ZARZĄDZENIE Nr 21/2016
BURMISTRZA ZWOLENIA
z dnia 15 lutego 2016r.

w sprawie wprowadzenia Polityki bezpieczeństwa informacji w Urzędzie Miejskim w Zwoleniu

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990r. o samorządzie gminnym (Dz.U. z 2015r. poz.1515, z późn. zm.), art.36 i art. 36a ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz.U. z 2015r. poz. 2135, z późń. zm.)zarządzam, co następuje:

§1.

Wprowadzam Politykę bezpieczeństwa informacji w Urzędzie Miejskim w Zwoleniu stanowiącą załącznik do niniejszego zarządzenia .

§2.

Wykonanie zarządzenia powierzam Administratorowi Bezpieczeństwa Informacji.

§3.

Traci moc Zarządzenie Nr 85/2008 Burmistrza Zwolenia z dnia 24 grudnia 2008r. w sprawie ustalenia Polityki bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Miejskim w Zwoleniu .

§4.

Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ
mgr inż. Bogusława Jaworska

RADCA PRAWNY
mgr Anna Kołłątaj
KL - R - 238

Załącznik do zarządzenia nr 21/2016
Burmistrza Zwolenia z dnia 15 lutego 2016 r.

Polityka Bezpieczeństwa Informacji w Urzędzie Miejskim w Zwoleniu

Spis treści

§ 1.
Część ogólna

1. Polityka bezpieczeństwa Informacji w Urzędzie Miejskim w Zwoleniu – zwana dalej Polityką została opracowana na podstawie obowiązujących przepisów prawa:
   1) 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 2004r. Nr 100, poz. 1024);
   2) ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2015 r. poz. 2135, z późn. zm.) oraz przepisów wykonawczych z nią związanych oraz innych przepisów, ustaw i rozporządzeń normujących przetwarzanie danych osobowych określonych kategorii;
   3) ustawy z dnia 29 września 1994r. o rachunkowości (Dz. U. z 2013 r. poz. 330, z późn. zm.).
2. Polityka określa zasady przetwarzania danych osobowych oraz ich zabezpieczenia, jako zestaw praw, reguł i zaleceń, regulujących sposób zarządzania, ochrony i dystrybucji wewnątrz Urzędu Miejskiego w Zwoleniu.
3. Polityka zawiera informacje dotyczące rozpoznawania procesów przetwarzania danych osobowych oraz wprowadzonych zabezpieczeń technicznych i organizacyjnych, zapewniających ochronę przetwarzania danych osobowych.
4. Niniejszą Politykę stosuję się do:
   1) danych osobowych:
      a) przetwarzanych w systemach informatycznych,
      b) zapisanych na zewnętrznych nośnikach informacji,
      c) przetwarzanych tradycyjnie.
   2) Informacji dotyczących bezpieczeństwa przetwarzania danych osobowych:
      a) służących do uwierzytelnienia w systemach informatycznych, w których są przetwarzane dane osobowe,
      b) dotyczących wdrożonych zabezpieczeń technicznych i organizacyjnych.
5. Bez względu na zajmowane stanowisko w Urzędzie Miejskim w Zwoleniu, miejsce wykonywanej pracy oraz charakter stosunku pracy, zasady określone w niniejszej Polityce oraz dokumentach powiązanych powinny być znane i stosowane przez pracowników oraz w niezbędnym zakresie przez współpracowników przetwarzających dane osobowe.

§ 2.
Definicje

Użyte w niniejszej Polityce pojęcia są wspólne dla wszystkich dokumentów powiązanych z niniejszą Polityką oraz wszystkich pozostałych dokumentów, które zostały przyjęte przez Urząd Miejski w Zwoleniu, w zakresie ochrony przetwarzania danych:

1) **Administrator Danych Osobowych – ADO** – Burmistrz Zwolenia;
2) **Administrator Bezpieczeństwa Informacji – ABI** – osoba wyznaczona przez ADO;
3) **Administrator Systemów Informatycznych – ASI** – osoba wyznaczona przez ADO;

4) **Bezpieczeństwo przetwarzania danych osobowych** – zachowanie poufności, integralności i rozliczalności danych osobowych; dodatkowo mogą być brane pod uwagę inne własności, takie jak dostępność, autentyczność, niezaprzeczalność i niezawodność;

5) **Dane osobowe** – każda informacja dotycząca żyjącej osoby fizycznej, która pozwala na bezpośrednią lub pośrednią identyfikację osoby;

6) **GIODO** – Generalny Inspektor Ochrony Danych Osobowych;

7) **Integralność danych** – właściwość zapewniająca, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

