Załącznik Nr 2
do Zarządzenia Nr 58/2011
Wójta Gminy Śniadowo
z dnia 08 września 2011r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

§1.
Postanowienia ogólne

1. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwana dalej „Instrukcją", określa procedury dotyczące zasad bezpieczeństwa przetwarzania danych osobowych oraz zasady postępowania administratora danych osobowych, osób przez niego wyznaczonych i użytkowników przetwarzających dane osobowe w Urzędzie.
2. Instrukcja ma zastosowanie także do podmiotów zewnętrznych i osób fizycznych, które współpracują z Urzędem i na podstawie przepisów współuczestniczą w procesie przetwarzania danych osobowych, a w szczególności:
   1) podmioty, którym na podstawie przepisów udostępniono dane osobowe,
   2) podmioty, którym na podstawie umowy przedstawiono lub udostępniono dane osobowe do przetwarzania,
   3) podmioty świadczące usługi związane z konserwacją systemu informatycznego,
   4) inne osoby niebędące pracownikami Urzędu, wykonujące pracę na podstawie stosunków cywilnoprawnych.
3. Instrukcja została opracowana na podstawie § 5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024) oraz ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, póz. 926 z późn. zm.).
4. Określenia i skróty użyte w Instrukcji oznaczają:
   1) **Ustawie** – należy przez to rozumieć - ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.)
   2) **Urzędzie** – należy przez to rozumieć - Urząd Gminy Śniadowo z siedzibą w Śniadowie, ul. Ostrołęcka 11, Zakład Gospodarki Komunalnej w Śniadowie z siedzibą przy ul. Ostrołęckiej 11, Gminny Ośrodek Kultury w Śniadowie z siedzibą przy ul. Ostrołęckiej 13 i Bibliotekę Publiczną w Śniadowie z siedzibą przy ul. Ostrołęckiej 7,
   3) **Administratorze Danych (ADO)**- należy przez to rozumieć Wójta Gminy Śniadowo,
   4) **Administratorze Bezpieczeństwa Informacji (ABI)** – należy przez to

rozumieć pracownika urzędu wyznaczonego przez Administratora Danych Osobowych (Wójta) do nadzorowania przestrzegania zasad ochrony danych osobowych oraz przygotowania dokumentów wymaganych przez przepisy ustawy o ochronie danych osobowych w Urzędzie Gminy Śniadowo, powołanego zarządzeniem Wójta Gminy Śniadowo,

5) **Użytkowniku systemu** – należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie. Użytkownikiem może być osoba zatrudniona w urzędzie na podstawie stosunku pracy, osoba wykonująca pracę na podstawie umowy zlecenia lub innej, umowy cywilno-prawnej, osoba odbywająca staż w urzędzie,

6) **Identyfikatorze użytkownika** – należy przez to rozumieć ciąg znaków jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,

7) **Administratorze Systemu Informatycznego (ASI)** – należy przez to rozumieć pracownika odpowiedzialnego za funkcjonowanie systemu teleinformatycznego, oraz stosowanie technicznych i organizacyjnych środków ochrony stosowanych w tym systemie, powołanego zarządzeniem Wójta Gminy Śniadowo,

8) **Sieci lokalnej** – należy przez to rozumieć połączenie komputerów pracujących w urzędzie w celu wymiany danych (informacji) dla własnych potrzeb, przy wykorzystaniu urządzeń telekomunikacyjnych,

9) **Sieci telekomunikacyjnej** – należy przez to rozumieć systemy transmisyjne oraz urządzenia komutacyjne lub przekierowujące, a także inne zasoby, które umożliwiają nadawanie, odbiór lub transmisję sygnałów za pomocą przewodów, fal radiowych, optycznych lub innych środków wykorzystujących energię elektromagnetyczną, niezależnie od ich rodzaju w rozumieniu ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800 z pożn. zm.),

10) **Publicznej sieci telekomunikacyjnej** - należy przez to rozumieć sieć telekomunikacyjną wykorzystywaną głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych w rozumieniu ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800 z pożn. zm.),

11) **Systemie informatycznym** – należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,

12) **Przetwarzaniu danych** – należy przez to rozumieć jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie,

