ZARZĄDZENIE NR 6/2009

Starosty Otwockiego

z dnia 13.02.2009.....

w sprawie:

1. Ustalenia Polityki bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Starostwie Powiatowym w Otwocku.
2. Ustalenia Instrukcji określającej sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Starostwie Powiatowym w Otwocku ,
3. Powołania Administratora Bezpieczeństwa Informacji i Administratora Systemów Informatycznych..

Na podstawie art. 35 ust. 2 ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (t. j. Dz. U. z 2001 roku Nr 142 poz. 1592 z późn. zm.), § 8 ust. 1 Regulaminu Organizacyjnego Starostwa Powiatowego w Otwocku stanowiącego załącznik do Uchwały Nr 114/XVIII/08 Rady Powiatu w Otwocku z dnia 26 czerwca 2008 r. w związku z ust. 1 i 2 art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t. j. Dz. U. z 2002 roku Nr 101 poz. 926 z późn. zm.) w związku §3 ust.3 oraz §4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy teleinformatyczne służące do przetwarzania danych osobowych (Dz. U z 2004 roku Nr 100 poz. 1024) oraz § 4 pkt. 1 rozporządzenia Prezesa Rady Ministrów z 25 sierpnia 2005, w sprawie podstawowych wymagań bezpieczeństwa informatycznego (Dz. U. Nr 171 poz. 1433), zarządzam, co następuje:

§ 1.

Ustalam "Politykę bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Starostwie Powiatowym w Otwocku" zwaną dalej "Polityką bezpieczeństwa", która stanowi załącznik nr 1 do niniejszego zarządzenia.

§ 2.

Ustalam "Instrukcję określającą sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Starostwie Powiatowym w Otwocku zwaną dalej "Instrukcją", która stanowi załącznik nr 2 do niniejszego zarządzenia..

§ 3.

Zobowiązuję pracowników Starostwa Powiatowego Otwocku w do stosowania zasad określonych w "Polityce bezpieczeństwa"

§ 4.

Wyznaczam Pana Łukasza Wróbla na Administratora Bezpieczeństwa Informacji (ABI) w Starostwie Powiatowym w Otwocku.

§ 5.

Wyznaczam Pana Wojciecha Okońskiego na Administratora Systemów Informatycznych (ASI) służących do przetwarzania danych osobowych w Starostwie Powiatowym w Otwocku.

§ 7.

Tracą moc Zarządzenia Starosty Nr 22/2004 i Nr 72/2007.

§ 8.

Zarządzenie wchodzi w życie z dniem podjęcia.

STAROSTA
mgr Krzysztof Soczarski

RADCA PRAWNY
Tadeusz Mojsa
W-wa 5717

Załącznik nr 1 do
Zarządzenia Starosty Otwockiego
nr 6/2009 z dnia 13.02.2009

Polityka bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Starostwie Powiatowym w Otwocku

Spis treści

Podstawowe pojęcia. 3
Wprowadzenie 6
Zasady postępowania przy przetwarzaniu danych osobowych. 8
Opis zdarzeń naruszających ochronę danych osobowych 13
Zabezpieczenie przed naruszeniem systemu ochrony danych osobowych. 15
Kontrola przestrzegania zasad zabezpieczania systemu ochrony danych osobowych 17
Środki techniczne i organizacyjne 18
Postępowanie w przypadku naruszenia zabezpieczenia systemu ochrony danych osobowych. 21
Postanowienia końcowe. 26

Podstawowe pojęcia.

Polityka Bezpieczeństwa – najważniejszy dokument stosowany w systemie zarządzania bezpieczeństwem informacji. Tworzy wytyczne i ramy dla pozostałych zasad. Opisuje wskazówki właściwe dla urzędu, które należy wziąć pod uwagę podczas tworzenia polityki bezpieczeństwa informacji;

Dane osobowe - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden z kilku specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne;

Administrator Danych Osobowych – organ, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych osobowych;

Zbiór danych osobowych - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;

Integralność danych – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

Poufność danych – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;

Przetwarzanie danych osobowych - jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;

Usuwanie danych – zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;

Administrator Bezpieczeństwa Informacji – wyznaczona przez Administratora Danych Osobowych osoba, która nadzoruje przestrzeganie zasad ochrony danych, określonych przez administratora, stosując odpowiednie do zagrożeń i kategorii danych objętych ochroną środki techniczne i organizacyjne, które mają zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem zwana dalej ABI;

System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

Administrator Systemu Informatycznego – osoba upoważniona przez Administratora Bezpieczeństwa Informacji – administrator konkretnego systemu informatycznego przetwarzającego dane osobowe zwana dalej ASI;

Zabezpieczenie danych w systemie informatycznym - wdrożenie i eksploatacja stosowanych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;

Osoba upoważniona lub użytkownik systemu - osoba posiadająca upoważnienie wydane przez ADO dopuszczona jako użytkownik do przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej, w zakresie wskazanym w upoważnieniu, zwana dalej użytkownikiem;

Odbiorcy danych - każdy, komu udostępnia się dane osobowe, z wyłączeniem:

- osoby, której dane dotyczą,
- osoby, upoważnionej do przetwarzania danych,
- przedstawiciela, o którym mowa w art. 31a ustawy o ochronie danych osobowych,
- podmiotu, o którym mowa w art. 31 ustawy o ochronie danych osobowych,
- organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

Osoba trzecia – każda osoba nieupoważniona do dostępu do danych osobowych lub zbiorów tych danych. Osobą trzecią jest również osoba posiadająca upoważnienie wydane przez ADO podejmująca czynności w zakresie przekraczającym ramy udzielonego jej upoważnienia;

Identyfikator użytkownika (login) – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;

Hasło – ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;

Uwierzytelnianie – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

Wprowadzenie

Dokument „Polityka bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Starostwie Powiatowym w Otwocku" zwany dalej „Polityką bezpieczeństwa" jest wewnętrznym dokumentem Starostwa Powiatowego w Otwocku i ma zastosowanie do wszelkich danych osobowych znajdujących się bądź mogących się znajdować w systemie informatycznym urzędu.

Ochrona i zabezpieczenie przetwarzanych danych w połączeniu z niezawodnością funkcjonowania są podstawowymi wymogami stawianymi systemom informatycznym.

Poruszone zagadnienia w dokumencie określają granice dopuszczalnego zachowania użytkowników systemu informatycznego oraz wskazują na konsekwencje jakie mogą ponosić osoby naruszające przepisy ustawy o ochronie danych osobowych (t. j. Dz. U. z 2002 roku Nr 101 poz. 926 z późn. zm.).

Potrzeba opracowania dokumentacji bezpieczeństwa informatycznego wynika z rozporządzenia Prezesa Rady Ministrów w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego z dnia 25 sierpnia 2005 r. (Dz. U. Nr 171 poz. 1433) oraz § 3 i 4 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. z 2004 roku Nr 100 poz. 1024).

„Polityka bezpieczeństwa" określa:

- sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych;
- podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych;
- wymagania w zakresie odnotowywania udostępniania i bezpieczeństwa przetwarzania danych osobowych;
- instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych;
- wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;
- wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;

- opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania miedzy nimi;
- sposób przepływu pomiędzy poszczególnymi systemami;
- określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przy przetwarzaniu danych.

