ZARZĄDZENIE NR 14/2012

STAROSTY RACIBORSKIEGO

z dnia 31 stycznia 2012 r.

w sprawie zasad ochrony danych osobowych przetwarzanych w Starostwie Powiatowym w Raciborzu

Działając na podstawie art. 35 ust. 2 ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (tekst jednolity: Dz. U. z 2001 r. Nr 142, poz.1592 z późn. zm.), art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.), § 3 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).

zarządzam co następuje:

§ 1. Wprowadzam do użytku służbowego w Starostwie Powiatowym w Raciborzu:

1) "Politykę bezpieczeństwa" stanowiącą załącznik nr 1 do Zarządzenia.

2) "Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych" stanowiącą załącznik nr 2 do Zarządzenia.

§ 2. Przestrzeganie zasad ochrony danych osobowych przetwarzanych w Starostwie Powiatowym w Raciborzu szczegółowo określonych w załącznikach, o których mowa w § 1 nadzoruje Administrator Bezpieczeństwa Informacji wyznaczony odrębnym zarządzeniem.

§ 3. Wykonanie niniejszego zarządzenia powierzam wszystkim pracownikom Starostwa Powiatowego w Raciborzu, a nadzór - kierownikom komórek organizacyjnych Starostwa.

§ 4. 1. Tracą moc:

1) Zarządzenie Wewnętrzne Nr 57/06 Starosty Raciborskiego z dnia 05 grudnia 2006 r. w sprawie wprowadzenia zasad ochrony danych oraz użytkowania sprzętu i oprogramowania komputerowego w Starostwie Powiatowym w Raciborzu.

2) Zarządzenie Wewnętrzne Nr 5/09 Starosty Raciborskiego z dnia 10 lutego 2009 r. dotyczące zmiany Zarządzenia Wewnętrznego Nr 57/06 Starosty Raciborskiego z dnia 05 grudnia 2006 r. w sprawie wprowadzenia zasad ochrony danych oraz użytkowania sprzętu i oprogramowania komputerowego w Starostwie Powiatowym w Raciborzu.

§ 5. Upoważnienia do przetwarzania danych osobowych i dostępu do systemów informatycznych nadane na podstawie dotychczas obowiązujących przepisów zachowują swoją moc.

§ 6. Aktualizacja załączników do dokumentów, o których mowa w § 1 pkt 1 i 2, nie powoduje konieczności zmiany niniejszego Zarządzenia.

§ 7. Zarządzenie wchodzi w życie z dniem podpisania i podlega publikacji w Bazie Rejestrów Urzędowych - Zarządzenia Starosty Raciborskiego na stronie internetowej www.bip.powiatraciborski.pl.

Starosta

Adam Hajduk

Załącznik Nr 1 do Zarządzenia Nr 14/2012

Starosty Raciborskiego

z dnia 31 stycznia 2012 r.

POLITYKA BEZPIECZEŃSTWA

§ 1. Celem Polityki Bezpieczeństwa jest wprowadzenie i przestrzeganie w Starostwie Powiatowym w Raciborzu zasad prawidłowego przetwarzania danych osobowych oraz stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych, określonych w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj: Dz. U. Nr 101, poz. 926 z 2002 r. z późn. zm.) – zwanej dalej ustawą, oraz w przepisach wykonawczych.

§ 2. Dane osobowe przetwarza się w Starostwie w celu realizacji zadań ustawowych. Przetwarzanie i ochrona danych osobowych podlega przepisom ustawy.

§ 3. Zasady bezpieczeństwa i ochrony danych osobowych przetwarzanych w Starostwie dotyczą wszystkich danych, niezależnie od formy ich przetwarzania w zbiorach danych lub poza nimi.

§ 4. Definicje

Administrator Danych	Starosta Raciborski jako organ samorządu terytorialnego decydujący o celach i środkach przetwarzania danych osobowych w Starostwie Powiatowym w Raciborzu zgodnie z art.7 ust. 4 ustawy.
Administrator Bezpieczeństwa Informacji	pracownik odpowiedzialny za nadzór nad bezpieczeństwem informacji przetwarzanych w Starostwie Powiatowym w Raciborzu wyznaczony przez Administratora Danych zgodnie z art. 36 ust. 3 ustawy.
Koordynator Bezpieczeństwa Informacji	pracownik koordynujący sprawy związane z ochroną danych osobowych w Starostwie Powiatowym w Raciborzu i sprawujący nadzór nad przestrzeganiem przepisów dotyczących ochrony danych osobowych.
Dane osobowe	wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej zgodnie z art. 6 ustawy.
Przetwarzanie danych	operacje wykonywane na danych osobowych takie jak zbieranie, przeglądanie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie zgodnie z art. 7 ust. 2 ustawy
System Informatyczny	zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych stosowanych w celu przetwarzania danych.
Administrator Systemu Informatycznego	pracownik odpowiedzialny za ciągłość pracy, bezpieczeństwo i rozwój poszczególnych systemów informatycznych zgodnie z zakresem czynności.
System Informatyczny Starostwa Powiatowego w Raciborzu	zbiór systemów informatycznych służących do przetwarzania informacji w Starostwie Powiatowym w Raciborzu.
Administrator Systemu Informatycznego Starostwa Powiatowego w Raciborzu	pracownik odpowiedzialny za ciągłość pracy, bezpieczeństwo i rozwój Systemu Informatycznego Starostwa Powiatowego w Raciborzu zgodnie z zakresem czynności
Aplikacja	program komputerowy, będący częścią systemu informatycznego oraz przetwarzający informacje.
Autoryzacja	weryfikowanie, czy dany użytkownik ma prawo dostępu do informacji, do których usiłuje uzyskać dostęp.
Identyfikator użytkownika	ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę, która jest użytkownikiem systemu informatycznego.
Incydent bezpieczeństwa	pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań i zagrażają bezpieczeństwu informacji.
Starostwo	Starostwo Powiatowe w Raciborzu.
Komórka organizacyjna	wyodrębniony element struktury Starostwa, w szczególności: wydział, referat, biuro oraz samodzielne stanowisko pracy.

