Załącznik Nr 2
do Zarządzenia Starosty Nr 24/2012
z dnia 26.10.2012r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W STAROSTWIE POWIATOWYM W ŁOSICACH

Rozdział 1
Przepisy ogólne

§ 1

Ilekroć w niniejszym dokumencie jest mowa o:

1) Starostwo – w tym dokumencie jest rozumiane, jako Starostwo Powiatowe w Łosicach, z siedzibą w Łosice 08-200, ul. Narutowicza 6.

2) Administratorze Danych – należy przez to rozumieć Starostę Powiatu Łosickiego

3) Administratorze Bezpieczeństwa Informacji (ABI)– należy przez to rozumieć osobę wyznaczoną przez Starostę do nadzorowania przestrzegania zasad ochrony określonych w niniejszym dokumencie oraz wymagań w zakresie ochrony wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych;

4) Administratorze Systemu Informatycznego (ASI)– należy przez to rozumieć osobę odpowiedzialną za funkcjonowanie systemu informatycznego Starostwa oraz stosowanie technicznych i organizacyjnych środków ochrony;

5) użytkowniku systemu – należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym starostwa, której nadano identyfikator i przyznano hasło, użytkownikiem może być pracownik Starostwa Powiatowego, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej lub osoba odbywająca staż, praktykę uczniowską studencką w Starostwie, lub pracującą w charakterze wolontariusza;

6) sieci lokalnej – należy przez to rozumieć połączenie systemów informatycznych Starostwa wyłącznie dla własnych jej potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych;

7) sieci rozległej – należy przez to rozumieć sieć publiczną w rozumieniu ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800 z późn. zm.).

§ 2

Instrukcja zarządzania systemem informatycznym, zwana dalej "instrukcją" określa:

- procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności,
- stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem,

- procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu,
- procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania,
- sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe i kopii zapasowych,
- sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego i utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej,
- zasady i sposób odnotowywania w systemie informacji o udostępnianiu danych osobowych,
- procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

Rozdział 2
Procedury nadawania i zmiany uprawnień do przetwarzania danych, rejestrowania tych uprawnień w systemach informatycznych oraz wskazanie osoby odpowiedzialnej za te czynności

§ 3

1. Administrator Systemu Informatycznego przyznaje uprawnienia w zakresie dostępu do systemu informatycznego na podstawie pisemnego upoważnienia Administratora Danych określającego zakres uprawnień pracownika.
2. Administrator Systemu Informatycznego rejestruje uprawnienia do systemu informatycznego na Karcie ewidencyjnej uprawnień pracownika, której wzór stanowi **Załącznik nr 1** do niniejszej instrukcji. Karty ewidencyjne powinny odzwierciedlać aktualny stan systemu w zakresie użytkowników i ich uprawnień oraz umożliwiać przeglądanie historii zmian uprawnień użytkowników.
3. Przyznanie uprawnień w zakresie dostępu do systemu informatycznego polega na wprowadzeniu przez ASI do systemu dla każdego użytkownika unikalnego identyfikatora, hasła oraz zakresu dostępnych danych i operacji. Użytkownik systemu informatycznego po zalogowaniu zmienia nadane mu przez Administratora Systemu Informatycznego hasło startowe.
4. Odebranie uprawnień pracownikowi następuje na wniosek Administratora Danych z podaniem daty oraz przyczyny odebrania uprawnień i podlega rejestracji w Karcie ewidencyjnej uprawnień pracownika. Konto osoby, która utraciła uprawnienia do dostępu do danych osobowych ASI niezwłocznie blokuje lub dezaktywuje w systemie informatycznym.
5. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.
6. Administrator Bezpieczeństwa Informacji prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych i przechowuje Karty ewidencyjne uprawnień pracowników.

Rozdział 3
Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem

§ 4

1. W systemie informatycznym stosuje się uwierzytelnianie dwustopniowe: na poziomie dostępu do systemu operacyjnego komputera i sieci lokalnej oraz dostępu do aplikacji. Do uwierzytelniania na obu poziomach stosuje się hasła. Identyfikator użytkownika w aplikacji (o ile działanie aplikacji na to pozwala), powinien być tożsamy z tym, jaki jest mu przydzielany w systemie operacyjnym komputera/sieci lokalnej.

2. Bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu hasła.
3. Pracownik ma prawo do wykonywania tylko tych czynności, do których został upoważniony i ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu. Pracownicy są odpowiedzialni za zachowanie poufności swoich haseł. Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności.
4. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie.
5. Przy wyborze hasła obowiązują następujące zasady:
   1) minimalna długość hasła - 5 znaków;
   2) zakazuje się stosować:
      a) swojej nazwy użytkownika w jakiejkolwiek formie (pisanej dużymi literami, w odwrotnym porządku, dublując każdą literę, itp.),
      b) swojego imienia, drugiego imienia, nazwiska, przezwiska, pseudonimu w jakiejkolwiek formie,
      c) imion (w szczególności imion osób z najbliższej rodziny),
      d) ogólnie dostępnych informacji o użytkowniku takich jak: numer telefonu, numer rejestracyjny samochodu, jego marka, numer dowodu osobistego, nazwa ulicy, na której mieszka lub pracuje, itp.,
      e) wyrazów słownikowych,
      f) przewidywalnych sekwencji znaków z klawiatury np.: QWERTY", "12345678", itp.,
   3) należy stosować:
      a) hasła zawierające kombinacje małych i dużych liter oraz 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.
6. Zmiany hasła nie można zlecać osobom trzecim, współpracownikom.
7. Hasło nie może być zapisywane i przetrzymywane w miejscach dostępnych dla osób trzecich (np. kartki, notesy, kalendarze itp.) lub w niezaszyfrowanych plikach na komputerze.
8. W systemach, które umożliwiają opcję zapamiętania nazw użytkownika lub jego hasła nie należy korzystać z tego ułatwienia.
9. Hasło użytkownika o prawach administratora powinno znajdować się w zalakowanej kopercie w zamykanej na klucz szafie metalowej, do której dostęp mają wyłącznie:
   3) Administrator Bezpieczeństwa Informacji;
   4) Administrator Danych;
   5) Administrator Systemu Informatycznego.

Rozdział 4
Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie

§ 5

I. Procedura rozpoczęcia pracy.

1. Uruchomić komputer wchodzący w skład systemu informatycznego i zalogować się do komputera lub sieci podając swój identyfikator i hasło dostępu.
2. Uruchomić aplikację podając następnie swój identyfikator i hasło dostępu do aplikacji.
3. Ustawić monitory w sposób uniemożliwiający podgląd osobom postronnym.

II. Procedura zawieszenia pracy w systemie.

1. W trakcie pracy, przy każdorazowym opuszczeniu stanowiska komputerowego, dopilnować, aby na ekranie nie były wyświetlane dane osobowe.

2. Przy opuszczeniu stanowiska pracy na odległość uniemożliwiającą jego obserwację należy zablokować komputer, np.:
   - poprzez naciśnięcie kombinacji klawiszy Windows + L ;
   - poprzez naciśnięcie kombinacji klawiszy Ctrl + Alt + Del następnie Zablokuj komputer.
3. Osoba udostępniająca stanowisko komputerowe innemu upoważnionemu pracownikowi zobowiązana jest wykonać funkcję wylogowania z systemu.

III. Procedura zakończenia pracy w systemie.

1. Zakończyć pracę uruchomionych programów – wylogować się lub zamknąć.
2. Zamknąć system.
3. Wyłączyć monitor, drukarkę i inne urządzenia zewnętrzne.
4. Niedopuszczalne jest wyłączanie komputera przed zamknięciem oprogramowania oraz zakończeniem pracy w sieci.

Rozdział 5
Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

§ 6

1. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych.
2. Kopie zapasowe zbioru danych osobowych wykonywane są na pamięciach USB typu Flash (pendrive), dyskach twardych, na nośnikach optycznych CD-R/DVD-R oraz taśmach magnetycznych. Za systematyczne wykonywanie kopii bezpieczeństwa odpowiada Administrator Systemu Informatycznego.
3. Administrator Bezpieczeństwa Informacji sprawuje nadzór nad wykonywaniem kopii zapasowych oraz weryfikuje ich poprawność.
4. Kopie zapasowe przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem i usuwa się niezwłocznie po ustaniu ich użyteczności.

