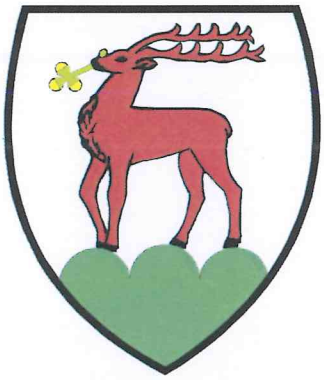
Załącznik Nr 3
do Zarządzenia Nr 0050.129.2012.VI
Prezydenta Miasta Jeleniej Góry
z dnia 15 maja 2012r.

Urząd Miasta Jelenia Góra



INSTRUKCJA ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI PRZETWARZAJĄCYMI DANE OSOBOWE

	Sporządził	Zatwierdził
Data	10.05.2012	15.05.2012
Osoba:	Kierownik Referatu Informatyki Marcin Błażków	Prezydent Miasta Marcin Zawiła

KIEROWNIK REFERATU Informatyki
Marcin Błażków

PREZYDENT MIASTA Jeleniej Góry
Marcin Zawiła

Podstawa prawna

- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r., Nr 101 poz. 926 z późn. zm.),
- Rozporządzenie 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).

Administrator danych:

Urząd Miasta Jelenia Góra, Plac Ratuszowy 58, Jelenia Góra

Spis treści

1. Cel

Celem instrukcji jest określenie procedur zarządzania systemami informatycznymi, służącymi do przetwarzania danych osobowych, a w szczególności określenie:

- procedury nadawania uprawnień do przetwarzania danych,
- stosowanych metod i środków uwierzytelnienia oraz procedur związanych z **ich** zarządzaniem i użytkowaniem,
- procedur tworzenia kopii zapasowych i ich przechowywania,
- sposobu zabezpieczenia danych osobowych przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego;
- procedur wykonywania przeglądów i konserwacji systemów oraz nośników informacji, służących do przetwarzania danych osobowych.

2. Zakres stosowania

Instrukcja dotyczy przetwarzania danych osobowych w systemach informatycznych w Urzędzie Miasta Jelenia Góra.

3. Nadawanie uprawnień w systemach informatycznych

3.1. Naczelnik Wydziału lub osoba zatrudniona na samodzielnym stanowisku pracy występuje do Administratora Bezpieczeństwa Informacji o upoważnienie do przetwarzania danych osobowych zgodnie z punktem 3.3. „Polityki bezpieczeństwa danych osobowych" i wzorem nr 1, stanowiącym załącznik do „Polityki Bezpieczeństwa Danych Osobowych". Administrator Bezpieczeństwa Informacji wystawia Upoważnienie wg wzoru nr 2, stanowiącego załącznik do „Polityki Bezpieczeństwa Danych Osobowych", następnie jeden egzemplarz przekazuje pracownikowi, drugi natomiast przechowuje we własnej dokumentacji.

3.2. Dokumentację dotyczącą uprawnień pracownika w zakresie przetwarzania danych osobowych przechowuje Administrator Bezpieczeństwa Informacji.

3.3. Pracownik korzystający z zasobów systemu informatycznego powinien być jednoznacznie identyfikowany poprzez indywidualny identyfikator (login/nazwa) użytkownika systemu.

3.4. Niedopuszczalne jest korzystanie z tego samego identyfikatora przez więcej niż jednego pracownika.

3.5. Odebranie uprawnień dostępu do systemów informatycznych następuje na wniosek Naczelnika/Kierownika komórki organizacyjnej, zgłoszony na formularzu, przygotowanym zgodnie

ze wzorem nr 1, stanowiącym załącznik do „Polityki bezpieczeństwa danych osobowych" lub - w przypadku odebrania upoważnienia do przetwarzania danych osobowych w związku z zakończeniem świadczenia pracy na rzecz Urzędu Miasta - na podstawie karty pracownika odchodzącego.

