PREZYDENT MIASTA
SUWAŁK

ZARZĄDZENIE NR 93/2017
PREZYDENTA MIASTA SUWAŁK

z dnia 20 marca 2017 r.

w sprawie ustalenia Polityki Bezpieczeństwa Urzędu Miejskiego w Suwałkach i wprowadzenia do użytku służbowego Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Suwałkach

Na podstawie art. 30 ust.1 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U. z 2016 r. poz. 446,1575,1948) w związku z art. 36 ust. 1 i 2 ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 roku (Dz.U. z 2016 r. poz. 922) oraz § 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. z 2004 r. Nr 100, poz. 1024), zarządzam co następuje:

§ 1. Ustalam „Politykę Bezpieczeństwa Urzędu Miejskiego w Suwałkach" w brzmieniu określonym w załączniku nr 1 do „zarządzenia.

§ 2. Wprowadzam do użytku służbowego „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Suwałkach", w brzmieniu określonym w załączniku nr 2 do zarządzenia.

§ 3. Wykonanie zarządzenia powierzam Sekretarzowi Miasta, Skarbnikowi Miasta, Naczelnikom wydziałów i Kierownikom równorzędnych komórek organizacyjnych Urzędu Miejskiego w Suwałkach.

§ 4. Uchylam zarządzenie nr 68/2016 Prezydenta Miasta Suwałk z dnia 7 marca 2016 r. w sprawie ustalenia Polityki Bezpieczeństwa Urzędu Miejskiego w Suwałkach i wprowadzenia do użytku służbowego Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Suwałkach

§ 5. Zarządzenie wchodzi w życie z dniem 20 marca 2017 r.

Zastępca Prezydenta Miasta Suwałk

Łukasz Kurzyna

Załącznik Nr 1 do Zarządzenia Nr 93/2017

Prezydenta Miasta Suwałk

z dnia ..20 marca 2017 r.

POLITYKA BEZPIECZEŃSTWA URZĘDU MIEJSKIEGO W SUWAŁKACH

Realizując postanowienia ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2016 poz. 922), 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 wskazanie zasad, środków i sposobów postępowania zapewniających ochronę przetwarzania danych osobowych, zgodnie z ustawą o ochronie danych osobowych oraz jej aktami wykonawczymi, w pełni zabezpieczając dostęp do danych osobowych osób do tego nieupoważnionych.

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 i automatyczny. Sposób przepływu danych pomiędzy systemami z wykorzystaniem urządzeń teleinformatycznych przedstawiony jest w załączniku.

§ 9. Urząd Miejski w Suwałkach posiada środki techniczne i organizacyjne niezbędne dla zapewnienia zabezpieczenia, poufności, integralności i rozliczalności przetwarzanych danych *opisane w załączniku nr 1.*

§ 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 zbiorów Urzędu Miejskiego w Suwałkach.

§ 12. Wymienione poniżej załączniki stanowią integralną część Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miejskim w Suwałkach:

1. Wykaz komórek organizacyjnych Urzędu Miejskiego z numerami pomieszczeń, w których przetwarzane są dane osobowe podlegające rejestracji – *załącznik nr 2.*

2. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych – *załącznik nr 3.*

3. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi – *załącznik nr 4.*

4. Sposób przepływu danych pomiędzy systemami, służącymi do przetwarzania danych osobowych – *załącznik nr 5.*

5. Procedura postępowania w przypadku zalania pomieszczeń biurowych, w których jest zlokalizowany sprzęt komputerowy przetwarzający dane – *załącznik nr 6.*

6. Procedura postępowania z kluczami od pomieszczeń biurowych , w których przetwarzane są dane osobowe - *załącznik nr 7.*

7. Wzór upoważnienia dla Administratora Bezpieczeństwa Informacji - *załącznik nr 8.*

8. Wzór umowy powierzenia do przetwarzania danych osobowych - *załącznik nr 9.*

9. Wzór wniosku zgłoszenia zbioru do rejestru wewnętrznego - *załącznik nr 10..*

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

Z up. PREZYDENTA
Łukasz Kurzyna
ZASTĘPCA PREZYDENTA

Załącznik Nr 2 do Zarządzenia Nr 93/2017

Prezydenta Miasta Suwałk

z dnia 20 marca 2017

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W URZĘDZIE MIEJSKIM W SUWAŁKACH

Rozdział 1.
Postanowienia ogólne

§ 1. Instrukcja reguluje zasady zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Suwałkach.