Ustawa	ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz. U. Nr 101 poz. 926 z 2002 r. z późn. zm.)
Użytkownik	pracownik posiadający upoważnienie do przetwarzania danych osobowych w Starostwie
Dysponent	pracownik odpowiedzialny za przetwarzanie danych w systemie informatycznym, aplikacji lub bazie danych osobowych zgodnie z zakresem czynności.
Gospodarz	pracownik odpowiedzialny za ciągłość pracy i rozwój systemu informatycznego lub aplikacji.

§ 5. Zadania i czynności

1. Administrator Danych – realizuje zadania w zakresie ochrony danych osobowych w szczególności:

1) Podejmuje decyzje o celach i środkach przetwarzania danych osobowych z uwzględnieniem przede wszystkim zmian w obowiązujących przepisach prawa, zmian w organizacji Starostwa oraz technik zabezpieczenia danych osobowych.
2) Upoważnia poszczególnych pracowników do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym zakresowi ich obowiązków.
3) Wyznacza: Administratora Bezpieczeństwa Informacji i Koordynatora Bezpieczeństwa Informacji oraz określa zakres ich zadań i czynności.
4) Zleca Kierownikowi Referatu Organizacyjno - Administracyjnego do którego obowiązków należą sprawy związane z zaopatrzeniem, by we współpracy z Administratorem Bezpieczeństwa Informacji oraz Koordynatorem zapewnił użytkownikom odpowiednie stanowiska pracy umożliwiające bezpieczne przetwarzanie danych.
5) Zatwierdza korespondencję z Generalnym Inspektorem Ochrony Danych Osobowych w tym dotyczącą rejestracji i aktualizacji zbiorów danych osobowych.
6) Podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur bezpiecznego przetwarzania danych osobowych.

2. Administrator Bezpieczeństwa Informacji realizuje zadania w zakresie nadzoru nad wdrożeniem i stosowaniem środków fizycznych, organizacyjnych i technicznych w celu zapewnienia bezpieczeństwa danych osobowych w szczególności:

1) Wprowadza i sprawuje nadzór nad funkcjonowaniem systemu zabezpieczeń, w tym także nad przestrzeganiem prawidłowego zabezpieczenia pomieszczeń biurowych i mebli.
2) Sprawuje nadzór nad prowadzeniem ewidencji z zakresu ochrony danych osobowych.
3) Sprawuje nadzór nad powierzaniem przetwarzania danych osobowych podmiotom zewnętrznym.
4) Zatwierdza dokumenty dotyczące ochrony danych osobowych, przygotowywane przez komórki organizacyjne Starostwa w tym zwłaszcza:
   a) wnioski o udzielenie upoważnienia do przetwarzania danych osobowych
   b) wnioski o powierzenie przetwarzania danych osobowych podmiotom zewnętrznym
   c) upoważnienia do przetwarzania danych osobowych
   d) umowy powierzenia przetwarzania danych osobowych podmiotom zewnętrznym
5) Wspólnie z kierownikiem komórki organizacyjnej odpowiedzialnej za przetwarzanie danych w zbiorze danych osobowych, przygotowuje wnioski zgłoszeń rejestracyjnych i aktualizacyjnych zbiorów danych osobowych do Generalnego Inspektora Ochrony Danych Osobowych.
6) Prowadzi korespondencję z Generalnym Inspektorem Ochrony Danych Osobowych.
7) Podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia przepisów z zakresu ochrony danych osobowych.
8) W porozumieniu z Administratorem Danych oraz Koordynatorem Bezpieczeństwa Informacji na czas nieobecności (urlop, choroba) wyznacza swojego zastępcę.

9) Przeprowadza kontrolę stosowania zasad przetwarzania danych osobowych w zakresie:

a) dostępu do danych osobowych (kontrola zgodności dokumentów upoważniających do przetwarzania danych osobowych z wykonywanymi czynnościami).

b) zabezpieczenia fizycznego (serwerownie, pomieszczenia biurowe, w których przechowywane są dane osobowe, szafy i inne meble biurowe, w których przechowywane są dane osobowe, zasada "czyste biurko").

c) zabezpieczeń programowych i sprzętowych (ochrona antywirusowa, ochrona przed dostępem z sieci zewnętrznej, identyfikatory, hasła, ustawnie monitorów).