13) **Zabezpieczeniu danych w systemie informatycznym** – należy przez to rozumieć wdrożenie i wykorzystywanie stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,

14) **Telekomunikacji** – należy przez to rozumieć nadawanie, odbiór lub transmisję

informacji, niezależnie od ich rodzaju, za pomocą przewodów, fal radiowych bądź optycznych lub innych środków wykorzystujących energię elektromagnetyczną,

15) **Aplikacji** – należy przez to rozumieć program komputerowy wykonujący konkretne zadanie,

16) **Komórce organizacyjnej** – należy przez to rozumieć gminne jednostki organizacyjna (GOK, ZGK, Biblioteka) referaty, samodzielne stanowiska pracy.

§2.
Nadawanie uprawnień do przetwarzania danych osobowych oraz ich rejestrowanie w systemie informatycznym

1. Przed przystąpieniem do pracy przy przetwarzaniu danych osobowych, każdy użytkownik powinien zostać zapoznany przez kierownika komórki organizacyjnej lub ABI z przepisami dotyczącymi ochrony danych osobowych.
2. Do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych, mogą zostać dopuszczone, z zastrzeżeniem ust. 3, wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych wydane przez ADO.
3. Do obsługi systemu informatycznego oraz do urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych, mogą zostać dopuszczone również osoby, którym udzielono upoważnień do przetwarzania danych osobowych na podstawie porozumień zawartych w sprawie powierzenia przetwarzania danych osobowych.
4. Wydanie upoważnienia oraz rejestracja użytkownika w systemie informatycznym przetwarzającym dane następuje na wniosek przełożonego użytkownika.
5. Procedury wydawania i odwoływania upoważnień dla użytkowników do przetwarzania danych osobowych realizowane są wg następujących zasad:
   1) przełożony składa do ADO pisemny wniosek, którego wzór stanowi **załącznik nr 1** do instrukcji;
   2) osoba ubiegająca się o nadanie upoważnienia składa pisemne oświadczenie o zachowaniu w tajemnicy zasad przetwarzania danych oraz sposobów ich zabezpieczania, obejmującej także okres po ustaniu stosunku pracy lub innej formy zatrudnienia bądź upoważnienia. Wzór oświadczenia stanowi **załącznik nr 2** do niniejszej instrukcji;
   3) oryginał upoważnienia zostaje przekazany użytkownikowi za potwierdzeniem odbioru, kopia zaś zostaje włączona do akt osobowych użytkownika oraz przekazana do wiadomości przełożonego.
6. Wyrejestrowanie użytkownika z systemu dokonuje się na wniosek ADO lub przełożonego użytkownika ASI po uzgodnieniu z ABI.
7. Osobie niebędącej pracownikiem Urzędu, ADO udziela upoważnienia na wniosek osoby przetwarzającej dane osobowe w systemach informatycznych Urzędu.
8. Użytkownik niebędący pracownikiem Urzędu otrzymuje oryginał upoważnienia za poświadczeniem odbioru. Kopia upoważnienia przechowywana jest na stanowisku ds. kadrowych Urzędu.
9. Przyznanie upoważnień do przetwarzania danych osobowych w systemie polega na wprowadzeniu do systemu identyfikatora, hasła oraz ustanowienia zakresu dostępnych danych i operacji dla każdego użytkownika. Wzór upoważnienia do przetwarzania danych stanowi **załącznik nr 3** do niniejszej instrukcji.
10. Za przydzielenie i wygenerowanie hasła użytkownikowi , który po raz pierwszy

korzysta z systemu , odpowiada ASI.

11. Identyfikator użytkownika nie może być zmieniany, a po wyrejestrowaniu użytkownika z systemu nie może być przydzielony innej osobie.
12. Przełożeni użytkownika zobowiązani są pisemnie informować ADO lub ABI o każdej zmianie dotyczącej użytkowników mającej wpływ na zakres posiadanych upoważnień do przetwarzania danych.
13. ABI jest zobowiązany do prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych według wzoru stanowiącego **załącznik nr 4** do instrukcji.

