Załącznik Nr 1 do zarządzenia
Nr OG.120.26.2012
Starosty Nowotomyskiego
z dnia19.12.2012r.

Polityka bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Starostwie Powiatowym w Nowym Tomyślu.

ZATWIERDZAM:

STAROSTA
.....
mgr Andrzej Wilkoński

Opracował : Administrator Bezpieczeństwa Informacji

Grudzień 2012 rok

SPIS TREŚCI:

WPROWADZENIE

Niniejszy dokument opisuje reguły dotyczące bezpieczeństwa danych osobowych zawartych w systemach informatycznych oraz zabezpieczenia danych przetwarzanych metodami tradycyjnymi w Starostwie Powiatowym w Nowym Tomyślu. Opisane reguły określają granice dopuszczalnego zachowania wszystkich użytkowników systemów informatycznych wspomagających pracę Urzędu. Dokument zwraca uwagę na konsekwencje jakie mogą ponosić osoby przekraczające określone granice oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń.

Odpowiednie zabezpieczenia, ochrona przetwarzanych danych oraz niezawodność funkcjonowania są podstawowymi wymogami stawianymi współczesnym systemom informatycznym.

Dokument Polityka bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie, zwany dalej „Polityką bezpieczeństwa", zawiera zestaw reguł i praktycznych działań oraz wskazuje sposób postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych w systemach informatycznych i przeznaczony jest dla osób zatrudnionych przy przetwarzaniu tych danych.

Potrzeba jego opracowania wynika z § 3 i 4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. 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)

Administratorzy danych osobowych są zobowiązani do zapewnienia środków technicznych i organizacyjnych pozwalających na pełną ochronę przetwarzanych danych osobowych, a w szczególności na zabezpieczeniu ich przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Mając na uwadze zabezpieczenie danych osobowych na administratorach danych osobowych spoczywa obowiązek opracowania, wdrożenia i prowadzenia

dokumentacji opisującej sposób przetwarzania danych oraz stosowania środków niezbędnych do zapewnienia pełnej ochrony w tym zakresie.

I Zasady ogólne

1. Bezpieczeństwo informacji - to wszelkiego rodzaju działania organizacyjne i niezbędne środki techniczne jakie zobowiązany jest stosować administrator danych osobowych, które mają na celu zabezpieczenie ich przed udostępnieniem osobom nieuprawnionym, zabraniem, zmianą, uszkodzeniem lub zniszczeniem.

2. Polityka bezpieczeństwa określa tryb postępowania w przypadku, gdy:
   1) stwierdzono naruszenie zabezpieczenia systemu informatycznego,
   2) stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci informatycznej mogą wskazywać na naruszenie zabezpieczeń tych danych.

3. Polityka bezpieczeństwa obowiązuje wszystkich pracowników Starostwa Powiatowego w Nowym Tomyślu. Obowiązek przestrzegania przepisów dotyczących ochrony danych osobowych spoczywa na każdym pracowniku Starostwa bez względu na charakter zatrudnienia oraz sposób przetwarzania danych osobowych.

4. 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 systemach informatycznym Urzędu.

5. Nadzór nad przestrzeganiem zasad ochrony danych osobowych przetwarzanych w Starostwie Powiatowym w Nowym Tomyślu w imieniu Administratora danych, którym jest Starosta Nowotomyski sprawuje Administrator Bezpieczeństwa Informacji zwany dalej "Administratorem Bezpieczeństwa", który jest powołany w drodze zarządzenia.

6. Administrator Bezpieczeństwa realizuje zadania w zakresie ochrony danych, a w szczególności:

1) ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych Urzędu,
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,
3) niezwłocznego informowania Administratora danych lub osoby przez niego upoważnionej o przypadkach naruszenia przepisów ustawy o ochronie danych osobowych,
4) nadzoru i kontroli systemów informatycznych służących do przetwarzania danych osobowych i osób przy nim zatrudnionych.