„Polityka bezpieczeństwa" obowiązuje wszystkich pracowników Starostwa Powiatowego w Otwocku.

Zastosowanie tego dokumentu zapewni bezpieczeństwo danych przetwarzanych w systemie informatycznym Starostwa Powiatowego w Otwocku.

Niniejszy dokument został opracowany zgodnie z następującymi aktami prawnymi:

- ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t. j. Dz. U. z 2002 roku Nr 101 poz. 926 z późn. zm.);
- ustawą z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (t. j. Dz. U. z 2005 roku Nr 196 poz. 1631 z późn. zm.);
- rozporządzeniem Prezesa Rady Ministrów w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego z dnia 25 sierpnia 2005 r. (Dz. U. Nr 171 poz. 1433);
- rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. (Dz. U z 2004 roku Nr 100 poz. 1024).

Dokument „Polityka bezpieczeństwa" został zatwierdzony przez kierownictwo, wprowadzony zarządzeniem Starosty oraz udostępniony pracownikom.

Rozdział I

Zasady postępowania przy przetwarzaniu danych osobowych.

1. Administratorem Danych Osobowych jest Starosta zwany dalej **ADO**.

2. Do głównych zadań ADO należy:

- zapewnienie aby dane osobowe były wykorzystywane zgodnie z prawem, były zbierane do jasno określonych, zgodnych z prawem celów i nie były wykorzystywane do innych celów niż te dla których zostały zebrane (zasada celowości);
- zastosowanie środków technicznych i organizacyjnych odpowiednich do zagrożeń oraz kategorii danych objętych ochroną;
- zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem niezgodnie z ustawą oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;
- prowadzenie dokumentacji opisującej sposób przetwarzania danych oraz podjęte środki organizacyjne i techniczne – na dokumentację składa się „Polityka bezpieczeństwa";
- wyznaczenie Administratora Bezpieczeństwa Informacji, tj. osoby odpowiedzialnej za nadzór nad procesem przetwarzania zwanej dalej **ABI**;
- nadanie upoważnień osobom mającym dostęp do danych osobowych;
- zapewnienie kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane. Sposób sprawowania takiej kontroli określa ADO, uwzględniając przede wszystkim podjęte środki organizacyjne i techniczne;
- zgłoszenie do rejestracji w Głównym Inspektoracie Ochrony Danych Osobowych, zbiorów danych przed przystąpieniem do ich przetwarzania, prowadzenia ewidencji osób zatrudnionych przy przetwarzaniu danych.

3. Do głównych zadań ABI należy:

- nadzór nad przestrzeganiem zasad ochrony danych, określonych przez ADO, poprzez zastosowanie odpowiednich do zagrożeń i kategorii danych objętych ochroną środków technicznych i organizacyjnych, które mają zabezpieczyć dane przed ich udostępnieniem

osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;

- tworzenie, modyfikacja i nadzór nad wdrażaniem procedur związanych z realizacją Instrukcji Zarządzania Systemami Informatycznymi;
- podejmowanie stosownych działań zgodnie z „Polityką bezpieczeństwa" w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych znajdujących się w systemie informatycznym, oraz informowanie ADO o przypadkach naruszenia przepisów ustawy o ochronie danych osobowych;
- przeprowadzanie regularnych kontroli raz na 3 miesiące funkcjonowania zabezpieczeń systemu ochrony danych osobowych;
- opracowywanie rocznych planów kontroli stanu bezpieczeństwa danych osobowych;
- prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych, **załącznik nr 1** do niniejszego dokumentu;
- zgłaszanie do rejestracji zbiorów danych osobowych GIODO.

4. Do głównych zadań ASI należy:

- wdrażanie procedur związanych z realizacją Instrukcji Zarządzania Systemami Informatycznymi oraz nadzór nad jej przestrzeganiem;
- podejmowanie odpowiednich działań w celu właściwego zabezpieczenia danych gromadzonych w systemach informatycznych;
- przeciwdziałanie dostępowi osób niepowołanych do systemu, w których przetwarzane są dane osobowe;
- nadzór nad wykorzystywanym w Starostwie Powiatowym w Otwocku oprogramowaniem oraz sprawdzeniem go pod kątem jego legalności;
- aktualizowanie oprogramowania antywirusowego i innego używanego w urzędzie;
- nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych zawierających dane osobowe;
- definiowanie użytkowników i haseł dostępu;
- wykonywanie kopii zapasowych, ich przechowywanie oraz okresowe sprawdzanie pod katem ich dalszej przydatności;
- prowadzenie ewidencji sprzętu komputerowego i oprogramowania używanego na terenie urzędu;

- przeprowadzanie bieżącej kontroli oraz dokonywanie ocen stanu bezpieczeństwa systemu informatycznego;

5. Administrator Danych Osobowych sam może pełnić funkcję Administratora Bezpieczeństwa Informacji.

6. Kierownicy komórek organizacyjnych Starostwa są zobowiązani do:

- współdziałania z ABI w zakresie przestrzegania instrukcji stanowiącej załącznik nr 2 do zarządzenia;
- opracowania dla każdej osoby zatrudnionej przy przetwarzaniu danych osobowych zakresu czynności z uwzględnieniem stopnia dostępu do danych osobowych oraz przewidzenia odpowiedzialności, za naruszenie tajemnicy danych, adekwatnej do zakresu obowiązków;
- sprawowania nadzoru nad pracą podległych pracowników w zakresie wykonywania czynności służbowych w sposób zapewniający ochronę danych osobowych;
- zwracania się do ADO o rozstrzygnięcie w przypadku istotnych wątpliwości co do stosowania - przepisów prawnych zakresu danych osobowych;
- niezwłocznego zawiadomienia ADO o konieczności utworzenia nowego zbioru danych osobowych, wymagającego rejestracji.

7. Pracownik upoważniony przez ADO do przetwarzania danych osobowych, jest zobowiązany do:

- zapoznania się z przepisami prawa w zakresie ochrony danych osobowych;
- stosowania określonych przez ADO procedur i środków mających na celu zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym,
- zachowania szczególnej staranności w trakcie wykonywania operacji przetwarzania danych w celu ochrony interesów osób, których te dane dotyczą,
- podporządkowania się poleceniom ABI oraz właściwego kierownika, w zakresie ochrony danych.

8. Czynności przetwarzania danych osobowych może dokonywać jedynie pracownik upoważniony przez ADO. Wzór upoważnienia stanowi **załącznik nr 2** do niniejszego dokumentu.

9. Bezpośredni nadzór nad przetwarzaniem danych osobowych w komórkach organizacyjnych Starostwa sprawują kierownicy tych komórek, a w przypadku pracowników na samodzielnych stanowiskach Starosta, Wicestarosta, Sekretarz – każdy w swoim pionie.

10. Pracownik, któremu administrator danych osobowych udzielił upoważnienia jest zobowiązany do podpisania oświadczenia. Wzór oświadczenia stanowi **załącznik nr 3** do niniejszego dokumentu.