§3.
Stosowane metody i środki uwierzytelniania użytkownika oraz procedury związane z ich zarządzaniem i uwierzytelnianiem

1. System, w którym przetwarza się dane osobowe wyposażony jest w mechanizmy uwierzytelnienia użytkownika oraz kontroli dostępu użytkowników. Jednym z elementów umożliwiającym dostęp do systemu jest hasło, które pełni rolę weryfikowania tożsamości użytkownika.
2. Hasło dostępu składa się z ciągu literowo - cyfrowego i nie może kojarzyć się bezpośrednio z użytkownikiem. Hasła dostępu nie mogą powtarzać się w danym roku.
3. Hasło dostępu zapisywane jest na ekranie monitora w formie niejawnej i znane jest tylko użytkownikowi.
4. W przypadku gdy hasła dostępu używa się do uwierzytelnienia użytkownika w systemie powinno ono składać się z:
   1) co najmniej z 6 znaków - przy podstawowym poziomie bezpieczeństwa;
   2) co najmniej z 8 znaków - przy podwyższonym i wysokim poziomie bezpieczeństwa.
5. Użytkownik sam ustala hasło dostępu i w przypadku podejrzenia lub stwierdzenia jego ujawnienia niezwłocznie je zmienia. Jeżeli system nie wymusza zmiany hasła, użytkownik ma obowiązek zmieniać je co najmniej raz w miesiącu.
6. Hasła dostępu do baz danych są różne od haseł uwierzytelniających użytkowników w systemie.
7. Identyfikator przyznaje się użytkownikom w przypadku dostępu do stanowiska komputerowego więcej niż jednej osoby.
8. Identyfikator użytkownika składa się z ciągu znaków literowych, cyfrowych lub innych jednoznacznie identyfikujących w systemie osobę upoważnioną do przetwarzania danych osobowych.
9. Identyfikator użytkownikowi przyznaje ASI, o czym informuje ABI.
10. Identyfikator podlega wpisowi do " Ewidencji osób upoważnionych do przetwarzania danych osobowych" i po jego wyrejestrowaniu nie może być przydzielony innej osobie.
11. Podczas przetwarzania danych osobowych w systemie posługiwanie się identyfikatorem innej osoby jest zabronione.
12. Użytkownik ponosi odpowiedzialność za czynności wykonywane w systemie przy użyciu identyfikatora i hasła. Nie dopuszcza się aby hasła były przechowywane przez użytkownika w formie jakiegokolwiek zapisu.
13. Administrator dopuszcza możliwość stosowania do weryfikacji tożsamości użytkowników w systemie innych sposobów, np: karty mikroprocesorowe lub metody biometryczne.
14. Osobą odpowiedzialną za prawidłowe funkcjonowanie w systemie mechanizmów uwierzytelniających jest ASI.

§4.
Rozpoczęcie, zawieszenie i zakończenie pracy przez użytkowników systemu

1. Użytkownik, rozpoczynając pracę na komputerze, loguje się do systemu informatycznego.
2. Dostęp do danych osobowych możliwy jest jedynie po dokonaniu uwierzytelnienia użytkownika.
3. Maksymalna liczba prób wprowadzenia hasła przy logowaniu się do systemu informatycznego wynosi 3. Po przekroczeniu tej liczby prób logowania system blokuje dostęp do zbioru danych na poziomie danego użytkownika. Odblokowania dostępu do zbioru danych może dokonać ASI w porozumieniu z ABI.
4. W przypadku braku aktywności użytkownika na komputerze przez czas dłuższy niż 10 minut następuje automatyczne włączenie wygaszacza ekranu.
5. Monitory stanowisk komputerowych, na których przetwarzane są dane osobowe, znajdujące się w pomieszczeniach, gdzie przebywają osoby, które nie posiadają upoważnień do przetwarzania danych, należy ustawić w taki sposób, aby uniemożliwić tym osobom wgląd w dane.
6. Przebywanie osób nieuprawnionych w pomieszczeniach znajdujących się na obszarze, w którym są przetwarzane dane osobowe, jest dopuszczalne tylko w obecności osoby upoważnionej.
7. Pomieszczenia, w których przetwarzane są dane osobowe, należy zamykać na czas nieobecności osób upoważnionych, w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym.
8. Przed opuszczeniem stanowiska pracy użytkownik jest obowiązany:
   1) wylogować się z systemu informatycznego
   albo
   2) wywołać blokowany hasłem wygaszacz ekranu.
9. Kończąc pracę użytkownik jest zobowiązany:
   1) wylogować się z systemu, a następnie wyłączyć sprzęt komputerowy,
   2) zabezpieczyć stanowisko pracy.
10. Wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się dane osobowe, przechowuje się szafach zamykanych na klucz.