§ 2. Przetwarzanie danych osobowych w Urzędzie Miejskim w Suwałkach odbywa się na zasadach określonych w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2016 r. poz. 922).

§ 3. Celem wprowadzenia niniejszej instrukcji jest ochrona danych osobowych zawartych w systemach informatycznych eksploatowanych w lokalnych sieciach komputerowych Urzędu. Instrukcja ta, zawiera w szczególności:

1) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności;

2) stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem;

3) procedury rozpoczęcia, zawieszenia i zakończenia pracy oraz postępowania w przypadku zaniku napięcia dla użytkowników systemu;

4) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;

5) sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe i kopii zapasowych zbiorów danych;

6) sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego;

7) sposób realizacji wymogu odnotowania informacji o odbiorcach, którym dane osobowe zostały udostępnione;

8) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

Rozdział 2.
Objaśnienia

§ 4. Przez użyte w instrukcji określenia należy rozumieć:

1) **dane osobowe** – wszelkie informacje o określonej lub dającej się określić osobie fizycznej;

2) **zbiór danych** – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;

3) **Administrator Danych Osobowych** – (zwany w dalszej części AD) rozumie się przez to Prezydenta Miasta Suwałk, decydującego o celach i środkach przetwarzania danych osobowych;

4) **przetwarzanie danych** – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, przeglądanie, opracowywanie, zmienianie, udostępnianie i usuwanie, zarówno w systemach informatycznych, jaki i metodami tradycyjnymi(kartoteki, księgi, wykazy);

5) **system informatyczny** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

6) **Administrator Systemu Informatycznego** – (zwany w dalszej części ASI) informatyk lub superużytkownik, zajmujący się zarządzaniem całością lub wydzieloną częścią systemu informatycznego, odpowiadający za jej sprawne działanie. Do zadań ASI należy nadzorowanie pracy serwerów, dodawanie i kasowanie kont ich użytkowników, konfiguracja komputerów, instalowanie oprogramowania, dbanie o bezpieczeństwo systemu

informatycznego, nadzorowanie, eliminowanie nieprawidłowości, asystowanie i współpraca z zewnętrznymi specjalistami przy pracach instalatorskich, konfiguracyjnych i naprawczych;

7) **użytkownik systemu informatycznego** – pracownik Urzędu posiadający odpowiednie upoważnienia;

8) **Urząd** – Urząd Miejski w Suwałkach;

9) **kierownik komórki organizacyjnej** – Sekretarz / Kierownik / Komendant / Naczelnik Wydziału, w którym zatrudniony jest pracownik przetwarzający dane osobowe;

10) **odbiorcy danych** – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:

a) osoby, której dane dotyczą,

b) osoby upoważnionej do przetwarzania danych,

c) przedstawiciela w Rzeczypospolitej Polskiej, podmiotu mającego siedzibę albo miejsce zamieszkania w państwie trzecim,

d) podmiotu mającego zawartą umowę na piśmie, w zakresie i celu przewidzianym w umowie,

e) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem,

f) państwie trzecim - rozumie się przez to państwo nienależące do Europejskiego Obszaru Gospodarczego;

11) **Administrator Bezpieczeństwa Informacji** – (zwany w dalszej części ABI) osoba wyznaczona przez Prezydenta Miasta, zgłoszona do GIODO. Do obowiązków ABI należy w szczególności:

a) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,

b) zapewnienie przestrzegania przepisów o ochronie danych osobowych w szczególności:

- sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowywanie w tym zakresie sprawozdania dla AD,

- nadzorowanie opracowania i aktualizowania dokumentacji, o której mowa w art. 36 ust. 2 ustawy o ochronie danych osobowych,

- zapewnienie zapoznania się z w/w przepisami osób upoważnionych do przetwarzania danych osobowych,

c) prowadzenie rejestru zbiorów przetwarzanych przez AD z wyjątkiem zbiorów, o których mowa w art 43 ust 1 zawierającego nazwę zbioru oraz informacje, o których mowa w art 41 ust 1 pkt 2-4a i 7 ustawy o ochronie danych osobowych.

12) **identyfikator użytkownika** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;

13) **hasło** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;

14) **karta mikroprocesorowa** – uniwersalny nośnik w postaci karty plastikowej z umieszczonym na niej mikroprocesorem, który pozwala na ochronę procesu logowania użytkownika, podpisywanie dokumentów i poczty elektronicznej oraz szyfrowanie;

15) **pin** – kod, przyznawany do każdej karty mikroprocesorowej, umożliwiający autoryzację użytkownika przy użyciu karty mikroprocesorowej;

16) **autoryzacja** – proces, w którym sprawdzane jest czy dana osoba ma prawo dostępu do systemu informatycznego. Odpowiednie uprawnienia są przypisane do konkretnej, zidentyfikowanej osoby. Autoryzacja jest zwykle poprzedzona uwierzytelnieniem (zidentyfikowaniem) osoby;

17) **uwierzytelnienie** – proces polegający na zweryfikowaniu zadeklarowanej tożsamości osoby. Uwierzytelnienie zwykle odbywa się przez podanie odpowiedniego loginu i hasła, można też użyć do tego celu karty mikroprocesorowej;

18) **BIOS/UEFI** – jest to program znajdujący się na stałe w komputerze, który jest uruchamiany, jako pierwszy po włączeniu komputera;

19) **UPS** – zasilacz awaryjny podtrzymujący pracę komputera po zaniku napięcia zasilającego,

20) **sieć LAN** – lokalna sieć komputerowa;

21) **sieć publiczna** – rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 29 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne

22) **zapora ogniowa** – (ang. firewall – "ściana ogniowa"), jeden ze sposobów zabezpieczania sieci i systemów informatycznych przed intruzami. Pełni rolę połączenia ochrony sprzętowej i programowej sieci wewnętrznej LAN

przed dostępem z zewnątrz tzn. sieci publicznych, Internetu. Chroni też przed nieuprawnionym wypływem danych z sieci lokalnej na zewnątrz;

23) **urządzenia klasy UTM** – (ang. unified threat management/zunifikowane zarządzanie zagrożeniami), oferujące kompletną wielowarstwową ochronę przed zagrożeniami z Internetu, takimi jak oprogramowanie szpiegowskie, wirusy, ataki sieciowe i inne.

Rozdział 3.
Obowiązki pracownicze wynikające z ochrony danych osobowych

§ 5. 1. Obowiązek przestrzegania tajemnicy danych osobowych dotyczy wszystkich pracowników, którzy mają dostęp do informacji o charakterze danych osobowych.

2. Naruszenie zasad ochrony danych osobowych, w efekcie którego nastąpiło udostępnienie danych osobie nieupoważnionej, jest ciężkim naruszeniem obowiązków pracowniczych.

3. Kierownicy komórek organizacyjnych Urzędu są zobowiązani do:

a) zastosowania niezbędnych środków technicznych i organizacyjnych, określonych w przepisach powszechnie obowiązujących w celu zapewnienia ochrony przetwarzania danych osobowych,

b) kontroli przestrzegania zasad i sposobu wykonywania operacji przetwarzania danych przez podległych pracowników,

c) sygnalizowania niezgodności aktów prawnych oraz aktów wewnętrznych Urzędu z przepisami ustawowymi w zakresie ochrony danych osobowych i przedstawienia stosownych projektów zmian, mających na celu ich dostosowanie do regulacji ustawowej.

