Urząd Miasta w Piławie Górnej

Polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

Piława Górna 2008 r.

Zasady realizacji przetwarzania danych osobowych oraz stosowanych środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych w Urzędzie Miasta w Piławie Górnej

Wstęp

Zasady przetwarzania danych osobowych zostały opracowane w wykonaniu obowiązków określonych w:

1) art. 36-39 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 Nr 101, poz. 926 ze zm.),
2) Rozporządzeniu 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).

Na dokumentację przetwarzania danych osobowych w Urzędzie Miasta w Piławie Górnej zwaną dalej „dokumentacją" składają się następujące dokumenty:

1. polityka bezpieczeństwa,

   a) wzór ewidencji osób przetwarzających dane – załącznik nr 1,

   b) wzór ewidencji oprogramowania – załącznik nr 2,

2. instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,

   a) wzór upoważnienia osoby do przetwarzania danych w systemie informatycznym - załącznik nr 4,

   b) wzór pozbawienia upoważnienia osoby do przetwarzania danych w systemie informatycznym - załącznik nr 5

   c) wzór zlecenia nadania \ usunięcia użytkownika \ uprawnień – załącznik nr 6,

   d) wzór wniosku o wydanie upoważnienia osoby do przetwarzania danych w systemie informatycznym- załącznik nr 7,

e) wzór wniosku o pozbawienie upoważnienia osoby do przetwarzania danych w systemie informatycznym- załącznik nr 8,

f) wzór oświadczenia użytkownika o zapoznaniu się z treścią polityki bezpieczeństwa i instrukcji zarządzania systemami informatycznymi – załącznik nr 9

POLITYKA BEZPIECZEŃSTWA

Polityka bezpieczeństwa, o której mowa w rozporządzeniu powinna odnosić się całościowo do problemu zabezpieczenia danych osobowych u **Administratora Danych Osobowych** tj. zarówno do zabezpieczenia danych przetwarzanych tradycyjnie jak i danych przetwarzanych w systemach informatycznych.

I. Zakres stosowania

Polityka dotyczy przetwarzania danych osobowych przez pracowników Urząd Miasta w Piławie Górnej i zawiera następujące dokumenty dotyczące rozpoznania procesów przetwarzających dane osobowe oraz określające wprowadzone zabezpieczenia techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych:

1. wykaz pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe (obszar przetwarzania danych osobowych),
2. wykaz zbiorów danych osobowych i programów zastosowanych do przetwarzania danych,
3. opis struktury zbiorów, zawartości poszczególnych pól informacyjnych i powiązania pomiędzy nimi,
4. sposób przepływu danych pomiędzy poszczególnymi systemami,
5. środki techniczne i organizacyjne niezbędne w celu zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

II. Obszar przetwarzania danych osobowych

Obszarem przetwarzania danych osobowych w Urzędzie Miasta w Piławie Górnej są pomieszczenia w budynku przy ul. Piastowska 29 zajmowane przez:

1. pomieszczenie zajmowane przez: Inspektora Ds. Gospodarki Mieniem – ZGM.
   Inspektora Ds. Rolnictwa i Ewidencji Działalności Gospodarczej – ZRG.
   pokój 1
2. pomieszczenie zajmowane przez: Kierownik Urzędu Stanu Cywilnego – Kadry - USC.
   Inspektor Ds. Ewidencji Ludności i Dowodów Osobistych - BEL.
   pokój 3
3. pomieszczenie zajmowane przez: Inspektor Kasjer – SKK.
   pokój 4
4. pomieszczenie zajmowane przez: Skarbnika Gminy – BS.
   pokój 5
5. pomieszczenie zajmowane przez: Inspektora Ds. Rachunkowości Podatkowej -SRP.
   Inspektor Ds. Wymiaru Podatków – SWP.
   pokój 6
6. pomieszczenie zajmowane przez : Zastępcę Skarbnika Gminy – SZS.
   Inspektora Ds. Księgowości –SRK.
   pokój 7
7. pomieszczenie zajmowane przez: Inspektora Ds. Administracyjnych – SA.
   pokój 8
8. pomieszczenie zajmowane przez: Burmistrza – B
   pokój 9
9. pomieszczenie zajmowane przez: Zastępca Burmistrza – BZ.
   pokój 10
10. pomieszczenie zajmowane przez: Zespół Obsługi Placówek Oświatowych – BO
    pokój 11
11. pomieszczenie zajmowane przez: Sekretarza Gminy – BSG.
    pokój 12
12. pomieszczenie zajmowane przez: Radców Prawnych - SRP.
    pokój 13
13. pomieszczenie zajmowane przez: Inspektora Ds. Gospodarki Lokalami i Handlu – ZLH

Inspektora Ds. Gospodarki Komunalnej i Ochrony Środowiska – ZKS

pokój 15

14. pomieszczenie zajmowane przez: Inspektor Ds. Obronnych i Obrony Cywilnej – BOC

pokój 17

15. pomieszczenie zajmowane przez: Inspektora Ds. Obsługi Rady Miejskiej – SRM.

pokój 18

16. pomieszczenie zajmowane przez: Inspektora Ds. Gospodarki Przestrzennej i Dróg – ZPD.

pokój 19

17. pomieszczenie zajmowane przez: Inspektora Ds. Budownictwa i Zamówień Publicznych – ZIM – ZPB
Inspektora Ds. Promocji i Funduszy
Strukturalnych – ZPF

pokój 19

A także budynek Gminnego Centrum Informacji, znajdujący się przy ulicy Piastowskiej 40 w Piławie Górnej. W którym zastosowano identyczne metody zabezpieczenia danych osobowych w zakresie na jaki zezwala istniejący system informatyczny.