8) **Naruszenie danych osobowych** – zamierzone lub przypadkowe naruszenie środków technicznych i organizacyjnych zastosowanych w celu ochrony danych osobowych. W szczególności, gdy stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie ochrony danych osobowych;

9) **Poufność** – właściwość zapewniająca, że informacja jest dostępna jedynie osobom upoważnionym;

10) **Przetwarzanie danych osobowych** – 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;

11) **Rozliczalność** – właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób **jednoznaczny** tylko temu podmiotowi;

12) **System informatyczny** – zespół współpracujących urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

13) **Urząd** – Urząd Miejski w Zwoleniu;

14) **Użytkownik systemu** – osoba upoważniona do bezpośredniego dostępu do danych osobowych przetwarzanych w systemie informatycznym, która posiada ustalony identyfikator i hasło;

15) **Użytkownik zewnętrzny** – osoba nie będąca pracownikiem lub stażystą Urzędu Miejskiego w Zwoleniu, posiadająca uprawnienia do przetwarzania informacji w związku z wykonywaniem czynności na rzecz urzędu;

16) **Właściciel zbioru danych osobowych** – osoba kierująca komórką organizacyjną, stanowisko samodzielne, odpowiedzialna za ochronę danych osobowych przetwarzanych w podległej komórce organizacyjnej lub na stanowisku samodzielnym. Jest ona zobowiązana zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzania danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieupoważnioną, przetwarzaniem z naruszeniem ustawy o ochronie danych osobowych oraz nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem;

17) **Zbiór danych osobowych** – każdy posiadający uporządkowaną strukturę zestaw danych o charakterze **osobowym**, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;

18) **Zbiór nieinformatyczny** – każdy posiadający uporządkowaną strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony lub podzielony funkcjonalnie, prowadzony

poza systemem informatycznym, w szczególności w formie kartoteki, skorowidza, księgi, wykazu lub innego zbioru ewidencyjnego;

19) **Sieć lokalna** – połączenie funkcjonujących w Urzędzie Miejskim w Zwoleniu systemów informatycznych i stacji roboczych przy wykorzystaniu urządzeń i sieci telekomunikacyjnych;

20) **Stacja robocza** - stacjonarny lub przenośny komputer, rozpoznawany przez system IT, wchodzący w skład systemu informatycznego, umożliwiający użytkownikom dostęp do danych znajdujących się w tym systemie;

21) **Sieć telekomunikacyjna** – sieć telekomunikacyjna w rozumieniu ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243, z późn. zm.).

§ 3.
Cele polityki

1. Wprowadzenie niniejszej Polityki ma na celu określenie jednolitych zasady dla całego systemu przetwarzania danych.

2. Procesy i procedury podlegające wdrożeniu to:

   1) ochrona przetwarzanych i gromadzonych informacji, w tym danych osobowych w urzędzie i dotyczy:

      a) zabezpieczenia przed dostępem do danych osób nieupoważnionych, na każdym etapie ich przetwarzania tj. wprowadzania, aktualizacji lub usuwania, wyświetlania lub drukowania zestawień i raportów, przemieszczania danych w sieci lokalnej pomiędzy programami i osobami je przetwarzającymi,

      b) metod archiwizacji oraz ochrony danych zarchiwizowanych na nośnikach zewnętrznych i wydrukach;

   2) procedur niszczenia niepotrzebnych wydruków lub nośników z danymi;

   3) ustalenia i wdrożenia zabezpieczeń przed dostępem osób niepowołanych do pomieszczeń, w których są eksploatowane urządzenia gromadzące i przetwarzające dane;

   4) określenia polityki i sposobów dostępu do tych pomieszczeń przez pracowników, personel pomocniczy oraz serwis zewnętrzny;

   5) oszacowanie i zmniejszenie ryzyka utraty informacji;

   6) określenia zakresu obowiązków pracowników – w części dotyczącej bezpieczeństwa danych w tym danych osobowych;

   7) podnoszenie świadomości pracowników i ich pełne zaangażowanie w ochronę przetwarzanych informacji.

3. Powyższe procedury systemu teleinformatycznego, odnoszą się w szczególności do:

   1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są lub będą informacje podlegające ochronie;

   2) informacji będących własnością Urzędu Miejskiego w Zwoleniu lub jednostek organizacyjnych gminy, o ile zostały przekazane do urzędu na podstawie umów lub porozumień;

   3) wszystkich nośników papierowych, magnetycznych lub optycznych, na których są lub będą znajdować się informacje podlegające ochronie;

   4) wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie;

5) wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, stażystów i innych osób mających dostęp do informacji podlegających ochronie.