Niniejszy dokument jest zgodny z następującymi aktami prawnymi:

1) ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883 z późn. zm.),
2) ustawą o ochronie informacji niejawnych z dnia 5 sierpnia 2010r. (Dz. U. NR 182, poz. 1228 z późn. zm.),

Rozdział I

OPIS ZDARZEŃ NARUSZAJĄCYCH OCHRONĘ DANYCH OSOBOWYCH

1. Podział zagrożeń:

1) zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu), których występowanie może prowadzić do utraty integralności danych, ich zniszczenia uszkodzenia infrastruktury technicznej systemu, ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych,

2) zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania), w wyniku których może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych,

3) zagrożenia zamierzone, świadome i celowe - najpoważniejsze zagrożenia powodujące naruszenie poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na: nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu), nieuprawniony dostęp do systemu z jego wnętrza, nieuprawniony przekaz danych, pogorszenie jakości sprzętu i oprogramowania, bezpośrednie zagrożenie materialnych składników systemu,

2. Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe to głównie:

1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.,
2) niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka

temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,

3) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru,
4) pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,
5) jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
6) naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,
7) próba lub modyfikacja danych lub zmiana w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
8) niedopuszczalna manipulacja danymi osobowymi w systemie,
9) ujawnienie osobom nieupoważnionym danych osobowych lub objętych tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń,
10) praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych - np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.,
11) ujawnienia istnienia nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki", itp.,
12) podmiana lub zniszczenie nośników z danymi osobowymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane osobowe,
13) rażące naruszenie dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.).

3. Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, dyskietkach w formie niezabezpieczonej itp.

Rozdział II

ZABEZPIECZENIE DANYCH OSOBOWYCH

1. Administratorem danych osobowych zawartych i przetwarzanych w systemach informatycznych Starostwa Powiatowego jest Starosta Nowotomyski.

2. Administrator danych osobowych jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w systemach informatycznych Urzędu, a w szczególności:

- zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym,
- zapobiegać przed zabraniem danych przez osobę nieuprawnioną,
- zapobiegać przetwarzaniu danych z naruszeniem ustawy oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych.

3. Zakres zadań należący do starostw powiatowych, wynikający z ustawy z dnia 5 czerwca 1998 r o samorządzie powiatowym (tekst jednolity z 2001 – Dz.U. nr 142, poz. 1592 – ze zmianami) oraz innych ustaw i przepisów szczególnych, związany jest w szerokim zakresie z przetwarzaniem danych osobowych. Przetwarzanie danych osobowych odbywa się praktycznie w każdym pomieszczeniu. Sposób przetwarzania danych jest różny, a determinuje go zakres realizowanych zadań.

4. W celu ochrony przed utratą danych w Starostwie Powiatowym stosowane są następujące zabezpieczenia:

A. Środki techniczne:

- dane przetwarzane są przy użyciu stacji roboczych lokalnie oraz na serwerach sieciowych pracujących w wewnętrznej sieci komputerowej,
- dane przetwarzane przy użyciu tradycyjnych środków pisarskich gromadzone są w rejestrach, księgach, zeszytach papierowych, segregatorach oraz w teczkach.

