Załącznik nr 1
do Zarządzenia nr WO/90/09
Burmistrza Miasta Świdwin
z dnia 23 września 2009 r.

Polityka Bezpieczeństwa Urzędu Miasta Świdwin

Podstawa prawna

§ 1.

§ 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).

Postanowienia ogólne

§ 2.

1. Ilekroć mowa w niniejszym dokumencie o Polityce, należy przez to rozumieć „Politykę Bezpieczeństwa Urzędu Miasta Świdwin".
2. Ilekroć mowa w niniejszym dokumencie o Urzędzie należy przez to rozumieć Urząd Miasta Świdwin.
3. Ilekroć mowa w niniejszym dokumencie o Burmistrzu należy przez to rozumieć Burmistrza Miasta Świdwin.

§ 3.

Administratorem danych osobowych zawartych i przetwarzanych w systemach informatycznych Urzędu oraz w wersji papierowej jest Burmistrz.

§ 4.

Administrator danych osobowych jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w systemach informatycznych oraz w wersji papierowej.
W celu zrealizowania tych obowiązków administrator danych wprowadza Politykę Bezpieczeństwa jako dokument obowiązujący w Urzędzie.

Zagadnienia organizacyjne

§ 5.

1. Burmistrz wyznacza Administratora bezpieczeństwa informacji, Administratora systemu informatycznego oraz osobę upoważnioną do zastępowania Administratora bezpieczeństwa informacji.
2. Do Burmistrza należy zapewnienie odpowiednich pomieszczeń, stosownie zabezpieczonych i wyposażonych do przetwarzania i przechowywania danych osobowych, zaznajomienie pracowników z prawnymi oraz pracowniczymi konsekwencjami naruszenia bezpieczeństwa danych osobowych.
3. Pracownicy upoważnieni do przetwarzania danych osobowych w systemie informatycznym jak i w wersji papierowej, zobowiązani są do zapoznania się i przestrzegania

Polityki.

4. Osoba przetwarzająca dane osobowe składa oświadczenie o zapoznaniu się z przepisami i odpowiedzialności karnej za naruszenie ochrony danych osobowych oraz zachowaniu tajemnicy, którego wzór stanowi załącznik nr 1 do Polityki.
5. Fakt zapoznania się z Polityką pracownik potwierdza własnoręcznym podpisem na stosownym wykazie, którego wzór stanowi załącznik nr 2 do Polityki.
6. Przetwarzanie danych osobowych może odbywać się w Urzędzie tylko w godzinach pracy Urzędu, a po godzinach pracy wyłącznie za zezwoleniem Burmistrza, Z-cy Burmistrza, Sekretarza Miasta.

Wykaz zbiorów danych osobowych i pomieszczeń, w których są przetwarzane

§ 6.

Wykaz zbiorów danych osobowych zarejestrowanych przez Urząd oraz określenie pokoju w którym są one przetwarzane stanowi załącznik nr 3 do Polityki.

Sposób przepływu danych

§ 7.

1. Stacje robocze w Urzędzie połączone są w sieć logiczną za pośrednictwem sieci Ethernet .
2. W systemie informatycznym Urzędu występują 3 serwery pełniące role bazodanowe w przypadku konieczności przetwarzania większych zbiorów lub udostępnienia na więcej niż jednej stacji roboczej. Serwer znajduje się w pokoju nr 38A. Scentralizowanie położenia baz danych pozwala na lepszą kontrolę nad tworzeniem kopii zapasowych. W przypadkach gdy wymagania środowiska lub koszty uniemożliwiają umiejscowienie bazy na serwerze – system bazy danych uruchamiany jest na stacji roboczej, na której przetwarzane są dane.

Opis struktury zbiorów danych

§ 8.

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi stanowi załącznik nr 4 do Polityki w formie płyty CD-ROM.

Zabezpieczenia fizyczne

§ 9.

