Załącznik Nr 2
do zarządzenia nr OG.120.29.2012
Starosty Nowotomyskiego
z dnia 19.12.2012r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM TELEINFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

Starostwo Powiatowe w Nowym Tomyślu

Nowy Tomyśl, 2012.....

ZATWIERDZAM:

STAROSTA

.....mgr Andrzej Wilkoński

Instrukcja zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Starostwie Powiatowym w Nowym Tomyślu

Opracował:

Administrator Systemu Informatycznego

§ 1.

Instrukcja określa zasady zarządzania systemem informatycznym służącym do przetwarzania danych osobowych zgodnie ze strategią określoną w „Polityce bezpieczeństwa systemu informatycznego" wprowadzoną w życie zarządzeniem nr OG.120.29.2012 Starosty Powiatu Nowotomyskiego z dnia 19 grudnia 2012r. oraz postanowień rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 9 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).

§ 2.

Definicje zawarte w dokumencie:

- **„dane osobowe"** oznaczają wszelkie informacje dotyczące zidentyfikowanej lub dającej się zidentyfikować osoby fizycznej („podmiotu danych"); osobą dająca się zidentyfikować jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, szczególnie poprzez odniesienie się do numeru identyfikacyjnego lub innych wskaźników charakterystycznych dla jej fizycznej, fizjologicznej, umysłowej, gospodarczej, kulturowej lub społecznej tożsamości;
- **„przetwarzanie danych osobowych"** („przetwarzanie") oznacza każdą czynność lub szereg czynności wykonywanych na danych osobowych, bez względu na to czy za pomocą automatycznych środków czy nie, takie jak gromadzenie, rejestrowanie, porządkowanie, przechowywanie, dostosowywanie lub zmienianie, odzyskiwanie, konsultowanie, używanie, ujawnianie przez przekazywanie, rozpowszechnianie bądź w inny sposób udostępnianie, wyrównywanie lub łączenie, blokowanie, usuwanie lub niszczenie;
- **„system ewidencjonowania danych osobowych"** („system ewidencyjny") oznacza wszelki zorganizowany zbiór danych osobowych dostępny po spełnieniu pewnych kryteriów, bez względu na to, czy jest zcentralizowany czy zdecentralizowany lub usytuowany na zasadzie funkcjonalnej czy geograficznej;
- **„Zbiór danych"** to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
- **„System informatyczny"** to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i urządzeń programowych zastosowanych w celu przetwarzania danych.
- **„Użytkownik systemu"** są to osoby upoważnione do przetwarzania danych osobowych w systemie informatycznym, wg ewidencji osób upoważnionych stanowiącej zał. Nr 1 do niniejszej instrukcji.
- **„Zabezpieczenie systemu informatycznego"** to wdrożenie stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.
- **„Ustawa"** – określa Ustawę o ochronie danych osobowych z dnia 29 sierpnia 1997r. (Dz. U. z 2002 r. Nr 101, poz. 926, ze zm.)
- **„Administrator danych"** - rozumie się przez to organ , jednostkę organizacyjną, podmiot lub osobę o których mowa w art. 3 „Ustawy", decydujące o celach i środkach

przetwarzania danych osobowych. W Starostwie Powiatowym w Nowym Tomyślu „Administratorem Danych" jest Starosta Nowotomyski.

- **„Administrator Bezpieczeństwa Informacji" (ABI)** to osoba odpowiedzialna za bezpieczeństwo danych osobowych w systemie informatycznym, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu w którym przetwarzane są dane osobowe, oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń. W Starostwie Powiatowym w Nowym Tomyślu jest to powołany przez Starostę Nowotomyskiego pracownik.
- **„Administrator Systemu Informatycznego" (ASI)** to administrator sieci komputerowej Starostwa.
- **„Kierownik komórki organizacyjnej"** to kierownik wydziału lub samodzielne stanowisko pracy.

§ 3.

Zasadniczym celem podejmowanych działań wynikających z instrukcji jest zabezpieczenie systemu informatycznego przed dostępem osób niepowołanych. Instrukcja określa wszelkie sposoby dotyczące zapewnienia bezpieczeństwa informacji a w szczególności elementy wymienione w §5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 9 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) na które składają się:

1) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności,
2) stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem,
3) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu,
4) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania,
5) sposób, miejsce i okres przechowywania:
    a) elektronicznych nośników informacji zawierających dane osobowe,
    b) kopii zapasowych, o których mowa w pkt. 4,
6) sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia,
7) sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4 rozporządzenia,
8) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

§ 4.

Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności (§ 5 pkt 1 rozporządzenia).

A) podstawowe zasady nadawania uprawnień w systemie informatycznym Starostwa Powiatowego w Nowym Tomyślu:
   1. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się z:
      - Ustawą o ochronie danych osobowych z dnia 29 sierpnia 1997r. (Dz. U. z 2002 r. Nr 101, poz. 926, ze zm.)
      - Zarządzeniem nr OG-0135/33/2005 Starosty Powiatu Nowotomyskiego z dnia 8 grudnia 2005r. w sprawie ustalenia Polityki bezpieczeństwa przetwarzania danych osobowych systemu informatycznego Starostwa Powiatowego w Nowym Tomyślu.
      - Niniejszą Instrukcją

B) Procedura nadawania uprawnień do przetwarzania danych osobowych.
   1. Administrator Danych:
   - nadaje upoważnienie do przetwarzania danych osobowych osobie, która w związku z wykonywanymi przez siebie obowiązkami będzie miała dostęp do danych osobowych
   - podpisuje dokument uprawnień dla osoby upoważnionej do przetwarzania danych osobowych w systemie informatycznym Starostwa
   - Administrator Danych przyznaje uprawnienia na wniosek kierownika komórki organizacyjnej.
   2. ABI bada poprawność przesłanego dokumentu oraz
   - w przypadku braku uwag przekazuje go ze swoją adnotacją ASI, w celu nadania uprawnień użytkownikowi w systemie,
   - w przypadku uwag, na dokumencie dokonuje adnotacji, w której podaje przyczynę odmowy zatwierdzenia dokumentu. Kroki w pkt. 2 powtarza się do czasu uzyskania akceptacji dokumentu przez ABI.
   3. ASI odpowiednio, zgodnie z przekazanym dokumentem:
   - rejestruje użytkownika w systemie i nadaje mu określone uprawnienia
   - drukuje raport z systemu zawierający informacje o zmianie uprawnień w systemie opatrując go swoim podpisem i datą
   - kieruje podpisany przez siebie raport do ABI w celu aktualizacji ewidencji osób upoważnionych do przetwarzania danych osobowych w systemie informatycznym Starostwa (wzór ewidencji w załączniku nr 1)
   4. ABI aktualizuje ewidencję, i przekazuję informację o zarejestrowaniu użytkownika w systemie kierownikowi komórki organizacyjnej
   5. Użytkownik systemu w obecności ASI uwierzytelnia się w systemie,
   6. Użytkownik zmienia nadane mu przez ASI hasło i rozpoczyna pracę w aplikacji.
   7. Wszelkie zmiany uprawnień do systemu zawierającego dane osobowe są ustanawiane na wniosek kierownika komórki organizacyjnej.
   8. W sytuacji gdy użytkownik systemu utraci prawo dostępu do zbiorów danych osobowych, jego identyfikator niezwłocznie wyrejestrowuje się z systemu informatycznego, w którym są one przetwarzane, unieważnia się jego hasło i blokuje dostęp do wszelkich danych.

§ 4.

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

A) metody i środki uwierzytelniania.

1. W systemie informatycznym Starostwa Powiatowego w Nowym Tomyślu stosuje się metody uwierzytelniania:

- dostępu do stacji komputerowej z poziomu BIOS
- dostępu do sieci lokalnej
- dostępu do aplikacji

2. Do uwierzytelniania użytkownika w systemie we wszystkich poziomach stosuje się hasła.
3. Identyfikator użytkownika nadawany jest na poziomie autoryzacji w sieci oraz aplikacji.
4. Bezpośredni dostęp do danych osobowych uzyskuje się wyłącznie po podaniu identyfikatora i właściwego hasła.
5. Hasło użytkownika do programu zmienia się raz na miesiąc.
6. Hasło na poziomie dostępu do aplikacji i sieci składa się co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.
7. Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów.
8. Hasło użytkowników systemów przy wpisywaniu nie może być wyświetlone na ekranie i utrzymywane jest w tajemnicy w trakcie użytkowania jak również po upływie jego ważności.
9. Zmiana hasła do systemu następuje w przypadku podejrzenia, że hasło mogło zostać ujawnione lub w sytuacji gdy użytkownik zapomniał swojego hasła.
10. Identyfikator użytkownika systemu nie powinien być zmieniany, a po jego wyrejestrowaniu z systemu informatycznego nie jest przydzielany innej osobie.
11. Czas pracy i ewentualne przerwy w pracy w systemie informatycznym dla poszczególnych użytkowników systemu ustalają kierownicy komórek organizacyjnych. Natomiast na pracę w systemie informatycznym poza godzinami funkcjonowania Starostwa musi wyrazić zgodę administrator danych.
12. Użytkownik systemu przed opuszczeniem stanowiska pracy zobowiązany jest do zakończenia pracy w tym systemie i wyjść (wylogować się) z programu i sieci.
13. W przypadku czasowego opuszczenia stanowiska pracy użytkownik systemu powinien wylogować się z systemu, lub po pięciu minutach musi uruchomić się wygaszacz ekranu zabezpieczony hasłem.