III. **Wykaz zbiorów danych osobowych i programów zastosowanych do przetwarzania danych.**

Wykaz zbiorów danych przetwarzanych w Urzędzie Miasta w Piławie Górnej i programów zastosowanych do przetwarzania danych winny zawierać następujące pola:

1. nazwa zbioru danych,
2. opis formy prowadzenia zbioru danych (baza danych – kartoteka papierowa),
3. środowisko pracy (platforma systemowa i bazodanowa),
4. zawartość pól informacyjnych (zakres danych),
5. jednostki organizacyjne wykorzystujące zbiór danych,
6. lokalizacja zbioru danych (oznaczenie budynków, pomieszczeń lub części pomieszczeń).

Wykaz poszczególnych zbiorów danych przedstawiony został w tabeli (załącznik nr 3)

IV. **Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi.**

W Urzędzie Miasta w Piławie Górnej znajdują się następujące zbiory danych o opisanych poniżej strukturach:

1) Płatnik

W zbiorze danych programu „Płatnik" przetwarzane są dane osobowe ubezpieczonych pracowników w zakresie:

a) dane ubezpieczonego- imie, nazwisko, dane adresowe (ulica, nr domu, miejscowość, kod pocztowy) PESEL, NIP

oraz

b) wszystkich dotyczących danego ubezpieczonego deklaracji (numer deklaracji, wysokość poszczególnych składek, wymiar etatu)

2) Radix

W zbiorze danych programu „Radix" przetwarzane są dane osobowe w zakresie:
NIP, regon, dane adresowe

Osób prawnych i osób fizycznych

3) MultiCash

W zbiorze danych programu „MultiCash" przetwarzane są dane osobowe w zakresie:
NIP, regon, dane adresowe

Nr konta osób prawnych i osób fizycznych

4) System komputerowej rejestracji stanu cywilnego

W zbiorze danych programu „System komputerowej rejestracji stanu cywilnego” przetwarzane są dane osobowe w zakresie:

Dane osób: imię, nazwisko, data urodzenia, miejsce urodzenia, imiona i nazwiska osób i rodziców, numery seryjne dowodów osobistych numery PESEL
Numery i daty aktów urodzenia.

5) System Ewidencji Ludności ELUD

W zbiorze danych programu „System Ewidencji Ludności ELUD” przetwarzane są dane osobowe w zakresie:

Dane osób: imię, nazwisko, data urodzenia, miejsce urodzenia, imiona i nazwiska osób i rodziców, numery seryjne dowodów osobistych numery PESEL
Numery i daty aktów urodzenia.

6) System wydawania dowodów osobistych

W zbiorze danych programu „System wydawania dowodów osobistych” przetwarzane są dane osobowe w zakresie:

Dane osób: imię, nazwisko, data urodzenia, miejsce urodzenia, imiona i nazwiska osób i rodziców, numery seryjne dowodów osobistych numery PESEL.

7) SIO System Informacji Oświatowej

W zbiorze danych programu „SIO System Informacji Oświatowej” przetwarzane są dane osobowe w zakresie:

Dane teleadresowe, identyfikacyjne oraz organizacyjne placówek oświatowych gminy. Informacje na temat spełnienia obowiązku nauki i obowiązku szkolnego. Informacje dotyczące form pomocy materialnej dla uczniów.

8) e-PFRON

W zbiorze danych programu „e-PFRON” przetwarzane są dane osobowe w zakresie:
Stan zatrudnienia urzędu miasta z uwzględnieniem osób niepełnosprawnych.

V. Sposób przepływu danych pomiędzy poszczególnymi systemami

W ramach procesów przetwarzania danych dochodzi do bezpośredniego przepływu danych pomiędzy różnymi systemami informatycznymi.

1. Pomiędzy programem RADIX a programem BESTIA dokonywaną przez: Zastępcę Skarbnika Gminy – SZS.
2. Pomiędzy programem ELUD a programem RADIX-POGROM dokonywaną przez: Inspektor Ds. Wymiaru Podatków – SWP.