1. Wejścia do budynku Urzędu zabezpieczone są zamkami drzwiowymi.
2. Do budynku Urzędu dostać można się wejściami:
   - głównym, od stronyPlacu Konstytucji 3 Maja chronionym zamkiem drzwiowym,
   - tylnym od strony ul. Łącznej chronionym zamkiem drzwiowym.
2. Poszczególne pokoje, w których odbywa się przetwarzanie danych muszą być wyposażone w niezależne zamki i muszą być zamykane podczas nieobecności pracownika.
   Po zakończeniu pracy osoba zamykająca pomieszczenie powinna umieścić klucz w specjalnie przeznaczonej to tego gablocie.
3. Stanowiska komputerowe w pomieszczeniach gdzie mogą przebywać osoby

nieupoważnione do przetwarzania danych osobowych (np. interesanci albo inni pracownicy Urzędu) winny być umieszczone w sposób, który uniemożliwi takim osobom wgląd do tych danych. W pokoju, do którego dostęp mają petenci monitory komputerowe ustawione są w ten sposób, by petenci nie widzieli zapisów na ekranie.

4. W przypadku dłuższej bezczynności uruchamiane są tzw. wygaszacze ekranu lub blokowanie systemu, których dezaktywacja jest możliwa po podaniu prawidłowego hasła użytkownika.
5. Wydruki zawierające dane osobowe powinny znajdować się w miejscu, które uniemożliwia dostęp osobom postronnym.
6. Kopie bezpieczeństwa (kopie zapasowe) wykonują okresowo pracownicy w ramach swoich obowiązków. Kopie bezpieczeństwa przechowywane są w szafie metalowej pok. nr 38 Urzędu. Dostęp do nośników zawierających kopie danych mają tylko uprawnione osoby.
7. Wydruk z ważnym hasłem należy przechowywać tak, by uniemożliwić dostęp do niego osobom postronnym (innym niż sam użytkownik, przełożeni i Administratorzy).

Zabezpieczenia niefizyczne

§ 10.

1. Zalogowanie się do systemu wymaga podania nazwy użytkownika i hasła. Każdy użytkownik ma przypisane uprawnienia do wykonywania operacji. Nieudane próby logowania są rejestrowane, a po 3 nieudanych próbach logowania następuje czasowa blokada konta użytkownika na stacji roboczej.
2. Dostęp do systemu stacji roboczych chroniony jest hasłem.
3. Oprogramowanie wykorzystywane do przetwarzania danych posiada własny (dodatkowy, oprócz systemowego) system autoryzacji użytkownika.
4. W celu ochrony przed dostępem do danych komputera z sieci publicznej wykorzystuje się sprzętową zaporę ogniową (ang. firewall) zarówno w przypadku stacji roboczych jak i serwerów.
5. Zgodnie z przyjętym harmonogramem wykonuje się kopie bezpieczeństwa.

Monitorowanie zabezpieczeń

§ 11.

1. Do monitorowania systemu zabezpieczeń, stosownie do swojego zakresu czynności zobligowani są:
   1) Administrator danych
   2) Administrator bezpieczeństwa informacji
   3) Administrator systemu informatycznego
2. W ramach monitoringu należy przeprowadzać następujące działania:
   1) okresowe sprawdzanie kopii bezpieczeństwa pod względem przydatności do odtworzenia danych,
   2) sprawdzania częstotliwości zmian haseł.
3. Administrator bezpieczeństwa informacji sporządza roczną ocenę stanu bezpieczeństwa danych osobowych i przedstawia ją Administratorowi danych.

Obowiązki Administratora danych

§ 12.