3. Koordynator Bezpieczeństwa Informacji sprawuje nadzór nad przestrzeganiem przepisów dotyczących ochrony danych osobowych w szczególności:

1) Prowadzi ewidencję osób upoważnionych i inną dokumentację z zakresu ochrony danych osobowych.

2) Prowadzi oraz aktualizuje dokumentację opisującą sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych.

3) Koordynuje wewnętrzne audyty przestrzegania przepisów o ochronie danych osobowych.

4) Przygotowuje szkolenia i materiały szkoleniowe z zakresu ochrony danych osobowych.

5) Przeprowadza szkolenie każdej osoby, która ma zostać upoważniona do przetwarzania danych osobowych.

4. Administrator Systemu Informatycznego realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym, w tym zwłaszcza:

1) Zarządza systemem informatycznym, w którym przetwarzane są dane osobowe, posługując się hasłem dostępu z pozycji administratora.

2) Na podstawie upoważnienia wydanego przez Administratora Danych przydziela każdemu użytkownikowi identyfikator oraz hasło dostępu do systemu informatycznego oraz dokonuje ewentualnych modyfikacji uprawnień, a także usuwa konta użytkowników zgodnie z zasadami określonymi w instrukcji zarządzania systemem informatycznym.

3) Przeciwdziała dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe.

4) Nadzoruje działanie mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych.

5) W sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informuje Administratora Bezpieczeństwa Informacji o naruszeniu i współdziała z nim przy usuwaniu skutków naruszenia.

6) Prowadzi szczegółowa dokumentację naruszeń bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym.

5. Administrator Systemu Informatycznego Starostwa realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad Systemem Informatycznym Starostwa , w tym zwłaszcza:

1) Zarządza Systemem Informatycznym Starostwa, posługując się hasłem dostępu do wszystkich stacji roboczych z pozycji administratora.

2) Na podstawie upoważnienia wydanego przez Administratora Danych przydziela każdemu użytkownikowi identyfikator oraz hasło dostępu do Systemu Informatycznego Starostwa oraz dokonuje ewentualnych modyfikacji uprawnień, a także dezaktywuje i usuwa konta użytkowników zgodnie z zasadami określonymi w instrukcji zarządzania systemem informatycznym.

3) Przeciwdziała dostępowi osób niepowołanych do Systemu Informatycznego Starostwa.

4) Prowadzi w systemie elektronicznym ewidencję użytkowników upoważnionych do przetwarzania danych w Systemie Informatycznym Starostwa, która powinna zawierać:

- nazwisko i imię użytkownika,
- identyfikator użytkownika,
- stanowisko użytkownika,
- komórkę organizacyjną Starostwa, w której użytkownik jest zatrudniony, odbywa staż, praktykę lub wykonuje czynności określone w innej umowie,
- wskazanie zbiorów danych osobowych, do których użytkownik ma upoważnienie i zakres uprawnień użytkownika w zakresie przetwarzania danych osobowych,
- wskazanie systemów informatycznych i aplikacji, do których użytkownik ma upoważnienie i zakres uprawnień użytkownika w tym zakresie,
- datę przyznania uprawnień,
- datę utraty ważności upoważnienia.

5) Prowadzi szczegółowa dokumentację naruszeń bezpieczeństwa Systemie Informatycznym Starostwa.

6) W sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informuje Administratora Bezpieczeństwa Informacji o naruszeniu i współdziała z nim przy usuwaniu skutków naruszenia.

7) Sprawuje nadzór nad wykonywaniem napraw, konserwacji oraz likwidacji urządzeń komputerowych, nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego.

8) Podejmuje działania służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji.

§ 6. Dostęp do danych osobowych

1. Do przetwarzania danych osobowych, dla których administratorem jest Starosta Raciborski dostęp może mieć wyłącznie osoba spełniająca następujące warunki:

1) posiada upoważnienie wydane przez Administratora Danych (Załącznik nr 1 do Polityki Bezpieczeństwa),

2) przed przystąpieniem do wykonywania czynności związanych z przetwarzaniem danych osobowych zapoznała się z obowiązującymi przepisami w zakresie ochrony danych osobowych i zobowiązała się do ich przestrzegania.

2. Upoważnienie o którym mowa w ust. 1 pkt 1 wydawane jest:

a) dla pracowników Starostwa zatrudnionych na podstawie umowy o pracę – na wniosek bezpośredniego przełożonego,

b) dla osób nie będących pracownikami Starostwa, w szczególności odbywających staż, praktykę lub wykonujących czynności określone w innej umowie – na wniosek kierownika komórki organizacyjnej Starostwa sprawującego nadzór nad realizacją powierzonych zadań.

3. Wniosek, o którym mowa w ust. 2 akceptowany jest przez kierowników komórek organizacyjnych odpowiedzialnych za przetwarzanie danych osobowych w zbiorach danych i dysponentów aplikacji służących do przetwarzania danych (Załącznik Nr 2 do Polityki Bezpieczeństwa).

4. Zobowiązanie, o którym mowa w ust. 1 pkt 2 udokumentowane jest oświadczeniem (Załącznik Nr 3 do Polityki Bezpieczeństwa) przechowywanym w aktach osobowych pracownika Starostwa lub jako załącznik do Rejestru Upoważnień – dla osób nie będących pracownikami Starostwa.

§ 7.