4. Czynności przetwarzania danych osobowych może dokonywać jedynie pracownik upoważniony przez AD, w zakresie indywidualnych obowiązków pracowniczych.

5. Osoba upoważniona przez Administratora Danych Osobowych, jest zobowiązana do:

a) zapoznania się z przepisami prawa w zakresie ochrony danych osobowych,

b) stosowania określonych procedur i środków, mających na celu zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym,

c) zachowania szczególnej staranności w trakcie wykonywania operacji przetwarzania danych w celu ochrony interesów osób, których dane dotyczą,

d) podporządkowanie się poleceniom kierownika komórki organizacyjnej i przestrzegania ustalonych przez niego szczegółowych zasad i procedur.

Rozdział 4.
Postępowanie przy upoważnianiu osób do przetwarzania danych osobowych

§ 6. 1. W przypadku przyjęcia do pracy nowego pracownika, którego zakres obowiązków obejmować będzie przetwarzanie danych osobowych, kierownik komórki organizacyjnej obowiązany jest skierować wniosek do ABI o wydanie upoważnienia do przetwarzania danych osobowych, którego treść stanowi załącznik nr 1.

2. W przypadku przyjęcia do pracy kierownika komórki organizacyjnej lub pracownika na samodzielnym stanowisku pracy, którego zakres obowiązków obejmować będzie przetwarzanie danych osobowych, Sekretarz Miasta obowiązany jest skierować wniosek do ABI o wydanie upoważnienia do przetwarzania danych osobowych.

3. Pracownik, któremu AD udzieli upoważnienia, którego treść stanowi załącznik nr 2, jest zobowiązany do podpisania oświadczenia, którego treść stanowi załącznik nr 3.

4. Przepisy ustępu 1, 3, 5, 9 i 10 stosuje się odpowiednio do praktykantów i stażystów odbywających praktykę lub staż w Urzędzie.

5. W przypadku zmiany stanowiska, bądź zakresu obowiązków pracowniczych, kierownik komórki organizacyjnej obowiązany jest bezzwłocznie skierować wniosek o wydanie nowego bądź cofnięcie dotychczasowego upoważnienia do przetwarzania danych osobowych do ABI.

6. W przypadku zmiany stanowiska, bądź zakresu obowiązków kierownika komórki organizacyjnej lub pracownika na samodzielnym stanowisku pracy, Sekretarz Miasta obowiązany jest bezzwłocznie skierować wniosek o wydanie nowego bądź cofnięcie dotychczasowego upoważnienia do przetwarzania danych osobowych do ABI.

7. Wypowiedzenie umowy o pracę przez pracodawcę jest równocześnie cofnięciem upoważnienia do przetwarzania danych osobowych.

8. W sytuacji wypowiedzenia umowy o pracę przez pracownika, upoważnienie traci moc z datą rozwiązania umowy o pracę.

9. Ewidencję pracowników upoważnionych do przetwarzania danych osobowych prowadzi ABI.

10. Oryginały wniosków o nadanie uprawnień, oświadczenia i oryginały upoważnień znajdują się w aktach ABI.

11. Kopie upoważnień do przetwarzania danych osobowych ABI przekazuje do kadr.

Rozdział 5.
Postępowanie w przypadku naruszenia ochrony zbioru danych osobowych

§ 7. 1. Za kontrolę, przeglądy i nadzór nad konserwacją systemów informatycznych służących do przetwarzania danych osobowych odpowiedzialny jest ASI, a w szczególności:

- na wniosek AD dokonuje kontroli oraz oceny stanu bezpieczeństwa danych osobowych,
- dokonuje kontroli systemu informatycznego po uzyskaniu informacji o próbie nieautoryzowanego dostępu, wystąpieniu zagrożenia wirusem komputerowym lub innym złośliwym programem,

2. W przypadku uzasadnionego podejrzenia naruszenia zasad ochrony danych osobowych w Urzędzie, pracownik zobowiązany jest do niezwłocznego poinformowania o tym kierownika komórki organizacyjnej.

