z systemu teleinformatycznego.	01 czerwiec 2011
12	Sposób, zakres i tryb udostępniania danych zgromadzonych w rejestrach publicznych prowadzonych w Urzędzie Gminy Stolno	01 czerwiec 2011

11. **Do 01.06.2011r.** Wydanie zarządzenie w/s używania legalnego oprogramowania.
Dostosowanie rzeczy aktualnych do dnia 30.07.2011r.
12. **Do 01.06.2011r.** – Wydanie zarządzenie w/s zarządzania oprogramowanie.
13. **Do 01.06.2011r.** – Wydanie zarządzenia w/s kontroli ruchem osobowym w poszczególnych pokojach – wydawania kluczy.
14. **Do 01.09.2011r.** Wydanie zarządzenia w/s wprowadzenia procedury niszczenia dokumentów.
15. **Do 01.08.2011r** Wprowadzenie procedur wynikających z załącznika nr 12 do Polityki bezpieczeństwa.