Załącznik Nr 1 do Zarządzenia Nr 207/2015

Prezydenta Miasta Suwałk

z dnia 12 czerwca 2015 r.

POLITYKA BEZPIECZEŃSTWA URZĘDU MIEJSKIEGO W SUWAŁKACH

Realizując postanowienia ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2014 poz. 1182, poz. 1662), przepisów 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 informacyjne służące do przetwarzania danych osobowych (Dz.U. z 2004 r. Nr 100, poz. 1024), rozporządzenia Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbioru danych (Dz.U. z 2015 r. poz. 719) ustalam reguły oraz zasady pozwalające na zapewnienie ochrony danych osobowych w Urzędzie Miejskim w Suwałkach.

§ 1. 1. Celem polityki bezpieczeństwa jest takie postępowanie, aby osoby upoważnione do przetwarzania danych osobowych w pełni zabezpieczyły dostęp do nich przed osobami nieupoważnionymi i gromadziły w zbiorach dane zgodnie z wymogami ustawy.

2. Polityką bezpieczeństwa objęte są dane osobowe, którymi zgodnie z ustawą wymienioną na wstępie są wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

3. Reguły i zasady przetwarzania danych osobowych prowadzonych zarówno w wersji papierowej (kartoteki, skorowidze, księgi, wykazy i inne zbiory ewidencyjne), jak i w wersji elektronicznej (systemy informatyczne) obowiązują także w przypadku przetwarzania danych poza zbiorem danych.

4. Całokształt działań w ramach polityki bezpieczeństwa jest wymogiem ustawowym i ma za zadanie ochronę prywatności osób, których dane są przetwarzane.

5. Niniejsza polityka bezpieczeństwa zawiera w szczególności:

1) wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;

2) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;

3) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;

4) sposób przepływu danych pomiędzy poszczególnymi systemami;

5) określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych;

6) opis postępowania w przypadku zalania pomieszczeń biurowych;

7) opis postępowania z kluczami do pomieszczeń biurowych, w których przetwarzane są dane osobowe.

§ 2. Obszar, w którym przetwarzane są dane osobowe stanowią budynki przy ul. Mickiewicza 1, ul. Kościuszki 45, ul. Noniewicza 71 A i ul. Sejneńskiej 13.

§ 3. Administrator Danych Osobowych w celu nadzorowania i przestrzegania zasad ochrony danych osobowych wyznacza Administratora Bezpieczeństwa Informacji. Jednocześnie może nadać mu upoważnienie do wydawania uprawnień do przetwarzania danych osobowych.

§ 4. Administrator Bezpieczeństwa Informacji zobowiązany jest zadbać aby dane osobowe zawarte w formie papierowej nie były dostępne osobom nieupoważnionym. Dokumenty powinny znajdować się w pomieszczeniach zamykanych na klucz, do których dostęp mogą mieć tylko osoby posiadające aktualne upoważnienie do przetwarzania danych osobowych.

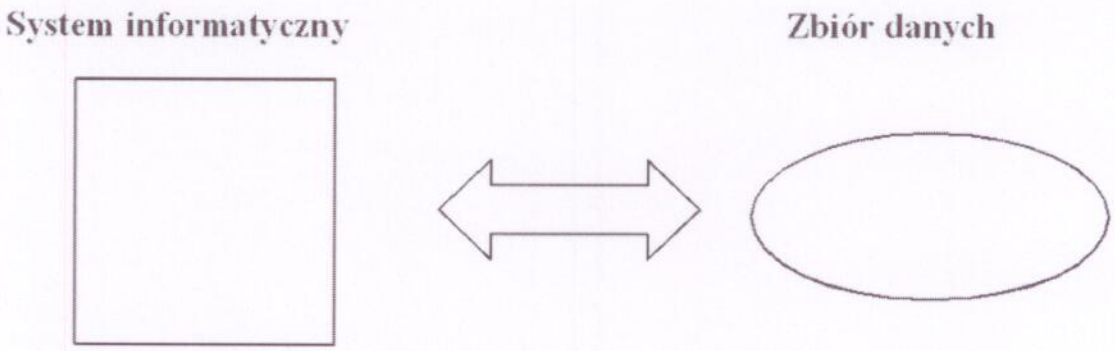
§ 5. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie do przetwarzania danych, nadane przez Administratora Danych Osobowych lub Administratora Bezpieczeństwa Informacji.

§ 6. Każdy pracownik upoważniony do przetwarzania danych osobowych powinien zastosować się do „zasady czystego biurka".

§ 7. W przypadku naruszenia zasad prawidłowego zabezpieczenia danych osobowych, każdy pracownik ma obowiązek niezwłocznego powiadomienia o incydencie ABI lub ASI. Z przeprowadzonej kontroli sporządza się protokół, w którym opisuje się stan faktyczny oraz działania i środki mające na celu zapobieżenie podobnym nieprawidłowościom ww przyszłości

§ 8. Przepływ danych pomiędzy poszczególnymi systemami odbywa się w sposób manualny (np. płyta CD, dokument papierowy) i automatyczny (sieć lokalna, Internet).

