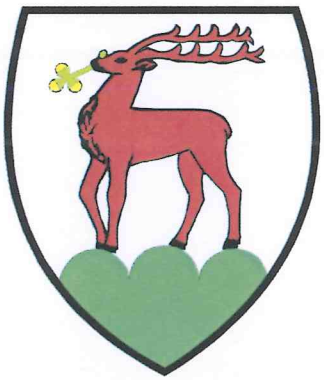
Załącznik Nr 2
do Zarządzenia Nr 0050.729 .2012.VI
Prezydenta Miasta Jeleniej Góry
z dnia 15 maja 2012r.

Urząd Miasta Jelenia Góra



INSTRUKCJA PRZETWARZANIA DANYCH OSOBOWYCH

	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 2002r., 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 3
2. Zakres stosowania 3
3. Zasady przetwarzania danych osobowych 3
4. Instrukcje rozpoczynania i kończenia pracy w systemach informatycznych przetwarzających dane osobowe 4
5. Zasady bezpieczeństwa przetwarzania danych 8
6. Procedura postępowania w przypadku naruszenia bezpieczeństwa danych osobowych 9
7. Terminologia 10
8. Dokumenty związane 11

1. Cel

Celem instrukcji przetwarzania danych osobowych jest określenie zasad bezpiecznego przetwarzania danych osobowych w Urzędzie Miasta Jelenia Góra.

2. Zakres stosowania

Instrukcja dotyczy zasad przetwarzania zbiorów danych osobowych w Urzędzie Miasta, zarówno w systemach informatycznych, jak i w zbiorach tradycyjnych.
Do stosowania instrukcji zobowiązani są wszyscy pracownicy Urzędu Miasta Jelenia Góra.

3. Zasady przetwarzania danych osobowych

3.1. Przetwarzanie danych osobowych przez pracownika jest dopuszczalne wyłącznie po uzyskaniu upoważnienia do przetwarzania danych osobowych. O upoważnienie występuje Naczelnik Wydziału lub osoba zatrudniona na samodzielnym stanowisku pracy. Stosowne uprawnienia na tych samych zasadach muszą uzyskać także osoby zatrudnione na umowę na zastępstwo. Wniosek o upoważnienie do przetwarzania danych osobowych stanowi wzór nr 1, stanowiący załącznik do „Polityki bezpieczeństwa danych osobowych".

3.2. Administrator Bezpieczeństwa Informacji wystawia Upoważnienie wg wzoru nr 2, stanowiącego załącznik do „Polityki Bezpieczeństwa Danych Osobowych", które sygnuje Administrator Danych Osobowych i przekazuje jeden egzemplarz pracownikowi, natomiast drugi przechowuje we własnej dokumentacji.

3.3. Pracownik korzystający z zasobów systemu informatycznego powinien być jednoznacznie identyfikowany poprzez indywidualny identyfikator (nazwę) użytkownika systemu. Niedopuszczalne jest korzystanie z tego samego identyfikatora przez więcej niż jednego pracownika.

3.4. Odebranie uprawnień dostępu do systemów informatycznych następuje na wniosek Naczelnika/Kierownika komórki organizacyjnej, zgłoszony na formularzu 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. Instrukcje rozpoczynania i kończenia pracy w systemach informatycznych przetwarzających dane osobowe

Aby rozpocząć i zakończyć pracę w systemie informatycznym przetwarzającym dane osobowe, należy postępować zgodnie z niniejszą instrukcją. W szczególności zabronione jest kończenie pracy przez odłączenie zasilania komputera.

4.1. Sygnity USCwin

Wejście do aplikacji

Wejście do aplikacji polega na wprowadzeniu identyfikatora użytkownika oraz hasła.

Wyjście z aplikacji

Wyjście z aplikacji polega na wybraniu z menu programu polecenia „Wyloguj" oraz potwierdzeniu wylogowania z aplikacji.

4.2. ARAM Ewidencja Ludności

Wejście do aplikacji

Wejście do aplikacji polega na wprowadzeniu identyfikatora użytkownika oraz hasła.

Wyjście z aplikacji

Wyjście z aplikacji polega na wybraniu z menu programu polecenia „Wyloguj" oraz potwierdzeniu wylogowania z aplikacji.

