Niniejszy załącznik uwzględnia:
- zarządzenie (pierwotne) Nr 18/04 Starosty z 28.12.2004 r.
- zarządzenie zmieniające Nr 33/09 z 10.12.2009 r.
- zarządzenie zmieniające Nr 37/10 z 23.07.2010 r.
- zarządzenie zmieniające Nr 51/2011 z 25.10.2011 r.

Załącznik Nr 1
do Zarządzenia Nr 18/04
Starosty Toruńskiego
z dnia 28 grudnia 2004r.

POLITYKA BEZPIECZEŃSTWA
przetwarzania danych osobowych w Starostwie Powiatowym w Toruniu

Spis treści:

Rozdział 1
Postanowienia ogólne

1. „Polityka bezpieczeństwa" jest to dokument regulujący sposób zarządzania, ochrony i dystrybucji danych osobowych przetwarzanych w Urzędzie i obowiązuje wszystkich pracowników.
2. Polityka bezpieczeństwa odnosi się do zabezpieczenia zarówno danych przetwarzanych tradycyjnie, zapisanych w postaci dokumentacji papierowej, jak i danych przetwarzanych w systemach informatycznych eksploatowanych w lokalnej sieci komputerowej Local Area Network (LAN).
3. Celem polityki bezpieczeństwa jest wskazanie działań, jakie należy wykonać oraz określenie zasad i reguł postępowania, które należy stosować, aby prawidłowo były realizowane obowiązki administratora danych w zakresie zabezpieczenia danych osobowych, o których mowa w § 36 ustawy.
4. W systemie informacyjnym Urzędu przetwarzane są informacje, w tym dane osobowe, służące do wykonywania zadań z zakresu administracji publicznej.

5. Określenia użyte w dokumencie oznaczają:
   1) **Urząd** - Starostwo Powiatowe w Toruniu,
   2) **Administrator Danych** - Starosta Toruński, który wyznacza Administratora Bezpieczeństwa Informacji danych osobowych zawartych w systemach informatycznych Urzędu,
   3) **Administrator Bezpieczeństwa Informacji (ABI)** - osoba wyznaczona do nadzorowania przestrzegania zasad ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych Urzędu,
   4) **użytkownik systemu** - osoba upoważniona do przetwarzania danych osobowych. Użytkownikiem może być pracownik Urzędu, osoba wykonująca pracę na podstawie umowy-zlecenia lub innej umowy cywilnoprawnej, osoba odbywająca staż lub przygotowanie zawodowe w Urzędzie,
   5) **Administrator Systemu Informatycznego (ASI)** - osoba odpowiedzialna za funkcjonowanie systemów informatycznych oraz stosowanie technicznych i organizacyjnych środków ochrony stosowanych w tych systemach,
   6) **sieć lokalna** - połączenie systemów informatycznych Urzędu dla jej własnych potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych,
   7) **sieć rozległa** - sieć publiczna w rozumieniu ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.),
   8) **ustawa** - ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.).
6. Potrzeba opracowania „Polityki bezpieczeństwa" wynika z § 3 i 4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).

Rozdział 2 [1)]
Identyfikacja zasobów systemu informatycznego

Starostwo Powiatowe w Toruniu zlokalizowane jest w budynku przy ul. Towarowej 4-6:
1) Sieć lokalna przyłączona jest do sieci rozległej poprzez łącze SDSL (6 Mbps) oraz łącze zapasowe KPSI (4 Mbps) i zabezpieczona jest firewallem sprzętowym ustawionym na styku tych dwóch sieci;
2) Wydział Komunikacji i Transportu posiada sieć wewnętrzną nie mającą dostępu do sieci rozległej. Istnieje natomiast dedykowane łącze z siedzibą PWPW realizowane za pomocą tunelu VPN.

W przypadku sieci określonej w p-cie 1 stosuje się wysoki poziom bezpieczeństwa, a sieci określonej w p-cie 2 stosuje się podwyższony poziom bezpieczeństwa.

Rozdział 3
Wykaz pomieszczeń tworzących obszar przetwarzania danych osobowych

1. Przetwarzanie danych osobowych to 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. Biorąc pod uwagę przepisy ustawy nakazujące jej stosowanie także w przypadkach przetwarzania danych poza zbiorem danych, przetwarzanie danych osobowych może wystąpić w większości pomieszczeń Urzędu. Ze względu jednak na

[1)] zm. zarządz. Nr 37/10 z dn. 23.07.2010 r.