4. Metody i środki uwierzytelnienia

4.1. Użytkownicy w systemach informatycznych są uwierzytelniani przez wprowadzenie nazwy użytkownika i hasła. W przypadku systemów informatycznych operujących na zbiorach „Dowody osobiste" i „Ewidencja pojazdów i kierowców" konieczne jest wykorzystanie uwierzytelnienia z pomocą karty chipowej. Użytkownicy są zobowiązani do stosowania haseł zgodnych z wymaganiami polityki haseł, określonymi w pkt. 8.7 „Polityki bezpieczeństwa danych osobowych".

4.2. Dostęp do systemów informatycznych spoza sieci wewnętrznej jest zabroniony.

4.3. Początkowe hasło użytkownika w systemie informatycznym jest ustalane przez administratora i przekazywane użytkownikowi ustnie. Użytkownik jest zobowiązany do bezzwłocznej zmiany hasła, o ile system ma taką funkcjonalność. Przekazywanie hasła za pośrednictwem innej osoby lub za pomocą poczty elektronicznej jest zabronione.

4.4. Hasła do systemów informatycznych powinny być zmieniane przez użytkowników nie rzadziej niż co 30 dni. Jeżeli systemy informatyczne nie wymuszają tego środkami technicznymi, za terminową zmianę hasła odpowiedzialny jest użytkownik.

4.5. Zasady długości i złożoności hasła określone są w pkt. 8.7 „Polityki bezpieczeństwa danych osobowych".

5. Procedury tworzenia kopii zapasowych

Poniżej opisano procedury tworzenia kopii zapasowych dla zbiorów danych osobowych, przetwarzanych w Urzędzie Miasta Jelenia Góra.

5.1. Wszystkie zbiory danych osobowych, przetwarzanych w Urzędzie Miasta w pierwszej kolejności automatycznie kopiowane są na zabezpieczony zasób sieciowy. Urząd Miasta wykorzystuje dwa urządzenia sieciowe, gromadzące kopie zapasowe, zlokalizowane w serwerowniach Urzędu Miasta. Urządzenie nr 1 znajduje się w serwerowni w pok. nr 103 w budynku przybudówki ratusza. Urządzenie nr 2 znajduje się w serwerowni w pok. nr 32 w budynku przy ul. Sudeckiej 29. Obydwa urządzenia wykonują i weryfikują kopie zapasowe w trybie codziennym (nadpisywane po 14 dniach) – kopie różnicowe. Kopiowaniu podlegają dane ze zbioru. Weryfikacja kopii zapasowej następuje automatycznie podczas wykonywania kopii dziennej. Na obydwu urządzeniach znajdują się kopie zapasowe wszystkich chronionych zbiorów danych osobowych. W pierwszym tygodniu każdego miesiąca jest wykonywana kopia miesięczna,

przechowywana przez 3 miesiące (pełna). W ostatnim roboczym tygodniu każdego roku ręcznie tworzona jest dodatkowa kopia zapasowa wszystkich zbiorów danych osobowych, która następnie jest przechowywana jako kopia roczna w osobnym, zabezpieczonym folderze na obu urządzeniach.

5.2. Administrator systemu związanego z każdym zbiorem danych osobowych raz w miesiącu w ostatnim tygodniu miesiąca testuje poprawność wykonywanej kopii poprzez próbę jej odczytania i rozpakowania.

5.3. Raz w roku (w ostatnim roboczym tygodniu roku) wykonywane są kopie roczne zbioru danych osobowych. Kopie roczne nagrywane są na płyty DVD (w 2 egz.) i przechowywane w sejfie w Wydziale Informatyki i Obsługi Technicznej w budynku Przybudówki Ratusza pok. 305 oraz w szafie pancernej w serwerowni w budynku przy ul. Sudeckiej 29. pok. 32. Zbiory, których rozmiar nie pozwala na kopiowanie ich na płyty DVD, kopiowane są na przenośne dyski twarde i przechowywane podobnie jak płyty DVD.

5.4. Z powyższej procedury nie korzystają zbiory przechowywane na komputerach lokalnych, nie połączonych fizycznie z siecią Urzędu Miasta, oraz zbiory związane z Centralną Ewidencją Pojazdów i Kierowców, jako zbiory, do których nie mają dostępu służby informatyczne Urzędu Miasta.