§5.
Tworzenie kopii zapasowych zbiorów danych oraz programów i narzędzi służących do ich przetwarzania

1. Dane osobowe przetwarzane w systemie informatycznym podlegają zabezpieczeniu, poprzez tworzenie kopii zapasowych.
2. Za tworzenie kopii zapasowych zbiorów danych osobowych odpowiedzialny jest ASI.
3. W przypadku lokalnego przetwarzania danych na służbowych komputerach, użytkownicy systemu informatycznego zobowiązani są do centralnego przechowywania kopii danych, tak aby możliwe było zabezpieczenie ich dostępności poprzez wykonanie kopii zapasowych.
4. Przez centralne przechowywanie kopii danych rozumie się cotygodniowe przegrywanie zbioru danych na specjalnie wydzielony do tego celu obszar dysku na serwerze. Jeśli z przyczyn technicznych nie jest to możliwe, użytkownicy są zobowiązani do sporządzenia kopii zapasowych zbiorów danych na nośniku danych i przechowywania w szafie zamykanej na klucz.
5. Kopie zapasowe zbiorów danych należy okresowo sprawdzać pod kątem ich

przydatności do odtworzenia w przypadku awarii systemu informatycznego. Za przeprowadzenie tej procedury odpowiedzialny jest ASI.

6. Kopie zapasowe wykonywane są zgodnie z następującym harmonogramem:
   1) kopia zapasowa aplikacji przetwarzającej dane osobowe - pełna kopia wykonywana jest po wprowadzeniu zmian do aplikacji i zapisywana na nośnikach danych;
   2) kopia zapasowa danych osobowych przetwarzanych przez aplikację - pełna kopia wykonywana jest raz w tygodniu, a w przypadku wprowadzania znacznych zmian danych, może być wykonywana częściej;
   3) kopia zapasowa danych konfiguracyjnych systemu, w tym uprawnień użytkownika systemu - pełna kopia wykonywana jest raz w miesiącu.
7. Kopie zapasowe przechowywane są w szafie zamykanej na klucz.

§6.
Sposób, miejsce i okres przechowywania elektronicznych nośników danych zawierających dane osobowe oraz kopii zapasowych

1. Użytkownicy nie mogą wynosić z terenu Urzędu nośników i wydruków z zapisanymi danymi osobowymi, bez zgody ADO lub ABI.
2. Elektroniczne nośniki informacji zawierające dane oraz wydruki przechowuje się wewnątrz obszaru przetwarzania danych, w meblach biurowych posiadających sprawne zamknięcia.
3. Kopie zapasowe przechowuje się w szafach metalowych w pomieszczeniach, które nie są stałym miejscem ich przetwarzania i zapewniają właściwą ochronę przed nieuprawnionym dostępem, modyfikacją uszkodzeniem lub zniszczeniem.
4. Usunięcie danych z systemu powinno być zrealizowane przy pomocy oprogramowania przeznaczonego do bezpiecznego usuwania danych z nośnika danych. Za zniszczenie kopii zapasowych sporządzanych indywidualnie przez użytkownika odpowiada użytkownik.
5. Dane osobowe w postaci elektronicznej należy usuwać z nośnika danych w sposób uniemożliwiający ich ponowne odtworzenie, nie później niż po upływie 5 dni po wykorzystaniu tych danych, chyba, że z odrębnych przepisów wynika obowiązek ich przechowywania.
6. Nośniki danych podlegają komisyjnemu zniszczeniu w przypadku wycofania z eksploatacji sprzętu komputerowego, na którym przetwarzane były dane osobowe oraz po przeniesieniu danych osobowych do zbiorów danych osobowych w systemie informatycznym z nośników, których ponowne wykorzystanie nie jest możliwe. Z przeprowadzonych czynności komisja sporządza protokół.
7. Przez zniszczenie nośników danych należy rozumieć ich trwałe i nieodwracalne zniszczenie fizyczne do stanu uniemożliwiającego ich rekonstrukcję i odzyskanie danych.
8. Niepotrzebne wydruki z systemu, które zawierają dane osobowe należy niszczyć w niszczarkach w sposób uniemożliwiający ich odtworzenie.