3. Kierownik komórki organizacyjnej, po dokonaniu oceny stanu faktycznego i stwierdzeniu naruszenia, jest zobowiązany poinformować o tym fakcie ABI.

4. W przypadku powtarzającego się naruszenia zasad ochrony danych osobowych, pracownik jest zobowiązany do niezwłocznego poinformowania o tym fakcie ABI.

5. Osobą odpowiedzialną za bezpieczeństwo danych osobowych w systemie informatycznym jest ASI, którego zadaniem jest w szczególności przeciwdziałanie dostępowi osób nieupoważnionych do systemu informatycznego, w którym przetwarzane są dane osobowe oraz podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń.

Rozdział 6.
Ogólne zasady eksploatacji systemów komputerowych i systemów przetwarzania danych osobowych

§ 8. 1. W obszarze przetwarzania danych osobowych mogą przebywać wyłącznie pracownicy zatrudnieni przy przetwarzaniu danych, osoby których dane dotyczą, ASI oraz inne osoby indywidualnie upoważnione przez Prezydenta Miasta.

2. Pomieszczenia w obszarze przetwarzania danych osobowych muszą być zamykane na zamek w czasie nieobecności pracowników.

3. Monitory komputerów, na których odbywa się przetwarzanie danych osobowych muszą być zlokalizowane w sposób uniemożliwiający wgląd w nie osobom trzecim.

4. Ekrany monitorów komputerów na których odbywa się przetwarzanie danych osobowych muszą być automatycznie wyłączane po upływie 15 minut nieaktywności użytkownika.

5. Nośniki informatyczne zawierające dane osobowe, a przeznaczone do likwidacji, naprawy lub przekazania podmiotowi nieuprawnionemu do otrzymania danych, przed oddaniem są pozbawiane zapisu.

6. Wydruki komputerowe zawierające dane osobowe, a przeznaczone do likwidacji, są w ciągu dnia gromadzone na stanowiskach pracy i na koniec dnia niszczone w niszczarce dokumentów.

7. Zabronione jest wykorzystywanie systemów informatycznych do celów niezgodnych z przeznaczeniem, a w szczególności instalowania gier, komunikatorów internetowych oraz oprogramowania innego niż niezbędne do realizacji przetwarzania danych i/lub realizacji innych zadań służbowych oraz instalowania oprogramowania przez osoby do tego nieuprawnione i bez wiedzy ASI.

8. Zabronione jest wykonywanie kopii danych osobowych oraz wydruków danych osobowych w celach innych niż wynikające z zasad przetwarzania danych, archiwizacji i/lub przekazania danych podmiotowi uprawnionemu.

9. Nośniki danych zawierające dane osobowe muszą być przechowywane w zamkniętych szafach.

Rozdział 7.
Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności

§ 9. 1. Nadawanie uprawnień do przetwarzania danych osobowych i rejestrowanie uprawnień w systemie informatycznym odbywa się na wniosek pisemny kierownika komórki organizacyjnej.

2. Osobą odpowiedzialną za przyznanie identyfikatora i hasła jest ASI. Działa on za zgodą ABI.

3. Każdemu z użytkowników systemu informatycznego ustala się identyfikator i hasło dostępu, a w przypadku kart mikroprocesorowych identyfikator i pin, jak również uprawnienia do poszczególnych funkcji systemu informatycznego określone według zakresu obowiązków pracownika. Odpowiada za to ASI.

4. Hasło dostępu zmienia się raz na miesiąc.

5. W przypadku stosowania kart mikroprocesorowych dane służące do uwierzytelniania użytkownika zmienia się raz na rok.

6. Użytkownik zmienia hasło w przypadku kompromitacji hasła.

7. Użytkownik zmienia pin w przypadku kompromitacji pinu.

8. Użytkownicy zobowiązani są do utrzymania w tajemnicy haseł dostępu i pinów, również po upływie ich ważności.

9. Przy stwierdzeniu próby włamania do systemu informatycznego lub podejrzeniu o kompromitację hasła, ASI blokuje konto i powiadamia ABI.