1. Do obowiązków Administratora danych należy w szczególności:
   1) zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym,
   2) zapobieganie zabraniu danych przez osobę nieuprawnioną,
   3) zapobieganie przetwarzaniu danych z naruszeniem ustawy oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych,
   4) zbierane danych dla oznaczonych, zgodnych z prawem celów,
   5) dbałość o merytoryczną poprawność danych i adekwatność w stosunku do celów w jakich są przetwarzane.
   6) opracowanie instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych, przeznaczoną dla osób zatrudnionych przy przetwarzaniu tych danych,
   7) określenie budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego.
   8) opracowanie instrukcji, określającej sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji,
   9) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,
   10) organizowanie szkoleń mających na celu zaznajomienie każdej osoby przetwarzającej dane osobowe z przepisami dotyczącymi ich ochrony.
2. Administrator danych odpowiada za to by zakres czynności osoby zatrudnionej przy przetwarzania danych osobowych określał odpowiedzialność tej osoby za:
   1) ochronę danych przed niepowołanym dostępem,
   2) nieuzasadnioną modyfikację lub zniszczenie danych,
   3) nielegalne ujawnienie danych.

   w stopniu odpowiednim do zadań realizowanych w procesie przetwarzania danych osobowych.
3. Zgłasza zbiory danych osobowych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych.

Obowiązki Administratora bezpieczeństwa informacji

§ 13.

Do obowiązków Administratora bezpieczeństwa informacji należy w szczególności:
1) nadzór na przestrzeganiem instrukcji określającej sposób zarządzania systemem informatycznym,
2) przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym Przetwarzane są dane osobowe,
3) podejmowanie odpowiednich działań w celu właściwego zabezpieczenia danych,
4) badanie ewentualnych naruszeń w systemie zabezpieczeń danych osobowych,
5) podejmowanie decyzji o instalowaniu nowych urządzeń oraz oprogramowania wykorzystywanego do przetwarzania danych osobowych,
6) nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych zawierających dane osobowe.

7) przeprowadzanie symulowanych włamań do systemu w celu ustalenia aktualnego poziomu zabezpieczeń,
8) nadzór nad wykonywaniem kopii zapasowych i przechowywaniem,
9) wdrożenie szkoleń z zakresu przepisów dotyczących ochrony danych osobowych środków technicznych i organizacyjnych przy przetwarzaniu danych w systemach informatycznych,
10) sporządzanie raportów z naruszenia bezpieczeństwa systemu informatycznego.

Obowiązki Administratora systemu informatycznego

§ 14.

Do obowiązków Administratora systemu informatycznego należy w szczególności:
1) naprawa, konserwacja oraz likwidacja urządzeń komputerowych zawierających dane osobowe,
2) definiowanie użytkowników i haseł dostępu w systemie,
3) aktualizowanie oprogramowania systemowego, chyba że aktualizacje wykonywane są automatycznie,
4) aktualizowanie oprogramowania antywirusowego, chyba że aktualizacje wykonywane są automatycznie,
5) okresowe sprawdzanie kopii zapasowych pod kątem ich dalszej przydatności.

Postępowanie w przypadku naruszenia ochrony danych osobowych

§ 15.

1. Każdy pracownik Urzędu, który poweźmie wiadomość w zakresie naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane osobowe bądź posiada informację mogącą mieć wpływ na bezpieczeństwo danych osobowych jest zobowiązany fakt ten niezwłocznie zgłosić Administratorowi bezpieczeństwa informacji.
2. W razie niemożliwości zawiadomienia Administratora bezpieczeństwa lub osoby upoważnionej do zastępowania Administratora bezpieczeństwa, należy powiadomić bezpośredniego przełożonego.
3. W przypadku wykrycia naruszenia ochrony danych osobowych Administrator bezpieczeństwa informacji lub osoba upoważniona do jego zastępowania informuje Burmistrza o zaistniałym zdarzeniu oraz przeprowadza wstępne dochodzenie, po czym sporządza raport opisujący okoliczności zdarzenia, którego wzór stanowi załącznik nr 5 do Polityki. Jeśli zdarzenie ma charakter przestępstwa sprawa kierowana jest do organów ścigania.