§7.
Sposób zabezpieczenia systemu informatycznego przed działaniem oprogramowani, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

1. Za ochronę antywirusową systemu informatycznego odpowiada ASI.
2. System antywirusowy zainstalowany jest w każdym komputerze.
3. Programy antywirusowe są uaktywnione przez cały czas pracy każdego komputera w systemie informatycznym.

4. Wszystkie pliki otrzymywane z zewnątrz, jak również wysyłane na zewnątrz, podlegają automatycznemu sprawdzeniu przez system antywirusowy pod kątem występowania wirusów, z zastosowaniem najnowszej dostępnej wersji programu antywirusowego.
5. W przypadku pojawienia się wirusa, użytkownik obowiązany jest zaprzestać wykonywania jakichkolwiek czynności w systemie i niezwłocznie powiadomić o tym fakcie ASI lub ABI.
6. Niedozwolone jest otwieranie wiadomości poczty elektronicznej i załączników od "niezaufanych" nadawców.
7. Niedozwolone jest wyłączanie, blokowanie i odinstalowywanie programów zabezpieczających komputer przed oprogramowaniem złośliwym oraz nieautoryzowanym dostępem (skaner antywirusowy, firewall).
8. ASI jest odpowiedzialny za aktywowanie i poprawne konfigurowanie specjalistycznego oprogramowania monitorującego wymianę danych na styku:
   1) sieci lokalnej i sieci publicznej;
   2) stanowiska komputerowego użytkownika systemu i pozostałych urządzeń wchodzących w skład sieci lokalnej.

§8.
Udostępnianie danych osobowych i sposób odnotowywania informacji o udostępnieniu danych

1. Dane osobowe przetwarzane w Urzędzie mogą być udostępnione osobom lub podmiotom uprawnionym do ich otrzymania, na mocy ustawy o ochronie danych osobowych oraz innych przepisów powszechnie obowiązujących.
2. Dane osobowe udostępnia się na pisemny, umotywowany wniosek, chyba że przepisy odrębne stanowią inaczej.
3. Dane udostępnione Urzędowi przez inne podmioty można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
4. ABI prowadzi ewidencję udostępnionych danych, która zawiera:
   1) adresata udostępnianych danych;
   2) zakres udostępnionych danych;
   3) datę udostępnienia.
5. Kierownicy komórek organizacyjnych są zobowiązani do zgłaszania faktu udostępniania danych Administratorowi Bezpieczeństwa Informacji, który dokonuje odpowiednich zapisów w ewidencji.
6. Zgłoszenie faktu udostępnienia danych oraz odnotowanie tej informacji w ewidencji powinno nastąpić niezwłocznie po udostępnieniu danych.

§9.
Wykonywanie przeglądów i konserwacji systemu oraz nośników danych służących do przetwarzania danych

1. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe mogą być wykonywane przez ASI.
2. ASI okresowo sprawdza możliwość odtworzenia danych z kopii zapasowych. Częstotliwość wykonywania procedury odtwarzania danych jest uzgadniana z ABI.
3. Aktualizacja oprogramowania powinna być przeprowadzana zgodnie z zaleceniami producentów oraz opinią rynkową, co do bezpieczeństwa i stabilności nowych wersji.
4. Za terminowość przeprowadzania przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada ASI.

5. Nieprawidłowości w działaniu systemu informatycznego oraz oprogramowania są niezwłocznie usuwane przez ASI, a ich przyczyny analizowane.
6. Zmiana konfiguracji sprzętu komputerowego, na którym znajdują się dane osobowe lub zmiana jego lokalizacji, może być dokonywana tylko za wiedzą i zgodą ABI.

§10.