11. W przypadku zatrudnienia nowego pracownika, zmiany stanowiska, zmiany zakresu obowiązków pracowniczych, utworzenia nowego zbioru danych osobowych, zmiany sposobu przetwarzania danych lub w innych przypadkach, które wpływają bezpośrednio na rodzaj i zakres przetwarzania danych, kierownik jest zobowiązany bezzwłocznie skierować wniosek do ADO o wydanie lub cofnięcie upoważnienia. W przypadku samodzielnych stanowisk pracy cofnięcia lub wydania upoważnienia dokonuje ADO. Wzór pisma o cofnięciu upoważnienia stanowi **załącznik nr 4** do niniejszego dokumentu.

12. Wypowiedzenie umowy o pracę jest równoznaczne z cofnięciem upoważnienia do przetwarzania danych osobowych.

13. Kierownik Referatu Kadr zobowiązany jest do przekazania pisemnej informacji o wygaśnięciu umowy do ABI.

14. W obiegu wewnętrznym między Wydziałami, referatami, a także pracownikami Starostwa wprowadza się następujące zasady udostępniania danych osobowych:

- informacje zawierające dane powszechnie dostępne może udostępnić pracownik przetwarzający dane w formie bezpośredniej lub telefonicznej,
- zgodę na udostępnienie danych osobowych w szerszym zakresie wyraża Starosta.

14. W obiegu zewnętrznym zgodę na udostępnienie danych osobowych wyraża ADO zgodnie z powszechnie obowiązującymi przepisami.

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

16. ADO może przenieść obowiązek utrzymywania lub przetwarzania zbioru/zbiorów danych osobowych, na podmiot trzeci jednak musi się to odbyć za pośrednictwem stosownej umowy oraz z zachowaniem reguł bezpieczeństwa danych opisanych w niniejszym dokumencie.

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

Rozdział II

Opis zdarzeń naruszających ochronę danych osobowych.

1. Podział zagrożeń naruszających ochronę danych osobowych:

- zagrożenia losowe zewnętrzne (klęski żywiołowe, przerwy w zasilaniu) – ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, ciągłość systemu zostaje naruszona, nie dochodzi do naruszenia poufności danych;
- zagrożenia losowe wewnętrzne (pomyłki użytkowników, administratora, awarie sprzętowe, błędy oprogramowania) – może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych;
- zagrożenia zamierzone, świadome i celowe – najpoważniejsze zagrożenia, naruszenie poufności danych, wśród tych zagrożeń możemy wyróżnić 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. Za naruszenie ochrony systemu informatycznego, w którym przechowywane są dane osobowe uważa się:

- naruszenie lub próby naruszenia integralności systemu oraz zbioru danych;
- nieuprawniony dostęp lub próbę zniszczenia danych zgromadzonych w systemie;
- zmianę lub utratę danych zapisanych na kopiach zapasowych lub archiwalnych dokonaną w sposób nieautoryzowany;
- nieuprawniony dostęp (sygnał o nielegalnym logowaniu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu);
- inny stan systemu pomieszczeń niż pozostawiony przez użytkownika po zakończeniu lub po przerwie w pracy z systemem;
- nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu (pożar, zalanie pomieszczeń, niepożądana ingerencja ekipy remontowej itp.);
- niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura;

- awarię sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych, a także niewłaściwe działanie serwisu;
- stwierdzoną próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia;
- ujawnienie osobom nieupoważnionym danych osobowych lub objętych tajemnicą procedur ochrony przetwarzania albo innych strzeżonych elementów systemu zabezpieczeń np. login użytkownika i jego hasło;
- podmianę, lub zniszczenie nośników z danymi osobowymi bez odpowiedniego upoważnienia lub w inny sposób niedozwolony skasowanie lub skopiowanie danych osobowych;
- 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, prace na danych osobowych w celach prywatnych, itp.);
- stwierdzenie nieprawidłowości w zakresie bezpieczeństwa miejsc przechowywania danych osobowych (otwarte biurka, szafy, urządzenia archiwalne i inne.).

Rozdział III

Zabezpieczenie przed naruszeniem systemu ochrony danych osobowych.

1. W celu uniemożliwienia osobom trzecim dostępu do zbioru danych osobowych Starostwa Powiatowego w Otwocku należy dokonać identyfikacji możliwych zagrożeń (w rozdziale II) oraz podejmować stosowne przedsięwzięcia techniczne jak i organizacyjne, których celem jest zapewnienie odpowiednich standardów zabezpieczeń systemu ochrony danych osobowych przed jego naruszeniem.

2. Do zastosowanych środków technicznych należy:

- zabezpieczenie wejścia do budynku stanowiącego siedzibę ADO;
- wydzielenie oraz zabezpieczenie wejścia do pomieszczeń, w których przetwarzane są dane osobowe;
- szczególne zabezpieczenie centrum przetwarzania danych (serwerownia);
- wyposażenie pomieszczeń w szafy dające gwarancję bezpieczeństwa przechowywanej dokumentacji.

3. Do zastosowanych środków organizacyjnych należą:

- zapoznanie przez ABI każdej osoby dopuszczonej do pracy przy przetwarzaniu danych osobowych z przepisami dotyczącymi ochrony danych osobowych;
- przeszkolenie przez ABI bądź ASI osób w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochrona danych osobowych;
- otwieranie pomieszczeń przez osobę, która rozpoczyna pracę jako pierwsza oraz zamykanie przez osobę, która ostatnia opuszcza pomieszczenia podlega na wpisaniu do rejestru. W rejestrze odnotowuje się datę, godzinę oraz nazwisko osoby i potwierdza podpisem.

4. Niezależnie od niniejszych zasad opisanych w dokumencie „Polityka bezpieczeństwa" 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.

5. Wykaz pomieszczeń w których przetwarzane są dane osobowe stanowi **załącznik nr 5** do niniejszego dokumentu.

6. Wykaz zbiorów przetwarzanych elektronicznie lub w inny sposób stanowi **załącznik nr 6** do niniejszego dokumentu.

7. Opis struktury zbiorów danych osobowych:

Zgodnie z § 4 pkt 3 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 Kwietnia 2004 r. (Dz. U. z 2004 roku Nr 100 poz. 1024), dla każdego zidentyfikowanego zbioru danych powinien być wskazany opis struktury zbioru i zakres informacji gromadzonych w danym zbiorze. Opisy poszczególnych pól informacyjnych w strukturze zbioru danych powinny jednoznacznie wskazywać jakie kategorie danych są w nich przechowywane.

W wyżej wymienionym paragrafie wyraźnie wskazano, że w polityce bezpieczeństwa ma być zawarty **opis struktury zbiorów danych** wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi.

Opis struktury zbioru danych powinien znajdować się w dokumentacji technicznej eksploatowanych systemów (Płatnik, system Cepik, systemy geodezyjne EWMAPA i EWOPIS, Elektroniczny Obieg Dokumentów). Dokumentacja może być opracowana w formie elektronicznej lub papierowej.

8. Sposób przepływu danych pomiędzy systemami:

W Starostwie Powiatowym w Otwocku nie istnieją żadne relacje pomiędzy odrębnymi systemami informatycznymi.