Zbiory danych osobowych

1. Wykaz zbiorów danych osobowych przetwarzanych w Starostwie wraz ze wskazaniem systemów informatycznych i aplikacji stosowanych do ich przetwarzania, opisem struktury i sposobem przepływu danych między systemami, znajduje się w Załączniku nr 4 do Polityki Bezpieczeństwa.

2. Wykaz systemów informatycznych i aplikacji stosowanych w Starostwie do przetwarzania danych osobowych, znajduje się w Załączniku nr 5 do Polityki Bezpieczeństwa.

3. Załączniki nr 4 i 5 do Polityki Bezpieczeństwa są aktualizowane na bieżąco przez Administratora Bezpieczeństwa Informacji.

§ 8. Rejestracja zbiorów danych osobowych

1. Kierownicy komórek organizacyjnych Starostwa zobowiązani są do niezwłocznego zgłoszenia Administratorowi Bezpieczeństwa Informacji w formie pisemnej o zamiarze utworzenia nowego zbioru danych osobowych, uzyskania dostępu do zbioru danych osobowych w skutek powierzenia przez inny podmiot, zmian informacji zawartych w zgłoszeniu zbioru danych osobowych GIODO lub wykreślenia zbioru danych osobowych zgodnie z art. 53 ustawy.

2. Administrator Bezpieczeństwa Informacji decyduje o konieczności zgłoszenia zbioru danych osobowych Generalnemu Inspektorowi Ochrony Danych Osobowych i dokonuje rejestracji na formularzu elektronicznym udostępnionym na platformie e-GIODO.

§ 9. Zasady przetwarzania danych osobowych

1. Osoba, która dokonuje operacji przetwarzania danych osobowych zobowiązana jest do ścisłego przestrzegania obowiązujących przepisów z zakresu ochrony danych osobowych, ze świadomością odpowiedzialności karnej, którą określa Rozdział 8 ustawy, a w szczególności do:

1) przetwarzania danych osobowych tylko w zakresie posiadanego upoważnienia, zgodnie z art. 49 ustawy,
2) nie udostępniania i nie umożliwiania dostępu do danych osobowych osobom nieupoważnionym, zgodnie z art. 51 ustawy,
3) prawidłowego zabezpieczania danych osobowych przed zabraniem, uszkodzeniem lub zniszczeniem, zgodnie z art. 52
4) informowania osób, których dane dotyczą o ich prawach wynikających z ustawy, zgodnie z art. 54 ustawy,
5) niezwłocznego informowania Administratora Bezpieczeństwa Informacji o wszelkich zauważonych nieprawidłowościach mających wpływ na bezpieczeństwo przetwarzania danych osobowych,
6) niezwłocznego informowania Administratora Bezpieczeństwa Informacji o zamierzonych i odbywających się czynnościach kontrolnych przeprowadzanych przez GIODO i inne upoważnione podmioty, zgodnie z art. 54a ustawy.

§ 10. Udostępnianie danych osobowych

1. Udostępnienie zbioru danych osobowych innemu podmiotowi jest dopuszczalne tylko po złożeniu pisemnego wniosku i zawarcia z nim umowy powierzenia przetwarzania danych (Załącznik Nr 6 do Polityki Bezpieczeństwa).

2. Wniosek, o którym mowa w ust. 1 powinien zawierać:

1) oznaczenie wnioskodawcy,
2) określenie celu przetwarzania powierzonych danych,
3) określenie zakresu przetwarzania powierzonych danych.

3. Podmiot, któremu przekazano dane osobowe musi zastosować odpowiednie do zagrożeń środki techniczne i organizacyjne w celu zapewnienia ochrony danych, zgodnie z art. 39-39a ustawy.

§ 11. Miejsca przetwarzania danych osobowych

1. Lokalizacja zbiorów danych osobowych przetwarzanych w Starostwie:

1) Zbiory kartotekowe (tradycyjne):

a) pomieszczenia biurowe w budynkach Starostwa Powiatowego w Raciborzu:

- Plac Okrzei 4,
- Plac Okrzei 4a,
- ul. Reymonta 8b.

2) Zbiory informatyczne lokalne:

a) serwerownia w budynku Plac Okrzei 4 - I piętro, pok.114,

b) serwerownia w budynku Plac Okrzei 4 - II piętro, pok. 212.

3) Zbiory informatyczne, dla których zawarto umowy powierzenia przetwarzania danych

a) lokalizacja określona w umowie powierzenia przetwarzania.

2. Przetwarzane danych osobowych ma miejsce wyłącznie w pomieszczeniach biurowych Starostwa i pomieszczeniach podmiotów, z którymi zawarto umowy powierzenia przetwarzania danych.

3. Przebywanie w pomieszczeniach ,o których mowa w ust.1, osób nieuprawnionych do przetwarzania danych osobowych, jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu tych danych.

4. Pomieszczenia, w których przetwarzane są dane osobowe powinny być zamykane i chronione na czas nieobecności w nich osób upoważnionych do przetwarzania danych osobowych, w sposób uniemożliwiający dostęp do nich osób trzecich.