4.3. EGB 2000

Wejście do aplikacji

Wejście do aplikacji polega na wprowadzeniu identyfikatora użytkownika oraz hasła.

Wyjście z aplikacji

Wyjście z aplikacji polega na wybraniu z menu programu polecenia „Wyloguj" oraz potwierdzeniu wylogowania z aplikacji.

4.4. GeoKataster

Wejście do aplikacji

Wejście do aplikacji polega na wprowadzeniu identyfikatora użytkownika oraz hasła.

Wyjście z aplikacji

Wyjście z aplikacji polega na wybraniu z menu programu polecenia „Wyloguj" oraz potwierdzeniu wylogowania z aplikacji.

4.5. TenSoft Dodatki Mieszkaniowe

Wejście do aplikacji

Wejście do aplikacji polega na wprowadzeniu identyfikatora użytkownika oraz hasła.

Wyjście z aplikacji

Wyjście z aplikacji polega na wybraniu z menu programu polecenia „Wyloguj" oraz potwierdzeniu wylogowania z aplikacji.

4.6. Sigid

Wejście do aplikacji

Wejście do aplikacji polega na wprowadzeniu identyfikatora użytkownika oraz hasła.

Wyjście z aplikacji

Wyjście z aplikacji polega na wybraniu z menu programu polecenia „Wyloguj" oraz potwierdzeniu wylogowania z aplikacji.

4.7. Dowody osobiste

Wejście do aplikacji

Wejście do aplikacji następuje przez umieszczenie karty chipowej w czytniku, uruchomienie programu, wprowadzenie numeru PESEL posiadacza karty chipowej oraz podanie hasła użytkownika.

Wyjście z aplikacji

Wyjście z aplikacji polega na usunięciu karty chipowej z czytnika.

4.8. Ewidencja pojazdów i kierowców

Wejście do aplikacji

Wejście do aplikacji polega na umieszczeniu karty chipowej w czytniku i podanie osobistego numeru identyfikacyjnego PIN.

Wyjście z aplikacji

Wyjście z aplikacji polega na wybraniu polecenia „Wyloguj" z menu programu.

4.9. Macrosoft Xpertis

Wejście do aplikacji

Wejście do aplikacji polega na wprowadzeniu identyfikatora użytkownika oraz hasła.

Wyjście z aplikacji

Wyjście z aplikacji polega na wybraniu z menu programu polecenia „Wyloguj" oraz potwierdzeniu wylogowania z aplikacji.

4.10. Microsoft Xpertis ZZL

Wejście do aplikacji

Wejście do aplikacji polega na wprowadzeniu identyfikatora użytkownika oraz hasła.

Wyjście z aplikacji

Wyjście z aplikacji polega na wybraniu z menu programu polecenia „Wyloguj" oraz potwierdzeniu wylogowania z aplikacji.

4.11. Płatnik

Wejście do aplikacji

Wejście do aplikacji polega na wprowadzeniu identyfikatora użytkownika oraz hasła.

Wyjście z aplikacji

Wyjście z aplikacji następuje przez wybranie polecenia „Wyjście" z menu głównego aplikacji.

4.12. Świadczenia

Wejście do aplikacji

Wejście do aplikacji polega na wprowadzeniu identyfikatora użytkownika oraz hasła.

Wyjście z aplikacji

Wyjście z aplikacji polega na wybraniu z menu programu polecenia „Wyloguj" oraz potwierdzeniu wylogowania z aplikacji.

4.13. Obsługa Obrony Cywilnej

Wejście do aplikacji

Rozpoczęcie pracy polega na wyjęciu komputera z szafy pancernej i podaniu loginu i hasła.

Wyjście z aplikacji

Wyjście polega na wylogowaniu się z komputera i schowaniu go w szafie pancernej.

4.14. Opłaty za użytkowanie wieczyste

Wejście do aplikacji

Wejście do aplikacji polega na wprowadzeniu identyfikatora użytkownika oraz hasła.

Wyjście z aplikacji

Wyjście z aplikacji polega na wybraniu z menu programu polecenia „Wyloguj" oraz potwierdzeniu wylogowania z aplikacji.

4.15. Wykaz umów na odbiór odpadów komunalnych

Wejście do aplikacji

Wejście do aplikacji polega na wprowadzeniu identyfikatora użytkownika oraz hasła.