W przypadku zmian tych relacji należy przedstawić w tym załączniku sposób współpracy pomiędzy różnymi systemami informatycznymi oraz relacje, jakie istnieją pomiędzy danymi zgromadzonymi w zbiorach do przetwarzania, których systemy te są wykorzystywane. Przedstawiając przepływ danych można posłużyć schematami, które

wskazują, z jakimi zbiorami dany system lub moduł systemu współpracuje, czy przepływ informacji pomiędzy zbiorem danych a systemem informatycznym jest jednokierunkowy, np. informacje pobierane są tylko do odczytu, czy dwukierunkowy (do odczytu i do zapisu). W sposobie przepływu danych pomiędzy poszczególnymi systemami należy zamieścić również informacje o danych, które przenoszone są pomiędzy systemami w sposób manualny (przy wykorzystaniu zewnętrznych nośników danych), lub półautomatycznie – za pomocą teletransmisji (przy wykorzystaniu specjalnych funkcji eksportu/importu danych), wykonywanych w określonych odstępach czasu.

9. Opis rejestracji baz danych:

W przypadku konieczności przetwarzania danych w nowej bazie danych, wymagana jest konsultacja z Administratorem Bezpieczeństwa Informacji (ABI). W przypadku konieczności rejestracji bazy danych w Generalnym Inspektoracie Danych Osobowych, rejestracja następuje na wniosek danego Wydziału.

Każdy wydział powinien prowadzić dokumentację opisującą bazy danych osobowych przetwarzanych w wydziale. Dokumentacja winna zawierać:

a. nazwę bazy,
b. imię i nazwisko osoby tworzącej,
c. datę utworzenia,
d. ewentualną datę zakończenia przetwarzania danych,
e. podstawę prawną przetwarzania,
f. cel przetwarzania,
g. listę osób przetwarzających dane,
h. zakres danych osobowych zawartych w bazie,
i. przewidywany czas użytkowania bazy (stały, okresowy, jednorazowy),
j. informacje o ewentualnym przekazywaniu danych (komu, kiedy, w jakim celu, podstawa prawna, jaki zakres przekazania danych),
k. dodatkowe ważne informacje (zmiany osób uprawnionych itp.).

10. Opis zabezpieczeń systemów informatycznych zawarty jest w **„Instrukcji określającej sposób zarządzania systemem informatycznym, służącym do przetwarzania danych**

osobowych w Starostwie Powiatowym w Otwocku" wprowadzonej tym samym zarządzeniem Starosty co Polityka Bezpieczeństwa.

Rozdział IV

Kontrola przestrzegania zasad zabezpieczania systemu ochrony danych osobowych.

1. ADO lub osoba przez niego wyznaczona, którą jest ABI sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych, określonych w ustawie o ochronie danych osobowych oraz wynikających z „Polityki bezpieczeństwa".

2. ABI sporządza roczne plany kontroli zatwierdzone przez Starostę i zgodnie z nimi przeprowadza kontrole oraz dokonuje kwartalnych ocen stanu bezpieczeństwa danych osobowych.

3. Na podstawie zgromadzonych materiałów ABI sporządza roczne sprawozdanie i przedstawia ADO (Staroście).

Rozdział V

Środki techniczne i organizacyjne

Opis środków technicznych, organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych.

1. Środki organizacyjne:

- dostęp do danych osobowych mogą mieć tylko i wyłącznie pracownicy posiadający pisemne, imienne upoważnienia podpisane przez ADO;
- każdy z pracowników powinien zachować szczególną ostrożność przy przetwarzaniu, przenoszeniu wszelkich danych osobowych;
- należy chronić dane przed wszelkim dostępem do nich osób nieupoważnionych;
- pomieszczenia, w których są przetwarzane dane osobowe, muszą być zamykane na klucz;
- dostęp do kluczy powinni posiadać tylko upoważnieni pracownicy;
- dostęp do pomieszczeń możliwy jest tylko i wyłącznie w godzinach pracy urzędu. W wypadku, gdy jest wymagany poza godzinami pracy - możliwy jest tylko na podstawie pisemnego zezwolenia ADO;
- dostęp do pomieszczeń, w których są przetwarzane dane osobowe mogą mieć tylko upoważnieni pracownicy urzędu;
- w przypadku pomieszczeń do których dostęp mają również osoby nieupoważnione, mogą przebywać w tych pomieszczeniach tylko w obecności osób upoważnionych, i tylko w czasie wymaganym na wykonanie niezbędnych czynności;
- szafy w których przechowywane są dane osobowe muszą być zamykane na klucz;
- klucze do tych szaf powinni posiadać tylko upoważnieni pracownicy;
- szafy z danymi powinny być otwarte tylko na czas potrzebny na dostęp do danych a następnie powinny być zamykane;
- dane osobowe w formie papierowej mogą znajdować się na biurkach tylko na czas niezbędny na dokonanie czynności służbowych a następnie muszą być chowane do szaf.

2. Środki techniczne

- dostęp do komputerów na których są przetwarzane dane osobowe mogą mieć tylko upoważnieni pracownicy urzędu;
- stacje komputerowe na których przetwarzane są dane osobowe powinny mieć tak ustawione monitory, aby nie miały wglądu w dane osoby nieupoważnione;
- w przypadku przetwarzania danych osobowych na komputerach przenośnych (notebook) należy zachować szczególną ostrożność przy ich przewożeniu;
- po zakończeniu pracy komputery (notebook) takie powinny być zabezpieczone w zamykanych na klucz szafach;
- komputerów tych nie należy wynosić poza budynek;
- w wypadku potrzeby wyniesienia (notebook-a) wcześniej należy dane osobowe przenieść na komputer stacjonarny w miejscu pracy;
- nie należy udostępniać osobom nieupoważnionym tych komputerów;
- w przypadku potrzeby przeniesienia danych osobowych pomiędzy komputerami należy dokonać tego z zachowaniem szczególnej ostrożności i za zgodą ABI;
- nośniki użyte do tego należy wyczyścić (skasować nieodwracalnie), aby nie zostały na nich dane osobowe;
- w wypadku niemożliwości skasowania danych z nośnika (płyta CD-ROM) należy taką płytę zniszczyć fizycznie;
- w przypadku wykorzystania do przenoszenia dysków, dane należy kasować z tych dysków;
- niezabezpieczonych danych osobowych nie należy przesyłać drogą elektroniczną;
- sieć komputerowa powinna być zabezpieczona przed wszelkim dostępem z zewnątrz;
- do zabezpieczenia sieci należy stosować:
    a) firewall;
    b) systemy wykrywania włamań IDS;
    c) logowanie wszelkich zdarzeń w dziennikach systemowych na serwerach;
    d) systemy antywirusowe;
    e) zabezpieczenia skrzynek poczty elektronicznej hasłami "trudnymi" (8 znaków w tym litery, cyfry, znaki dodatkowe);
    f) zabezpieczenie przed dostępem na zewnątrz ze stacji roboczych do innych usług niż WWW;

g) dostęp do poczty elektronicznej tylko na serwerach autoryzowanych przez Starostwo;
h) zabezpieczenia stacji roboczych poprzez hasła na BIOS, w systemach MS Windows 2000, i XP poprzez użytkowników i hasła;
i) zabezpieczenie wszelkich systemów teleinformatycznych hasłami (8 znaków w tym litery, cyfry, znaki dodatkowe) zmienianymi raz na miesiąc;
j) ustawienie odpowiednich poziomów dostępu dla odpowiednich użytkowników w systemach teleinformatycznych.