§ 12. Zasady zabezpieczenia danych osobowych przetwarzanych w sposób tradycyjny

1. Dokumenty zawierające dane osobowe przechowywane są w pomieszczeniach biurowych, w meblach zamykanych na klucz.

1) Pomieszczenia biurowe, o których mowa w ust. 1 są:

a) przed rozpoczęciem pracy - sprawdzane, czy nie ma śladów włamania lub uszkodzenia. Takiemu samemu sprawdzeniu podlegają meble biurowe, w których przechowywane są dokumenty zawierające dane osobowe,

b) w trakcie godzin pracy - zamykane na czas nieobecności osoby zatrudnionej przy przetwarzaniu danych osobowych,

c) po zakończeniu pracy – sprawdzane, czy nie pozostały niezabezpieczone dokumenty zawierające dane osobowe oraz niezamknięte meble biurowe i szafy,

2. Osoby nieupoważnione przebywają w pomieszczeniach biurowych tylko w obecności osoby zatrudnionej przy przetwarzaniu danych.

3. Dostęp do zbioru danych osobowych posiada tylko osoba upoważniona.

4. Zasady postępowania z kluczami od pomieszczeń i mebli biurowych określają odrębne przepisy.

5. Nadzór nad prawidłowym zabezpieczeniem pomieszczeń biurowych i mebli sprawuje Kierownik Referatu Organizacyjno - Administracyjnego.

§ 13. Zasady zabezpieczenia danych przetwarzanych w systemie informatycznym

1. W Starostwie z uwagi na fakt, że urządzenia systemu teleinformatycznego służącego do przetwarzania danych osobowych połączone są z siecią publiczną, stosuje się wysoki poziom bezpieczeństwa teleinformatycznego.

2. Bezpieczeństwo teleinformatyczne na poziomie wysokim zapewnia się przez:

1) Środki prawne - spełnienie wymogów określonych w ustawie a w szczególności:

a) Został wyznaczony Administrator Bezpieczeństwa Informacji nadzorujący przestrzeganie zasad ochrony przetwarzanych danych osobowych,

b) Do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez Administratora Danych,

c) Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych,

d) Została opracowana i wdrożona polityka bezpieczeństwa,

e) Została opracowana i wdrożona instrukcja zarządzania systemem informatycznym.

2) Środki ochrony fizycznej danych:

a) Zbiory danych osobowych przechowywane są w pomieszczeniach zabezpieczonych drzwiami zwykłymi wyposażonymi w min. dwa zamki klasy B,

b) Zbiory danych osobowych przechowywane są w pomieszczeniach, w których okna zabezpieczone są za pomocą rolet antywłamaniowych,

c) Pomieszczenia, w których przechowywane są zbiory danych osobowych wyposażone są w system alarmowy przeciwwłamaniowy,

d) Dostęp do pomieszczeń, w których przetwarzane są zbiory danych osobowych objęte są systemem kontroli dostępu,

e) Dostęp do pomieszczeń, w których przetwarzane są zbiory danych osobowych jest w czasie nieobecności zatrudnionych tam pracowników nadzorowany przez służbę ochrony,

f) Zbiory danych osobowych w formie papierowej przechowywane są w zamkniętej metalowej szafie (lub w razie jej braku w zamkniętej niemetalowej szafie),

g) Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętej niemetalowej szafie – w zamkniętej kasecie posiadającej certyfikat producenta w zakresie odporności mechanicznej, wodnej i termicznej,

h) Pomieszczenia, w których przetwarzane są zbiory danych osobowych zabezpieczone są przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy,

i) Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.

3) Środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej:

a) Dostęp do zbioru danych osobowych, który przetwarzany jest na wydzielonej stacji komputerowej/ komputerze przenośnym zabezpieczony został przed nieautoryzowanym uruchomieniem za pomocą hasła BIOS,

b) Zastosowano urządzenia typu UPS, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania,

c) Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła,

d) Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem karty procesorowej oraz kodu PIN lub tokena (dla komputerów spełniających warunki techniczne),

e) Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem technologii biometrycznej (dla komputerów spełniajacych warunki techniczne),

f) Zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych,

g) Zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych,

h) Zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji,

i) Dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia,

j) Zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej.

k) Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity,

l) Do ochrony dostępu do sieci komputerowej użyto sprzętowego systemu Firewall, IPS, AVG, - z aktualnymi licencjami producenta.

4) Środki ochrony w ramach narzędzi programowych i baz danych:

a) Dostęp do Systemu Informatycznego Starostwa mają użytkownicy posiadający identyfikator i hasło dostępu nadane przez Administratora Systemu Informatycznego Starostwa na podstawie upoważnienienia wydanego przez Administratora Danych,

b) Wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych,

c) Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych,

d) Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła,

e) Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego,

f) Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do aplikacji obsługujących zbiory danych osobowych,

g) Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe,

h) Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

5)

Środki organizacyjne:

a) Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych,

b) Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego,

c) Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy,

d) Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane,

e) Kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco,

f) Użycie komputerów przenośnych służących do przetwarzania danych osobowych poza terenem Starostwa Powiatowego jest możliwe tylko po uzyskaniu zgody Administratora Danych.

§ 14. Postępowanie w sytuacji naruszenia zasad ochrony danych osobowych

1. W razie stwierdzenia przez osobę zatrudnioną przy przetwarzaniu danych naruszenia ich ochrony zobowiązana jest ona do:

1) natychmiastowego powiadomienia o zdarzeniu swojego bezpośredniego przełożonego oraz Administratora Bezpieczeństwa Informacji

2) zabezpieczenia miejsce zdarzenia,

3) fizycznego odłączenia urządzenia i segmentów sieci , które mogły umożliwić dostęp do zbiorów danych osobom nieupoważnionym.