§ 4.
Uprawnienia do przetwarzania danych

1. Dostęp do systemu informatycznego, programów przetwarzających dane osobowe oraz urządzeń z nimi powiązanych możliwy jest wyłącznie na podstawie upoważnienia wydanego przez ADO.
2. Przed dopuszczeniem do pracy w systemie informatycznym, każda osoba powinna być zaznajomiona z przepisami dotyczącymi ochrony danych osobowych oraz niniejszą Polityką.
3. Użytkownicy danych osobowych obowiązani są do zachowania ich w tajemnicy podczas wykonywania czynności służbowych, jak i po ustaniu zatrudnienia.
4. W celu organizacji zasad ochrony, zabezpieczenia i kontroli przetwarzania danych osobowych w systemach informatycznych urzędu, ADO powołuje **administratora bezpieczeństwa informacji.**
5. W celu prawidłowego funkcjonowania infrastruktury informatycznej (sprzęt, systemy i aplikacje informatyczne) ADO powołuje **administratora systemów informatycznych**.

§ 5.
Zakres działania ABI

1. ABI w zakresie swojego działania w urzędzie podlega bezpośrednio ADO lub pełnomocnikowi ADO lub osobie przez niego upoważnionej.
2. ABI sprawuje nadzór nad kierownikami komórek organizacyjnych urzędu w zakresie przetwarzania danych osobowych w ich komórkach.
3. ABI prowadzi rejestr osób upoważnionych do przetwarzania danych osobowych w systemach informatycznych, zgodnie z wzorem stanowiącym załącznik nr 1 do niniejszej Polityki.
4. ABI prowadzi elektroniczny wykaz baz danych w systemach informatycznych, w których przetwarzane są informacje prawnie chronione – dane osobowe.
5. Do zakresu działania ABI należy również:
   a) nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których przetwarzane są dane osobowe oraz kontrola przebywających w nich osób,
   b) zapewnienie awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania,
   c) dopilnowanie aby komputery przenośne, w których przetwarzane są dane osobowe zabezpieczone były hasłem dostępu przed nieautoryzowanym uruchomieniem oraz aby komputery te nie były udostępniane osobom nieupoważnionym do przetwarzania danych osobowych,
   d) nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe,
   e) zarządzanie hasłami użytkowników i nadzór nad przestrzeganiem procedur określających częstotliwość ich zmiany zgodnie z wytycznymi, które zawarte są w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,

f) nadzór nad czynnościami związanymi ze sprawdzaniem systemu pod kątem obecności wirusów komputerowych, częstości ich sprawdzania oraz nadzorowanie wykonywania procedur uaktualniania systemów antywirusowych i ich konfiguracji,

g) nadzór nad wykonywaniem kopii awaryjnych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania w przypadku awarii systemu,

h) f) nadzór nad przeglądami, konserwacjami oraz uaktualnieniami systemów służących do przetwarzania danych osobowych oraz wszystkimi innymi czynnościami wykonywanymi na bazach danych osobowych,

i) nadzór nad systemem komunikacji w sieci komputerowej oraz przesyłaniem danych za pośrednictwem urządzeń teletransmisji,

j) nadzór nad obiegiem oraz przechowywaniem dokumentów i wydawnictw zawierających dane osobowe generowane przez system informatyczny,

k) nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane osobowe oraz kontrolą dostępu do danych osobowych,

l) podejmowanie natychmiastowych działań zabezpieczających stan systemu informatycznego w przypadku otrzymania informacji o naruszeniach zabezpieczeń systemu informatycznego lub informacji o zmianach w sposobie działania programu lub urządzeń wskazujących na naruszenie bezpieczeństwa danych,

m) analiza sytuacji, okoliczności i przyczyn, które doprowadziły do naruszenia bezpieczeństwa danych (jeśli takie wystąpiło) i przygotowanie oraz przedstawienie ADO odpowiednich zmian do Instrukcji zarządzania systemem informatycznym, służącym do przetwarzania danych,

n) koordynacja procesu analizy i oceny ryzyka związanego z przetwarzaniem danych osobowych z uwzględnieniem zabezpieczenia systemu informatycznego w urzędzie w tym: proponowanie ADO mechanizmów ochrony i środków bezpieczeństwa przetwarzania danych osobowych,

o) ścisła współpraca ze służbami prawnymi i wyznaczonymi pracownikami urzędami w prawnych aspektów procesu przetwarzania danych osobowych,

p) koordynacja wprowadzania poziomów bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym,

q) określanie i nadzór nad wdrażaniem standardów zabezpieczeń,

r) opiniowanie wszelkich zmian zachodzących w procesie przetwarzania danych osobowych, pod kątem ich wpływu na bezpieczeństwo,