Rozdział VI

Postępowanie w przypadku naruszenia zabezpieczenia systemu ochrony danych osobowych.

1. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenie systemu ochrony danych osobowych użytkownik, oraz pozostali pracownicy zobowiązani są do natychmiastowego powiadomienia o tym fakcie ABI.

2. O naruszeniu ochrony danych osobowych może świadczyć:

- brak możliwości uruchomienia przez użytkownika aplikacji pozwalającej na dostęp do danych osobowych;
- brak możliwości zalogowania się do aplikacji;
- ograniczone, w stosunku do normalnej sytuacji, uprawnienia użytkownika aplikacji lub uprawnienia poszerzone w stosunku do normalnej sytuacji;
- wygląd aplikacji inny niż normalnie;
- inny zakres danych niż normalnie dostępny dla użytkownika – więcej lub mniej danych;
- pojawienie się nic standardowych komunikatów generowanych przez system informatyczny;
- ślady włamania lub prób włamania do obszaru, w którym przetwarzane są dane osobowe;
- 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;
- włamanie lub próby włamania do szafek, w których przechowywane są w postaci elektronicznej lub papierowej – nośniki danych osobowych;
- zgubienie lub kradzież nośnika danych osobowych;
- zagubienie lub kradzież nośnika materiału krypotograficznego (karty mikroprocesorowej, dyskietki itp);
- kradzież sprzętu informatycznego, w którym przechowywane były dane osobowe;
- informacja z systemu antywirusowego o zainfekowaniu systemu informatycznego wirusami;
- fizyczne zniszczenie lub podejrzenie zniszczenia elementów systemu informatycznego

przetwarzającego dane osobowe na skutek przypadkowych lub celowych działań albo zaistnienia siły wyższej;

- podejrzenie nieautoryzowanej modyfikacji danych osobowych przetwarzanych w systemie informatycznym.

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

4. W stosunku do danych, które zostały zagubione, pozostawione bez nadzoru poza obszarem bezpieczeństwa należy przeprowadzić postępowanie wyjaśniające, czy dane osobowe należy uznać za ujawnione.

5. 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 ABI lub osoby przez niego upoważnionej .

6. Każda osoba zatrudniona w Starostwie, która stwierdzi lub podejrzewa naruszenie zabezpieczenia ochrony danych osobowych powinna niezwłocznie poinformować o tym osobę zatrudnioną przy przetwarzaniu danych osobowych, ABI bądź osobę przez niego upoważnioną.

7. W przypadku niemożliwości zawiadomienia ABI lub osoby przez niego upoważnionej, pracownik winien powiadomić bezpośredniego przełożonego.

8. Informacja o pojawieniu się zagrożenia lub wystąpieniu zagrożenia danych osobowych przekazywana jest przez pracownika osobiście, telefonicznie lub pocztą elektroniczną.

9. W przypadku gdy zgłoszenie o podejrzeniu zaistnienia incydentu otrzyma osoba inna niż Administrator Bezpieczeństwa Informacji, jest ona obowiązana poinformować o tym fakcie Administratora Bezpieczeństwa Informacji.

10. Pracownik może zostać poproszony przez ABI o potwierdzenie zauważonego faktu na piśmie.

11. Do czasu przybycia ABI lub upoważnionej przez niego osoby, zgłaszający:

- zabezpiecza dostęp do miejsca lub urządzenia przez osoby trzecie;
- wstrzymuje pracę na komputerze na którym zaistniało naruszenie ochrony danych osobowych;
- podejmuje, stosownie do zaistniałej sytuacji, inne niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych lub informacji.

12. Dokonywanie zmian w miejscu naruszenia ochrony jest dopuszczalne jeżeli zachodzi konieczność ratowania osób lub mienia albo zapobieżenia grożącemu niebezpieczeństwu.

13. ABI po przybyciu na miejsce, w którym doszło do naruszenia ochrony danych osobowych:

- ocenia zaistniałą sytuację biorąc pod uwagę w szczególności stan pomieszczeń, w których przetwarzane są dane, stan urządzeń i zbioru danych oraz identyfikuje wielkości negatywnych następstw naruszania ochrony danych osobowych;
- wysłuchuje relacji osoby zatrudnionej przy przetwarzaniu danych, która dokonała powiadomienia;
- zapisuje wszelkie informacje związane z danym zdarzeniem;
- dokonuje fizycznego odłączenia urządzeń i segmentów sieci, które mogły umożliwić dostęp do bazy danych osobie nie uprawnionej;
- wylogowuje użytkownika podejrzanego o naruszenie zabezpieczenia ochrony danych.
- dokonuje zmiany hasła użytkownika, poprzez które uzyskano nielegalny dostęp w celu uniknięcia ponownej próby włamania;
- w uzasadnionych przypadkach powiadamia o naruszeniu ochrony danych osobowych Starostę;
- jeżeli zachodzi taka potrzeba, nawiązuje bezpośredni kontakt ze specjalistami spoza Starostwa;
- zamyka i opieczętowuje urządzenia, w których przechowywane są dane osobowe w

formie analogowej.

14. Po zapoznaniu się z zaistniałą sytuacją ABI jest zobowiązany do podjęcia kroków w celu:

- wyjaśnienia zdarzenia - w szczególności czy miało miejsce naruszenie ochrony danych osobowych;
- wyjaśnienia przyczyn naruszenia bezpieczeństwa danych osobowych i zebranie ewentualnych dowodów - w szczególności, gdy zdarzenie było związane z celowym działaniem pracowników bądź osób trzecich;
- zabezpieczenia systemu informatycznego przed dalszym rozprzestrzenianiem się zagrożenia;
- usunięcie skutków incydentu i przywrócenie pierwotnego stanu systemu informatycznego;
- ewentualnego ukarania sprawców incydentu.

15. Działania podejmowane przez ABI związane z usunięciem skutków incydentu i przywróceniem prawidłowego przebiegu procesu przetwarzania danych osobowych mogą obejmować:

- przeprowadzenie naprawy sprzętu informatycznego;
- wprowadzenie poprawek do oprogramowania;
- odtworzenie danych z kopii awaryjnych;
- modyfikację danych w celu odtworzenia ich integralności;
- inne naprawy urządzeń wchodzących w skład infrastruktury informatycznej wspomagających lub zabezpieczających działanie systemu informatycznego.

16. ABI może odstąpić od usuwania skutków incydentu, jeżeli został on spowodowany działaniem celowym, a całkowite wyjaśnienie zdarzenia i wyciągnięcie konsekwencji wobec sprawców jest istotniejsze niż przerwa w działaniu systemu. Istniejący stan systemu informatycznego pozostaje bez zmian w celach dowodowych do czasu wyjaśnienia sprawy.

17. ABI określa, na podstawie przeprowadzonych wyjaśnień, przyczyny naruszenia danych osobowych.

18. Jeżeli naruszenie było spowodowane celowym działaniem, ABI jest zobowiązany do pisemnego powiadomienia ADO – Starosty.

19. Administrator Danych Osobowych, biorąc pod uwagę charakter zdarzenia, może poinformować organy uprawnione do ścigania przestępstw o fakcie celowego naruszenia bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym.