2. W razie naruszenia ochrony zabezpieczenia danych osobowych przetwarzanych w systemie informatycznym Administrator Bezpieczeństwa Informacji zobowiązany jest do:

1) wylogowania użytkownika podejrzanego o naruszenie zabezpieczenia ochrony danych,

2) zmiany hasła na konto administratora i użytkownika poprzez które uzyskano nielegalny dostęp w celu uniknięcia ponownego włamania,

3) zapisania wszelkich informacji związanych z danym zdarzeniem a szczególnie czas uzyskania informacji o naruszeniu zabezpieczenia danych osobowych lub czas samodzielnego wykrycia tego faktu,

4) wygenerowania i wydrukowania (jeżeli zasoby systemu na to pozwalają) wszystkich możliwych dokumentów i raportów, które mogą pomóc w ustaleniu okoliczności zdarzenia. Należy opatrzyć je datą i podpisem,

5) sprawdzenia:

a) stanu urządzeń wykorzystywanych do przetwarzania danych osobowych,

b) zawartości zbioru danych,

c) sposobu działania programu,

d) jakości komunikacji w sieci telekomunikacyjnej.

6) wykluczenia możliwości obecności wirusów komputerowych,

7) przystąpienia do zidentyfikowania rodzaju zaistniałego zdarzenia, zwłaszcza do określenia skali szkód i sposobu dostępu do danych osoby niepowołanej.

3. Administrator Bezpieczeństwa Informacji sporządza protokół ze stwierdzonego naruszenia ochrony danych osobowych zawierający w szczególności:

1) rodzaj zaistniałego zdarzenia,

2) dokładny czas uzyskania informacji o naruszeniu zabezpieczenia danych osobowych,

3) określenie sposobu naruszenia zabezpieczenia ochrony danych osobowych,

4) określenie ewentualnych szkód lub zniszczeń,

5) określenie przyczyny naruszenia danych osobowych.

4. Protokół sporządza się w terminie 14 dni od daty zaistnienia zdarzenia i przekazuje Administratorowi Danych.

Załącznik Nr 1 do Zarządzenia Nr 14/2012
Starosty Raciborskiego
z dnia 31 stycznia 2012 r.
Plik dostępny w sekcji 'Załączniki'

Załacznik Nr 1 do Polityki Bezpieczeństwa

Załącznik Nr 2 do Zarządzenia Nr 14/2012
Starosty Raciborskiego
z dnia 31 stycznia 2012 r.
Plik dostępny w sekcji 'Załączniki'

Załącznik Nr 2 do Polityki Bezpieczeństwa

Załącznik Nr 3 do Zarządzenia Nr 14/2012
Starosty Raciborskiego
z dnia 31 stycznia 2012 r.
Plik dostępny w sekcji 'Załączniki'

Załącznik Nr 3 do Polityki Bezpieczeństwa

Załącznik Nr 4 do Zarządzenia Nr 14/2012
Starosty Raciborskiego
z dnia 31 stycznia 2012 r.
Plik dostępny w sekcji 'Załączniki'

Załącznik Nr 4 do Polityki Bezpieczeństwa

Załącznik Nr 5 do Zarządzenia Nr 14/2012
Starosty Raciborskiego
z dnia 31 stycznia 2012 r.
Plik dostępny w sekcji 'Załączniki'

Załącznik Nr 5 do Polityki Bezpieczeństwa

Załącznik Nr 6 do Zarządzenia Nr 14/2012
Starosty Raciborskiego

z dnia 31 stycznia 2012 r.

Plik dostępny w sekcji 'Załączniki'

Załącznik Nr 6 do Polityki Bezpieczeństwa

Załącznik Nr 2 do Zarządzenia Nr 14/2012

Starosty Raciborskiego

z dnia 31 stycznia 2012 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

§ 1. Cele

1. Instrukcja zarządzania systemem informatycznym ma na celu określenie obowiązujących w Starostwie zasad ochrony danych osobowych przetwarzanych w systemie informatycznym, w szczególności zapewnienie bezpieczeństwa ich przetwarzania.

§ 2. Identyfikacja zagrożeń w przetwarzaniu danych.

1. Bezpieczeństwo przetwarzanych danych osobowych, a szczególnie ich poufność, rozliczalność oraz integralność narażona jest przez:

1) włamanie do systemu informatycznego i pozyskanie danych przez osoby nieuprawnione,

2) pozyskanie danych przez osoby nieuprawnione na skutek bezpośredniego dostępu do komputera,

3) pozyskanie danych osobowych w trakcie przesyłania ich drogą internetową,

4) dokonywanie modyfikacji danych przez osoby nieuprawnione.

§ 3. Przydział uprawnień dostępu do systemu informatycznego.