VI. Określenie środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

1. Do elementów zabezpieczenia danych osobowych w Urzędzie Miasta w Piławie Górnej zalicza się:
   1.1. stosowane metody ochrony pomieszczeń, w których przetwarzane są dane osobowe (zabezpieczenia fizyczne),
   1.2. zabezpieczenie wszystkich procesów przetwarzania danych (w szczególności dokumentów papierowych i informatycznych),
   1.3. nadzór Administratora Bezpieczeństwa Informacji (ABI) nad realizacją wprowadzonych zasad i procedur zabezpieczenia danych (zabezpieczenia organizacyjne),
   1.4. kompleksowe i całościowe traktowanie zabezpieczenia danych przez wszystkie podmioty i osoby biorące udział w przetwarzaniu danych.
2. W Urzędzie Miasta w Piławie Górnej rozróżnia się następujące kategorie środków zabezpieczeń danych osobowych:
   2.1. zabezpieczenia fizyczne:
      2.1.1.system alarmowy w budynku w Urzędzu Miasta w Piławie Górnej,
      2.1.2.monitoring obiektu przez firmę “Odra” specjalizującą się w ochronie mienia,
      2.1.3.pomieszczenia zamykane na klucz,
      2.1.4.szafy z zamkami,
      2.1.5.szafy pancerne,
      2.1.6.kraty antywłamaniowe na drzwiach i oknach,
      2.1.7.serwer w osobnym pomieszczeniu.
   2.2. zabezpieczenia procesów przetwarzania danych w dokumentacji papierowej:
      2.2.1.przetwarzanie danych osobowych następuje w wyznaczonych pomieszczeniach,
      2.2.2.przetwarzanie danych osobowych następuje przez wyznaczone do tego celu osoby.

2.2.3. ogólne zasady przetwarzania i ochrony danych osobowych są identyczne jak w przypadku korzystania z elektronicznych nośników danych.

2.3. zabezpieczenia organizacyjne:

2.3.1. osobą odpowiedzialną za bezpieczeństwo danych jest Administrator Bezpieczeństwa Informacji (ABI),

2.3.2. ABI na bieżąco kontroluje pracę systemu informatycznego z należytą starannością, zgodnie z aktualnie obowiązującą w tym zakresie wiedzą i z obowiązującymi procedurami,

2.3.3. nie rzadziej, niż raz na miesiąc są prowadzone przez ABI kontrole stanu bezpieczeństwa systemów informatycznych i przestrzegania zasad ochrony informacji i sporządzony protokół, w przypadku wykrycia rażących zaniedbań ABI sporządza ich opis i niezwłocznie przedkłada je Administratorowi Danych Osobowych (ADO).

2.4. **organizacja pracy przy przetwarzaniu danych osobowych i zasady przetwarzania:**

2.4.1. wykaz pracowników w Urzędzie Miasta w Piławie Górnej uprawnionych do przetwarzania danych osobowych, znajduje się u Administratora Bezpieczeństwa Informacji.

2.4.2. przetwarzać dane osobowe mogą jedynie pracownicy, którzy posiadają stosowne upoważnienie przyznane przez Administratora Danych Osobowych,

2.4.3. w trakcie przetwarzania danych osobowych, pracownik jest osobiście odpowiedzialny za bezpieczeństwo powierzonych mu danych,

2.4.4. przed przystąpieniem do realizacji zadań związanych z przetwarzaniem danych osobowych, pracownik winien sprawdzić, czy posiadane przez niego dane były należycie zabezpieczone, oraz czy zabezpieczenia te nie były naruszone,

2.4.5. w trakcie przetwarzania danych osobowych, pracownik winien dbać o należyte ich zabezpieczenie przed możliwością wglądu, bądź zmiany przez osoby do tego celu nieupoważnione,

2.4.6. po zakończeniu przetwarzania danych pracownik winien należycie zabezpieczyć dane osobowe przed możliwością dostępu do nich osób nieupoważnionych,

3. W ramach zabezpieczenia danych osobowych ochronie podlegają:

3.1. sprzęt komputerowy – serwer, komputery osobiste, drukarki i inne urządzenia zewnętrzne,

3.2. oprogramowanie – programy użytkowe, systemy operacyjne, narzędzia wspomagające i programy komunikacyjne,
3.3. dane zapisane na dyskach oraz dane podlegające przetwarzaniu w systemie,
3.4. hasła użytkowników,
3.5. pliki dziennych operacji systemowych i baz danych, kopie zapasowe i archiwa,
3.6. użytkownicy i administratorzy, którzy obsługują i używają system,
3.7. dokumentacja – zawierająca dane systemu, opisująca jego zastosowanie, przetwarzane informacje, itp.,
3.8. wydruki,
3.9. związana z przetwarzaniem danych dokumentacja papierowa, z których zawarte w nich dane są wprowadzane do systemu informatycznego lub też funkcjonują autonomicznie od niego.