20. Zgodę na uruchomienie komputerów i innych urządzeń lub dokonanie zmian w miejscu naruszenia ochrony wyraża ABI lub osoba przez niego upoważniona.

21. ABI sporządza z przebiegu zdarzenia raport, w którym powinny znaleźć się w szczególności:

- dane personalne osoby, która stwierdziła naruszenie;
- dane personalne osoby przyjmującej zgłoszenie;
- datę i godzinę powiadomienia;
- określenie czasu i miejsca naruszenia;
- opis zgłoszonego naruszenia oraz okoliczności towarzyszące;
- przyczyny wystąpienia naruszenia;
- opis podjętych czynności i ich uzasadnienie;
- wyniki przeprowadzonego badania wyjaśniającego;
- ocenę skuteczności przeprowadzonego postępowania naprawczego;
- podjęte środki techniczne, organizacyjne i dyscyplinarne w celu zapobiegania w przyszłości naruszenia ochrony danych osobowych.

22. Kopia raportu przekazywana jest niezwłocznie Administratorowi Danych Osobowych.

23. Wzór raportu określa **załącznik nr 7** do „Polityki bezpieczeństwa".

Rozdział VII

Postanowienia końcowe.

1. Osoba zatrudniona przy przetwarzaniu danych osobowych za naruszenie obowiązków wynikających z „Polityki bezpieczeństwa" i przepisów o ochronie danych osobowych ponosi odpowiedzialność przewidzianą w Regulaminie Pracy, Kodeksie Pracy oraz wynikające z ustawy o ochronie danych osobowych (t. j. Dz. U. z 2002 roku Nr 101 poz. 926 z późn. zm.).

2. ABI 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 8** do „Polityki bezpieczeństwa".

3. 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.

4. 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 Informacji.

5. Orzeczona kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia Administratora Bezpieczeństwa Informacji nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą o ochronie danych osobowych (t. j. Dz. U. z 2002 roku Nr 101 poz. 926 z późn. zm.).

6. W sprawach nieuregulowanych niniejszym dokumentem mają zastosowanie przepisy ustawy o ochronie danych osobowych (t. j. Dz. U. z 2002 roku Nr 101 poz. 926 z późn. zm.), rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia

2004r. w sprawie dokumentacji przetwarzania danych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 roku Nr 100 poz. 1024) oraz rozporządzenie Ministra Sprawiedliwości z dnia 28 kwietnia 2004r. 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. z 2004 roku Nr 100 poz. 1023).

7. Niniejsza „Polityka bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Starostwie Powiatowym w Otwocku" wchodzi w życie z dniem jej podpisania przez Starostę.

Starosta Powiatu
mgr Helena Pękorska

Informatyk
inż. Łukasz Wróbel

Załącznik nr 1
do Polityki Bezpieczeństwa

Ewidencja osób upoważnionych do przetwarzania danych osobowych w Starostwie Powiatowym w Otwocku.

L.p.	Nazwisko i Imię	Nr upoważnienia	Komórka organizacyjna	Stanowisko	Data	
					Nadania upoważnienia	Wygaśnięcia upoważnienia

Sekretarz

mgr Helena Poko

Informatyk

inż. Łukasz Wróbel

Załącznik Nr 2
do Polityki Bezpieczeństwa

Wzór upoważnienia do przetwarzania danych osobowych

Data nadania upoważnienia .....

Upoważnienie do przetwarzania danych osobowych

Upoważniam Panią/Pana .....
(imię i nazwisko upoważnionego)
Zatrudnioną- - ego na stanowisku .....

w .....
(oznaczenie Wydziału)

do przetwarzania danych osobowych:

.....
.....
(zakres upoważnienia: wskazanie kategorii danych, które może przetwarzać określona w upoważnieniu osoba lub rodzaj czynności jakich może dokonywać na danych osobowych)

Identyfikator .....
(w systemie informatycznym)

Okres trwania upoważnienia: .....

.....
(podpis i pieczęć Administratora Danych Osobowych)

Osoba upoważniona do przetwarzania danych jest zobowiązana do:

1) Zapoznania się i wypełniania obowiązków wynikających z:
   a) przepisów ustawy o ochronie danych osobowych (t. j. Dz. U. z 2002 roku Nr 101 poz. 926 z późn. zm.) oraz przepisów wykonawczych wydanych na jej podstawie;
   b) przepisów Dyrektyw dotyczących danych osobowych, w tym Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych.
2) Zachowania w tajemnicy danych oraz informacji o ich zabezpieczeniu, również po ustaniu zatrudnienia.
3) Zapewnienia bezpieczeństwa przetwarzania danych osobowych poprzez ich ochronę przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem.

.....
(podpis osoby upoważnionej)

Sekretarz Powiatu
mgr Helena Pokorska

Informatyk
inż. Łukasz Wróbel

Załącznik Nr 3
do Polityki Bezpieczeństwa

.....
(imię i nazwisko)

.....
(Wydział)

.....
(stanowisko)

OŚWIADCZENIE

Oświadczam, że zapoznałem(łam) się z przepisami prawa dotyczącymi ochrony danych osobowych, a w szczególności z ustawą o ochronie danych osobowych (t. j. Dz. U. z 2002 roku Nr 101 poz. 926 z późn. zm.) oraz rozporządzeniem ministra spraw wewnętrznych i administracji z 29 kwietnia 2004 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemu informatyczne, służące do przetwarzania danych osobowych (Dz. U. z 2004 roku Nr 100 poz. 1024) i zobowiązuję się do ich przestrzegania.

Oświadczam ponadto, że zapoznałem(łam) się z Polityką bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Starostwie Powiatowym w Otwocku wprowadzoną zarządzeniem nr ..... Starosty Otwockiego z dnia ..... oraz Instrukcją określającą sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Starostwie Powiatowym Otwocku wprowadzoną zarządzeniem nr .....Starosty Otwockiego z dnia .....

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:

Starostwo Powiatowe w Otwocku
ul. Górna 13
05 – 400 Otwock

Otrzymałem(łam) dnia:

.....
(podpis pracownika)

....., dnia .....

Sekretarz Powiatu
mgr Helena Pokorska

Informatyk
inż. Łukasz Wróbel

Załącznik Nr 4
do Polityki Bezpieczeństwa

Wycofanie upoważnienia

Na podstawie Rozdz. I pkt. 11 „Polityki bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Starostwie Powiatowym w Otwocku wprowadzoną Zarządzeniem Starosty Otwockiego nr ..... z dnia .....

w związku z:

.....

.....

.....

.....

cofam upoważnienie

Pana/Pani.....

zatrudnionego/zatrudnionej

w.....

na stanowisku.....

do przetwarzania danych osobowych, wynikającego z zakresu obowiązków pracowniczych.

Otwock, dnia.....

Sekretarz Powiatu
mgr Helena Pokorska

Informatyk
inż. Łukasz Wróbel

Załącznik Nr 5
do Polityki Bezpieczeństwa

Wykaz pomieszczeń lub części pomieszczeń w których przetwarzane są dane osobowe.

Lp.	Nr pokoju	Wydział/Referat/Sam. Stanowisko	Określenie części pomieszczenia, w którym przetwarza się, lub archiwizuje dane
Budynek			
Budynek			

Sekretarz Powiatu
mgr Helena Pokorska

Informatyk
Łukasz Wróbel

Załącznik Nr 6
do Polityki Bezpieczeństwa

a)

Wykaz zbiorów przetwarzanych elektronicznie.