B. Środki ochrony fizycznej:

- pomieszczenia, w których przetwarzane są dane osobowe oraz biurka i szafy zawierające nośniki z danymi osobowymi, po godzinach pracy winny być zamykane na klucz. Klucze do biurek i szaf przechowują u siebie pracownicy, natomiast klucze do pomieszczeń przechowywane są w wyznaczonym pomieszczeniu. W przypadku konieczności opuszczenia pomieszczeń, o których mowa wyżej, w trakcie godzin pracy przez zatrudnionych w nich pracowników, pomieszczenia te należy zamykać na klucz bez pozostawienia w nich osób nieupoważnionych,
- urządzenia służące do przetwarzania danych osobowych znajdują się w pomieszczeniach zabezpieczonych zamkami patentowymi,
- dostęp do pokoi nr 3 i 3a w budynku C oraz do pokoju nr 2 w budynku F jest zabezpieczony antywłamaniowymi drzwiami zabezpieczonymi kontrolą dostępu na karty chipowe,
- pokój nr 3 w budynku C i pokój nr 2 w budynku F jest wyposażony w system klimatyzacyjny,
- okna w pokojach nr 61 i 66 w budynku B, w pokojach na I piętrze w budynku D oraz na parterze w budynku F (serwerownia i składnica akt) są zabezpieczone szybami antywłamaniowymi,
- wejście do pomieszczeń archiwalnych w budynku B oraz D zabezpieczone są dodatkowo kratami,
- zastosowano sejfy do przechowywania kopii zapasowych i wymiennych nośników danych,

- w pomieszczeniu w którym znajduje się serwer zamontowano klimatyzację, która zapewnia właściwą temperaturę i wilgotność powietrza dla sprzętu komputerowego,
- w pobliżu wejścia do pomieszczenia z serwerem i innymi urządzeniami znajduje się gaśnica, która okresowo jest napełniana i kontrolowana przez specjalistę,
- większość urządzeń w serwerowni umieszczona jest w szafach serwerowych i sieciowych,
- w pomieszczeniach gdzie przebywają osoby postronne monitory stanowisk dostępu do danych osobowych powinny być ustawione w taki sposób, żeby uniemożliwić tym osobom wgląd w dane.
- osoba użytkująca przenośny komputer, służący do przetwarzania danych osobowych, obowiązana jest zachować szczególną ostrożność podczas transportu i przechowywania tego komputera poza obszarem przewidziane do przetwarzania, w celu zapobieżenia dostępowi do tych danych osobie niepowołanej, a w szczególności powinna:

  - dostęp do komputera zabezpieczony hasłem,
  - nie zezwalać na używanie komputera osobom nieupoważnionym do dostępu do danych osobowych,

- przetwarzanie danych osobowych w wydzielonych pomieszczeniach położonych w strefie administracyjnej,
- zabezpieczenie wejść do pomieszczeń, o których mowa w wyżej punkcie,
- szczególne zabezpieczenie centrum przetwarzania danych (komputer centralny, serwerownia) poprzez zastosowanie systemu kontroli dostępu,
- wyposażenie pomieszczeń w szafy dające gwarancję bezpieczeństwa dokumentacji.

C. <u>Środki sprzętowe, informatyczne i telekomunikacyjne</u>

- zastosowano niszczarki dokumentów,
- urządzenia wchodzące w skład systemu informatycznego podłączone są do odrębnego obwodu elektrycznego, zabezpieczonego na wypadek zaniku napięcia albo awarii w sieci zasilającej,

- zastosowano sieć lokalną (Ethernet) w topologii gwiazdy,
- dane są przetwarzane w sposób scentralizowany,
- sieć lokalna podłączona do Internetu za pomocą routera,
- kopie awaryjne wykonywane są na serwerach, nośnikach taśmowych i zewnętrznych dyskach w zależności od danego serwera,
- ochrona serwerów przed zanikiem zasilania poprzez stosowanie zasilaczy zapasowych UPS.

D. Środki ochrony w ramach oprogramowania urządzeń teletransmisji

- zastosowano sprzężony firewall na styku z siecią Internet,
- zastosowano program antywirusowy na komputerach użytkowników,
- zastosowano firewall na komputerach użytkowników systemu, który ma za zadanie uwierzytelnienie źródła przychodzących wiadomości oraz filtrowanie pakietów w oparciu o adres IP, numer portu i inne parametry. Ściana ogniowa składa się z bezpiecznego systemu operacyjnego i filtra pakietów. Ruch pakietów, który firewall przepuszcza jest określony przez administratora. Firewall zapisuje do logu fakt zaistnienia wyjątkowych zdarzeń i śledzi ruch pakietów przechodzących przez nią,
- zastosowano system wykrywający obecność wirusów w poczcie elektronicznej. W efekcie zapewnione jest:
  - zabezpieczenie sieci przed atakiem z zewnątrz poprzez blokowanie wybranych portów ;
  - filtrowanie pakietów i blokowanie niektórych usług;
  - objęcie ochroną antywirusową wszystkich danych ściąganych z Internetu na stacjach lokalnych;
  - zapisywanie logów połączeń użytkowników z siecią Internet.