s) niezwłoczne reagowanie na incydenty w zakresie bezpieczeństwa systemu informatycznego, informowanie ADO o incydentach, skutkach i propozycjach konsekwencji służbowych dla pracowników,

t) nadzór nad przestrzeganiem przez pracowników zasad ochrony danych osobowych obowiązujących w urzędzie,

u) monitorowanie zmian w przepisach prawnych dotyczących sposobu zabezpieczenia danych osobowych przetwarzanych w systemie informatycznym i dopasowanie systemu do wymagań prawnych,

v) koordynacja bieżących działań związanych ze szkoleniami pracowników, informowaniem pracowników o zagrożeniach,

w) opracowanie i aktualizowanie „Polityki bezpieczeństwa informacji w Urzędzie Miejskim w Zwoleniu" oraz „Instrukcji zarządzania systemem informatycznym

służącym do przetwarzania informacji prawnie chronionych, w tym danych osobowych w Urzędzie Miejskim w Zwoleniu" zgodnie z 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.

x) rejestracja zbiorów danych osobowych w ogólnopolskim rejestrze zbiorów danych prowadzonych przez GIODO i aktualizacja danych w rejestrze,

y) monitorowanie zaleceń i interpretacji GIODO w zakresie ochrony danych osobowych i implementowanie ich w urzędzie,

z) nadzorowanie wewnętrznego audytu bezpieczeństwa systemu w porozumieniu z ADO.

6. ABI reprezentuje ADO w obszarach związanych z nadzorowaniem przestrzegania obowiązujących zasad bezpieczeństwa danych osobowych oraz koordynuje procesy związane z zarządzaniem systemem informatycznym, przetwarzającym dane osobowe w aspekcie ich bezpieczeństwa.

§ 6.
Zakres działania ASI

Do zakresu działania ASI należy w szczególności:

1) zarządzanie i administrowanie bazami danych;

2) zapewnienie poufności, integralności, dostępności i rozliczalności danych przetwarzanych w systemach informatycznych;

3) zapewnienie zgodności wszystkich wdrażanych systemów przetwarzania danych osobowych z obowiązującymi przepisami, Polityką bezpieczeństwa oraz Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych
w Urzędzie Miejskim w Zwoleniu;

4) zarządzanie i administrowanie serwerami aplikacyjnymi: konfigurowanie, optymalizacja, monitorowanie, analizowanie zdarzeń systemowych, lokalizowanie błędów, diagnostyka i ich usuwanie;

5) kontrola i wdrażanie polityki bezpieczeństwa na serwerach;

6) implementacja odpowiednich mechanizmów bezpieczeństwa w administrowanej infrastrukturze informatycznej;

7) techniczne nadawanie i odbieranie uprawnień zgodnie z przydzielonymi upoważnieniami, w porozumieniu z ABI;

8) tworzenie kopii zapasowych zgodnie z **Instrukcją zarządzania systemem informatycznym służącym do przetwarzania informacji prawnie chronionych, w tym danych osobowych w Urzędzie Miejskim w Zwoleniu;**

9) bieżące monitorowanie poziomu bezpieczeństwa w systemie informatycznym, w szczególności bieżącego stanu aktualizacji systemów operacyjnych i serwerów oraz sygnatur programów antywirusowych;

10) bieżące monitorowanie systemu informatycznego i systemu monitoringu wizyjnego urzędu i przekazywanie informacji o zagrożeniach ABI, a w przypadku jego nieobecności ADO;

11) aktywny udział w procesie reagowania na incydenty w zakresie bezpieczeństwa oraz usuwanie ich skutków;

12) zarządzanie określonymi rozwiązaniami technicznymi związanymi z ochroną systemu informatycznego;

13) cykliczne przeglądy i weryfikacja:

a) pomieszczeń dopuszczonych do przetwarzania danych,

b) rozmieszczenia stacji roboczych,

c) sprawności użytkowanego sprzętu, w tym konserwację i likwidację sprzętu i oprogramowania,

d) legalności zainstalowanego oprogramowania,

e) harmonogramu logowania do systemu informatycznego dla poszczególnych użytkowników,

f) systemu informatycznego pod kątem obecności nieuprawnionego i szkodliwego oprogramowania;

14) monitorowanie działania instalacji telewizji przemysłowej i kontroli dostępu;

15) cykliczna kontrola sprawności zasilania awaryjnego infrastruktury telekomunikacji i sieci PC;

16) przeprowadzanie szkoleń dla pracowników, w tym szczególnie dla nowo przyjętych;

17) diagnozowanie i usuwanie awarii sprzętu komputerowego oraz realizacja umów z firmami świadczącymi usługi pogwarancyjne sprzętu komputerowego;

18) prowadzenie bieżącej ewidencji licencji oprogramowania;

19) przygotowywanie niezbędnej dokumentacji związanej z prawidłowym funkcjonowaniem sieci informatycznej (w tym: opisy systemów IT i zasilania);

20) uczestnictwo w pracach projektowych i wdrożeniowych nowych rozwiązań.

