Załącznik nr 1
do Zarządzenia nr 11/2013
Starosty Sejneńskiego
z dnia 13 maja 2013r.

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH W STAROSTWIE POWIATOWYM W SEJNACH

I. Wprowadzenie

Niniejszy dokument opisuje reguły dotyczące bezpieczeństwa danych osobowych w Starostwie Powiatowym w Sejnach, zarówno danych przetwarzanych w wersji papierowej, jak i danych zawartych w systemach informatycznych.

Potrzeba jego opracowania wynika z 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). Polityka bezpieczeństwa obowiązuje wszystkich pracowników Starostwa Powiatowego w Sejnach. Wykonywanie postanowień tego dokumentu ma zapewnić właściwą reakcję, ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa systemów oraz zapewnić właściwy tryb działania w celu przywrócenia bezpieczeństwa danych przetwarzanych w Starostwie Powiatowym w Sejnach.

Ilekroć w niniejszym dokumencie jest mowa o:

1) Administratorze Danych Osobowych– należy przez to rozumieć Starostę Sejneńskiego,
2) Administratorze Bezpieczeństwa Informacji – należy przez to rozumieć pracownika Starostwa wyznaczonego do nadzorowania przestrzegania zasad ochrony określonych w niniejszym dokumencie oraz wymagań w zakresie ochrony wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych,
3) użytkowniku systemu – należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym Starostwa. Użytkownikiem może być pracownik Starostwa, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, osoba odbywająca staż w Starostwie lub wolontariusz,
4) sieci lokalnej – należy przez to rozumieć połączenie systemów informatycznych w Starostwie wyłącznie dla własnych jej potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych.

II. Wyznaczenie Administratora Bezpieczeństwa Informacji.

1. Administrator Danych Osobowych, którym jest Starosta, swoją decyzją wyznacza Administratora Bezpieczeństwa Informacji oraz osobę upoważnioną do zastępowania Administratora Bezpieczeństwa Informacji.
2. Administrator Danych Osobowych jest zobowiązany do:
   1) czuwania nad tym, by będące w jego posiadaniu dane osobowe były przetwarzane zgodnie z prawem,
   2) zastosowania niezbędnych środków technicznych i organizacyjnych w celu zapewnienia ochrony przetwarzanych w Starostwie danych osobowych,
   3) sprawowania kontroli nad bezpieczeństwem oraz sposobem przetwarzania danych,
3. Administrator Bezpieczeństwa Informacji realizuje zadania w zakresie ochrony danych, a w szczególności:
   1) ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych Starostwa Powiatowego,

2) podejmowania stosownych działań zgodnie z niniejszą Polityką bezpieczeństwa w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych znajdujących się w systemie informatycznym,

4) niezwłocznego informowania Administratora Danych Osobowych lub osoby przez niego upoważnionej o przypadkach naruszenia przepisów ustawy o ochronie danych osobowych,

5) nadzoru i kontroli systemów informatycznych służących do przetwarzania danych osobowych i osób przy nim zatrudnionych.

4. Osoba zastępująca Administratora Bezpieczeństwa Informacji powyższe zadania realizuje tylko w przypadku nieobecności Administratora Bezpieczeństwa Informacji.

5. Osoba zastępująca składa Administratorowi Bezpieczeństwa Informacji relację z podejmowanych działań w czasie jego zastępstwa.

6. Kierownicy komórek organizacyjnych Starostwa są zobowiązani do:

l) współdziałania z Administratorem Bezpieczeństwa Informacji w zakresie ochrony danych osobowych,

2) sprawowanie nadzoru nad pracą podległych pracowników w zakresie wykonywania czynności służbowych w sposób zapewniający ochronę danych osobowych,

3) zwracania się do Administratora Danych Osobowych o rozstrzygnięcie w przypadku istotnych wątpliwości co do stosowania - przepisów prawnych z zakresu danych osobowych,

4) niezwłocznego zawiadomienia Administratora Danych Osobowych o konieczności utworzenia nowego zbioru danych osobowych, wymagającego rejestracji.

7. Pracownik upoważniony przez Administratora Danych Osobowych do przetwarzania danych osobowych, jest zobowiązany do:

1) zapoznania się z przepisami prawa w zakresie ochrony danych osobowych,

2) stosowania określonych przez Administratora Danych Osobowych, procedur i środków mających na celu zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym,

3) zachowania szczególnej staranności w trakcie wykonywania operacji przetwarzania danych w celu ochrony interesów osób, których te dane dotyczą.