Postępowanie w przypadku naruszenia ochrony danych osobowych

1. Każdy użytkownik, który stwierdza lub podejrzewa naruszenie ochrony danych w systemie informatycznym, zobowiązany jest niezwłocznie poinformować ASI.
2. Do czasu przybycia ASI na miejsce naruszenia lub ujawnienia naruszenia ochrony danych, należy:
   1) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia;
   2) rozważyć wstrzymanie bieżącej pracy na komputerze w celu zabezpieczenia miejsca zdarzenia;
   3) zaniechać, o ile to możliwe, dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić jego udokumentowanie i analizę;
   4) udokumentować wstępnie zaistniałe naruszenie;
   5) nie opuszczać, bez uzasadnionej potrzeby, miejsca zdarzenia do czasu przybycia ASI lub ABI.
3. Po przybyciu na miejsce naruszenia lub ujawnienia naruszenia ochrony danych osobowych ASI:
   1) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania;
   2) może żądać wyjaśnień dotyczących zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem;
   3) dokonuje zabezpieczenia systemu informatycznego przed dalszym rozprzestrzenianiem się skutków naruszenia;
   4) podejmuje odpowiednie kroki w celu powstrzymania lub ograniczenia dostępu osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów lub naruszenia;
   5) rozważa celowość i potrzebę powiadomienia o zaistniałym naruszeniu ADO.
4. Po wyczerpaniu niezbędnych środków doraźnych, ASI zasięga niezbędnych opinii i proponuje działania mające na celu usunięcie naruszenia i jego skutków oraz ustosunkowuje się do kwestii ewentualnego odtworzenia danych z kopii zapasowej i terminu wznowienia przetwarzania danych.
5. ABI dokumentuje zaistniały przypadek naruszenia oraz sporządza raport według wzoru stanowiącego **załącznik nr 5** do niniejszej Instrukcji.
6. ABI przekazuje raport ADO w terminie 14 dnia od daty zdarzenia.
7. Po przywróceniu prawidłowego funkcjonowania systemu informatycznego, ASI przeprowadza szczegółową analizę w celu określenia przyczyn naruszenia ochrony danych osobowych lub podejrzenia takiego naruszenia oraz podejmuje kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.
8. Za naruszanie ochrony danych osobowych obowiązują następujące kary:
   1) Kto przetwarza w zbiorze dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do których przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
   2) Kto będąc obowiązany do ochrony danych osobowych udostępnia je lub

umożliwia dostęp do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawiania wolności do lat 2.

3) Jeżeli sprawca działa nieumyślnie, podlega grzywnie, karze ograniczenia wolności lub pozbawienia wolności do roku.

4) Kto narusza choćby nieumyślnie obowiązek zabezpieczenia ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

5) Za naruszenie ochrony danych osobowych kierownik urzędu może stosować kary porządkowe, niezależnie od zastosowania kar, o których mowa wyżej.

WÓJT

mgr Rafał Pstrągowski

Załącznik nr 1
do Instrukcji zarządzania
systemem informatycznym

WZÓR

WNIOSEK O NADANIE UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM/ NADANIE UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM

Nowy użytkownik*/**	**Modyfikacja uprawnień*/****	**Odebranie uprawnień w systemie*/****
Imię nazwisko użytkownika		**Komórka organizacyjna**
.....		.....
<u>Opis zakresu uprawnień użytkownika w systemie informatycznym:</u> Wprowadzanie, edycja i modyfikacja danych w systemie ..... Udostępnianie i przesyłanie zgromadzonych danych z programu ..... jednostce monitorującej –		
Data wystawienia:		**Popis bezpośredniego przełożonego użytkownika systemu:** .....
Podpis Kierownika Urzędu		

-właściwe podkreśl/ - niepotrzebne skreśl*

PRZYKŁAD

WNIOSEK O NADANIE UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM

Nowy użytkownik	~~**Modyfikacja uprawnień**~~	~~**Odebranie uprawnień w systemie**~~

Imię nazwisko użytkownika	**Komórka organizacyjna**
Ewa Nowak	Referat Finansów

Opis zakresu uprawnień użytkownika w systemie informatycznym:

Wprowadzanie, edycja i modyfikacja danych w systemie Płatnik,

Udostępnianie i przesyłanie zgromadzonych danych z programu Płatnik jednostce monitorującej – Zakład Ubezpieczeń Społecznych,

Wprowadzanie, edycja i modyfikacja danych w systemie Home - Banking,

Data wystawienia:	**Popis bezpośredniego przełożonego użytkownika systemu:**
.....	.....