§ 7.

Zasady postępowania w przypadku stwierdzenia naruszenia ochrony danych osobowych

1. O naruszeniu ochrony danych osobowych mogą świadczyć symptomy występujące w następujących obszarach:

1) w obrębie pomieszczeń, szaf lub miejsc przechowywania:

a) ślady włamania lub prób włamania do pomieszczeń, w których odbywa się przetwarzanie danych , w szczególności do serwerowni oraz kas pancernych,

b) włamanie lub próby włamania do szaf, w których przechowywane są w postaci elektronicznej lub papierowej , nośniki danych osobowych;

2) w obrębie sprzętu informatycznego:

a) kradzież komputera, w którym przechowywane są dane osobowe,

b) rozkręcona obudowa komputera;

3) w obrębie systemu informatycznego i aplikacji:

a) brak możliwości uruchomienia aplikacji pozwalającej na dostęp do danych osobowych,

b) brak możliwości zalogowania się do tej aplikacji,

c) ograniczone, w stosunku do normalnej sytuacji, uprawnienia użytkownika w strukturze aplikacji (na przykład brak możliwości wykonania pewnych operacji normalnie dostępnych),

d) poszerzone uprawnienia w obrębie aplikacji w stosunku do dotychczas przyznanych
(na przykład wgląd do szerszego zakresu danych o pracownikach),

e) inny zakres lub różnice w zawartości zbioru danych osobowych dostępnych dla użytkownika (np. ich całkowity lub częściowy brak lub nadmiar),

Inne:

f) zagubienie bądź kradzież nośnika materiału kryptograficznego (karty mikroprocesorowej, pendrive'a itp.),

g) zagubienie bądź kradzież nośnika z zawartością danych osobowych.

2. Każda osoba, która zauważyła niepokojące zdarzenie, wystąpienie powyżej wymienionych symptomów lub innych objawów, które jej zdaniem mogą spowodować zagrożenie bądź mogą być przyczyną naruszenia ochrony danych osobowych i bezpieczeństwa informacji, zobowiązana jest do natychmiastowego poinformowania: bezpośredniego przełożonego, ASI, ABI lub ADO.

3. Informacja o pojawieniu się zagrożenia jest przekazywana przez pracownika osobiście, telefonicznie lub pocztą elektroniczną. Taka informacja powinna zawierać imię i nazwisko osoby zgłaszającej oraz zauważone symptomy zagrożenia. W przypadku, gdy zgłoszenie o podejrzeniu incydentu otrzyma osoba inna niż ADO, jest ona zobowiązana poinformować o tym fakcie ADO.

4. Po otrzymaniu zgłoszenia o wystąpieniu symptomów wskazujących na możliwość zaistnienia w urzędzie naruszenia bezpieczeństwa danych osobowych, ABI we współpracy
z ASI, jest zobowiązany do podjęcia następujących kroków:

1) stwierdzenia czy rzeczywiście doszło do naruszenia ochrony danych osobowych, w tym:

a) sprawdzenia okoliczności zdarzenia,

b) wyjaśnienia jego przyczyn, w szczególności, gdy zdarzenie było związane z celowym działaniem pracownika bądź osób trzecich;

2) w przypadku, gdy doszło do naruszenia ochrony danych osobowych to:

a) zebranie ewentualnych dowodów,

b) zabezpieczenia systemu informatycznego przed dalszym rozprzestrzenianiem się zagrożenia,

c) zabezpieczenia danych przetwarzanych w systemie informatycznym, jego logów systemowych, logów programu i bazy w których nastąpiło naruszenie bezpieczeństwa oraz danych konfiguracyjnych całego systemu w celu późniejszej analizy,

d) usunięcia skutków incydentu i przywrócenia pierwotnego stanu systemu informatycznego tj. stanu sprzed incydentu, polegające na:

- przeprowadzeniu analizy spójności danych osobowych przetwarzanych w systemie,
- ewentualnym odtworzeniu kopii zapasowych danych i plików konfiguracyjnych,
- przeprowadzeniu analizy poprawności funkcjonowania systemu informatycznego,
- powtórnym zabezpieczeniu danych przetwarzanych w systemie informatycznym, w szczególności danych konfiguracyjnych tego systemu.