Rozdział 6
Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe i kopii zapasowych

§ 7

1. Elektroniczne nośniki informacji:
   1) dane osobowe w postaci elektronicznej przetwarzane w systemie zapisywane na nośnikach danych: np. na pamięciach USB typu Flash (pendrive), nośnikach optycznych, dyskach twardych oraz taśmach magnetycznych, nie mogą być wynoszone poza obszar przetwarzania danych osobowych, chyba że jest to niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa.
   2) wymienne elektroniczne nośniki informacji są przechowywane w pokojach stanowiących obszar przetwarzania danych osobowych, określonych w „Polityce bezpieczeństwa przetwarzania danych osobowych”;
   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 zgodnie z normą DIN 66399;
5) urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych w sposób uniemożliwiający ich odzyskanie, sprzęt przekazywany do naprawy poza siedzibą Starostwa Powiatowego pozbawia się nośników danych albo naprawia się sprzęt na miejscu 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 szafie metalowej w pokoju nr 31 w siedzibie Starostwa Powiatowego .
   2) dostęp do kopii wymienionych w punkcie 1) mają Administrator Danych, Administrator Bezpieczeństwa Informacji i Administrator Systemu Informatycznego.
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 stopniu uniemożliwiającym ich odczytanie zgodnie z normą DIN 66399.

Rozdział 7

Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego i przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej

§ 8

1. Sprawdzenie obecności wirusów komputerowych w systemie informatycznym oraz ich usuwanie odbywa się za pomocą licencjonowanego oprogramowania zainstalowanego na wszystkich komputerach.
2. Oprogramowanie, o którym mowa w ust. 1, sprawuje ciągły nadzór (ciągła praca w tle) nad pracą systemu i jego zasobami.
3. Oprogramowanie antywirusowe jest aktualizowane automatycznie poprzez Internet lub gdy nie jest to możliwe poprzez pakiety aktualizacyjne w trybie "offline" (ręcznie).
4. Użytkownik systemu na stanowisku komputerowym, przetwarzający dane osobowe w systemie informatycznym jest odpowiedzialny za sprawdzenie tych danych pod kątem możliwości występowania wirusów.
5. Zabrania się podłączania do stacji roboczych lub sieci komputerowej Starostwa Powiatowego prywatnych urządzeń oraz nośników danych należących do pracowników, w tym: komputerów, telefonów komórkowych, modemów, urządzeń sieci bezprzewodowej, aparatów fotograficznych, pamięci USB, dysków przenośnych.
6. Wszystkie nośniki zewnętrzne np. pamięci USB, dyski przenośne należy przed użyciem zgromadzonych na nich danych, w celu ochrony przed wirusami i innymi niepożądanymi kodami, sprawdzić przez zaktualizowany program antywirusowy.
7. Użytkownik systemu, który zauważy, że program antywirusowy na jego stacji jest niezaktualizowany, bądź zauważy komunikat o wystąpieniu zagrożenia wywołanego

szkodliwym oprogramowaniem jest zobowiązany do niezwłocznego powiadomienia o tym fakcie Administratora Systemu Informatycznego.

8. W godzinach pracy zabrania się korzystania z internetu w celach prywatnych, otwierania stron mogących potencjalnie zawierać szkodliwe oprogramowanie a szczególnie stron o charakterze pornograficznym i zawierających nielegalne oprogramowanie.
9. Urządzenia sieciowe wchodzące w skład systemu informatycznego należy podłączać do odrębnego obwodu elektrycznego dedykowanego dla sprzętu komputerowego. W przypadku stacji roboczych najbardziej newralgicznych z punktu widzenia przetwarzania danych osobowych należy zapewnić im bezprzerwowe zasilanie poprzez zastosowanie zasilaczy awaryjnych UPS.

Rozdział 8
Zasady i sposób odnotowywania w systemie informacji o udostępnieniu danych osobowych

§ 9

1. Dane osobowe z eksploatowanych systemów mogą być udostępniane osobom upoważnionym.
2. Udostępnienie danych osobowych, w jakiejkolwiek postaci, jednostkom nieuprawnionym wymaga pisemnego upoważnienia Administratora Danych.
3. Udostępnienie danych osobowych może nastąpić wyłącznie na pisemną prośbę odbiorcy danych, pisemnie zaakceptowaną przez Administratora Danych.
4. Prowadzony jest rejestr udostępnionych danych osobowych zawierający, co najmniej: datę udostępnienia, podstawę, zakres udostępnionych informacji oraz dane osoby lub instytucji, dla której dane udostępniono.