5.5. W celu przyspieszenia, ewentualnego odzyskania funkcjonalności systemu wykonywane są dodatkowo kopie zapasowe zbiorów, wymienionych w pkt. 5.4, a także dodatkowo kopie zapasowe zbiorów, wyszczególnionych poniżej. na inne nośniki.

Dla zbiorów **„Urząd Stanu Cywilnego w Jeleniej Górze"** oraz **„Ewidencja ludności i dowodów osobistych"**:

1. Kopie są tworzone codziennie na taśmach magnetycznych.
2. Kopiowaniu podlegają dane ze zbioru.
3. Kopie wykonywane są automatycznie.
4. Weryfikacja kopii zapasowej następuje automatycznie podczas wykonywania kopii dziennej.
5. Kopie są testowane w drugi piątek każdego miesiąca poprzez odczytanie zawartości taśm magnetycznych oraz zaszyfrowanego archiwum.
6. Taśmy magnetyczne służące do wykonywania kopii zapasowych przechowywane są w sejfie w Wydziale Informatyki i Obsługi Technicznej (budynek Przybudówki Ratusza).
7. Kopie na taśmach nadpisywane są po upływie 7 dni.

Dla zbiorów **„Ewidencja pojazdów i kierowców"**:

1. Kopie są wykonywane automatycznie przez oprogramowanie na serwerze, bez ingerencji pracowników Urzędu Miasta. Pracownicy Urzędu Miasta nie zarządzają serwerem, który jest udostępniony przez Państwową Wytwórnię Papierów Wartościowych.

2. Nie można ustalić, co jest kopiowane.
3. Kopie dzienne są wykonywane automatycznie. Za wymianę kartdridży odpowiedzialny jest pracownik obsługujący system.
4. Kopie są automatycznie weryfikowane przez oprogramowanie.
5. Kopie nie są testowane przez pracowników Urzędu.
6. Kopie są przechowywane w sejfie w pomieszczeniu nr 9, w budynku przy ul. Sudeckiej 29.
7. Kopie na kardridżach są nadpisywane w okresie tygodniowym.

Dla zbioru **„Obsługa Obrony Cywilnej"**:

1. Kopie zapasowe są wykonywane przez nagranie na płytę DVD-RW przez pracownika obsługującego system.
2. Kopie wykonywane raz w tygodniu.
3. Kopiowaniu podlegają dane i programy.
4. Kopie wykonuje ręcznie pracownik obsługujący system.
5. Kopie są automatycznie weryfikowane przez oprogramowanie do nagrywania płyt.
6. Kopie są testowane raz na dwa miesiące przez próbę uruchomienia systemu z kopii zapasowej.
7. Płyty są przechowywane w szafie pancernej, zabezpieczone przed dostępem osób niepowołanych oraz przed wpływem sił natury.
8. Kopie są przechowywane w szafie pancernej w pomieszczeniu nr 7, przy ul. Armii Krajowej 19. Ostatnia kopia z danego miesiąca jest przechowywana w tej samej szafie.
9. Kopie są nadpisywane po tygodniu. Kopie miesięczne są przechowywane przez rok i nadpisywane.
10. Ostatnia kopia miesięczna wykonywana w roku kalendarzowym oznaczana jest jako kopia roczna i nie podlega nadpisywaniu.

Dla zbioru **„ESOD":**

1. Na taśmach magnetycznych wykonywane są kopie bazy danych, opisujących rejestrowane dokumenty.
2. Skany dokumentów i repozytorium plików kopiowane są tylko poprzez urządzenia sieciowe.
3. Kopiowaniu podlegają dane ze zbioru.
4. Kopie wykonywane są automatycznie.
5. Weryfikacja kopii zapasowej na zasobie sieciowym następuje automatycznie podczas wykonywania kopii dziennej.
6. Kopie z taśm są testowane raz w miesiącu poprzez odczytanie zawartości taśm magnetycznych.
7. Taśmy magnetyczne służące do wykonywania kopii zapasowych przechowywane są w sejfie w Wydziale Informatyki i Obsługi Technicznej (budynek przybudówki ratusza) pok 305.
8. Kopie na taśmach nadpisywane są po upływie 7 dni.