5. System informatyczny, którego prawidłowe działanie zostało odtworzone powinien zostać poddany szczegółowej obserwacji w celu stwierdzenia całkowitego usunięcia symptomów incydentu.
6. ABI określa, na podstawie zebranych informacji, przyczyny zaistnienia incydentu. Jeżeli incydent był spowodowany celowym działaniem, może poinformować organy uprawnione do ścigania przestępstw o fakcie celowego naruszenia bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym urzędu.
7. ABI prowadzi ewidencję interwencji związanej z zaistniałymi incydentami w zakresie bezpieczeństwa danych osobowych. Ewidencja taka obejmuje następujące informacje:
   1) imię i nazwisko osoby zgłaszającej incydent;
   2) imię i nazwisko osoby przyjmującej zgłoszenie incydentu;
   3) datę zgłoszenia incydentu;
   4) przeprowadzone działania wyjaśniające przyczyny zaistnienia incydentu;
   5) wyniki przeprowadzonych działań;
   6) podjęte akcje naprawcze i ich skuteczność.
8. ABI odpowiedzialny jest za przeprowadzenie przynajmniej raz w roku analizy zaistniałych incydentów w celu:
   1) określenia skuteczności podejmowanych działań wyjaśniających i naprawczych;
   2) określenia wymaganych działań zwiększających bezpieczeństwo systemu informatycznego i minimalizujących ryzyko zaistnienia incydentów;
   3) określenia potrzeb w zakresie szkoleń administratorów systemu i użytkowników systemu informatycznego przetwarzającego dane osobowe.

§ 8.
Obszary przetwarzania informacji prawnie chronionych, w tym danych osobowych

1. Wykaz pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe stanowi **załącznik nr 2** do niniejszej Polityki.
2. Wykaz zbiorów danych osobowych ze wskazaniem programów zastosowanych do przetwarzania danych stanowi **załącznik nr 3** do niniejszej Polityki.
3. W szczególnie uzasadnionych przypadkach możliwe jest przetwarzanie danych osobowych poza wyznaczonym obszarem (np. na komputerach przenośnych) wyłącznie za zgodą ADO i na zasadach określonych przez ABI.
4. W zakresie przetwarzania danych osobowych w systemach finansowo-księgowych, stosuje się również Politykę Rachunkowości oraz Instrukcję kasową.

§ 9.
Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

1. Mając świadomość, że żadne zabezpieczenie techniczne nie gwarantuje stu procentowego bezpieczeństwa danych, konieczne jest, aby każdy użytkownik mający styczność z przetwarzanymi danymi, świadom odpowiedzialności, postępował zgodnie z przyjętymi w niniejszym dokumencie zasadami i minimalizował zagrożenie wynikające z błędów ludzkich.
2. Ochrona danych osobowych przetwarzanych w urzędzie obowiązuje wszystkie osoby, które mają dostęp do informacji zbieranych, przetwarzanych oraz przechowywanych w Urzędzie Miejskim w Zwoleniu, bez względu na zajmowane stanowisko oraz miejsce wykonywania jak również charakter stosunku pracy.

3. Osoby mające dostęp do danych osobowych są zobligowane do stosowania niezbędnych środków zapobiegających ujawnieniu tych danych osobom nieupoważnionym.
4. Przetwarzać dane osobowe w systemach informatycznych jak i tradycyjnych zbiorach papierowych może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych otrzymane od ADO.
5. Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.
6. Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi. Użytkownik odpowiedzialny jest za wszystkie czynności wykonane przy użyciu identyfikatora, którym się posługuje lub posługiwał.
7. Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione oraz ogólne stwierdzenie poprawności działania systemu.
8. Zachowanie tajemnicy służbowej obowiązuje pracownika zarówno podczas trwania stosunku pracy jak i po jego ustaniu.
9. ABI i ADO jest odpowiedzialny za tworzenie, wdrażanie, administrację i interpretację polityki bezpieczeństwa informacji, standardów, zaleceń oraz procedur w całym systemie urzędu.
10. Techniczne środki zabezpieczające:
    a) monitoring wizyjny CCTV z archiwizacją 30 dniową,
    b) instalacja alarmowa połączona z agencją ochrony,
    c) instalacja sygnalizacji pożaru i atestowane gaśnice przeciwpożarowe w pomieszczeniach biurowych,
    d) kontrola dostępu do pomieszczeń: ewidencji ludności, archiwów, serwerowni i centralnego UPS-a,
    e) zamki magnetyczne w serwerowni urzędu,
    f) pełne drzwi do pomieszczeń biurowych z zamkiem YETI,
    g) szyby o podwyższonej odporności w pomieszczeniach zlokalizowanych na parterze,
    h) kasy pancerne do dokumentów kadrowo-płacowych i backup danych i aplikacji IT,
    i) ochrona przed awarią podsystemu dyskowego poprzez używanie macierzy dyskowych (mirroring) i sieciowego serwera plików.
11. Informatyczne środki zabezpieczające:
    a) identyfikacja użytkownika komputera dopuszczonego do pracy, system informatyczny żąda podania loginu i hasła. Login i hasło wprowadzane jest indywidualnie użytkownikowi komputera przez ASI,
    b) wyposażenie stacji roboczych w mechanizm „wygaszacza ekranu" z wymuszoną procedurą ponownego logowania do stacji roboczej,
    c) identyfikacja użytkownika systemu dziedzinowego przy pomocy hasła i loginu,
    d) uprawnienia użytkownika systemu dziedzinowego nadawane przez ABI,
    e) mechanizm rejestracji czynności wykonywanych w systemie dziedzinowym przez użytkownika,