E. Środki ochrony w ramach oprogramowania systemu

- Konfiguracja systemu umożliwia użytkownikom końcowym dostęp do danych osobowych jedynie za pośrednictwem aplikacji,

- Zastosowano działający w „tle" program antywirusowy na komputerach użytkowników,
- W systemie operacyjnym zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do systemu operacyjnego i programów sieciowych,
- Zastosowano specjalistyczne oprogramowanie do tworzenia kopii zapasowych;

F. Środki ochrony w ramach narzędzi baz danych i innych narzędzi programowych

- automatycznie rejestrowany jest identyfikator użytkownika wprowadzającego dane oraz datę pierwszego wprowadzenia tych danych,
- zastosowano identyfikator i hasło dostępu do danych na poziomie aplikacji,
- dla każdego użytkownika systemu jest ustalony odrębny identyfikator,
- zdefiniowano użytkowników i ich prawa dostępu do danych osobowych na poziomie aplikacji,
- w systemie informatycznym Urzędu zastosowano autoryzację użytkownika. uruchamiając program użytkowy, podając login użytkownika i hasło.

G. Środki ochrony w ramach systemu użytkowego

- zastosowano automatyczne wygaszanie ekranu monitora w przypadku dłuższej nieaktywności użytkownika,
- komputer, z którego możliwy jest dostęp do danych osobowych zabezpieczony jest hasłem uruchomieniowym.

H. Środki organizacyjne

- wyznaczono administratora bezpieczeństwa informacji,
- tymczasowe wydruki z danymi osobowymi są po ustaniu ich przydatności zniszczone w stopniu uniemożliwiającym ich odczytanie,

- osoby upoważnione do przetwarzania danych osobowych są przed dopuszczeniem ich do tych danych szkolone w zakresie obwiązujących przepisów o ochronie danych osobowych, procedur przetwarzania danych oraz informowane o podstawowych zagrożeniach związanych z przetwarzaniem danych w systemie informatycznym i są zobowiązane do zachowania w tajemnicy informacji uzyskanych w trakcie dokonywania operacji związanych z przetwarzaniem danych osobowych **zał nr 1**,
- przeszkolenie osób upoważnionych w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochroną danych osobowych,
- kontrolowanie otwierania i zamykania pomieszczeń, w których są przetwarzane dane osobowe, polegające na otwarciu pomieszczenia przez pierwszą osobę, która rozpoczyna pracę oraz zamknięciu pomieszczenia przez ostatnią wychodzącą osobę,
- prowadzona jest ewidencja osób upoważnionych do przetwarzaniu danych osobowych,
- ustalono instrukcję zarządzania systemem informatycznym,
- zdefiniowano procedury postępowania w sytuacji:

  a) naruszenia ochrony danych osobowych,

  b) słabości systemu,

  c) niewłaściwego funkcjonowania oprogramowania;

- w przypadku, gdy zachodzi konieczność naprawy sprzętu poza siedzibą Starostwa, należy wymontować z niego nośniki informacji zawierające dane osobowe,
- 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. Niezależnie od niniejszych zasad opisanych w dokumencie „Polityka bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Starostwie Powiatowym" w zakresie bezpieczeństwa mają zastosowanie wszelkie wewnętrzne regulaminy lub instrukcje dotyczące

bezpieczeństwa ludzi i zasobów informacyjnych oraz indywidualne zakresy zadań osób zatrudnionych przy przetwarzaniu danych osobowych w określonym systemie.