6. Zabezpieczenia systemu informatycznego

1. Wszystkie komputery są zabezpieczone oprogramowaniem antywirusowym.
2. Aktualizacje oprogramowania komputerów pracowniczych są pobierane i instalowane automatycznie. W wypadku serwerów – aktualizacje pobierane są automatycznie, instalacja odbywa się ręcznie. Tam gdzie nie jest to możliwe ze względu na ograniczenia sieci – aktualizacje są pobierane i wykonywane poprzez serwer aktualizacji.
3. Sieć komputerowa jest zabezpieczona przez zapory sieciowe komputerów oraz przez serwery Proxy i IPS. W sieci stosowane są zabezpieczenia logiczne – grupy robocze, domena Active Directory oraz odrębne adresy podsieci.
4. Dyski twarde, dyskietki, taśmy magnetyczne i inne nośniki informacji przeznaczone do likwidacji, Administrator Bezpieczeństwa Informacji lub wyznaczony przez niego pracownik Referatu Informatyki pozbawia wcześniejszego zapisu danych, a w przypadku, gdy nie jest to możliwe, uszkadza w sposób uniemożliwiający odczytanie informacji. Z czynności tych sporządza się protokół.
5. W przypadku konieczności dokonania naprawy przez serwis zewnętrzny, Administrator Bezpieczeństwa Informacji wyznacza osobę, która prowadzi stały nadzór nad pracami lub, w przypadku naprawy sprzętu poza Urzędem Miasta, kopiuje dane osobowe i przekazuje sprzęt do naprawy dopiero po trwałym usunięciu danych z nośników.

7. Realizacja ewidencji wpisów i udostępnień danych

Realizację ewidencji spisów i udostępnień danych osobowych przedstawia następująca tabela.

System	Pierwszy wpis[1]	Identyfikator[2]	Źródło[3]	Udostępnianie[4]	Sprzeciw[5]	Raport[6]
Sygnity USCwin	System zapisuje automatycznie	System zapisuje automatycznie	System pozwala operatorowi wprowadzić wymagane informacje	System pozwala operatorowi wprowadzić wymagane informacje	System pozwala operatorowi wprowadzić wymagane informacje	System pozwala sporządzić raport
ARAM Ewidencja Ludności	System zapisuje automatycznie	System zapisuje automatycznie	System pozwala operatorowi wprowadzić wymagane informacje	System pozwala operatorowi wprowadzić wymagane informacje	System pozwala operatorowi wprowadzić wymagane informacje	System pozwala sporządzić raport
EGB 2000	System zapisuje automatycznie	System zapisuje automatycznie	System pozwala operatorowi wprowadzić wymagane informacje	System pozwala operatorowi wprowadzić wymagane informacje	System pozwala operatorowi wprowadzić wymagane informacje	System pozwala sporządzić raport
Geo Kataster	System zapisuje automatycznie	System zapisuje automatycznie	System pozwala operatorowi wprowadzić wymagane informacje	System pozwala operatorowi wprowadzić wymagane informacje	System pozwala operatorowi wprowadzić wymagane informacje	System pozwala sporządzić raport

