Załącznik nr 2
do Zarządzenia nr 11/2013
Starosty Sejneńskiego
z dnia 13 maja 2013r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM STAROSTWA POWIATOWEGO W SEJNACH

I. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemach informatycznych oraz wskazanie osoby odpowiedzialnej za te czynności.

1. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się z:

1) Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 Nr 101, poz. 926 z późn. zm.),

2) Polityką bezpieczeństwa przetwarzania danych osobowych w Starostwie Powiatowym w Sejnach,

3) niniejszym dokumentem.

2. Wzór upoważnienia do przetwarzania danych osobowych oraz obsługi systemu informatycznego służącego do przetwarzania danych osobowych w Starostwie Powiatowym w Sejnach stanowi załącznik nr 1.

3. Przyznanie uprawnień w zakresie dostępu do systemu informatycznego polega na wprowadzeniu do systemu dla każdego użytkownika unikalnego identyfikatora, hasła oraz zakresu dostępnych danych i operacji.

4. Hasło ustanowione podczas przyznawania uprawnień przez Administratora Bezpieczeństwa Informacji należy zmienić na indywidualne podczas pierwszego logowania się w systemie informatycznym.

5. Pracownik ma prawo do wykonywania tylko tych czynności, do których został upoważniony.

6. Pracownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu. Bezpośredni przełożony zapoznaje pracownika upoważnionego do przetwarzania danych osobowych z obowiązującymi przepisami w tym zakresie, o odpowiedzialności karnej za ich naruszenie, wynikającej z ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2002r. Nr 101, poz. 926 z późn. zm.) oraz kontroluje przestrzeganie przez nich przepisów prawa.

7. Wszelkie przekroczenia lub próby przekroczenia przyznanych uprawnień traktowane będą jako naruszenie podstawowych obowiązków pracowniczych.

8. Pracownik zatrudniony przy przetwarzaniu danych osobowych zobowiązany jest do zachowania ich w tajemnicy. Tajemnica obowiązuje go również po ustaniu zatrudnienia.

9. W systemie informatycznym stosuje się uwierzytelnianie dwustopniowe: na poziomie dostępu do sieci lokalnej oraz dostępu do aplikacji.

10. Identyfikator użytkownika w aplikacji (o ile działanie aplikacji na to pozwala), powinien być tożsamy z tym, jaki jest mu przydzielany w sieci lokalnej.

11 Odebranie uprawnień pracownikowi następuje na pisemny wniosek kierownika, któremu pracownik podlega z podaniem daty oraz przyczyny odebrania uprawnień.
12. Kierownicy komórek organizacyjnych zobowiązani są pisemnie informować Administratora Bezpieczeństwa Informacji o każdej zmianie dotyczącej podległych pracowników mającej wpływ na zakres posiadanych uprawnień w systemie informatycznym.

13. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych należy niezwłocznie wyrejestrować z systemu informatycznego, w którym są one przetwarzane oraz unieważnić jej hasło.

14. Administrator Bezpieczeństwa Informacji zobowiązany jest do prowadzenia rejestru pracowników Starostwa upoważnionych do przetwarzania danych osobowych oraz obsługi systemu informatycznego służącego do przetwarzania danych osobowych zgodnie z wzorem stanowiącym załącznik nr 2.

II. Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

1. Bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła. Identyfikator i hasło nadaje, osobą zajmującą się obsługą informatyczną w formie ustnej. Użytkownik jest zobowiązany do zmiany hasła po jego otrzymaniu.

2. Hasło użytkownika powinno być zmieniane co najmniej raz w miesiącu.

3. Identyfikator użytkownika nie powinien być zmieniany bez wyraźnej przyczyny, a po wyrejestrowaniu użytkownika z systemu informatycznego nie powinien być przydzielany innej osobie.

4. Pracownicy są odpowiedzialni za zachowanie poufności swoich haseł.

5. Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności.

6. Pracownik nie ma prawa do udostępniania haseł danej grupy osobom spoza tej grupy, dla której zostały one utworzone.

7. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie.

8. W sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, pracownik zobowiązany jest do natychmiastowej zmiany hasła.

9. Przy wyborze hasła obowiązują następujące zasady:
1) minimalna długość hasła - 8 znaków,
2) należy stosować:
a) hasła zawierające kombinacje małych i wielkich liter i cyfr,
b) hasła zawierające znaki specjalne: znaki interpunkcyjne, nawiasy, symbole @, #, &, itp. o ile system informatyczny na to pozwala

c) hasła, które można zapamiętać bez zapisywania,
d) hasła łatwe i szybkie do wprowadzenia, po to by trudniej było podejrzeć je osobom trzecim.

10. Zmiany hasła nie wolno zlecać innym osobom.

11. W systemach, które umożliwiają opcję zapamiętania nazw użytkownika lub jego hasła nie należy korzystać z tego ułatwienia.

12. Hasło użytkownika o prawach administratora powinno znajdować się w kopercie w zamykanej na klucz ognioodpornej szafie metalowej, do której dostęp mają Administrator Danych Osobowych lub osoba przez niego wyznaczona.

III. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu

1) Przed rozpoczęciem pracy w systemie komputerowym należy zameldować się do systemu przy użyciu indywidualnego identyfikatora oraz hasła.

2) Przy opuszczeniu stanowiska pracy na odległość uniemożliwiającą jego obserwację należy wykonać opcję wymeldowania z systemu (zablokowania dostępu), lub jeżeli taka możliwość nie istnieje wyjść z programu.

3) Osoba udostępniająca stanowisko komputerowe innemu upoważnionemu pracownikowi zobowiązana jest wykonać funkcję wymeldowania z systemu.

4) Przed wyłączeniem komputera należy bezwzględnie zakończyć pracę uruchomionych programów, wykonać zamknięcie systemu i jeżeli jest to konieczne wymeldować się z sieci komputerowej.

5) Niedopuszczalne jest wyłączanie komputera przed zamknięciem oprogramowania oraz zakończeniem pracy w sieci.

IV. Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narządzi programowych służących do ich przetwarzania

1. Za systematyczne przygotowanie kopii bezpieczeństwa odpowiada osobą zajmującą się obsługą informatyczną.
2. Kopie bezpieczeństwa wykonywane są raz na miesiąc po zakończeniu pracy wszystkich użytkowników w sieci komputerowej.
3. Zabezpieczenie wszystkich programów i danych wykonywane jest w pierwszym tygodniu po 15 dniu każdego miesiąca w postaci zapisu na przenośnym dysku twardym.
4. Przenośny dysk twardy przechowuje się w ognioodpornej szafie metalowej Starostwa Powiatowego w Sejnach.
5. Kopie baz danych wykonywane są codziennie i przechowywane na macierzy dyskowej w serwerowni.

V. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz wydruków

1. Elektroniczne nośniki informacji

1) Dane osobowe w postaci elektronicznej - zapisane na dyskietkach, dyskach magnetooptycznych czy dyskach twardych nie są wynoszone poza siedzibę Starostwa Powiatowego w Sejnach.

2) Wymienne elektroniczne nośniki informacji są przechowywane w pokojach stanowiących obszar przetwarzania danych osobowych, określony w Polityce Bezpieczeństwa Przetwarzania Danych Osobowych w Starostwie Powiatowym w Sejnach.

3) Po zakończeniu pracy przez użytkowników systemu, wymienne elektroniczne nośniki informacji są przechowywane w zamykanych szafach biurowych lub kasetkach.

4) Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie.

5)Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymywania danych osobowych pozbawia się wcześniej zapisu tych danych.

6)Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej.

2. Kopie zapasowe

1) Kopie zapasowe zbioru danych osobowych oraz oprogramowania i narzędzi programowych zastosowanych do przetwarzania danych są przechowywane w sejfie.
2) Dostęp do ww. sejfu mają tylko upoważnieni pracownicy.

3. Wydruki

1) W przypadku konieczności przechowywania wydruków zawierających dane osobowe należy je przechowywać w miejscu uniemożliwiającym bezpośredni dostęp osobom niepowołanym.

2) Pomieszczenie, w którym przechowywane są wydruki robocze musi być należycie zabezpieczone po godzinach pracy.

3) Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w niszczarce w stopniu uniemożliwiającym ich odczytanie.

VI. Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego.

1. Na każdym stanowisku komputerowym oraz serwerze musi być zainstalowane oprogramowanie antywirusowe pracujące w trybie monitora.

2. Każdy e-mail wpływający do Starostwa musi być sprawdzony pod kątem występowania wirusów przez bramę antywirusową.

3. Zabrania się używania nośników niewiadomego pochodzenia bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje użytkownik, który nośnik zamierza użyć.

4. Zabrania się pobierania z Internetu plików niewiadomego pochodzenia. Każdy plik pobrany z Internetu musi być sprawdzony programem antywirusowym. Sprawdzenia dokonuje użytkownik, który pobrał plik.
Zabrania się odczytywania załączników poczty elektronicznej bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje pracownik, który pocztę otrzymał.

5. Osobą zajmującą się obsługą informatyczną przeprowadza cykliczne kontrole antywirusowe na wszystkich komputerach - minimum co trzy miesiące.
Kontrola antywirusowa przeprowadzana jest również na wybranym komputerze w przypadku zgłoszenia nieprawidłowości w funkcjonowaniu sprzętu komputerowego lub oprogramowania.

7. W przypadku wykrycia wirusów komputerowych sprawdzane jest stanowisko komputerowe na którym wirusa wykryto oraz wszystkie posiadane przez użytkownika dyskietki.

VII. Sposób realizacji wymogów związanych z zabezpieczeniem przetwarzanych danych osobowych.

1. Dane osobowe z eksploatowanych systemów mogą być udostępniane wyłącznie osobom upoważnionym.

2. Udostępnienie danych osobowych, w jakiejkolwiek postaci, jednostkom nieuprawnionym wymaga pisemnego upoważnienia Administratora Danych Osobowych.

3. Udostępnienie danych osobowych nie może być realizowane drogą telefoniczną.

4. Udostępnienie danych osobowych może nastąpić wyłącznie po przedstawieniu wniosku, którego wzór stanowi załącznik nr 3 do niniejszej instrukcji.