Lp.	Nazwa zbioru	Program zastosowany do przetwarzania	Pomieszczenie, w którym przetwarza się dane	Osoby przetwarzające dane

Sekretarz Powiatu
mgr Helena Pokorska

Informatyk
inż. Łukasz Wróbel

Załącznik Nr 6
do Polityki Bezpieczeństwa

b)

Wykaz zbiorów przetwarzanych w inny sposób niż elektronicznie.

Lp.	Nazwa zbioru	Wydział	Rodzaj danych	Osoby przetwarzające dane	Pomieszczenie, w który przetwarza się dane

Sekretarz Powiatu
mgr Helena Pokorska

Informatyk
inż. Łukasz Wróbel

Załącznik nr 2 do
Zarządzenia Starosty Otwockiego
nr 6/2009 z dnia 13.02.2009

Instrukcja określająca sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Starostwie Powiatowym w Otwocku.

1. Określenie sposobu przydziału haseł dla użytkowników i częstotliwość ich zmiany oraz wskazanie osoby odpowiedzialnej za te czynności.

- hasło przydziela ASI lub ABI (użytkownik o haśle poinformowany jest w sposób ustny);
- hasło nie powinno zawierać mniej niż 8 znaków;
- hasło nie może być takie samo jak identyfikator;
- hasło musi być zmieniane przynajmniej raz w miesiącu przez użytkownika, ASI, ABI lub automatycznie przez system;
- użytkownikowi nie wolno zapisywać hasła na papierze;
- użytkownik jest zobowiązany do utrzymania hasła w tajemnicy, również po utracie jego ważności;
- komputery nie pracujące w sieci muszą mieć hasło założone na BIOS;
- w przypadku czasowego opuszczenia stanowiska pracy, użytkownik powinien wylogować się z systemu, lub po 5 minutach musi uruchomić się wygaszacz ekranu zabezpieczony hasłem;
- hasło przy wpisywaniu nie może być wyświetlane na ekranie;
- hasła do komputerów użytkowników przechowywane są w sposób zaszyfrowany na serwerze w zabezpieczonym pomieszczeniu (serwerownia), do którego dostęp mają tylko ABI i ASI;
- hasła dodatkowo przechowywane są na nośniku informacji w zamkniętej kasetce metalowej do której dostęp mają tylko ASI i ABI;
- awaryjne użycie hasła do komputera użytkownika (np. podczas jego nieobecności) możliwe jest tylko za zgodą i pod nadzorem ASI bądź ABI.

2. Określenie sposobu rejestrowania i wyrejestrowania użytkowników oraz wskazanie osoby odpowiedzialnej za te czynności.

- ABI prowadzi ewidencję osób upoważnionych do przetwarzania danych,
- rejestracji użytkowników w systemie dokonuje ABI, ASI lub osoba przez nich upoważniona;
- zarejestrować można wyłącznie osoby, które ADO wpisał do ewidencji osób upoważnionych do przetwarzania danych;
- wyłączenie z ewidencji osób upoważnionych do przetwarzania danych, obliguje ABI do

odebrania dostępu do danych osobowych;

- zalecane jest aby identyfikator składał się z pierwszej litery imienia i pierwszych pięciu liter nazwiska.

3. Procedury rozpoczęcia i zakończenia pracy.

- ABI w porozumieniu z kierownikiem urzędu, ustala czas pracy użytkownikom systemu, na pracę poza godzinami funkcjonowania urzędu musi wyrazić zgodę na piśmie kierownik jednostki, w formie upoważnienia jednorazowego lub stałego;
- ASI lub osoby upoważnione, nadzorują rozpoczęcie i zakończenie pracy systemu informatycznego;
- w pomieszczeniach gdzie przyjmowani są interesanci, monitory powinny być tak ustawione, aby uniemożliwić osobie niepowołanej wgląd w dane;
- dopuszcza się pozostawianie włączonego serwera w nocy, jeżeli pomieszczenie w którym on pracuje wyposażone jest w sprawny system powiadamiania p-poż, UPS oraz alarm;
- kontrola wprowadzanych danych prowadzona jest na bieżąco na każdym stanowisku merytorycznym, nadzór prowadzi kierownik danej komórki organizacyjnej;
- o przekazywaniu danych osobowych innym podmiotom decyduje ADO.

4. Metoda i częstotliwość tworzenia kopii awaryjnych

- za sporządzanie i bezpieczeństwo kopii odpowiedzialny jest ASI, lub osoba przez niego upoważniona;
- kopii należy dokonywać poprzez przegrywanie (backup) całej bazy danych (bez kompresji);
- w każdej chwili powinno być dostępnych jednocześnie pięć kopii: z ostatniego dnia, tygodnia, miesiąca, kwartału i roku. Kopie dzienne i tygodniowe należy zapisywać na HDD a pozostałe na CD;
- kopie awaryjne może tworzyć jedynie ASI, lub osoba przez niego upoważniona;
- w czasie tworzenia kopii awaryjnej przez ASI, dostęp do bazy dla wszystkich użytkowników powinien być zablokowany;
- dyski wymienne z kopiami bezpieczeństwa powinny być wyjęte z komputera w czasie bieżącej pracy;

- ASI wykonuje backup lub archiwizacje systemu wykorzystując jak najlepiej swoje umiejętności.

5. Metody i częstotliwość sprawdzania obecności wirusów komputerowych oraz metody ich usuwania.

- za ochronę antywirusową odpowiedzialny jest ASI;
- do ochrony antywirusowej należy stosować jednostanowiskowy program antywirusowy, zainstalowany na komputerze, gdzie odbierana jest poczta elektroniczna i sprawdzane są wszystkie dyskietki i płyty CD, przed ich uruchomieniem w sieci oraz na komputerach wolno stojących;
- sprawdzanie dostępnymi programami antywirusowymi odbywać się powinno przynajmniej raz w miesiącu;
- zalecane jest wykorzystanie programów pracujących w tle;
- przy kontroli szczególną uwagę należy zwrócić na makra;
- każdą przesyłkę otrzymaną za pomocą transmisji danych (e-mail, ftp) należy sprawdzić programem antywirusowym;
- korzystanie z zewnętrznych nośników informacji (dyskietek, dysków wymiennych, płyt CD, Internetu, poczty elektronicznej) może mieć miejsce wyłącznie po uzyskaniu zgody ASI;
- w przypadku wykrycia wirusa choćby na jednym komputerze, należy sprawdzić wszystkie stacje robocze w Starostwie.