1. Każdy użytkownik systemu informatycznego lub aplikacji posługuje się przyznanym identyfikatorem i hasłem.

1) Identyfikator wraz hasłem przyznawany jest na wniosek , o którym mowa w Załączniku nr 2 do Polityki Bezpieczeństwa,

2) Uprawnienia dostępu do systemu lub aplikacji są odbierane w chwili zwolnienia pracownika, co Administrator Bezpieczeństwa Informacji potwierdza w karcie obiegowej pracownika,

3) Uprawnienia dostępu do systemu lub aplikacji mogą być odebrane lub zablokowane także na pisemny wniosek bezpośredniego przełożonego lub przez Administratora Bezpieczeństwa Informacji w razie stwierdzenia niewłaściwego użytkowania systemu informatycznego.

2. Identyfikator :

1) jest nazwą użytkownika (jednoznacznie go identyfikuje) w systemie informatycznym,

2) składa się z unikalnego i niepowtarzalnego ciągu znaków literowo-cyfrowych,

3) nie może być zmieniony bez wiedzy użytkownika,

4) nie będzie nigdy przyznany innemu użytkownikowi.

3. Hasło:

1) powinno być znane tylko osobie, która się nim posługuje. W przypadku powstania podejrzenia o możliwości poznania hasła przez inne osoby należy je natychmiast zmienić,

2) pierwsze hasło użytkownika - po pierwszym zalogowaniu do systemu informatycznego użytkownik winien zmienić hasło wg zasad nadawania haseł w określonym systemie informatycznym,

3) musi być zmieniane przez użytkownika co miesiąc,

4. Za przydział identyfikatorów i haseł w systemie informatycznym odpowiedzialny jest Administrator Systemu.

5. Zabronione jest :

1) zapisywanie identyfikatorów i haseł w miejscach ogólnodostępnych,

2) przekazywania identyfikatorów i haseł użytkowników innym osobom,

6. Dostęp do systemu informatycznego służącego do przetwarzania danych osobowych mają wyłącznie użytkownicy Systemu Informatycznego Starostwa.

1) Za przydział identyfikatorów i hasłeł w Systemie Informatycznym Starostwa odpowiedzialny jest Administrator Systemu Informatycznego Starostwa,

2) Do identyfikatorów i haseł Systemu Informatycznego Starostwa stosuje się reguły dotyczące wszystkich systemów informatycznych,

§ 4. Zasady obowiązujące użytkownika w trakcie pracy w systemie

1. Rozpoczęcie pracy w systemie informatycznym następuje przez zalogowanie się poprzez podanie identyfikatora użytkownika i hasła dostępu lub użycie karty procesorowej i wprowadzenie kodu PIN lub tokena (w zależności od możliwości technicznych sprzętu).

2. W czasie pracy (przerw w korzystaniu z systemu) przed odejściem od komputera należy się wyrejestrować z systemu,

3. Zakończenie pracy w systemie następuje przez wydanie polecenia systemowego kończącego sesję z użytkownikiem i wyłączeniu wszystkich urządzeń,

4. Zabrania się wyłączania komputera bez poprawnego wyrejestrowania.

§ 5. Tworzenie kopii zapasowych (bezpieczeństwa) baz danych osobowych

1. Za wykonywanie kopii bezpieczeństwa baz danych osobowych odpowiedzialny jest Administrator Bezpieczeństwa Informacji.

1) Administrator Bezpieczeństwa Informacji wyznacza osoby wykonujące kopie bezpieczeństwa baz danych osobowych w systemach informatycznych (Załącznik nr 1 do Instrukcji),

2. Kopie bezpieczeństwa baz danych osobowych przetwarzanych na serwerach Starostwa Powiatowego w Raciborzu:

1) wykonywane są codziennie od poniedziałku do piątku po godzinach pracy Starostwa, na osobnych nośnikach dla każdego dnia,

2) deponowane są w oddzielnym pomieszczeniu.

3) za prawidłowe zabezpieczenie nośników odpowiada wyznaczony przez Administratora Bezpieczeństwa Informacji pracownik,

4) komplet nośników awaryjnych wymieniany jest co 12 miesięcy; uszkodzone nośniki podlegają zniszczeniu.

3. Kopie bezpieczeństwa baz danych osobowych przetwarzanych lokalnie (na komputerze użytkownika).

1) wykonywane są codziennie przez użytkownika,

2) archiwizowane na serwerze sieciowym w udostępnionym przez Administratora Systemu Informatycznego Starostwa katalogu.

3) zabranione jest wykonywanie kopii baz danych osobowych przetwarzanych lokalnie na nośnikach wymiennych.

§ 6. Sposób zabezpieczenia nośników danych.

1. Nośniki informacji muszą być:

1) składowane w zamykanych meblach biurowych,

2) zabezpieczone przed działaniem czynników zewnętrzych (ogień, woda) w specjalnej kasecie posiadajacej certyfikat producenta,

3) przed likwidacją pozbawione zapisu danych, a jeśli jest to niemożliwe nośnik należy uszkodzić w sposób uniemożliwiający odczytanie,

4) Nośniki zawierające kopie zapasowe, o których mowa w §6 ust. 2 niniejszej Instrukcji przechowywane są w Kancelarii Starostwa Powiatowego w Raciborzu,

§ 7. Wydruki komputerowe

1. Wykonywanie wydruków komputerowych zawierających dane osobowe na drukarce systemowej lub stanowiskowej odbywa się pod kontrolą osoby wykonującej wydruk.