5. Kierownicy komórek organizacyjnych prowadzą rejestry udostępnionych danych osobowych zawierające co najmniej: datę udostępnienia, podstawę, zakres udostępnionych informacji oraz osobę lub instytucję dla której dane udostępniono.

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

1. Przeglądy i konserwacja urządzeń wchodzących w skład systemu informatycznego powinny być wykonywane w terminach określonym przez producenta sprzętu.

2. Nieprawidłowości ujawnione w trakcie tych działań powinny być niezwłocznie usunięte, a ich przyczyny przeanalizowane. O fakcie ujawnienia nieprawidłowości należy zawiadomić Administratora Bezpieczeństwa Informacji i osobę zajmującą się obsługa informatyczną Starostwa Powiatowego w Sejnach.

3. Konserwacja baz danych przeprowadzana jest zgodnie z zaleceniami twórców poszczególnych programów.

4. Wszystkie logi opisujące pracę systemu, zameldowania i wymeldowania użytkowników oraz rejestr z systemu śledzenia wykonywanych operacji w programie należy przed usunięciem zapisać na nośniku informatycznym.

5. Sprzęt informatyczny przed oddaniem do naprawy poza Starostwo Powiatowe w Sejnach, pozbawić należy zapisu danych osobowych w sposób uniemożliwiający odczytanie. Nośniki, które uległy uszkodzeniu, zawierające dane osobowe można przekazać do naprawy pod warunkiem, że dokonujący naprawy wystawi stosowne oświadczenie o zapewnieniu poufności ewentualnie pozyskanych informacji.

Załącznik nr 1
do instrukcji zarządzania
systemem informatycznym
w Starostwie Powiatowym w Sejnach
z dnia 13 maja 2013r.

…….

(miejscowość, data)

……..

(znak pisma)

UPOWAŻNIENIE

Na podstawie art.37 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity *Dz. U. z 2002 r. Nr 101, poz. 926 z póź. zm.)* upoważniam Panią/a ……..... zatrudnioną/ego w Starostwie Powiatowym, w Sejnach na stanowisku .... legitymującego/-cą się dowodem osobistym nr ……..wydanym przez ……. do przetwarzania danych osobowych.

W szczególności do przetwarzanie danych osobowych w następujących zbiorach danych:……

…….

Identyfikator (przypadku przetwarzania danych w systemie informatycznym):

…….

……

Pouczenie

Osoba upoważniona obowiązana jest do zachowania w tajemnicy informacji uzyskanych w trakcie dokonywania operacji związanych z przetwarzaniem danych osobowych. Obowiązek ten istnieje również po ustaniu zatrudnienia /podstawa prawna: art. 37 i art. 39 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2002r. Nr 101 poz. 926 z późn. zm.)/.

…… ……

podpis Administratora Danych Osobowych podpis pracownika

Załącznik nr 2
do instrukcji zarządzania
systemem informatycznym
w Starostwie Powiatowym w Sejnach
z dnia 13 maja 2013r.

Rejestr pracowników Starostwa Powiatowego w Sejnach upoważnionych do przetwarzania danych osobowych

L.p.	Imię i nazwisko pracownika /stanowisko	Data nadania upoważnienia	Data ustania upoważnienia	Zakres upoważnienia do przetwarzania danych	Identyfikator	Uwagi

Załącznik nr 3
do instrukcji zarządzania
systemem informatycznym
w Starostwie Powiatowym w Sejnach
z dnia 13 maja 2013r.

.

Wniosek o udostępnienie danych ze zbioru danych osobowych

1.Wniosek do Starosty Sejneńskiego
2.Wnioskodawca……
……
(nazwa firmy i jej siedziba albo nazwisko, imię i adres zamieszkania wnioskodawcy, ew. NIP oraz nr REGON)

……..

3. Podstawa prawna upoważniająca do pozyskania danych albo wskazanie wiarygodnie uzasadnionej potrzeby posiadania danych w przypadku osób innych niż wymienione w art. 29 ust. 1 ustawy o ochronie danych osobowych…….
……..
……
4. Wskazanie przeznaczenia dla udostępnionych danych
……
……..
……..
……
5. Oznaczenie lub nazwa zbioru, z którego mają być udostępnione dane:…….
……
……
6. Zakres żądanych informacji ze zbioru…….
……
……
……
7. Informacje umożliwiające wyszukanie w zbiorze danych
……..
……
……

……
(data, podpis i ew. pieczęć wnioskodawcy)

Załącznik nr 4
do instrukcji zarządzania
systemem informatycznym
w Starostwie Powiatowym w Sejnach
z dnia 13 maja 2013r.

Wycofanie upoważnienia

Na podstawie art.37 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych

(Dz. U. z 2002r. Nr 101, poz. 926 z póź. zm.)

w związku z:

.....

.....

.....

.....

cofam upoważnienie

Pana/Pani.....
zatrudnionego/ zatrudnionej
w.....
na stanowisku……
do przetwarzania danych osobowych, wynikającego z zakresu obowiązków pracowniczych.

Sejny, dnia.....