6. Sposób i czas przechowywania nośników informacji, w tym kopii informatycznych i wydruków.

- nie należy magazynować zbędnych plików i wydruków, kopie bezpieczeństwa po upływie okresu przechowywania muszą być skasowane, lub fizycznie zniszczone w sposób uniemożliwiający odczytanie danych;
- kopie bezpieczeństwa na płytach CD powinny być przechowywane w zamkniętej metalowej szafie;
- kopie na płytach CD nie powinny być przechowywane w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych eksploatowanych na bieżąco;

- kopie awaryjne sprawdza się pod kątem ich dalszej przydatności do odtworzenia danych w przypadku awarii systemu – co najmniej jednorazowo po przegraniu danych;
- wydruki należy przechowywać w pomieszczeniach, uniemożliwiających dostęp do nich przez osoby niepowołane;
- kopie przechowuje się w zamkniętej kasetce metalowej do której dostęp mają tylko ASI i ABI co najmniej:
    a) dzienne przez siedem dni;
    b) tygodniowe przez kolejny tydzień;
    c) miesięczne przez kolejny miesiąc;
    d) kwartalne przez kolejny kwartał;
    e) roczne przez cały kolejny rok od daty sporządzenia;
- osoba użytkująca przenośny komputer, służący do przetwarzania danych osobowych, obowiązana jest zachować szczególną ostrożność podczas transportu i przechowywania tego komputera, w celu zapobieżenia dostępowi do tych danych osobie niepowołanej, a w szczególności powinna zabezpieczyć dostęp do komputera hasłem i nie zezwalać na używanie komputera osobom nieupoważnionym do dostępu do danych osobowych, w szczególności komputera nie należy pozostawiać w samochodzie;

7. Niszczenie zbędnych danych osobowych i/lub ich zbiorów.

ADO realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych sprawuje kontrolę i nadzór nad niszczeniem zbędnych danych osobowych i/lub ich zbiorów. Niszczenie to powinno polegać w szczególności na:

- trwałym, fizycznym niszczeniu danych osobowych i/lub ich zbiorów wraz z ich nośnikami w stopniu uniemożliwiającym ich późniejsze odtworzenie przez osoby niepowołane przy zastosowaniu powszechnie dostępnych metod.
- anonimizacji danych osobowych i/lub ich zbiorów polegającej na pozbawieniu ich cech pozwalających na identyfikacje podmiotów, których dane dotyczą;
- osoby przetwarzające dane osobowe mają obowiązek stosowania oddanych im do dyspozycji narzędzi (niszczarki) i technik niszczenia zbędnych danych osobowych i/lub ich zbiorów;
- naruszenie przez zatrudnione, w ramach stosunku pracy, osoby upoważnione do dostępu

i/lub przetwarzania danych osobowych procedur niszczenia zbędnych danych osobowych i/lub ich zbiorów traktowane będzie, jako ciężkie naruszenie podstawowych obowiązków pracowniczych z wszystkimi wynikającymi stąd konsekwencjami, z rozwiązaniem stosunku pracy włącznie;

- kontrola i nadzór nad niszczeniem zbędnych danych osobowych i/lub ich zbiorów może w szczególności polegać na wprowadzeniu odpowiednich procedur niszczenia danych, a także zlecaniu niszczenia ich, wyspecjalizowanym podmiotom zewnętrznym, gwarantującym bezpieczeństwo procesu niszczenia danych odpowiednie do rodzaju nośnika tych danych.

8. Sposób dokonywania przeglądów i konserwacji systemu i zbioru danych osobowych.

- przeglądu i konserwacji dokonuje ASI, lub osoba przez niego upoważniona, przynajmniej dwa razy w roku;
- zasilacz UPS powinien zapewnić automatyczne zakończenie pracy i wyłączenie serwerów przy zaniku lub nadmiernym wahaniu napięcia – min. czas podtrzymania pracy wynosi 5 min;
- w przypadku przekazywania komputera z dyskiem lub innym nośnikiem danych osobowych do naprawy, należy nośnik zdemontować, zabezpieczyć dostęp hasłem lub dokonać naprawy w obecności osoby upoważnionej przez ADO, w przypadku przekazania nośnika innemu podmiotowi należy dane nieodwracalnie skasować;
- o wszelkich nieprawidłowościach, awariach, próbie lub naruszeniu bezpieczeństwa danych osobowych, użytkownik powinien niezwłocznie powiadomić ABI;
- zabronione jest dokonywanie napraw sprzętu komputerowego samodzielnie przez pracowników urzędu;
- w przypadku naprawy sprzętu komputerowego należy urządzenia, dyski lub elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do naprawy pozbawić wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie bądź też naprawiać je pod nadzorem osoby upoważnionej przez administratora danych.

9. Sposób postępowania w zakresie komunikacji w sieci komputerowej.

System informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych, lub logicznych

zabezpieczeń, chroniących przed nieuprawnionym dostępem (załącznik do Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 Kwietnia 2004 poz. 1024).

- przy przydzielaniu uprawnień obowiązuje zasada „wszystko co nie jest dozwolone, jest zabronione";
- ABI z ADO określi zasoby dostępne dla każdego użytkownika;
- dostęp do serwerowi mają tylko ABI, ASI i pracownicy przez niego upoważnieni;
- dostęp do konsoli serwera winien być zabezpieczony hasłem;
- ASI winien monitorować pracę w sieci za pomocą dostępnego oprogramowania narzędziowego i plików .log;
- w pomieszczeniu, gdzie ustawiony jest serwer powinien pracować tylko ABI, ASI lub osoby przez niego upoważnione;
- nie wolno instalować w sieci własnego oprogramowania bez zgody ASI;
- użytkownicy nie powinni mieć dostępu do zasobów systemowych serwera, katalogów roboczych, danych i wolumenów z poziomu systemu operacyjnego;
- dostęp do archiwalnych plików pocztowych należy zabezpieczyć hasłem.

Sekretarz Powiatu

mgr Helena Pokorska

Informatyk

inż. Łukasz Wróbel

Załącznik Nr 7
do Polityki Bezpieczeństwa

Wzór raportu z naruszenia ochrony danych osobowych.

Raport nr ...../.....
z naruszenia ochrony danych osobowych w Starostwie Powiatowym w Otwocku

1. Data:..... Godzina:.....
2. Osoba powiadamiająca o zaistniałym zdarzeniu:

.....

(Imię i Nazwisko, stanowisko służbowe, nazwa użytkownika jeśli występuje)

3. Osoba przyjmująca zgłoszenie o zaistniałym zdarzeniu:

.....

(Imię i Nazwisko, stanowisko służbowe, nazwa użytkownika jeśli występuje)

4. Lokalizacja zdarzenia:

.....

(nr pokoju)

5. Rodzaj naruszenia bezpieczeństwa, oraz okoliczności towarzyszące:

.....

.....

.....

6. Podjęte działania:

.....

.....

7. Przyczyny wystąpienia zdarzenia:

.....

.....

8. Postępowanie wyjaśniające:

.....

.....

9. Ocena skuteczności przeprowadzonego postępowania naprawczego:

.....

.....

10. Podjęte środki techniczne, organizacyjne i dyscyplinarne w celu zapobiegania w przyszłości podobnym naruszeniom ochrony danych osobowych:

.....

.....

.....

data, podpis Administratora Bezpieczeństwa Informacji

Sekretarz Powiatu
mgr Helena Piłaszka

Informatyk
inż. Łukasz Wróbel

Załącznik Nr 8
do Polityki Bezpieczeństwa

Ewidencja osób, które zostały zapoznane z Polityką Bezpieczeństwa i zobowiązują się do stosowania zasad w niej zawartych.

Lp.	Nazwisko i Imię	Data	Podpis

Sekretarz Powiatu
mgr Helena Pokorska

Informatyk
Wróbel
inż. Łukasz Wróbel