Używany model współpracy systemów informatycznych ze zbiorem danych jest następujący:



§ 9. Urząd Miejski w Suwałkach posiada następujące środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych (zabezpieczenia):

1. Budynek przy ul. Mickiewicza 1.

a) dostęp do budynku i pomieszczeń:

- kontrola dostępu do budynku i pomieszczeń, w których przetwarza się i archiwizuje dane osobowe,
- okna w pomieszczeniach parterowych posiadają szyby kuloodporne i zabezpieczenia antywłamaniowe,
- system alarmowy oraz system ostrzegania pożarowego,
- dozór całodobowy,
- wewnętrzny i zewnętrzny wizyjny monitoring całodobowy,

- elektroniczny zamek dostępu do serwerowni,

b) zasilanie systemów informatycznych:

- dedykowana sieć elektryczną,
- zastosowanie urządzeń podtrzymujących napięcie: w serwerowni centralny UPS i agregat prądotwórczy, a na stanowiskach komputerowych indywidualne UPS-y,

c) zabezpieczenie systemów informatycznych:

- dostęp do systemu jedynie przez osoby upoważnione (system identyfikatorów i haseł, elektroniczne karty dostępu),
- poziomy uprawnień,
- odpowiednia architektura systemu użytkownika (webservice, klient-serwer),
- kopie awaryjne,
- przechowywanie nośników z kopiami awaryjnymi w metalowych szafach,

2. Budynek przy ul. Kościuszki 45

a) dostęp do budynku i pomieszczeń:

- kontrola dostępu do budynku i pomieszczeń, w których przetwarza się dane osobowe,
- okna do pomieszczeń, w których przetwarza się dane osobowe, są zabezpieczone kratą,
- system alarmowy połączony z centrum monitorującym,

b) zasilania systemów informatycznych:

- zastosowanie urządzeń podtrzymujących napięcie (UPS) na stanowiskach komputerowych,

c) zabezpieczenie systemów informatycznych:

- dostęp do systemu jedynie przez osoby upoważnione (system identyfikatorów i haseł, elektroniczne karty dostępu),
- poziomy uprawnień,
- odpowiednia architektura systemu użytkownika (webservice, klient-serwer),
- kopie awaryjne,

3. Budynek przy ul. Noniewicza 71 A

a) dostępu do budynku i pomieszczeń:

- kontrola dostępu do budynku i pomieszczeń, w których przetwarza się dane osobowe,
- system alarmowy połączony z centrum monitorującym,

b) zasilania systemów informatycznych:

- zastosowanie urządzeń podtrzymujących napięcie (UPS) w serwerowni,

c) zabezpieczenie systemów informatycznych:

- dostęp do systemu jedynie przez osoby upoważnione (system identyfikatorów i haseł, elektroniczne karty dostępu),
- poziomy uprawnień,
- odpowiednia architektura systemu użytkownika (webservice, klient-serwer),
- kopie awaryjne,

4. Budynek przy ul. Sejneńskiej 13

a) dostępu do budynku i pomieszczeń:

- kontrola dostępu do budynku i pomieszczeń, w których przetwarza się dane osobowe,

- dozór całodobowy budynku,

b) zasilania systemów informatycznych:

- zastosowanie urządzeń podtrzymujących napięcie: centralny UPS dla serwerowni i dla stanowisk komputerowych,

c) zabezpieczenie systemów informatycznych:

- dostęp do systemu jedynie przez osoby upoważnione (system identyfikatorów i haseł, elektroniczne karty dostępu),

- poziomy uprawnień,

- odpowiednia architektura systemu użytkownika (webservice, klient-serwer),

- kopie awaryjne,

§ 10. Administrator danych Osobowych w drodze umowy zawartej na piśmie może powierzyć innemu podmiotowi przetwarzanie danych osobowych w podmiocie. Podmiot ten może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie.

§ 11. Zbiory, w których przetwarzane są dane osobowe podlegają z wyjątkiem wyłączeń na podstawie art 43 ust 1 i 1 a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, zgłoszeniu i rejestracji do GIODO lub do rejestru wewnętrznego Urzędu Miejskiego.

§ 12. Wymienione załączniki stanowią integralną część niniejszej polityki bezpieczeństwa:

1. Wykaz komórek organizacyjnych Urzędu Miejskiego z numerami pomieszczeń, w których przetwarzane są dane osobowe podlegające rejestracji – *załącznik nr 1, który może być zmieniany decyzją ABI.*

2. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych – *załącznik nr 2, który może być zmieniany decyzją ABI.*

3. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi – *załącznik nr 3, który może być zmieniany decyzją ABI.*

4. Procedura postępowania w przypadku zalania pomieszczeń biurowych, w których jest zlokalizowany sprzęt komputerowy przetwarzający dane – *załącznik nr 4, który może być zmieniany decyzją ABI.*

5. Procedura postępowania z kluczami od pomieszczeń biurowych , w których przetwarzane są dane osobowe - *załącznik nr 5, który może być zmieniany za zgodą ABI.*

6. Wzór upoważnienia dla Administratora Bezpieczeństwa Informacji - *załącznik nr 6, który może być zmieniany decyzją ABI.*

7. Wzór umowy powierzenia do przetwarzania danych osobowych - *załącznik nr 7, który może być zmieniany decyzją ABI.*

8. Wzór wniosku zgłoszenia zbioru do rejestru wewnętrznego - *załącznik nr 8, który może być zmieniany decyzją ABI.*

§ 13. Zobowiązuję wszystkie osoby posiadające upoważnienie nadane przez Administratora Danych Osobowych do bezwzględnego przestrzegania podanych w niniejszym opracowaniu reguł i zasad tworzących politykę bezpieczeństwa.