14. Monitory stanowisk dostępu do danych osobowych użytkownicy systemu ustawiają w ten sposób, żeby uniemożliwić osobom postronnym wgląd w te dane.

B) Procedury zarządzania środkami uwierzytelniania:

1. ASI nadaje indywidualny identyfikator i hasło dostępu do aplikacji dla nowego użytkownika umieszczając w systemie jego dane osobowe /imie, nazwisko, itd../
2. ASI po wprowadzeniu do systemu identyfikatora i hasła przekazuje te dane w zamkniętej kopercie użytkownikowi systemu.

3. Użytkownik systemu loguje się po raz pierwszy w systemie i niezwłocznie ustala swoje, znane tylko jemu hasło i przekazuję w zamkniętej kopercie ASI.

4. ASI prowadzi rejestr haseł dostępu. Rejestry te są dokumentami o klauzuli tajności „zastrzeżone" w rozumieniu ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95 z zmianami) i przechowywane w sejfie znajdującym się w budynku C w pomieszczeniu 3A, do którego dostęp jest zabezpieczony antywłamaniowymi drzwiami zabezpieczonymi kontrolą dostępu na karty chipowe.

§ 5.

Procedury rozpoczęcia, zawieszania i zakończenia pracy w systemie.

A) Procedury rozpoczęcia pracy w systemie informatycznym.

1. Uruchomić komputer wchodzący w skład systemu informatycznego, podłączony fizycznie do sieci lokalnej i zalogować się do systemu podając hasło BIOIS a następnie do sieci podając swój identyfikator i hasło dostępu,

2. Uruchomić aplikację zawierającą dane osobowe, podając następnie swój identyfikator i hasło dostępu do aplikacji.

3. Rozpocząć pracę.

B) Procedury zawieszania pracy w systemie informatycznym.

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

2. Przy opuszczaniu pokoju ustawić ręcznie blokadę klawiatury i wygaszacz ekranu.

C) Procedury zakończenia pracy w systemie informatycznym.

1. Zamknąć aplikację,
2. Zamknąć system,
3. Wyłączyć monitor i drukarkę.

§ 6.

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

1. Kopie awaryjne tworzy się codziennie na dysku lokalnym po zakończeniu dnia pracy, w programie w którym wprowadzono zmiany.
2. Kopie o których mowa w pkt.1 są tworzone przez użytkowników pracujących w danym programie zainstalowanym na jego stacji roboczej.
3. Na zewnętrznych nośnikach informacji kopie całego sieciowego systemu operacyjnego i archiwizację bazy danych znajdujących się na serwerze lokalnym przeprowadza się jeden raz w tygodniu.
4. Archiwizację bazy danych i sieciowego systemu operacyjnego przeprowadza ASI.
5. Sporządzone kopie awaryjne są okresowo sprawdzane pod kątem dalszej ich przydatności do odtworzenia danych w przypadku awarii systemu.
6. Kopie awaryjne, po utracie przydatności są bezzwłocznie usuwane.
7. W przypadku uszkodzenia lub zużycia nośnika zawierającego dane osobowe należy fizycznie zniszczyć nośnik.

§ 7.

Dane osobowe w postaci elektronicznej przetwarzane w systemie informatycznym Starostwa Powiatowego w Nowym Tomyślu, zapisane na dyskach magnetooptycznych czy dyskach twardych nie są wynoszone poza siedzibę Starostwa. Sposób, miejsce i okres przechowywania kopii informacji zawierających dane osobowe dotyczy:

A) elektronicznych nośników informacji zawierających dane osobowe,

1. Kopie zawierające dane osobowe znajdujące się na pojedynczych stanowiskach pracy są przechowywane w specjalnie do tego przeznaczonych szafach metalowych lub sejfach
2. Kopie zawierające dane osobowe znajdujące w aplikacjach sieciowych są przechowywane na dyskach twardych.