6. Wykaz pomieszczeń w których przetwarzane są dane osobowe **(zał nr 2)** oraz opis systemów informatycznych Starostwa Powiatowego **(zał nr 3)** zawierają załączniki do niniejszego dokumentu.

Rozdział III

KONTROLA PRZESTRZEGANIA ZASAD ZABEZPIECZENIA DANYCH OSOBOWYCH

1. Administrator danych - Starosta lub osoba przez niego wyznaczona, którą jest „Administrator Bezpieczeństwa Informacji" sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych wynikających z ustawy o ochronie danych osobowych oraz zasad ustanowionych w niniejszym dokumencie.
2. Administrator Bezpieczeństwa Informacji sporządza roczne plany kontroli zatwierdzone przez Administratora Danych i zgodnie z nimi przeprowadza kontrole oraz dokonuje analizy i oceny przestrzegania przepisów i stanu bezpieczeństwa danych osobowych.

3. Na podstawie zgromadzonych materiałów, o których mowa w pkt. 2, Administrator Bezpieczeństwa sporządza roczne sprawozdanie i przedstawia Administratorowi danych –Staroście Nowotomyskiemu.

Rozdział IV

POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. W przypadku stwierdzenia naruszenia:

- zabezpieczenia systemu informatycznego,

- technicznego stanu urządzeń,
- zawartości zbioru danych osobowych,
- ujawnienia metody pracy lub sposobu działania programu,
- jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych,
- innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. zalanie, pożar, itp.)

<u>każda osoba zatrudniona przy przetwarzaniu danych osobowych jest obowiązana niezwłocznie powiadomić o tym fakcie Administratora Bezpieczeństwa.</u>

2. W razie niemożliwości zawiadomienia Administratora Bezpieczeństwa lub osoby przez niego upoważnionej, należy powiadomić bezpośredniego przełożonego.

3. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych Administratora Bezpieczeństwa lub upoważnionej przez niego osoby, należy:

- niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców,
- rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
- zaniechać - o ile to możliwe - dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,
- podjąć inne działania przewidziane i określone w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących naruszeniu,
- podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej,
- zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku,
- udokumentować wstępnie zaistniałe naruszenie,

- nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora Bezpieczeństwa lub osoby upoważnionej.

4. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych, Administrator Bezpieczeństwa lub osoba go zastępująca:

- zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy Urzędu,
- może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
- rozważa celowość i potrzebę powiadamia o zaistniałym naruszeniu Administratora danych,
- nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba, ze specjalistami spoza Urzędu.

5. Administrator Bezpieczeństwa dokumentuje zaistniały przypadek naruszenia oraz sporządza raport wg wzoru stanowiącego załącznik **nr 4**, który powinien zawierać w szczególności:

- wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem,
- określenie czasu i miejsca naruszenia i powiadomienia,
- określenie okoliczności towarzyszących i rodzaju naruszenia,
- wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania,
- wstępną ocenę przyczyn wystąpienia naruszenia,
- ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.

6. Raport, o którym mowa w pkt 5, Administrator Bezpieczeństwa niezwłocznie przekazuje Administratorowi danych, a w przypadku jego nieobecności osobie uprawnionej.

7. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu Administrator Bezpieczeństwa zasięga niezbędnych opinii i proponuje postępowanie naprawcze, a w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.

8. Zaistniałe naruszenie może stać się przedmiotem szczegółowej, zespołowej analizy prowadzonej przez Kierownictwo urzędu, Administratora Bezpieczeństwa Informacji, Pełnomocnika ds. Ochrony Informacji Niejawnych.

9. Analiza, o której mowa w ust. 8, powinna zawierać wszechstronną ocenę zaistniałego naruszenia, wskazanie odpowiedzialnych, wnioski co do ewentualnych przedsięwzięć proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

Rozdział 5

POSTANOWIENIA KOŃCOWE

1. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie dyscyplinarne.