f) przetwarzanie informacji na bazach danych wyłącznie w pomieszczeniu serwerowni,

g) licencjonowane programy antywirusowe, automatyczna aktualizacja baz wirusów,

h) firewall na routerze,

i) system wykrywający obecność wirusów na poczcie elektronicznej,

j) stosowanie ochrony newralgicznych elementów sieciowych – switche.

12. Organizacyjne środki zabezpieczające:

a) indywidualne upoważnienia do dysponowania kluczami do pomieszczeń i budynków,

b) indywidualne kody dostępu do stref elektronicznie chronionych,

c) indywidualne hasła i loginy do systemów operacyjnych PC,

d) indywidualne hasła i loginy do systemów dziedzinowych,

e) uprawnienia wynikające z zakresu obowiązków i imiennych upoważnień,

f) obowiązek zapoznania się z Polityką bezpieczeństwa oraz Instrukcją zarządzania systemem informatycznym,

g) obowiązek nadzoru nad pracownikami przez bezpośrednich przełożonych, obowiązek udziału w szkoleniach z zakresu bezpieczeństwa przetwarzania danych,

h) dokumentacja urzędu w zakresie ochrony danych osobowych,

i) obowiązkowe szkolenia pracowników.

§ 10.
Sposób postępowania w zakresie komunikacji poza siecią informatyczną urzędu

1. Przy przesyłaniu danych osobowych poza siecią dedykowaną do transferu danych osobowych wymagane jest zastosowanie szczególnych wymagań w zakresie bezpieczeństwa. Obejmują one:

a) zatwierdzenia w formie pisemnej lub w formie elektronicznej przez ADO celu wysłania danych osobowych,

b) zastosowanie mechanizmów szyfrowania danych osobowych.

2. W przypadku stosowania mechanizmów kryptograficznych ADO określa wymagania w zakresie materiału kryptograficznego stosowanego do ochrony danych osobowych.

3. W wypadku, gdy podmiot zewnętrzny, z którym wymieniane są dane osobowe, korzysta z innych mechanizmów kryptograficznych niż stosowane w Urzędzie Miejskim w Zwoleniu, możliwe jest zastosowanie tych mechanizmów lub mechanizmów z nimi zgodnych pod warunkiem zapewnienia zbliżonej do obowiązującej ochrony przesyłanych danych osobowych. W tym celu ASI lub osoba specjalnie do tego celu wyznaczona, może przeprowadzić analizę poziomu bezpieczeństwa mechanizmu kryptograficznego oraz zgodności tego mechanizmu z komponentami systemu informatycznego.

4. W przypadku wystąpienia podejrzenia przechwycenia kluczy kryptograficznych lub dostania się ich w niepowołane ręce, ABI zobowiązany jest poinformować o tym fakcie ADO i zmienić parametry klucza szyfrującego.

§ 11.
Zasady korzystania z komputerów przenośnych, na których są przetwarzane dane osobowe poza siedzibą urzędu