szczególne nagromadzenie danych osobowych, szczególnie chronione powinny być pomieszczenia serwerowni, pomieszczenia, w których przechowuje się i składuje kopie zapasowe, pomieszczenia Wydziału Komunikacji i Transportu, pomieszczenia komórek finansowo-księgowych i kadrowych oraz pomieszczenia archiwum zakładowego.
2. Obszar przetwarzania danych osobowych tworzą pomieszczenia, w których wykonuje się operacje na danych osobowych (wpisuje, modyfikuje, kopiuje), jak również miejsca, gdzie przechowuje się wszelkie nośniki informacji zawierające dane osobowe (szafy z dokumentacją papierową w formie kartotek, rejestrów i innych). Do obszaru przetwarzania danych należy zaliczyć również pomieszczenia, gdzie składowane są komputerowe nośniki informacji z kopiami zapasowymi danych (taśmy, dyski, płyty CD, uszkodzone komputery), stacje komputerowe, serwery itp.
3. Wykaz pomieszczeń tworzących w Urzędzie obszar, w którym przetwarzane są dane osobowe został opisany *w załączniku Nr 1 do niniejszego dokumentu*.

Rozdział 4
Wykaz zbiorów danych osobowych, programy zastosowane do przetwarzania tych danych oraz sposób przepływu danych pomiędzy poszczególnymi systemami.

1. Wykaz zbiorów danych osobowych oraz programy zastosowane do przetwarzania tych danych stanowią *załącznik Nr 2 do niniejszego dokumentu*.
2. Szczegóły dotyczące charakterystyki technicznej i konfiguracji stosowanych narzędzi objęte są ochroną i zastrzeżone wyłącznie do użytku służbowego przez ABI.

Rozdział 5
Struktura zbiorów danych osobowych i powiązania między nimi

Opis struktur zbiorów danych osobowych oraz powiązań między nimi zawarty jest w *załączniku Nr 3 do niniejszego dokumentu.*

Rozdział 6
Środki techniczne i organizacyjne służące zapewnieniu poufności, integralności i rozliczalności przetwarzanych danych

System informatyczny Urzędu zapewnia środki bezpieczeństwa określone dla podwyższonego i wysokiego poziomu bezpieczeństwa (§ 6 ust. 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. Nr 100, poz. 1024).

A. Środki ochrony fizycznej

Gwarancją zapewnienia bezpieczeństwa systemu informatycznego Urzędu oraz przetwarzanych i przechowywanych danych jest zapewnienie bezpieczeństwa fizycznego. Warunkiem zapewnienia bezpieczeństwa fizycznego systemu jest kontrola dostępu do wszystkich stacji roboczych. W związku z tym szczególną ochroną obejmuje się pomieszczenia, w których znajdują się serwery oraz te, w których przechowywane są zapasowe dane. W/wym. pomieszczenia powinny być stale zamknięte, a dostęp do nich powinni mieć wyłącznie upoważnieni administratorzy.

Obowiązkiem osoby użytkującej komputer przenośny zawierający dane osobowe jest zachowanie szczególnej ostrożności podczas jego transportu, przechowywania i użytkowania

poza pomieszczeniami tworzącymi obszar, w którym przetwarzane są dane osobowe. Należy dążyć do powszechnego stosowania ochrony kryptograficznej w takich przypadkach.

1. Dostęp do siedziby przy ul. Towarowej 4-6 chroniony jest poprzez elektroniczny system alarmowy objęty całodobowym nadzorem specjalistycznej firmy ochroniarskiej.
2. Urządzenia służące do przetwarzania danych osobowych znajdują się w pomieszczeniach zabezpieczonych zamkami patentowymi.
3. Pomieszczenie, w którym znajdują się serwery jest zabezpieczone poprzez elektroniczny system alarmowy. W/w pomieszczenia powinny być stale zamknięte, a dostęp do nich powinny mieć tylko uprawnione osoby (ABI, ASI).
4. Kopie zapasowe z danymi zawarte na nośnikach magnetycznych i optycznych przechowywane są poza pomieszczeniami serwerowni. Dostęp do nośników mają tylko uprawnione osoby.
5. Sieć komputerowa Wydziału Komunikacji i Transportu dotycząca rejestracji pojazdów i wydawania praw jazdy jest wydzielona z sieci obsługującej pozostałą część Urzędu i objęta dodatkowymi zabezpieczeniami.
6. Fizyczny dostęp do pomieszczeń serwerowni blokują drzwi o przedłużonej odporności ogniowej oraz elektroniczny system alarmowy (antywłamaniowy). [2)]

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

1. Zastosowano niszczarki dokumentów.
2. Ochronę przed awariami zasilania oraz zakłóceniami w sieci energetycznej serwera i stacji roboczych, na których przetwarzane są dane osobowe zapewnia stosowanie zasilaczy awaryjnych UPS.
3. Zabezpieczenie na poziomie BIOS-u - uruchomienie stacji roboczych, na których przetwarzane są dane osobowe wymaga podania indywidualnego hasła użytkownika pozwalającego włączyć komputer w celu załadowania systemu operacyjnego.
4. W przypadku wejścia do sieci lokalnej, każdy z użytkowników musi podać login i hasło, które go identyfikują.
5. Każdy z serwerów plików w sieciach LAN wyposażony jest w streamer na którym codziennie wykonywane są kopie zapasowe na nośnikach taśmowych.