10. W przypadku rozwiązania, ustania stosunku pracy lub cofnięcia upoważnienia konto jest blokowane w systemie informatycznym. Czynność tą wykonuje ASI na wniosek ABI. Fakt ten musi być odnotowany w ewidencji osób przetwarzających dane osobowe.

§ 10. W przypadku gdy użytkownik systemu informatycznego zmienił stanowisko pracy stosuje się zasady z § 9.

Rozdział 8.
Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem

§ 11. 1. Przydziału identyfikatora i hasła oraz kart mikroprocesorowych dokonuje osobiście ASI.

2. Użytkownik przy pierwszym dostępie do systemu informatycznego jest zobowiązany do zmiany hasła.

3. Hasło musi składać się z co najmniej 8 znaków, zawierać duże i małe litery, cyfry i co najmniej jeden znak specjalny.

4. Pin do karty mikroprocesorowej musi składać się z co najmniej 4 znaków.

5. Hasła są przechowywane w systemach bazodanowych w postaci zaszyfrowanej.

6. Dane uwierzytelniające są przechowywane na karcie mikroprocesorowej w postaci zaszyfrowanej.

7. Konto użytkownika jest blokowane w przypadku trzech nieudanych prób dostępu.

8. Pin użytkownika na karcie mikroprocesorowej jest blokowany w przypadku trzech nieudanych prób dostępu.

9. Karty mikroprocesorowe nie mogą być udostępniane innym osobom.

10. Hasło i pin nie może być zapisywane lub przechowywane w miejscu dostępnym dla osób niepowołanych.

Rozdział 9.
Procedury rozpoczęcia, zawieszenia i zakończenia pracy oraz postępowania w przypadku zaniku napięcia dla użytkowników systemu informatycznego

§ 12. 1. Przed rozpoczęciem pracy użytkownik zobowiązany jest do sprawdzenia stanu stacji komputerowej. W szczególności uszkodzeń lub ingerencji osób trzecich.

2. Rozpoczynając pracę na komputerze użytkownik wprowadza wszystkie wymagane identyfikatory i hasła w sposób uniemożliwiający ich ujawnienie innym osobom.

3. W przypadku niemożliwości dostępu do systemu informatycznego z powodu zablokowania konta poprzez nieudane próby dostępu użytkownik powiadamia o tym fakcie ASI.

4. W przypadku dłuższej przerwy w korzystaniu z systemu informatycznego użytkownik obowiązany jest zawiesić pracę w systemie poprzez zablokowanie konta użytkownika, wylogowanie się z systemu informatycznego lub w inny sposób zablokowanie stacji roboczej.

5. W przypadku braku aktywności użytkownika w systemie informatycznym trwającej dłużej niż 15 minut automatycznie włącza się wygaszacz ekranowy. Ponowny dostęp do systemu informatycznego następuje po poprawnym uwierzytelnieniu.

6. Po zakończeniu pracy użytkownik powinien, prawidłowo wylogować się z systemu informatycznego, wyłączyć komputer oraz UPS, wybrać kartę mikroprocesorową z czytnika.

7. W przypadku zaniku napięcia, które ma charakter trwały, użytkownik powinien:

a) jeśli otrzymał komunikat, o braku napięcia, wyłączeniu serwera po określonym czasie natychmiast zapisać dane, wylogować się z systemu informatycznego i bezpiecznie wyłączyć komputer,

b) jeśli nie otrzymał komunikatu lub nie korzysta z sieci LAN powinien zapisać dane i bezpiecznie wyłączyć komputer.

8. Ponowna praca jest możliwa po przywróceniu napięcia w sieci energetycznej.

9. W przypadku serii krótkich zaników napięcia (sygnalizowane dźwiękiem przez zasilacz awaryjny lub komunikatami na ekranie monitora) należy zakończyć pracę oraz powiadomić ASI o niestabilności sieci energetycznej, który określi czy UPS jest sprawny.