Rozdział 9
Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych

§ 10

1. Przeglądy i konserwacja urządzeń:
   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.

2. Przegląd programów i narzędzi programowych:
   1) konserwacja baz danych przeprowadzana jest zgodnie z zaleceniami twórców poszczególnych programów;
   2) zapisy logów systemowych opisujących pracę systemu, logowania i wylogowania użytkowników nadzoruje ASI i przegląda je każdorazowo po wykryciu naruszenia zasad bezpieczeństwa.

Rozdział 10
Postępowanie w przypadku stwierdzenia naruszenia bezpieczeństwa systemu informatycznego

§ 11

Naruszenie systemu ochrony danych osobowych może zostać stwierdzone na podstawie oceny:

1. stanu urządzeń technicznych;
2. zawartości zbiorów danych osobowych;
3. sposobu działania programu lub jakości komunikacji w sieci teleinformatycznej;
4. metod pracy (w tym obiegu dokumentów);
5. analizy logów systemowych i programowych.

§ 12

W sytuacji podejrzenia naruszenia bezpieczeństwa systemu np. w przypadku braku możliwości zalogowania się użytkownika na jego konto czy też w przypadku stwierdzenia fizycznej ingerencji w przetwarzane dane lub użytkowane narzędzia programowe lub sprzętowe należy bezzwłocznie:

1. powiadomić Administratora Systemu Informatycznego lub Administratora Bezpieczeństwa Informacji;
2. zablokować dostęp do systemu dla użytkowników oraz osób nieupoważnionych;
3. podjąć działania mające na celu zminimalizowanie lub całkowite wyeliminowanie powstałego zagrożenia - o ile czynności te nie spowodują przekroczenia uprawnień pracownika;
4. zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia bezpieczeństwa systemu.

§ 13

1. Administrator Bezpieczeństwa Informacji po otrzymaniu powiadomienia o naruszeniu bezpieczeństwa danych osobowych i potwierdzeniu tegoż faktu przez Administratora Systemu Informatycznego jest zobowiązany niezwłocznie podjąć działania chroniące system przed ponownym naruszeniem oraz przeprowadzić postępowanie wyjaśniające mające na celu ustalenie:
   a. przyczyn i okoliczności naruszenia bezpieczeństwa danych osobowych;
   b. osób winnych naruszenia bezpieczeństwa danych osobowych;
   c. skutków naruszenia.
2. Administrator Bezpieczeństwa Informacji zobowiązany jest do sporządzenia pisemnego raportu wg wzoru określonego w **załączniku nr 2** do niniejszej instrukcji na temat zaistniałej sytuacji, zawierającego, co najmniej:
   a. datę i miejsce wystąpienia naruszenia;
   b. zakres ujawnionych danych;
   c. przyczynę ujawnienia, osoby odpowiedzialne oraz stosowne dowody winy;
   d. sposób rozwiązania problemu;
   e. przyjęte rozwiązania mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.
3. Raport ten Administrator Bezpieczeństwa Informacji przekazuje Administratorowi Danych.
4. Administrator Danych po zapoznaniu się z raportem podejmuje decyzję o dalszym trybie postępowania, powiadomieniu właściwych organów oraz podjęciu innych, szczególnych czynności zapewniających bezpieczeństwo systemu informatycznego.

Załącznik Nr 1
do Instrukcji Zarządzania Systemem
Informatycznym w Starostwie Powiatowym w Łosicach

Karta ewidencyjna uprawnień w zakresie dostępu i obsługi programów i aplikacji systemu informatycznego w Starostwie Powiatowym w Łosicach związanych z przetwarzaniem danych osobowych

Identyfikator użytkownika	Nazwisko i imię użytkownika

l.p	Rodzaj uprawnienia	Data nadania uprawnień	Podpis ASI	Akceptacja AD / ABI	Data i przyczyna odebrania uprawnień
1	Uprawnienie do przetwarzania danych osobowych				
2					
3					
4					
5					
6					
7					
8					

Załącznik Nr 2
do Instrukcji Zarządzania Systemem
Informatycznym w Starostwie Powiatowym w Łosicach

R a p o r t
z naruszenia Bezpieczeństwa Systemu Informatycznego w Starostwie Powiatowym w Łosicach

1. Data: ..... Godzina: .....
(dd.mm.rrrr) (00:00)

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

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

3. Lokalizacja zdarzenia:

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

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

.....

.....

5. Podjęte działania:

.....

.....

6. Przyczyny wystąpienia zdarzenia:

.....

.....

7. Postępowanie wyjaśniające:

.....

.....

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