2. Administrator Bezpieczeństwa zobowiązany jest prowadzić ewidencję osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych wg wzoru stanowiącego załącznik **nr 5** do niniejszego dokumentu.

3. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, w szczególności przez osobę, która wobec naruszenia zabezpieczenia systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym Administratora Bezpieczeństwa.

4. Orzeczona kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia administratora bezpieczeństwa informacji nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926) oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

5. W sprawach nie uregulowanych niniejszym dokumentem mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926), rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. 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 rozporządzenie Ministra Sprawiedliwości z dnia 28 kwietnia 2004 r. w sprawie sposobu technicznego przygotowania systemów i sieci do przekazywania informacji – do gromadzenia wykazów połączeń telefonicznych i innych przekazów informacji oraz sposobów zabezpieczenia danych informatycznych (Dz. U. Nr 100, poz. 1023).

6. Niniejsza „Polityka bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Starostwie Powiatowym w Nowym Tomyślu wchodzi w życie z dniem jej podpisania przez Starostę Nowotomyskiego.

Załącznik nr 1
do Polityki bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Starostwie Powiatowym w Nowym Tomyślu

Oświadczenie

.....

(imię i nazwisko)

.....

(wydział)

.....

(stanowisko)

Oświadczam, że zapoznałem(łam) się z przepisami prawa dotyczącymi ochrony danych osobowych, a w szczególności z ustawą z 29 sierpnia 19977r. o chronię danych osobowych(Dz. U. z 2002r. Nr 101, poz. 926 z późn. zm.) oraz rozporządzeniem ministra spraw wewnętrznych i administracji z 29 kwietnia 2004r. w sprawie dokumentacji i 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) i zobowiązuje się do ich przestrzegania.

Oświadczam ponadto, że zapoznałem(łam) się z dokumentacją polityki bezpieczeństwa, wewnętrzną instrukcja zarządzania systemem informatycznym, służącym przetwarzaniu danych osobowych ze szczególnym uwzględnieniem bezpieczeństwa informacji i instrukcją postępowania w sytuacji naruszenia ochrony danych osobowych.

Świadomy(a) odpowiedzialności porządkowej i karnej oświadczam, że znane mi dane osobowe będę przetwarzać zgodnie z prawem i nie dopuszczę do bezprawnego naruszenia tajemnicy również w sytuacji , gdy ustanie moje zatrudnienie w placówce Starostwie Powiatowym w Nowym Tomyślu.

.....

(podpis pracownika)

Załącznik nr 2
do Polityki bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Starostwie Powiatowym w Nowym Tomyślu

Wykaz pomieszczeń w których przetwarzane są dane osobowe w Starostwie Powiatowym w Nowym Tomyślu i ich zabezpieczeń.

1. Wykaz pomieszczeń, w których przetwarzane są dane osobowe.

Nr pokoju	Komórka organizacyjna	System

Załącznik nr 3
do Polityki bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Starostwie Powiatowym w Nowym Tomyślu

1. Opis systemów informatycznych

Nazwa zbioru (opis)	Program do przetwarzania

Załącznik nr 4
do Polityki bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Starostwie Powiatowym w Nowym Tomyślu

W z ó r

R a p o r t
z naruszenia bezpieczeństwa systemu informatycznego w Starostwie Powiatowym w Nowym Tomyślu

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

Załącznik nr 5
do Polityki bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Starostwie Powiatowym w Nowym Tomyślu

W z ó r

Wykaz osób, które zostały zapoznane z „Polityką bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Starostwie Powiatowym w Nowym Tomyślu, przeznaczonej dla osób zatrudnionych przy przetwarzaniu tych danych.

Przyjąłem/am/ do wiadomości i stosowania zapisy Polityki bezpieczeństwa.

Nazwisko i Imię	Komórka organizacyjna	Data, podpis