VII. Postanowienia końcowe

1. ABI okresowo będzie analizował zagrożenia i ryzyko w celu weryfikacji środków zabezpieczających, a także dokonywał inwentaryzacji systemów informatycznych i zbiorów danych w celu zapewnienia aktualności opisowi zawartemu w polityce bezpieczeństwa.
2. W systemie informatycznym obowiązują zabezpieczenia na poziomie wysokim.
3. Najważniejszymi zastosowanymi środkami zabezpieczenia danych w systemach informatycznych w Urzędzie Miasta w Piławie Górnej są :
   3.1. hasła dostępu do systemu,
   3.2. odpowiednie uprawnienia nadawane użytkownikom które określają do jakich danych ma dostęp użytkownik systemu informatycznego.
   3.3. hasła dostępu do aplikacji,
   3.4. programy uniemożliwiające dostęp nieuprawnionych podmiotów do danych osobowych,
      3.4.1.programy antywirusowe.
      3.4.2.zapory ogniowe.
   3.5. wygaszacze ekranu.
4. Dokumentem, który normuje procedury zarządzania systemem informatycznym służącym do przetwarzania danych osobowych jest instrukcja. Określa ona m.in.:

4.1. procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności,

4.2. stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem,

4.3. procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu,

4.4. procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania,

4.5. sposób, miejsce i okres przechowywania:

4.5.1. elektronicznych nośników informacji zawierających dane osobowe,

4.5.2. kopii zapasowych,

4.5.3. sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego,

4.5.4. sposób realizacji wymogów odnotowywania przez system informatyczny informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia,

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

INSTRUKCJA ZARZĄDZANIA BEZPIECZEŃSTWEM

SYSTEMU INFORMATYCZNEGO

W URZĘDZIE MIASTA W PIŁAWIE GÓRNEJ

Dokument niniejszy stanowi instrukcja zarządzania bezpieczeństwem systemu informatycznego o której mowa w § 3 rozporządzenia Ministra Sprawa 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), zwanego dalej „rozporządzeniem".

I. Cel instrukcji

Celem wydania dokumentu jest realizacja zapisów Polityki Bezpieczeństwa przetwarzania danych osobowych obowiązującej w Urzędzie Miasta w Piławie Górnej oraz postanowień § 5 rozporządzenia Ministra Sprawa 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.

Instrukcja ma charakter uniwersalny i precyzuje zagadnienia zarządzania wszystkimi, wymienionymi w Polityce Bezpieczeństwa, systemami komputerowymi w Urzędzie Miasta w Piławie Górnej, służącymi do przetwarzaniu danych osobowych.

II. Zakres i warunki stosowania

Wdraża się niniejszą Instrukcję oraz dokumenty z nią związane w celu stworzenia kompleksowego programu zapewnienia bezpieczeństwa systemów informatycznych służących do przetwarzania danych w Urzędzie Miasta w Piławie Górnej.

Postanowienia ogólne

Ilekroć w instrukcji jest mowa o:

1. **Administratorze Danych Osobowych (ADO)** – rozumie się przez to osobę decydującą o celach i środkach przetwarzania danych osobowych;
2. **Administratorze Bezpieczeństwa Informacji (ABI)** – rozumie się przez to osobę odpowiedzialną za stworzenie, wdrożenie i nadzorowanie standardów zabezpieczenia danych przetwarzanych w systemie informatycznym;
3. **Administratora Systemu Informatycznego (ASI)** – rozumie się przez to osobę odpowiedzialną za zapewnienie prawidłowego funkcjonowania systemu informatycznego;
4. **Osobie upoważnionej lub użytkowniku systemu (użytkownik)** – rozumie się przez to osobę posiadającą upoważnienie wydane przez ABI do dostępu i przetwarzania danych w systemie informatycznym;
5. **Osobie trzeciej** – rozumie się przez to każdą osobę nie posiadającą uprawnień dostępu do danych na terenie Urzędu Miasta w Piławie Górnej . Osobą trzecią jest również osoba posiadająca upoważnienie wydane przez ABI podejmująca czynności w zakresie przekraczającym ramy jego upoważnienia;
6. **Zbiorze danych** - rozumie się przez to każdy posiadający strukturę zestaw danych, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
7. **Przetwarzaniu danych** - rozumie się przez to jakiekolwiek operacje wykonywane na danych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, które wykonuje się w systemach informatycznych;
8. **Systemie Informatycznym** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
9. **Serwisancie** – rozumie się przez to upoważnionego pracownika firmy świadczącej usługi w zakresie naprawy i konserwacji sprzętu i oprogramowania;
10. **Danych „wrażliwych”** – rozumie się przez to dane których ujawnienie może spowodować istotne straty finansowe lub problemy prawne (np. dane osobowe, dane finansowe, itd...).