10. Ustawienie monitora powinno uniemożliwiać podgląd danych osobom nieuprawnionym szczególnie w procesie obsługi klienta.

11. Wydruki po wykorzystaniu niszczy się w niszczarkach dokumentów.

12. Pomieszczenia w których są przetwarzane dane osobowe zamyka się na czas nieobecności osób zatrudnionych przy przetwarzaniu danych osobowych.

13. Osoby nieuprawnione mogą przebywać w pomieszczeniach, w których są przetwarzane dane osobowe tylko w obecności osoby uprawnionej.

14. Zabrania się pod rygorem odpowiedzialności służbowej i karnej:

a) ujawniania danych osobowych,

b) kopiowania bazy danych lub jej części poza przewidzianymi kopiami bezpieczeństwa,

c) przetwarzania danych w sposób inny niż opisany instrukcją,

d) instalacji nielegalnego oprogramowania mogącego naruszyć bezpieczeństwo danych osobowych.

Rozdział 10.
Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.

§ 13. 1. Kopie bezpieczeństwa wykonywane są w trybie dziennym.

2. Kopie bezpieczeństwa są sporządzane automatycznie.

3. Raz na kwartał są wykonywane kopie zapasowe na nośnikach jednorazowego zapisu.

4. Prowadzona jest ewidencja wykonywania kopii zapasowych.

5. Nośniki kopii zapasowych są opisane.

6. Tworzone są kopie bezpieczeństwa nowych i aktualizowanych programów oraz narzędzi programistycznych do przetwarzania zbiorów danych. Przechowuje się je w szafie pancernej.

7. Kopiowanie danych osobowych na nośniki informacji oraz robienie wydruków jest zabronione, chyba że istnieje konieczność ich sporządzania, która wynika z nałożonych na użytkownika obowiązków i dozwolona jest przepisami prawa.

8. Wykorzystywanie nośników informacji lub wydruków w celu innym niż wskazany jest zabronione.

Rozdział 11.
Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe i kopii zapasowych zbiorów danych

§ 14. 1. Elektroniczne nośniki danych i kopie bezpieczeństwa przechowuje się poza miejscem przetwarzania danych osobowych w szafie pancernej w zabezpieczonych pudełkach lub innym opakowaniu które chroni przed kurzem i wilgocią.

2. Dostęp do nośników zawierających dane osobowe jest zabezpieczony poprzez:

a) całodobowy monitoring,

b) system alarmowy,

c) szafę pancerną,

3. Szczegółowe zabezpieczenia pomieszczeń zawarte są w załączniku nr 10 do „Polityki bezpieczeństwa Urzędu Miejskiego w Suwałkach".

4. Kopie dzienne są przechowywane przez okres miesiąca.

5. Kopie kwartalne są przechowywane przez okres minimum 5 lat.

6. Kopie bezpieczeństwa, które uległy uszkodzeniu lub stały się niepotrzebne pozbawia się zapisu danych, a w przypadku gdy nie jest to możliwe, niszczy fizycznie w stopniu uniemożliwiającym ich odczytanie. Sporządza się protokół zniszczenia nośnika.

7. Uszkodzone nośniki przed ich wyrzuceniem należy fizycznie zniszczyć (przeciąć, przełamać zarysować itp.).

Rozdział 12.
Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

§ 15. 1. Wszystkie stacje na których przetwarzane są dane osobowe posiadają wysoki poziom zabezpieczeń.

2. W celu ochrony dostępu do danych komputera z sieci publicznej wykorzystuje się system zapory ogniowej w systemie operacyjnym oraz sprzętowe rozwiązania np. Firewall lub urządzenia klasy UTM.

3. Na każdej stacji komputerowej na której przetwarzane są dane osobowe stosuje się aktywną ochronę antywirusową, działającą w czasie rzeczywistym.