System	Pierwszy wpis[1]	Identyfikator[2]	Źródło[3]	Udostępnianie[4]	Sprzeciw[5]	Raport[6]
TenSoft Dodatki Mieszkaniowe	System zapisuje automatycznie	System zapisuje automatycznie	System pozwala operatorowi wprowadzić wymagane informacje	System pozwala operatorowi wprowadzić wymagane informacje	System pozwala operatorowi wprowadzić wymagane informacje	System pozwala sporządzić raport
SIGID	System zapisuje automatycznie	System zapisuje automatycznie	System pozwala operatorowi wprowadzić wymagane informacje	System pozwala operatorowi wprowadzić wymagane informacje	System pozwala operatorowi wprowadzić wymagane informacje	System pozwala sporządzić raport
Dowody osobiste	bd.	bd.	bd.	bd.	bd.	bd.
Ewidencja pojazdów i kierowców	bd.	bd.	bd.	bd.	bd.	bd.
Macrosoft Xpertis	System zapisuje automatycznie	System zapisuje automatycznie	System pozwala operatorowi wprowadzić wymagane informacje	System pozwala operatorowi wprowadzić wymagane informacje	System pozwala operatorowi wprowadzić wymagane informacje	System pozwala sporządzić raport
Macrosoft Xpertis ZZL	System zapisuje automatycznie	System zapisuje automatycznie	System pozwala operatorowi wprowadzić wymagane informacje	System pozwala operatorowi wprowadzić wymagane informacje	System pozwala operatorowi wprowadzić wymagane informacje	System pozwala sporządzić raport
Płatnik	bd.	bd.	bd.	bd.	bd.	bd.
Obsługa Obrony Cywilnej	Dopuszczalny tylko jeden użytkownik	Dopuszczalny tylko jeden użytkownik	Dopuszczalny tylko jeden użytkownik	Dopuszczalny tylko jeden użytkownik	Dopuszczalny tylko jeden użytkownik	Dopuszczalny tylko jeden użytkownik
Opłaty za użytkowanie wieczyste	Dopuszczalny tylko jeden użytkownik	System zapisuje automatycznie	System pozwala operatorowi wprowadzić wymagane informacje	System pozwala operatorowi wprowadzić wymagane informacje	System pozwala operatorowi wprowadzić wymagane informacje	System pozwala sporządzić raport
Wykaz umów na odbiór odpadów komunalnych	System zapisuje automatycznie	System zapisuje automatycznie	System pozwala operatorowi wprowadzić wymagane informacje	System pozwala operatorowi wprowadzić wymagane informacje	System pozwala operatorowi wprowadzić wymagane informacje	System pozwala sporządzić raport
VULCAN – Kadry/Arkusz Optivum	System zapisuje automatycznie	System zapisuje automatycznie	System pozwala operatorowi wprowadzić wymagane informacje	System pozwala operatorowi wprowadzić wymagane informacje	System pozwala operatorowi wprowadzić wymagane informacje	System pozwala sporządzić raport
Opłaty Parkingowe	System zapisuje automatycznie	System zapisuje automatycznie	System pozwala operatorowi wprowadzić wymagane informacje	System pozwala operatorowi wprowadzić wymagane informacje	System pozwala operatorowi wprowadzić wymagane informacje	System pozwala sporządzić raport
ESOD	System zapisuje automatycznie	System zapisuje automatycznie	System pozwala operatorowi wprowadzić wymagane informacje	System pozwala operatorowi wprowadzić wymagane informacje	System pozwala operatorowi wprowadzić wymagane informacje	System pozwala sporządzić raport

[1] Data pierwszego wprowadzenia danych osobowych do zbioru.

[2] Identyfikator osoby wprowadzającej te dane.

[3] Źródło danych (w przypadku pozyskania nie od osoby, której te dane dotyczą).

[4] Informacja o udostępnieniu danych osobowych.

[5] Sprzeciw dotyczący przetwarzania danych osobowych.

[6] Możliwość wydrukowania raportu.

8. Postępowanie w przypadku wystąpienia przez osobę o udzielenie informacji dotyczącej przetwarzania jej danych osobowych

8.1. Osobom, których dane są przetwarzane, przysługuje prawo do kontroli przetwarzania danych. W przypadku wystąpienia o udzielenie informacji o przetwarzaniu danych, pracownicy są zobowiązani skierować osobę do Opiekuna Zbioru.

8.2. Opiekun zbioru w ciągu 30 dni od otrzymania żądania raportu (wpłynięcia wniosku określonego w pkt. 8.1) od osoby sporządza raport i przekazuje go wnioskodawcy pocztą listem poleconym.