Wyjście z aplikacji

Wyjście z aplikacji polega na wybraniu z menu programu polecenia „Zakończ" oraz potwierdzeniu zakończenia pracy aplikacji.

4.16. Vulcan zarządzanie Oświatą – Arkusz i Kadry

Wejście do aplikacji

Wejście do aplikacji polega na wprowadzeniu identyfikatora użytkownika oraz hasła.

Wyjście z aplikacji

Wyjście z aplikacji polega na wybraniu z menu programu polecenia „Zakończ" oraz potwierdzeniu zakończenia pracy aplikacji.

4.17. Opłaty Parkingowe

Wejście do aplikacji

Wejście do aplikacji polega na wprowadzeniu identyfikatora użytkownika oraz hasła.

Wyjście z aplikacji

Wyjście z aplikacji polega na wybraniu z menu programu polecenia „Zakończ" oraz potwierdzeniu zakończenia pracy aplikacji.

4.18. ESOD – Wasko Intra Dok

Wejście do aplikacji

Wejście do aplikacji polega na wprowadzeniu identyfikatora użytkownika oraz hasła.

Wyjście z aplikacji

Wyjście z aplikacji polega na wybraniu z menu programu polecenia „Wyloguj".

5. Zasady bezpieczeństwa przetwarzania danych

5.1. Ochrona zbiorów danych polega na zabezpieczeniu informacji wprowadzonej, przetwarzanej, przesyłanej w systemie informatycznym oraz na nośnikach informacji przed nielegalnym ujawnieniem, kradzieżą oraz nieuprawnioną modyfikacją lub usunięciem.

5.2. W celu ochrony danych, przetwarzanych w systemach informatycznych, należy stosować wchodzące w ich skład mechanizmy zarówno sprzętowe (techniczne?) jak i programowe oraz inne rozwiązania, zwiększające bezpieczeństwo danych.

5.3. Użytkownik komputera, któremu został przydzielony sprzęt, jest bezpośrednio odpowiedzialny za bezpieczeństwo i dostęp do komputera oraz za prawidłową eksploatację systemu.

5.4. Przemieszczanie elektronicznych nośników danych (w tym komputerów przenośnych), zawierających dane osobowe, poza pomieszczenia, w których są przetwarzane, wymaga stosowania środków ochrony, gwarantujących ich zabezpieczenie przed nieuprawnionym dostępem.

5.5. Na nośnikach służących do wymiany danych (np. pendrive) nie wolno przechowywać danych osobowych dłużej niż jest to konieczne do przeniesienia tych danych, po ich przeniesieniu należy dane z nośnika bezwzględnie skasować.

5.6. Nośniki danych, które były wykorzystywane do przenoszenia przechowywania danych osobowych nie mogą być wykorzystywane poza tym Wydziałem, w którym dane były przetwarzane, bez wcześniejszego odpowiedniego ich przygotowania tj. trwałego usunięcia danych.

5.7. Wszystkie wydruki z danymi osobowymi i ich kopie należy niszczyć w niszczarkach do papieru lub przekazywać do WIiOT do przekazania firmie niszczącej dokumenty. Usuwanie wydruków lub ich kopii przez wyrzucenie ich do kosza na odpady komunalne jest zabronione.

5.8. Ostatnia osoba opuszczająca pomieszczenie, w którym przetwarzane są dane osobowe, ma obowiązek zamknięcia pomieszczenia na klucz. Dotyczy to także opuszczania pomieszczenia w godzinach pracy.

5.9. Przekazywanie hasła dostępu do systemu informatycznego innym osobom jest zabronione.

5.10. Początkowe hasło użytkownika w systemie informatycznym jest ustalane przez administratora systemu i przekazywane użytkownikowi ustnie. Użytkownik jest zobowiązany do

bezzwłocznej zmiany hasła, przy pierwszym zalogowaniu się do systemu, o ile system ma taką funkcjonalność. Przekazywanie hasła za pośrednictwem innej osoby lub za pomocą poczty elektronicznej jest zabronione.

5.11. Użytkownicy są zobowiązani do przestrzegania zasad polityki haseł odnośnie złożoności, długości i wieku hasła, określonych w pkt. 8.7 „Polityki bezpieczeństwa danych osobowych".