2. Wszystkie wydruki zawierające dane osobowe przeznaczone do zniszczenia należy zniszczyć w niszczarkach dokumentów.

§ 8. Przeglądy i konserwacja sprzętu komputerowego

1. Użytkownicy systemu komputerowego zgłaszają Administratorowi Systemu Informatycznego Starostwa wszelkie awarie sprzętu komputerowego.

2. W przypadku stwierdzenia awarii sprzętu zawierającego dane osobowe:

1) naprawa i konserwacja sprzętu winna odbyć się na miejscu,

2) naprawa uszkodzenia informacji dotyczących baz danych osobowych winna odbyć się na miejscu,

3) w razie konieczności dokonania naprawy w serwisie Administrator Systemu Informatycznego Starostwa zabezpiecza dane poprzez wymontowanie nośnika danych lub nadzoruje naprawę.

§ 9. Ochrona i zasady korzystania z komputerów lokalnych użytkowników

1. Ochrona komputerów uzytkowników przed wirusami komputerowymi i innym szkodliwym oprogramowaniem:

1) Administratora Systemu Informatycznego Starostwa instaluje na każdym stanowisku komputerowym oprogramowanie przeciwdziałające wirusom komputerowym i innemu szkodliwemu oprogramowaniu,

2) użytkownik komputera kontroluje stan oprogramowania antywirusowego poprzez sprawdzenie poprawności codziennych aktualizacji,

3) zabrania się używania zewnętrzych nośników informacji nie sprawdzonych na obecność wirusów komputerowych i innego szkodliwego oprogramowania,

4) fakt znalezienia wirusa należy zgłaszać Administratorowi Systemu Informatycznego Starostwa,

5) zabrania się samodzielnego instalowania oprogramowania bez wiedzy Administratora Systemu Informatycznego Starostwa,

6) zabrania się prób nawiązywania połączeń z siecią publiczną (INTERNET) nie związanych z wykonywanymi czynnościami służbowymi,

7) zabrania się udostępniania w sieci komputerowej zasobów komputera zawierających dane osobowe,

2. Ochrona komputerów lokalnych użytkowników przed nieautoryzowanym dostępem następuje poprzez:

1) zabezpieczenie sieci teleinformatycznej Systemu Informatycznego Starostwa, w skład której wchodzą serwery baz danych, serwery aplikacji oraz stanowiska komputerowe przed nieautoryzowanym

dostępem z sieci publicznej (INTERNET) za pomocą sprzętowego systemu Firewall z aktualnymi licencjami producenta,

2) monitorowanie i rejestrację dostępu z sieci komputerowej do sieci publicznej (INTERNET) oraz rejestrację prób nieautoryzowanego dostępu z sieci INTERNET,

3) skanowanie wszystkich stanowisk komputerowych oprogramowaniem antywirusowym zarządznym i aktualizowanym przez Administratora Systemu Informatycznego Starostwa,

4) skanowanie poczty elektonicznej przez skaner antywirusowy zainstalowany na serwerze pocztowym.

3. **Instalacja oprogramowania komputerowego** .

1) Instalacji oprogramowania na stanowiskach komputerowych dokonuje się za wiedzą Administratora Systemu Informatycznego Starostwa.

2) każde oprogramowanie przed zainstalowaniem na stanowisku komputerowym podlega rejestracji przez Administratora Systemu Informatycznego Starostwa.

3) zabrania się użytkownikom stanowisk komputerowych:

a) instalowania i użytkowania nielegalnego oprogramowania,

b) przechowywania kopii nielegalnego oprogramowania,

c) instalowania oprogramowania nie przeznaczonego do wykonywania obowiązków służbowych,

d) deinstalowania zainstalowanego na stanowisku komputerowym oprogramowania,

e) przeinstalowania oprogramowania na inne stanowisko,

4. **Użytkowanie sprzętu komputerowego**

1) za każde stanowisko komputerowe znajdujące się w Starostwie odpowiedzialny jest wyznaczony przez Starostę Raciborskiego pracownik,

2) zabrania się użytkownikom stanowisk komputerowych:

a) samodzielnego instalowania lub demontowania zainstalowanego osprzętu,

b) podłączania do sieci komputerowej sprzętu komputerowego nie będącego własnością Starostwa bez zgody Administratora Systemu Informatycznego Starostwa i Administratora Bezpieczeństwa Informacji,

c) dokonywania samodzielnych napraw sprzętu,

d) dokonywania samodzielnych zmian miejsca użytkowania sprzętu,

3) wszelkie awarie sprzętu należy zgłaszać Administratorowi Systemu Informatycznego Starostwa.

5. Administrator Systemu Informatycznego Starostwa prowadzi rejestr sprzętu i oprogramowania użytkowanego w Starostwie zawierający:

- numer inwentarzowy
- imię i nazwisko użytkownika
- identyfikator użytkownika
- numer IP w sieci teleinformatycznej
- parametry techniczne sprzętu
- datę instalacji
- zainstalowane oprogramowanie na zasadach licencji OEM (przeznaczone wyłacznie do tego sprzętu)

Załącznik do Zarządzenia Nr 14/2012
Starosty Raciborskiego
z dnia 31 stycznia 2012 r.
Plik dostępny w sekcji 'Załączniki'

Załącznik Nr 1 do Instrukcji Zarządzania Systemem Informatycznym