8. Bezpośredni nadzór nad przetwarzaniem danych osobowych w komórkach organizacyjnych Starostwa sprawują kierownicy wydziałów, a w przypadku pracowników na samodzielnych stanowiskach Starosta i Wicestarosta.

9. Obowiązek przestrzegania tajemnicy danych osobowych spoczywa na wszystkich pracownikach, którzy mają do nich dostęp, również po ustaniu stosunku pracy.

10. Przetwarzanie danych osobowych sprzeczne z przepisami ustawy o ochronie danych osobowych może stanowić ciężkie naruszenie obowiązków pracowniczych.

III. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe.

1. Dane osobowe przetwarzane są w budynkach Starostwa Powiatowego w Sejnach ul. 1 Maja 1 oraz w budynku ul. Piłsudskiego 34.

2. Opis obszaru w którym są przetwarzane dane osobowe zawarty jest w wykazie zbiorów danych osobowych i zawiera następujące dane oznaczające:

1)budynek,

2)wydział,

3)pokój,

4) sprzęt, szafy, kasetki itp.

IV. Wykaz zbiorów danych osobowych wraz z ze wskazaniem programów zastosowanych do przetwarzania tych danych

1. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych prowadzi Administrator Bezpieczeństwa Informacji.

2. W przypadku przetwarzania danych i konieczności rejestracji bazy danych w Generalnym Inspektoracie Danych Osobowych, rejestracja następuje na wniosek danego wydziału lub samodzielnego stanowiska pracy.

3. Wykaz zbioru danych zawiera:

1) nazwę zbioru danych,
2) datę utworzenia,
3) wydziały przetwarzające zbiór,
4) listę osób przetwarzająca dane,
5) przewidywany czas użytkowania bazy (stały, okresowy, jednorazowy),
6) wskazanie pomieszczeń w których przetwarzane są dane osobowe, tzn. jaki:
    a)budynek,
    b)wydział,
    c)pokój,
    d) sprzęt, szafy, kasetki itp.
7) nazwę programu zastosowanego do przetwarzania danych,
8) inne ważne informacje (np. zmiany osób uprawnionych).

4. O zmianach w wykazie zbiorów danych informują Administratora Bezpieczeństwa Informacji kierownicy poszczególnych wydziałów, samodzielne stanowiska pracy.

V. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pół informatycznych i powiązania między nimi

1. Opis struktury zbiorów danych osobowych znajdująca się w poszczególnych zbiorach zawarta jest w ,,Zgłoszeniu zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych".

2. Zbiór zgłoszeń prowadzi Administrator Bezpieczeństwa Informacji wraz z zakresem przetwarzanych danych w poszczególnych zbiorach danych.

VI. Sposób przepływu danych pomiędzy poszczególnymi systemami

1. Zbiory właściwe danych osobowych ujęte są w formie dokumentacji drukowanej i w formie elektronicznej.

2. Dostęp do komputera, systemu informatycznego oraz nośników elektronicznych ma wyłącznie osoba upoważniona.

3. Uzupełnianie danych dokonywane jest wyłącznie przez osobę uprawnioną z użyciem programu przewidzianego do tego celu.

4. Aktualizowane dane w formie wydruku włączane są do właściwego zbioru.

5. Wydruki z danymi osobowymi oraz nośniki elektroniczne przechowywane są w obszarze przetwarzania danych posiadającym właściwe zabezpieczenia.

6. W Starostwie Powiatowym w Sejnach nie są przetwarzane dane, o których mowa w art. 27 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych w systemie informatycznym.

VII. Środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

1. Środki ochrony fizycznej

1) Budynki Starostwa, w których zlokalizowany jest obszar przetwarzania danych osobowych są zamykane po zakończeniu pracy. Budynek ul. 1 Maja 1 posiada alarm.
2) Urządzenia służące do przetwarzania danych osobowych znajdują się w pomieszczeniach zabezpieczonych zamkami patentowymi.
3)W pomieszczeniu serwerów zainstalowano drzwi antywłamaniowe.
4) Przebywanie osób nieuprawnionych w pomieszczeniach tworzących obszar przetwarzania danych osobowych dopuszczalne jest tylko w obecności osoby zatrudnionej przy przetwarzaniu danych lub w obecności kierownika wydziału.
5) Pomieszczenia, o których mowa wyżej, powinny być zamykane na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich.
6) W przypadku przebywania osób postronnych w pomieszczeniach, o których mowa wyżej, monitory stanowisk dostępu do danych osobowych powinny być ustawione w taki sposób, aby uniemożliwić tym osobom wgląd w dane.
7) Do przebywania w pomieszczeniu serwerowi uprawnieni są: Administrator Bezpieczeństwa Informacji, osoby odpowiedzialne za obsługę informatyczną Starostwa.
8)Przebywanie w pomieszczeniu serwerowi osób nieuprawnionych (konserwator, elektryk, sprzątaczka) dopuszczalne jest tylko w obecności jednej z osób upoważnionych, o których mowa w pkt 7, a w przypadku ich nieobecności - w obecności osoby pisemnie upoważnionej przez Starostę.