8.3. W raporcie zawarte są następujące informacje:

a) adres, siedziba i pełna nazwa Urzędu,
b) cel przetwarzania zbioru,
c) data pierwszego wprowadzenia danych do zbioru i identyfikator użytkownika wprowadzającego te dane,
d) jeżeli dane nie były zebrane od osoby, której dotyczą – informacje o źródle danych,
e) informacje o udostępnianiu danych innym podmiotom.

8.4. Systemy informatyczne powinny posiadać możliwość wydrukowania raportu z przetwarzania danych osobowych, zawierającego informacje z punktów c, d i e pkt. 8.3.

9. Procedury przeglądów systemów informatycznych

9.1. Dwa razy do roku, co 6 miesięcy przeglądowi podlegają wszystkie systemy informatyczne, przetwarzające dane osobowe w Urzędzie Miasta oraz zabezpieczenia fizyczne.

9.2. Administrator Bezpieczeństwa Informacji wraz z pracownikami Referatu Informatyki przygotowuje plan przeglądu, uwzględniając jego zakres oraz potrzebne zasoby fizyczne, czasowe i osobowe.

9.3. Przeglądowi podlega warstwa sprzętowa, systemy operacyjne oraz aplikacje, a także realizacja zabezpieczeń przez pracowników Urzędu.

9.4. Administrator Bezpieczeństwa Informacji przygotowuje raport z przeprowadzonego przeglądu, informując na jego podstawie Sekretarza Miasta o konieczności podjęcia właściwych działań korygujących i doskonalących.

9.5. Zakres przeglądu systemów informatycznych powinien obejmować co najmniej:

a) zgodność z wymaganiami prawnymi w zakresie przetwarzania danych osobowych,

b) sprawność warstwy sprzętowej do realizacji wszystkich funkcji, niezbędnych z punktu widzenia wykonywanych działań,

c) poprawność funkcjonowania systemu operacyjnego (m.in. analiza dzienników zdarzeń) oraz poprawność konfiguracji pod względem wydajnościowym, jak i zapewnienia bezpieczeństwa,

d) poprawność funkcjonowania aplikacji przetwarzających dane osobowe,

e) zgodność liczby użytkowników i ich uprawnień ze stanem oczekiwanym,

f) funkcjonowanie zabezpieczeń systemu informatycznego ze względu na potencjalne zagrożenia (np. brak zasilania, atak wirusowy, itp.).

10. Terminologia

Administrator Bezpieczeństwa Informacji - ABI – osoba nadzorująca przestrzeganie stosowania środków technicznych i organizacyjnych, zapewniających ochronę przetwarzanych danych osobowych. W Urzędzie Miasta Jelenia Góra funkcję tę pełni Kierownik Referatu Informatyki.

Administrator Danych Osobowych– administratorem danych jest Urząd Miasta Jelenia Góra, Plac Ratuszowy 58, Jelenia Góra, reprezentowany przez Prezydenta Miasta.

Administrator systemu - informatyk zajmujący się zarządzaniem systemem informatycznym i odpowiadający za jego sprawne działanie a także kontrolę uprawnień i administrowanie użytkownikami.

Dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.

Opiekun zbioru – Naczelnik/Kierownik komórki organizacyjnej, która tworzy i bezpośrednio pracuje na danym zbiorze danych osobowych.

System informatyczny - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

Użytkownik systemu informatycznego – osoba wykorzystująca system informatyczny w bieżącej pracy.

Zapora sieciowa – urządzenie komputerowe zabezpieczające sieć komputerową przed nieautoryzowanym dostępem z Internetu.

Zbiór danych osobowych – posiadający strukturę zestaw danych o charakterze osobowym.

Złośliwe oprogramowanie – oprogramowanie, którego celem jest uzyskanie nieuprawnionego dostępu do danych, na przykład wirusy, oprogramowanie szpiegujące działania użytkownika, itp.

11. Dokumenty związane

„Polityka bezpieczeństwa danych osobowych"

„Instrukcja przetwarzania danych osobowych"