III. Nadawanie, pozbawianie oraz rejestracja uprawnień dostępu do przetwarzania danych w Systemie Informatycznym.

1. Osoby przetwarzające dane w systemie informatycznym muszą posiadać upoważnienie wydane łącznie przez ABI oraz ADO.
2. Upoważnienie do przetwarzania danych jest wydawane po przedłożeniu przez przełożonego danej osoby wniosku zawierającego:
   2.1. imię i nazwisko pracownika;
   2.2. stanowisko zajmowane przez pracownika;
   2.3. określenie wnioskowanego zakresu dostępu do danych i sposobu ich przetwarzania.
3. Wzór wniosku, o którym mowa w ust.2 określa załącznik nr 7
4. Wniosek o którym mowa ust. 3 składany jest do ABI.
5. Fakt nadania użytkownikowi uprawnień winien być potwierdzony przez ABI i ADO poprzez wydanie dokumentu „UPOWAŻNIENIE OSOBY DO PRZETWARZANIA DANYCH W SYSTEMIE INFORMATYCZNYM" (załącznik nr 4).
6. Informacja o wydanym upoważnieniu, o którym mowa w art.1 ust.1 przekazywana jest przez ABI do ASI, który nadaje identyfikator w systemie informatycznym.
7. Identyfikator winien być:
   7.1. niepowtarzalny w skali systemu;
   7.2. nadany tylko raz i nie powinien być później zmieniany.
8. Fakt nadania użytkownikowi identyfikatora w systemie informatycznym ASI potwierdza raportem wyszczególniającym nadane prawa. Raport ten powinien być przekazany użytkownikowi i ABI, który go przechowuje.
9. Nowy użytkownik systemu informatycznego otrzymuje także do zapoznania się komplet dokumentów określających zasady bezpiecznej pracy w systemie informatycznym. Użytkownik po zapoznaniu się z niniejszymi dokumentami, a przed podjęciem pracy w systemie informatycznym powinien zobowiązać się pisemnie do przestrzegania zasad bezpiecznego korzystania z systemów informatycznych (załącznik nr 9).
10. W systemie istnieje możliwość nadawania tymczasowych uprawnień użytkownikom korzystającym czasowo z określonych zasobów systemu informatycznego.
11. Zmiana uprawnień użytkownika w systemie informatycznym następuje w przypadku zmiany obowiązków służbowych. Zmiana uprawnień użytkownika zostaje przeprowadzona na wniosek bezpośredniego przełożonego.

12. Całkowite odebranie pracownikowi uprawnień do korzystania z systemu przetwarzającego dane ma miejsce, gdy:
    12.1. z pracownikiem została rozwiązana umowa o pracę;
    12.2. zmiana zakresu obowiązków służbowych spowodowała utratę potrzeby korzystania z systemu informatycznego przetwarzającego dane;
    12.3. pracownik swoim celowym działaniem spowodował zagrożenie dla bezpieczeństwa systemu informatycznego i przetwarzanych w nim danych;
    12.4. istnieje uzasadniona obawa, że korzystanie przez pracownika z systemu informatycznego przetwarzającego dane wiąże się z poważnym ryzykiem utraty poufności, integralności lub dostępności danych.
13. Proces odebrania uprawnień, o którym mowa w ust 12, obejmuje przekazanie w tej sprawie wniosku do ABI. Wniosek taki ma obowiązek sporządzić przełożony lub inspektor ds. pracowniczych w przypadku rozwiązania z pracownikiem umowy o pracę (załącznik nr 8)
14. ABI prowadzi ewidencję osób zatrudnionych przy przetwarzaniu danych (załącznik nr 1).
15. Ewidencja niniejsza powinna obejmować:
    15.1. imię i nazwisko pracownika;
    15.2. datę nadania upoważnienia dostępu do przetwarzania danych;
    15.3. datę ustania upoważnienia dostępu do przetwarzania danych;
    15.4. zakres upoważnienia dostępu do danych;
    15.5. identyfikator użytkownika w systemie informatycznym.
16. Przegląd uprawnień użytkowników w systemie informatycznym dokonywany jest kwartalnie. Odpowiedzialnym za przeprowadzenie przeglądów są bezpośredni przełożeni zgodnie ze Schematem Struktury Organizacyjnej i ASI.
17. ABI może wnioskować do kierownika komórki organizacyjnej o wyjaśnienie potrzeby posiadania przez użytkownika określonych uprawnień.

IV. Uwierzytelnianie Użytkownika

1. Rejestracji i wyrejestrowania użytkowników z systemu informatycznego dokonuje ASI.
2. ASI jest odpowiedzialny za przydzielenie identyfikatora oraz hasła użytkownikowi.
3. Użytkownik nie może samodzielnie zmieniać przydzielonego hasła.
4. Hasło, o którym mowa w ust. 2 i 3 powinno:
    4.1. być znane tylko użytkownikowi;

4.2. nie może być ujawniane osobom trzecim;
4.3. składać się z co najmniej 8 znaków;
4.4. zawierać duże i małe litery, cyfry i znaki specjalne;
4.5. być łatwe do zapamiętania i trudne do odgadnięcia, nie powinno określać bezpośrednio danego użytkownika np. imienia i nazwiska, daty urodzin itp.;
4.6. nie może być zapisywane;

5. W przypadku podejrzenia, iż hasło zostało poznane przez osoby, do tego nieupoważnione należy natychmiast poinformować o tym ABI, i zmienić hasło. ABI wyjaśni czy hasło nie zostało wykorzystane do nieuprawnionego dostępu do systemów informatycznych i czy w związku z tym nie zaistniały szkody.
6. Dostęp użytkownika do zbioru danych znajdujących się w systemie informatycznym polega na wybraniu własnego identyfikatora (jeżeli aplikacja, która obsługuje zbiór danych pozwala na taką możliwość) oraz wprowadzeniu hasła dostępu. Po poprawnym wykonaniu tych operacji użytkownik może wykonywać wszystkie czynności zgodnie z przydzielonym dostępem.