2. Środki sprzętowe, informatyczne i telekomunikacyjne
1) Każdy dokument papierowy przeznaczony do wyrzucenia powinien być uprzednio zniszczony w sposób uniemożliwiający jego odczytanie (np. przy pomocy niszczarki dokumentów).
2) Urządzenia wchodzące w skład systemu informatycznego podłączone są do odrębnego obwodu elektrycznego, zabezpieczonego na wypadek zaniku napięcia albo awarii w sieci zasilającej centralnym UPS-em.
3) Siec lokalna podłączona do Internetu za pomocą odrębnego komputera spełniającego funkcje Proxy Server'a oraz Firewall'a (zapory ogniowej).
4) Zastosowano oprogramowanie do tworzenia kopii zapasowych.
5)Na wszystkich serwerach oraz stacjach roboczych zainstalowano oprogramowanie antywirusowe. Poczta elektroniczna wpływająca do Starostwo skanowana jest programem antywirusowym przed przesłaniem jej do użytkownika.
6) Kopie awaryjne wykonywane są na macierzach dyskowych.

3. Środki ochrony w ramach oprogramowania systemu
1) Dostęp fizyczny do baz danych osobowych zastrzeżony jest wyłącznie dla osób zajmujących się obsługą informatyczną Starostwa.
2) Konfiguracja systemu umożliwia użytkownikom końcowym dostęp do danych osobowych jedynie za pośrednictwem aplikacji.
3) System informatyczny pozwala zdefiniować odpowiednie prawa dostępu do zasobów informatycznych systemu.
4) W sieciowym systemie operacyjnym zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do sieci.

4. Środki ochrony w ramach narzędzi baz danych i innych narzędzi programowych
1) Zastosowano identyfikator i hasło dostępu do danych na poziomie aplikacji
2) Dla każdego użytkownika systemu jest ustalony odrębny identyfikator

3) Zdefiniowano użytkowników i ich prawa dostępu do danych osobowych na poziomie aplikacji (unikalny identyfikator i hasło)

5. Środki ochrony w ramach systemu użytkowego
1) Zastosowano wygaszanie ekranu w przypadku dłuższej nieaktywności użytkownika.
2) Komputer, z którego możliwy jest dostęp do danych osobowych zabezpieczony jest hasłem uruchomieniowym.

6. Środki organizacyjne
1) Wyznaczono Administratora Bezpieczeństwa Informacji oraz na podstawie pisemnego upoważnienia Starosty Sejneńskiego określa się zakres uprawnień pracowników posiadających dostęp do danych osobowych.
2) Osoby upoważnione do przetwarzania danych osobowych są przed dopuszczeniem ich do pracy z tymi danymi szkolone w zakresie obwiązujących przepisów o ochronie danych osobowych, procedur przetwarzania danych oraz informowane o podstawowych zagrożeniach związanych z przetwarzaniem danych w systemie informatycznym.
3) Prowadzona jest ewidencja osób upoważnionych do przetwarzaniu danych osobowych
4) Wprowadzono instrukcję zarządzania systemem informatycznym
5) Zdefiniowano procedury postępowania w sytuacji naruszenia ochrony danych osobowych
6)Wprowadzono obowiązek rejestracji wszystkich przypadków awarii systemu (rejestr zawiera informacje: data i godzina zdarzenia, opis zdarzenia, podjęte działania/wnioski, podpis).
7) Określono sposób postępowania z nośnikami informacji.