B) kopii zapasowych, o których mowa w par. 6 pkt. 2,

1.Kopie przechowywane są w specjalnie do tego celu przeznaczonym sejfie (par.4 pkt B poz. 4)

2.Dostęp do sejfu mają tylko upoważnieni pracownicy, tj. ABI oraz ASI.

C) wydruków, zawierających dane osobowe

1. Wydruki, zawierające dane osobowe, należy przechowywać w pokojach stanowiących obszar przetwarzania danych osobowych
2. Wydruki, zawierające dane osobowe, należy zniszczyć przez pocięcie w specjalnym urządzeniu nie później niż po upływie 3 dni, po ich wykorzystaniu chyba, że z odrębnych przepisów wynika obowiązek ich przechowywania.

D) Dane wejściowe do systemu

1. Dane osobowe zapisane w formie papierowej innej niż wydruki z systemu (pisma, ankiety itp.) są przechowywane na podobnych zasadach co wydruki zawierające dane osobowe.
2. Dane wejściowe do systemu zawierające dane osobowe, należy zniszczyć przez pocięcie w specjalnym urządzeniu nie później niż po upływie 3 dni, po ich wykorzystaniu chyba, że z odrębnych przepisów wynika obowiązek ich przechowywania.

§ 8.

Sposób zabezpieczenia systemu informatycznego przed działalnością złośliwego oprogramowania, w tym wirusami komputerowymi.

A) Ochrona antywirusowa.
   1. Za ochronę antywirusową odpowiada ASI.

   2. Czynności związane z ochroną antywirusową sieciowego systemu informatycznego wykonuje ASI, wykorzystując w trakcie pracy moduł programu antywirusowego w aktualnej wersji, sprawdzającego na bieżąco zasoby sieciowego systemu informatycznego.

   3. Całkowite skanowanie pojedynczych stacji roboczych powinno być robione przynajmniej raz w tygodniu przez użytkownika danej stacji roboczej.

   4. Każdy użytkownik komputera w Starostwie Powiatowym w Nowym Tomyślu zobowiązany jest do używania w pracy CD i innych nośników zakupionych przez Starostwo (nie prywatnych) i przechowywania na nich tylko i wyłącznie danych związanych z charakterem pracy.

5. Użytkownik systemu na stanowisku komputerowym, importujący dane osobowe do systemu informatycznego jest odpowiedzialny za sprawdzenie tych danych pod kątem możliwości występowania wirusów.

§ 9.

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

A) Przeglądy i konserwacja urządzeń

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

2. Nieprawidłowości ujawnione w trakcie tych działań powinny być niezwłocznie usunięte, a ich przyczyny przeanalizowane. O fakcie ujawnienia nieprawidłowości należy zawiadomić ABI.

3. Za terminowość przeprowadzenia przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada ASI.

4. Urządzenia, dyski lub inne nośniki informatyczne zawierające dane osobowe przeznaczone do:

   - likwidacji - pozbawia się je wcześniej zapisu danych, a gdy nie jest to możliwe, uszkadza się je w sposób uniemożliwiający odczyt;
   - naprawy - pozbawia się je wcześniej zapisu danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora bezpieczeństwa informacji,
   - przekazania innemu podmiotowi nieuprawnionemu do otrzymania danych osobowych, pozbawia się je wcześniej zapisu danych w sposób uniemożliwiający ich odzyskanie.

B) Przegląd oprogramowania

1. Za prawidłowość przeprowadzenia przeglądów i konserwacji systemu odpowiada ASI,

2. Przegląd przeprowadza projektant systemu lub inna osoba do tego upoważniona w obecności ASI,

3. przegląd oprogramowania następuje w sytuacjach wykonania zmian w projekcie systemu spowodowanych koniecznością zmiany wersji oprogramowania, naprawy, konserwacji lub modyfikacji systemu

4. w uzasadnionych przypadkach przeglądu dokonuje ASI

5. Aktualizację, zmianę ustawień oprogramowania, konfigurację i zmianę zabezpieczeń zarówno na stacjach roboczych jak i sieciowe przeprowadza wyłącznie ASI

C) Konserwacja oprogramowania

1. Konserwację oprogramowania przeprowadza się po zgłoszeniu przez użytkownika systemu potrzeby wprowadzenia zmian pozwalających utrzymać funkcjonalność systemu.

2. Przed dokonaniem zmian w systemie informatycznym należy dokonać archiwizacji danych, przeglądu działania systemu w zmienionej konfiguracji w warunkach testowych na testowej bazie danych na podobnych zasadach jak ma to miejsce w przypadku przeglądu oprogramowania.