V. Rozpoczęcie, zawieszenie i zakończenie pracy w Systemie Informatycznym

1. Rozpoczęcie pracy w systemie informatycznym powinno rozpocząć się od zalogowania do systemu identyfikatorem oraz hasłem otrzymanym od ASI.
2. W przypadku braku możliwości zalogowania się użytkownika na jego konto czy też w przypadku stwierdzenia fizycznej ingerencji w przetwarzane dane lub użytkowane narzędzia programowe lub sprzętowe - użytkownik powinien to niezwłocznie zgłosić na piśmie ASI, a on powiadamia ABI.

VI. Tworzenie i przechowywanie kopii zapasowych

1. Odpowiedzialnymi za wyznaczenie danych do archiwizacji w komórkach organizacyjnych są bezpośredni przełożeni zgodnie ze Schematem Struktury Organizacyjnej.

2. Tworzenie, przechowywanie i likwidację kopii bezpieczeństwa regulują szczegółowe instrukcje operacyjne dla poszczególnych aplikacji i systemów przetwarzania oraz powszechnie obowiązujące przepisy prawa.
3. Plan tworzenia kopii zapasowych:

Kopie zapasowe danych, baz danych oraz aplikacji bazodanowych zlokalizowanych na serwerze wykonywane są:

1. Kopie bezpieczeństwa powinny być tworzone w regularnych odstępach czasu, w cyklu:
   1.1. dziennym - tworzone są dzienne kopie bezpieczeństwa na serwerze.
   1.2. tygodniowym, - tworzone są w każdym tygodniu kopie bezpieczeństwa na zewnętrznym urządzeniu magazynującym.
   1.3. miesięcznym - tworzone są kopie na zewnętrznych (trwałych) nośnikach danych np. płytach DVD.
2. Kopie bezpieczeństwa powinny być tworzone na nośnikach informacji zapewniających trwałość danych w okresie ich przechowywania. Nośniki powinny być opisane w sposób pozwalający na łatwą identyfikację ich zawartości.
3. Kopie bezpieczeństwa nie mogą być przechowywane w tych samych pomieszczeniach, w których przechowywane są zbiory danych eksploatowane na bieżąco.
4. Kopie bezpieczeństwa, które uległy uszkodzeniu lub stały się niepotrzebne pozbawia się zapisu danych, a w przypadku gdy nie jest to możliwe, niszczy w stopniu uniemożliwiającym ich odczytanie zgodnie z przyjętymi procedurami.

VII. Zabezpieczenie Systemu Informatycznego
Pomieszczenia

1. Pomieszczenia w których znajduje się kluczowy sprzęt informatyczny (np. serwery, komputery do bankowości elektronicznej) powinny być zabezpieczone w sposób uniemożliwiający włamanie. Nadto powinny być wyposażone w system alarmowy i p. poż. Pomieszczenia takie winny znajdować się z dala od instalacji wodno - kanalizacyjnej z uwagi na możliwość zalania.
2. Pomieszczenia, w których znajduje się sprzęt komputerowy, powinny być zabezpieczone przed dostępem osób nieupoważnionych.

3. Kluczowy sprzęt informatyczny powinien być zabezpieczony przy pomocy urządzeń podtrzymujących zasilanie „UPS-ów”.
4. Uprawnienia do przebywania w strefach wymagających specjalnej ochrony (np. serwerownia) powinny być nadawane przez ABI.

Nośniki

1. Użytkownicy systemu informatycznego powinni zabezpieczać powierzone im informacje przed dostępem osób nieupoważnionych. W szczególności dotyczy to nośników danych (dyskietki, CD-ROM-y), które powinny być przechowywane w zamykanych szafkach.
2. Dopuszcza się wynoszenie przez użytkowników nośników poza siedzibę Urzędu Miasta w Piłwie Górnej wyłącznie po uzyskaniu zgody przełożonego i wskazaniu celu i daty wynoszenia oraz daty zwrotu. Powyższe fakty winne być odnotowane.
3. W przypadku wynoszenia poza siedzibę Urzędu Miasta w Piłwie Górnej nośników zawierających dane tzw. „wrażliwe” (tzn. dane osobowe, finansowe) użytkownik musi uzyskać zgodę ABI. Fakt ten zostaje odnotowany wraz z określeniem daty, celu wyniesienia oraz daty zwrotu.
4. Wprowadzenie i wyprowadzenie danych do/z systemu informatycznego Urzędu Miasta w Piłwie Górnej jest możliwe tylko po przeprowadzeniu kontroli antywirusowej tych danych.
5. Nośniki muszą być oznakowane.
6. Korzystanie z własnych nośników jest zabronione.
7. Przekazywanie nośników powinno być przeprowadzane z uwzględnieniem zasad bezpieczeństwa.
8. Nośniki przygotowane do transportu powinny być zapakowane tak, aby zminimalizować ryzyko ich uszkodzenia.
9. Nośniki zawierające tzw. dane „wrażliwe” powinny być dodatkowo zabezpieczone poprzez użycie zamykanych kopert pozwalających na wykrycie prób otwierania.