VIII. Postępowanie w sytuacji naruszenia ochrony danych osobowych

1. O naruszeniu ochrony danych osobowych mogą świadczyć w szczególności następujące symptomy:
1) brak możliwości uruchomienia przez użytkownika aplikacji pozwalającej na dostęp do danych osobowych,
2) brak możliwości zalogowania się do tej aplikacji,
3) ograniczone, w stosunku do normalnej sytuacji, uprawnienia użytkownika aplikacji (np. brak możliwości wykonywania pewnych operacji normalnie dostępnych użytkownikowi) lub uprawnienia poszerzone w stosunku do normalnej sytuacji,
4)wygląd aplikacji inny niż normalnie,
5) inny zakres danych niż normalnie dostępny dla użytkownika - dużo więcej lub dużo mniej danych,
6) znaczne spowolnienie działania systemu informatycznego,
7)pojawienie się niestandardowych komunikatów generowanych przez system informatyczny,
8) ślady włamania lub prób włamania do obszaru, w którym przetwarzane są dane osobowe,
9) ślady włamania lub prób włamania do pomieszczeń, w których odbywa się przetwarzanie danych osobowych, w szczególności do serwerowni oraz do pomieszczeń, w których przechowywane są nośniki kopii awaryjnych,
10) włamanie lub próby włamania do szafek, w których przechowywane są w postaci elektronicznej lub papierowej - nośniki danych osobowych,
11) zagubienie lub kradzież nośnika danych osobowych,
12) zagubienie lub kradzież nośnika materiału kryptograficznego (karty mikroprocesorowej, dyskietki itp),
13) kradzież sprzętu informatycznego, w którym przechowywane były dane osobowe,

14) informacja z systemu antywirusowego o zainfekowaniu systemu informatycznego wirusami,
15) fizyczne zniszczenie lub podejrzenie zniszczenia elementów systemu informatycznego przetwarzającego dane osobowe na skutek przypadkowych lub celowych działań albo zaistnienia siły wyższej,
16) podejrzenie nieautoryzowanej modyfikacji danych osobowych przetwarzanych w systemie informatycznym.

2. Dane osobowe zostają ujawnione, gdy stają się znane w całości lub części pozwalającej na określenie osobom nie uprawnionym tożsamości osoby, której dane dotyczą.

3. Każdy pracownik Starostwa biorący udział w przetwarzaniu danych osobowych w systemie informatycznym jest odpowiedzialny za bezpieczeństwo tych danych. W szczególności osoba, która zauważyła zdarzenie mogące być przyczyną naruszenia ochrony danych osobowych lub mogących spowodować naruszenie bezpieczeństwa danych, zobowiązana jest do natychmiastowego poinformowania Administratora Danych Osobowych, Administratora Bezpieczeństwa Informacji i osobę zajmującą się obsługą informatyczną Starostwa.

4. Każda osoba zatrudniona w Starostwie, która stwierdzi lub podejrzewa naruszenie zabezpieczenia ochrony danych osobowych w systemie informatycznym (lub przetwarzanych w inny sposób), powinna niezwłocznie poinformować o tym Administratora Danych Osobowych, Administratora Bezpieczeństwa Informacji i osobą zajmującą się obsługą informatyczną Starostwa.

5.Do czasu przybycia Administratora Danych Osobowych, Administratora Bezpieczeństwa Informacji lub osoby zajmującej się obsługą informatyczną Starostwa, zgłaszający:
1) niezwłocznie podejmuje czynności niezbędne do powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnia w działaniu również ustalenie przyczyn lub sprawców,
2) zabezpiecza dostęp do miejsca lub urządzenia przez osoby trzecie,
3)wstrzymuje pracę na komputerze na którym zaistniało naruszenie ochrony oraz nie uruchamia bez koniecznej potrzeby komputerów i innych urządzeń, których funkcjonowanie w związku naruszeniem ochrony zostało wstrzymane,
4) nie zmienia położenia przedmiotów, które pozwalają stwierdzić naruszenie ochrony lub odtworzyć jej okoliczności,
5) podejmuje, stosownie do zaistniałej sytuacji, inne niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych,
6) podejmuje inne działania określone w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących naruszeniu,
7) może dokonywać zmian w miejscu naruszenia danych osobowych, jeżeli zachodzi konieczność ratowania osób lub mienia albo zapobieżenia grożącemu niebezpieczeństwu.

6. Osoba zajmujące się obsługą informatyczną Starostwa niezwłocznie po uzyskaniu sygnału o naruszeniu danych osobowych, powinna:
1) zapoznać się z zaistniałą sytuacją i dokonać wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy Starostwa.
2) zapisać wszelkie informacje związane z danym zdarzeniem.
3) na bieżąco wygenerować i wydrukować wszystkie możliwe dokumenty i raporty, które mogą pomóc w ustaleniu okoliczności zdarzenia.

4) przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, zwłaszcza do określenia skali zniszczeń i metody dostępu do danych osoby niepowołanej.
5) dokonać fizycznego odłączenia urządzeń i segmentów sieci, które mogły umożliwić dostęp do bazy danych osobie nie uprawnionej.
6) wylogować użytkownika podejrzanego o naruszenie zabezpieczenia ochrony danych.
7) dokonać zmiany hasła na konto osoby zajmującej się obsługą informatyczną poprzez które uzyskano nielegalny dostęp w celu uniknięcia ponownej próby włamania.
8) zażądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem.

7. Administrator Bezpieczeństwa Informacji w porozumieniu z osobą zajmującą się obsługą informatyczną, podejmuje działania zmierzające do wyjaśnienia zgłoszonego zdarzenia. W szczególności może on dokonywać, w zależności od zgłoszonego zdarzenia:
1) przeprowadzenia wywiadów z pracownikami w celu ustalenia zaistniałych faktów,
2) przeprowadzenia analizy poprawności funkcjonowania systemu informatycznego, jeżeli zgłoszone zdarzenie było związane z nieprawidłowym jego funkcjonowaniem,
3) przeprowadzenia analizy zapisu zdarzeń w systemie informatycznym z uwzględnieniem zapisu operacji realizowanych przez użytkowników,
4) przeprowadzenia analizy danych przetwarzanych w systemie informatycznym, jeżeli zgłoszone zdarzenie mogło być spowodowane utratą dostępności lub integralności przetwarzanych danych,
5)zabezpieczenia danych przetwarzanych w systemie informatycznym dotkniętym incydentem, w szczególności danych konfiguracyjnych tego systemu,
6) zebrania innych materiałów pozwalających na wyjaśnienie przyczyn zaistnienia incydentu, jego charakteru i potencjalnych skutków.

8. Osobą zajmującą się obsługą informatyczną Starostwa Powiatowego w Sejnach przystępuje do usuwania skutków incydentu i przywrócenia prawidłowego przebiegu procesu przetwarzania danych osobowych. W szczególności działania związane z usuwaniem skutków incydentu mogą obejmować:
1) przeprowadzenie naprawy sprzętu informatycznego,
2) rekonfigurację sprzętu informatycznego,
3) wprowadzenie poprawek do oprogramowania,
4) rekonfigurację oprogramowania,
5) odtworzenie danych z kopii awaryjnych,
6) modyfikację danych w celu odtworzenia ich integralności,
7) wycofanie z użycia materiału kryptograficznego,
8) inne naprawy urządzeń wchodzących w skład infrastruktury informatycznej wspomagających lub zabezpieczających działanie systemu informatycznego.

9. Przy usuwaniu skutków incydentu z wykorzystaniem odtwarzania danych z kopii awaryjnych, osoba zajmującą się obsługą informatyczną, obowiązana jest upewnić się, że odtworzone dane zostały zapisane przed wystąpieniem incydentu - w szczególności dotyczy to przypadków odtwarzania systemu po infekcji wirusowej.

10. Zgodę na uruchomienie komputerów i innych urządzeń lub dokonanie zmian w miejscu naruszenia ochrony wyraża Administrator Danych Osobowych.

11. System informatyczny, którego prawidłowe działanie zostało odtworzone, powinien zostać poddany szczegółowej obserwacji w celu stwierdzenia całkowitego usunięcia symptomów incydentu.

12. Administrator Bezpieczeństwa Informacji dokumentuje w raporcie każdy zaistniały przypadek naruszenia ochrony danych osobowych. Raport przedkłada się Administratorowi Danych Osobowych. Raport obejmuje następujące informacje:
1) imię i nazwisko osoby zgłaszającej incydent,
2) imię i nazwisko osoby przyjmującej zgłoszenie incydentu,
3) datę i godzinę przyjęcia zgłoszenia incydentu,
4) określenie czasu i miejsca incydentu,
5) opis zgłoszonego incydentu oraz okoliczności towarzyszące(zgłoszenia policji),
6) przyczyny wystąpienia naruszenia,
7) opis podjętych działań naprawczych,
8) wyniki przeprowadzonego badania wyjaśniającego,
9) ocenę skuteczności przeprowadzonego postępowania naprawczego,
10) podjęte środki techniczne, organizacyjne w celu zapobiegania w przyszłości naruszenia ochrony danych osobowych.

IX. Znajomość polityki bezpieczeństwa systemu informatycznego
Do zapoznania się z niniejszym dokumentem oraz stosowania zawartych w nim zasad zobowiązani są wszyscy pracownicy Starostwa Powiatowego w Sejnach upoważnieni do przetwarzania danych.