5.12. Dostęp do systemu informatycznego powinien być nawiązywany tylko w godzinach pracy Urzędu. Konieczność uzyskania dostępu do systemu informatycznego poza ustalonymi godzinami pracy należy zgłosić do Naczelnika Wydziału Informatyki i Obsługi Technicznej, zgodnie z procedurą występowania o pracę w godzinach nadliczbowych.

5.13. Osobom, których dane są przetwarzane, przysługuje prawo do kontroli danych, a w szczególności do ich aktualizacji oraz otrzymania raportu o przetwarzaniu danych. Osobę, która zwróciła się z wnioskiem o wydanie raportu o przetwarzaniu danych, należy skierować do opiekuna zbioru. Lista opiekunów zbiorów została zapisana w „Polityce bezpieczeństwa danych osobowych" (pkt 4).

5.14. Zabrania się udostępniania nośników danych osobowych osobom nieuprawnionym.

5.15. W przypadku podejrzenia lub stwierdzenia naruszenia zasad bezpieczeństwa danych osobowych, pracownik zobowiązany jest powiadomić Administratora Bezpieczeństwa Informacji, który analizuje sytuację, okoliczności i przyczyny, które doprowadziły do naruszenia bezpieczeństwa danych (jeśli takie wystąpiło), a następnie przedstawia Administratorowi Danych Osobowych odpowiednie propozycje zmian do instrukcji zarządzania systemem informatycznym, które zapewnią bezpieczeństwo danych, a w razie potrzeby informuje organa ścigania o podejrzeniu popełnienia przestępstwa.

6. Procedura postępowania w przypadku naruszenia bezpieczeństwa danych osobowych

6.1. Każdy pracownik w przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych, polegających m. in. na:

a. włamaniu się osób nieuprawnionych do pokoju wchodzącego w skład obszaru przetwarzania danych osobowych,
b. próbie włamania się do systemu informatycznego,
c. stwierdzenia wszelkiego rodzaju różnic w funkcjonowaniu systemu lub programu,
d. stwierdzeniu różnic w zawartości zbiorów,
e. włączeniu sprzętu komputerowego poza wyznaczonymi godzinami pracy,
f. kradzieży sprzętu komputerowego, nośników danych lub wydruków,

zobowiązany jest natychmiast zgłosić ten fakt Administratorowi Bezpieczeństwa Informacji.

6.2. Administrator Bezpieczeństwa Informacji po przyjęciu zgłoszenia w sprawie naruszenia ochrony danych:

a. powiadamia Administratora Danych o zaistniałym zdarzeniu,
b. zabezpiecza ślady nieprawidłowych działań,
c. ocenia zakres oraz rodzaj naruszenia bezpieczeństwa zbiorów danych,
d. określa przyczyny oraz skutki naruszenia bezpieczeństwa zbiorów,
e. ustala, z którego stanowiska nastąpiło włamanie i czy użytkownik pracujący przy stanowisku, z którego nastąpiło włamanie, dostatecznie zabezpieczył stanowisko pracy przed wyłączeniem komputera,
f. określa działania i środki, jakie należy podjąć w celu przywrócenia systemu do poprawnego funkcjonowania oraz przybliżony czasu odtworzenia,
g. określa działania i środki jakie należy podjąć w celu uniemożliwienia naruszenia ochrony zbiorów danych osobowych w przyszłości,
h. sporządza szczegółowy raport z przeprowadzonego postępowania.

6.3. Administrator Danych po otrzymaniu zgłoszenia od Administratora Bezpieczeństwa Informacji decyduje o powiadomieniu organów ścigania o podejrzeniu popełnienia przestępstwa.

W przypadku:

a. zaniedbania zabezpieczenia zbiorów danych osobowych,
b. utrudniania i uniemożliwiania wykrycia naruszenia zabezpieczenia baz danych

Administrator Danych Osobowych stosuje środki dyscyplinarne.

7. Terminologia

Administrator Bezpieczeństwa Informacji - ABI – oznacza osobę 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 za 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.

8. Dokumenty związane

„Polityka bezpieczeństwa danych osobowych"

„Instrukcja zarządzania systemami informatycznymi przetwarzającymi dane osobowe."