Stacje robocze

1. Użytkownik odchodzący od stacji roboczej powinien ją zablokować. Odblokowanie następuje po ponownym wprowadzeniu hasła.
2. Ustala się ograniczenia w korzystaniu przez użytkowników z systemu informatycznego w zależności od miejsca i czasu. O miejscu pracy i czasie w jakim użytkownicy upoważnieni są do korzystania z systemu informatycznego decydują przełożeni.
3. Stacje robocze nie mogą być samodzielnie przez użytkowników przenoszone.
4. Niedozwolone jest instalowanie przez użytkowników nowego oprogramowania oraz modyfikowanie konfiguracji już zainstalowanego, w szczególności: systemu operacyjnego, oprogramowania antywirusowego i innych składników systemu niezbędnych do bezpiecznego i prawidłowego funkcjonowania systemu informatycznego.

Komputery przenośne

1. Użytkownik komputera przenośnego winien zabezpieczyć poufność i dostępność przetwarzanych na urządzeniu danych.
2. W przypadku korzystania z komputera przenośnego poza obszarem przetwarzania danych osobowych dane osobowe będą chronione z wykorzystaniem środków ochrony kryptograficznej.
3. Transport komputera przenośnego winien odbywać się pod kontrolą użytkownika lub innej osoby upoważnionej,
4. Komputer o którym mowa w ust 1 musi być zabezpieczony przed kradzieżą poprzez niepozostawianie go w miejscach ogólnie dostępnych bez nadzoru lub zamknięcie w szafie.
5. W przypadku kradzieży lub zgubienia komputera użytkownik powinien ten fakt natychmiast zgłosić pisemnie do ABI, z zaznaczeniem jakie dane były przechowywane na tym urządzeniu.
6. Pracując na komputerze w miejscu publicznym użytkownik powinien zabezpieczyć informacje wyświetlane na monitorze przed dostępem innych osób do tego nieuprawnionych.

7. Użytkownik otrzymujący komputer przenośny musi podpisać oświadczenie o zobowiązaniu się do przestrzegania zaleceń związanych z ochroną powierzonego sprzętu.

Połączenia między sieciami informatycznymi

1. Sieci służące do przetwarzania danych „wrażliwych" muszą być chronione zabezpieczeniami logicznymi lub fizycznymi. W przypadku zastosowania zabezpieczeń logicznych muszą one zapewniać kontrolę przepływu informacji pomiędzy systemem informatycznym w Urzędzie Miasta w Piławie Górnej a siecią publiczną oraz kontrolę działań inicjowanych z sieci publicznej i z systemu informatycznego Urzędu Miasta w Piławie Górnej.
2. Ochrona realizowana jest z wykorzystaniem odpowiedniego sprzętu i/lub oprogramowania.
3. O ile jest to wymagane istnieje możliwość połączenia systemu informatycznego z sieciami zewnętrznymi za zgodą ABI.

Wykorzystanie Internetu

1. Użytkownicy systemu informatycznego mający dostęp do internetu mogą używać go tylko i wyłącznie do celów służbowych.
2. Wprowadza się zakaz ściągania plików oraz przeglądania stron – informacji o treści prawnie zabronionej (obscenicznej bądź pornograficznej).
3. Pliki wykonywalne powinny być ściągane tylko za zgodą ABI.
4. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie ściągnięte z internetu i przez niego zainstalowane oraz ponosi odpowiedzialność za wykorzystanie oprogramowania niezgodnie z jego licencją, a w szczególności za wykorzystanie oprogramowania, do którego Urzędu Miasta w Piławie Górnej nie nabyło odpowiednich praw.

System poczty elektronicznej

1. Poczta elektroniczna powinna służyć jedynie do wymiany informacji służbowych.
2. Ogólne zasady korespondencji elektronicznej są analogiczne jak dla wymiany dokumentów w formie papierowej.

3. Użytkownicy nie powinni otwierać przesyłek od nieznanych sobie osób, których temat nie sugeruje związku z ich obowiązkami służbowymi. W takim przypadku należy ją zniszczyć lub zasięgnąć opinii ASI, który sprawdzi czy ta przesyłka nie stanowi zagrożenia dla bezpieczeństwa systemu informatycznego.
4. Zakładanie, modyfikacja i usuwanie kont poczty elektronicznej następuje na wniosek przełożonego przez ASI za zgodą ABI.

Systemy antywirusowe

1. System informatyczny przetwarzający dane powinien być wyposażony w mechanizmy ochrony antywirusowej.
2. System antywirusowy powinien być systematycznie uaktualniany.
3. System antywirusowy może być instalowany, modyfikowany w systemie informatycznym tylko przez uprawnione do tego osoby. Upoważnienia takiego udziela ASI.
4. Jeżeli użytkownik zauważy niewłaściwą pracę systemu informatycznego lub gdy otrzyma komunikat o zagrożeniu przez niebezpieczny kod wyświetlony przez system antywirusowy musi niezwłocznie powiadomić o tym ASI, który określi dalsze postępowanie.
5. ABI odpowiedzialny jest za stworzenie koncepcji ochrony antywirusowej.

Poprawność informacji

1. Użytkownicy systemu informatycznego odpowiedzialni są za poprawność wprowadzanych przez nich informacji.
2. Użytkownicy systemu informatycznego zobowiązani są do analizy poprawności informacji generowanych przez aplikacje.