C. <u>Środki ochrony w ramach oprogramowania urządzeń teletransmisji</u>

1. Połączenia z sieci wewnętrznej z siecią zewnętrzną (Intranet) wykonywane są za pośrednictwem systemu firewall.

2. Komputery przenośne pracowników Urzędu podczas połączeń z siecią Internet, wykonywanych poza siecią wewnętrzną Urzędu, powinny być chronione swoimi autonomicznymi systemami firewall.

3. Zasadą konfigurowania systemów firewall powinno być blokowanie wszystkich usług, które są zbędne dla statutowej działalności Urzędu.

D. <u>Środki ochrony w ramach oprogramowania systemu</u>

1. Dostęp fizyczny do bazy danych osobowych zastrzeżony jest wyłącznie dla pracowników którzy zostali upoważnieni do obsługi danej bazy.

[2)] zm. zarządz. Nr 37/10 z dn. 23.07.2010 r.

2. Konfiguracja systemu umożliwia użytkownikom końcowym dostęp do danych osobowych jedynie za pośrednictwem aplikacji.

3. System informatyczny pozwala zdefiniować odpowiednie prawa dostępu do zasobów informatycznych systemu.

5. Zastosowano działający w „tle" program antywirusowy na komputerach użytkowników.

6. W systemie operacyjnym zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do sieci.

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

1. Automatycznie rejestrowany jest identyfikator użytkownika wprowadzającego dane oraz datę pierwszego wprowadzenia tych danych.

2. Zastosowano identyfikator i hasło dostępu do danych na poziomie aplikacji.

3. Dla każdego użytkownika systemu jest ustalony odrębny identyfikator.

4. Zdefiniowano użytkowników i ich prawa dostępu do danych osobowych na poziomie aplikacji.

F. Środki ochrony w ramach systemu użytkowego

1. Zastosowano wygaszanie ekranu w przypadku dłuższej nieaktywności użytkownika.

2. Komputer, z którego możliwy jest dostęp do danych osobowych zabezpieczony jest hasłem uruchomieniowym.

G. Środki organizacyjne

1. Wyznaczono Administratora Bezpieczeństwa Informacji (ABI). [3)]

2. Tymczasowe wydruki z danymi osobowymi po ustaniu ich przydatności są niszczone w niszczarkach.

3. Do obsługi określonego systemu informatycznego dopuszczane są osoby na podstawie indywidualnego wniosku o dostęp.

4. Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane są do zachowania ich w tajemnicy.

5. Każdy użytkownik powinien mieć świadomość zagrożeń wpływających na bezpieczeństwo systemu informatycznego, z którego korzysta. Każda osoba upoważniona do przetwarzania danych osobowych przed dopuszczeniem jej do przetwarzania tych danych powinna być przeszkolona w zakresie obwiązujących przepisów o ochronie danych osobowych, procedur przetwarzania danych oraz informowana o podstawowych zagrożeniach związanych z przetwarzaniem danych w systemie informatycznym.

[3)] zm. zarządz. Nr 33/09 z dn. 10.12.2009 r.

6. Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych.

7. Ustalono instrukcję zarządzania systemem informatycznym, która stanowi oddzielny dokument.

8. Rejestracji podlegają wszystkie przypadki awarii systemu, działania konserwacyjne w systemie oraz naprawy systemu.

9. Wszelkie naprawy i konserwacje sprzętu i oprogramowania mogą odbywać się tylko w obecności osób uprawnionych. Urządzenia informatyczne służące do przetwarzania danych osobowych, gdy zachodzi konieczność ich naprawy poza siedzibą Urzędu, można przekazać dopiero po uzyskaniu zgody ABI. W tym przypadku należy wymontować z niego nośniki informacji zawierające dane osobowe.

Rozdział 7
Przepisy końcowe

1. Nad całością polityki bezpieczeństwa danych osobowych czuwa ABI.
2. Nad przestrzeganiem bezpieczeństwa systemu informatycznego czuwa ASI.
3. Polityka Bezpieczeństwa obowiązuje wszystkich pracowników Urzędu niezależnie od tego, czy posiadają czy też nie uprawnienia do obsługi określonych aplikacji.