1. Przetwarzanie danych osobowych na komputerach przenośnych poza siedzibą Urzędu, powinno być ograniczone do niezbędnego minimum i może się odbywać wyłącznie na podstawie umowy z ADO.
2. Umowa, o której mowa w ust.1 określa zasady korzystania z komputerów przenośnych, czas korzystania oraz wskazanie zakresu danych osobowych, których nie wolno przetwarzać na komputerze przenośnym.
3. Każdy komputer przenośny musi być zabezpieczony indywidualnym hasłem i loginem.
4. Pracownik korzystający z komputera przenośnego do przetwarzania danych osobowych lub dokumentów stanowiących tajemnicę służbową, zwłaszcza mających charakter lokalnej bazy lub pliku czyli zlokalizowanych bezpośrednio na użytkowanym komputerze, zobowiązany jest do zwrócenia szczególnej uwagi na zabezpieczenie przetwarzanych informacji, zwłaszcza przed dostępem do nich osób nieupoważnionych oraz przed zniszczeniem. W związku z powyższym użytkownik komputera przenośnego zobowiązany jest do:
   a) przechowywania przedmiotowych danych na dysku szyfrowanym, zabezpieczonym hasłem co najmniej ośmioznakowym zawierającym : duże i małe litery, znaki specjalne lub cyfry,
   b) transportu komputera w sposób minimalizujący ryzyko kradzieży lub zniszczenia, a w szczególności:
      - transportowania komputera w odpowiedniej, przeznaczonej do tego celu torbie jako bagażu podręcznego,
      - nie pozostawiania komputera w samochodzie, przechowalni bagażu, środkach transportu publicznego itp.,
   c) korzystania z komputera w sposób minimalizujący ryzyko podejrzenia przetwarzanych danych przez osoby nieupoważnione, w szczególności zabrania się korzystania z komputera w miejscach publicznych i w środkach transportu publicznego,
   d) zdecydowanego uniemożliwienia korzystania z komputera osobom niepowołanym (np. rodzinie, dzieciom, znajomym),
   e) zabezpieczenia komputera przenośnego hasłem i utrzymanie konfiguracji oprogramowania systemowego w stanie wymuszającym korzystanie z tego hasła,
   f) wykorzystywanie haseł odpowiedniej jakości zgodnie z wytycznymi dotyczącymi tworzenia haseł w systemie informatycznym przetwarzającym dane osobowe,
   g) zmianę haseł co 30 dni,
   h) blokowania dostępu do komputera przenośnego w przypadku, gdy nie jest on wykorzystywany przez pracownika,
   i) regularnego i częstego kopiowania danych przetwarzanych na komputerze przenośnym, do systemu informatycznego Urzędu w celu umożliwienia wykonania kopii awaryjnej,
   j) cyklicznego podłączania komputera do sieci informatycznej Urzędu w celu wykonania aktualizacji wzorców wirusów w programie antywirusowym.

5. ASI zobowiązany jest do podjęcia działań mających na celu zabezpieczenie komputerów przenośnych, w szczególności:
   a) dokonać konfiguracji oprogramowania w sposób wymuszający korzystanie z haseł odpowiedniej jakości oraz ich cyklicznej zmiany, zgodnie z wytycznymi dotyczącymi polityki posługiwania się hasłami w systemie informatycznym Urzędu,
   b) w przypadku przetwarzania danych osobowych znajdujących się bezpośrednio na komputerze przenośnym - zabezpieczyć je dodatkowo poprzez wykorzystanie oprogramowania szyfrującego,
   c) dokonać instalacji i konfiguracji oprogramowania antywirusowego,
   d) przeprowadzić aktualizację wzorców wirusów zgodnie z zasadami zarządzania programem antywirusowym.
6. ASI jest odpowiedzialny za prowadzenie ewidencji komputerów przenośnych wykorzystywanych do przetwarzania danych poza siedzibą Urzędu. W szczególności ewidencja powinna obejmować:
   a) typ i numer seryjny komputera przenośnego,
   b) imię i nazwisko osoby będącej użytkownikiem komputera,
   c) wykaz oprogramowania zainstalowanego na komputerze, służącego do przetwarzania danych osobowych,
   d) rodzaj i zakres danych osobowych przetwarzanych na komputerze.
7. W razie zgubienia lub kradzieży komputera przenośnego, pracownik zobowiązany jest do natychmiastowego powiadomienia ABI lub osoby uprawnionej zgodnie z zasadami informowania w przypadku naruszenia ochrony danych osobowych.
8. Kopie informacji przetwarzanych na komputerze przenośnym tworzone są indywidualnie przez ich użytkowników, na ich odpowiedzialność.

§ 12.
Elektroniczne zewnętrzne nośniki danych

1. W urzędzie stosuje się wyłącznie elektroniczne zewnętrzne nośniki danych (oznaczone i zarejestrowane przez ASI) oraz CD-ROM.
2. Nośniki pochodzące od jednostek zewnętrznych mogą być wykorzystane tylko do jednorazowego odczytu ich zawartości po uprzednim sprawdzeniu licencjonowanym programem antywirusowym w obecności ABI lub ASI.
3. Każdy użytkownik ma obowiązek usunięcia danych osobowych z nośników, które przeznaczone są do przekazania innemu podmiotów informacji związanych z realizacją zadań.
4. Deszyfracja i wprowadzenie do systemy informatycznego danych z nośników zewnętrznych dokonywana jest wyłącznie przez ABI.

BURMISTRZ

mgr inż. Bogusława Jaworska