Niszczenie informacji

1. Urządzenia, dyski lub inne elektroniczne nośniki informacji zawierające dane osobowe przeznaczone do likwidacji przekazane podmiotowi nieuprawnionemu do ich przetwarzania pozbawia się zapisu tych danych w sposób uniemożliwiający ich odczytanie i/lub odzyskanie.

2. Urządzenia, dyski lub inne elektroniczne nośniki informacji zawierające dane osobowe przeznaczone do naprawy pozbawia się zapisu tych danych w sposób uniemożliwiający ich odczytanie i/lub odzyskanie lub naprawia się je pod nadzorem osoby upoważnionej przez ADO.

VIII. Wykonywanie przeglądów i konserwacji Systemu Informatycznego oraz nośników

1. ASI jest odpowiedzialny za kontrolę prawidłowego działania urządzeń i oprogramowania.
2. ABI odpowiedzialny jest za monitorowanie zabezpieczeń systemów informatycznych.
3. ASI lub osoby przez niego upoważnione dokonują przeglądu systemu informatycznego pod względem prawidłowości zabezpieczeń raz w roku. W szczególności należy zwrócić uwagę na:
   3.1. zakres uprawnień użytkowników;
   3.2. przestrzeganie zasad ochrony dostępu do informacji (zabezpieczenie pomieszczeń, blokowanie stacji roboczych, zachowanie zasady czystego biurka);
   3.3. przestrzeganie zasad dotyczących zapewnienia poprawności informacji wrażliwych;
   3.4. przestrzeganie zasad tworzenia kopii bezpieczeństwa;
   3.5. konfigurację systemu pod względem jego bezpieczeństwa.
4. Z dokonania przeglądu sporządza się protokół ze szczególnym wskazaniem braków w systemie zabezpieczeń. Dokumenty te przedstawione są ABI i przez niego przechowywane.
5. ASI może przeprowadzać dodatkowe przeglądy mające na celu sprawdzenie poziomu zabezpieczenia danych. Z każdego takiego przeglądu sporządzany jest protokół.
6. Konserwacja systemu informatycznego dokonywana jest na bieżąco. Odpowiedzialny za to jest ASI lub osoba przez niego upoważniona.

IX. Oprogramowanie

1. Oprogramowanie wykorzystywane jest w zakresie i w sposób określony w licencji autora która została udostępniona Urzędowi Miasta w Piławie Górnej przez producenta lub sprzedawcę oprogramowania.

2. Instalacja, kopiowanie i wykorzystanie oprogramowania odbywa się wyłącznie za zgodą ABI i ASI tylko w sytuacji, gdy Urząd Miasta w Piławie Górnej nabył prawa do wykorzystania oprogramowania na podstawie stosownych umów.7
3. Instalacja, kopiowanie i wykorzystanie nielegalnego oprogramowania jest zabronione, a osoby odpowiedzialne za jego wykorzystanie podlegają sankcjom przewidzianym w przepisach prawa oraz wewnętrznych regulaminach Urzędu Miasta w Piławie Górnej. Oprogramowanie uznaje się za nielegalne w przypadku wykorzystania go niezgodnie z licencją, na której udostępniono oprogramowanie i/lub w przypadku gdy Urząd Miasta w Piławie Górnej nie nabył praw do wykorzystania oprogramowania na podstawie odrębnych umów.
4. ASI jest odpowiedzialny za ewidencję, kontrolę wykorzystywanego oprogramowania, identyfikację i usuwanie nieprawidłowości oraz zgłaszanie ABI stwierdzonych nieprawidłowości.
5. Kontrola legalności oprogramowania odbywać się będzie:
   5.1. z chwilą nabycia praw do wykorzystania oprogramowania;
   5.2. doraźnie podczas realizowania obowiązków służbowych;
   5.3. okresowo w formie pełnego przeglądu – co najmniej jeden raz w roku.
6. Wyniki kontroli przedstawione będą w formie pisemnego raportu dla ADO wraz z zaleceniami.

X. Wykaz załączników

1. wzór ewidencji osób przetwarzających dane – załącznik nr 1,
2. wzór ewidencji oprogramowania – załącznik nr 2,
3. Tabela-Wykaz poszczególnych zbiorów danych- załącznik nr 3,
4. wzór upoważnienia osoby do przetwarzania danych w systemie informatycznym - załącznik nr 4,
5. wzór pozbawienia upoważnienia osoby do przetwarzania danych w systemie informatycznym - załącznik nr 5,
6. wzór zlecenia nadania \ usunięcia użytkownika \ uprawnień – załącznik nr 6,
7. wzór wniosku o wydanie upoważnienia osoby do przetwarzania danych w systemie informatycznym- załącznik nr 7,

8. wzór wniosku o pozbawienie upoważnienia osoby do przetwarzania danych w systemie informatycznym- załącznik nr 8,
9. wzór oświadczenia użytkownika o zapoznaniu się z treścią polityki bezpieczeństwa i instrukcji zarządzania systemami informatycznymi – załącznik nr 9