4. Aktualizacja programu antywirusowego przeprowadzana jest codziennie, automatycznie bez udziału użytkownika.

5. Pełne sprawdzenie systemu operacyjnego odbywa się raz w tygodniu.

6. Wszystkie nośniki, których zawartość jest wczytywana do komputera muszą być każdorazowo sprawdzane programem antywirusowym. Odpowiedzialnym za te czynności jest pracownik obsługujący komputer.

7. Każdy użytkownik w przypadku stwierdzenia wystąpienia komunikatu ostrzegającego lub podejrzenia działalności wirusa komputerowego lub szkodliwego oprogramowania ma obowiązek zgłosić ten fakt ASI.

8. Do obowiązków ASI należy okresowe sprawdzenie funkcjonowania i aktualność programu antywirusowego na wszystkich stacjach komputerowych przetwarzających dane osobowe.

9. W przypadku naruszenia bezpieczeństwa danych użytkownik jest zobowiązany zgłosić ten fakt ABI.

Rozdział 13.
Sposób realizacji wymogu odnotowania informacji o odbiorcach, którym dane osobowe zostały udostępnione

§ 16. 1. Dane osobowe udostępnia się na pisemny, umotywowany wniosek, chyba że przepis innej ustawy stanowi inaczej. Wniosek powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać ich zakres i przeznaczenie.

2. W przypadkach, kiedy przetwarzane są dane osobowe w systemie informatycznym, należy odnotować informacje o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych.

Rozdział 14.
Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych

§ 17. 1. Prace dotyczące przeglądów, konserwacji i napraw wymagające zaangażowania autoryzowanych firm zewnętrznych, są wykonywane pod nadzorem ASI, bez możliwości dostępu do danych osobowych.

2. Urządzenia komputerowe, dyski twarde lub inne informatyczne nośniki danych, przeznaczone do naprawy, pozbawia się przed naprawą zapisu danych osobowych w sposób trwały lub naprawia się je pod nadzorem ASI.

3. Okresową weryfikację kopii bezpieczeństwa pod kontem ich przydatności do odtworzenia danych przeprowadza ASI.

4. Nośniki informacji przekazywane na zewnątrz są pozbawiane zapisów zawierających dane osobowe. Niszczenie zapisów odbywa się poprzez usuniecie danych w sposób uniemożliwiający ich odzyskanie.

Rozdział 15.
Zasady postępowania z komputerami przenośnymi

§ 18. Komputery przenośne, używane do przetwarzania danych osobowych, zabezpiecza się podczas transportu oraz użytkowania przed dostępem do tych danych osób nieuprawnionych, w szczególności należy:

a) zabezpieczyć dostęp do komputera hasłem na poziomie BIOS/UEFI,

b) zabezpieczyć dostęp do systemu operacyjnego poprzez obligatoryjne wprowadzenie nazwy użytkownika i hasła,

c) nie zezwalać na używanie komputera osobom nieupoważnionym do dostępu do danych osobowych,

d) nie przechowywać lokalnie zbiorów z danymi osobowymi - możliwa tylko praca zdalna w systemie przetwarzania danych osobowych.

Rozdział 16.
Przepisy końcowe

§ 19. 1. Niniejsza instrukcja przeznaczona jest dla użytkowników systemu informatycznego i ich przełożonych, którzy nadzorują przetwarzanie danych osobowych.

2. Wykonanie postanowień instrukcji ma na celu ujednolicenie zarządzania systemem informatycznym w Urzędzie Miejskim w Suwałkach.

3. Wszelkie zmiany Instrukcji mogą być wprowadzane tylko na podstawie zarządzeń AD.

4. 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 wszczyna się postępowanie dyscyplinarne.

5. 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 ABI.

6. Orzeczona kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia ABI nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

7. W sprawach nieuregulowanych niniejszym dokumentem mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych oraz rozporządzenie Ministra Sprawiedliwości z dnia 28 kwietnia 2004 roku 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 .