Podpis Kierownika Urzędu

.....

Załącznik nr 2
do Instrukcji zarządzania
systemem informatycznym

WZÓR

.....
(imię i nazwisko pracownika)
.....
(adres)
.....

Śniadowo, dnia. .....

OŚWIADCZENIE

Oświadczam, iż w związku z wykonywanymi obowiązkami służbowymi, przetwarzam lub mam dostęp do zbiorów, dokumentów, zestawień, kartotek lub systemów informatycznych zawierających dane osobowe i w związku z tym:

1. stwierdzam własnoręcznym podpisem, iż znana mi jest treść przepisów:
a) ustawy o ochronie danych osobowych,
b) 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 osobowych,
c) „Polityki bezpieczeństwa ",
d) „Instrukcji zarządzania systemem informatycznym".

2. zobowiązuję się nie ujawniać wiadomości, z którymi zapoznałem/zapoznałam* się z racji wykonywanej pracy w Urzędzie, a w szczególności nie będę:
a) ujawniać danych zawartych w użytkowanych w Urzędzie systemach informatycznych, zwłaszcza danych osobowych znajdujących się w tych systemach,
b) ujawniać szczegółów technologicznych używanych w Urzędzie systemów oraz oprogramowań,
c) udostępniać osobom nieupoważnionym nośników magnetycznych i optycznych oraz wydruków komputerowych zawierających dane osobowe,
d) kopiować lub przetwarzać danych w sposób inny niż dopuszczony obowiązującą „Instrukcją zarządzania systemem informatycznym " .

.....
(podpis pracownika składającego oświadczenie)

* niepotrzebne

Załącznik nr 3
do Instrukcji zarządzania
systemem informatycznym

WZÓR

Śniadowo, dnia .....

UPOWAŻNIENIE IMIENNE NR .....
do przetwarzania danych osobowych

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) **upoważniam Panią / Pana**:

....
(imię i nazwisko osoby upoważnionej)

zatrudnioną (ego) w:

...
....
(nazwa jednostki i komórki organizacyjnej)

na stanowisku:

....

do przetwarzania danych osobowych w zakresie:

....

Nadaję identyfikator: .....

.....
(podpis administratora danych)

Otrzymałam (em) i przyjęłam (em) do realizacji:

dnia .....

.....
(podpis upoważnionego pracownika)

Załącznik nr 4
do Instrukcji zarządzania
systemem informatycznym

WZÓR

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH W SYSTEMIE INFORMATYCZNYM

L.p.	Identyfikator użytkownika*	Imię i nazwisko	Zakres upoważnienia do przetwarzania danych osobowych	Data nadania uprawnień w systemie	Data odebrania uprawnień w systemie
1					
	Zmiany danych**				
2					
	Zmiany danych**				
3					
	Zmiany danych**				
4					
	Zmiany danych**				

**Wypełnia się tylko dla osób upoważnionych do przetwarzania danych osobowych, które zostały dopuszczone do przetwarzania danych osobowych w systemie,*
***Jeżeli zmiany danych dotyczą tylko niektórych rubryk, np. miejsca pracy; pozostałe rubryki w wierszu powinny zostać przekreślone, tak, aby było jasne, jakich danych dotyczyła zmiana.*

Załącznik nr 5
do Instrukcji zarządzania
systemem informatycznym

WZÓR

RAPORT
Z NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Data: ..... **Godzina:** .....
(dd.mm.rrrr) *(gg:mm)*

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

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

3. Lokalizacja zdarzenia:

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

4. Zakres ujawnionych danych:

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

5. Przyczyny wystąpienia zdarzenia, osoby odpowiedzialne oraz stosowne dowody:

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

6. Podjęte działania w celu rozwiązania problemu:

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

7. Przyjęte rozwiązania mające na celu wyeliminowanie podobnych zdarzeń w przyszłości:

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

.....
(data, podpis Administratora Bezpieczeństwa Informacji)