**Zarządzenie Nr ..105/2011**
**Burmistrza Miasta Sanoka**
**z dnia 16 sierpnia 2011**
**w sprawie Polityki Bezpieczeństwa w Urzędzie Miasta w Sanoku.**

Na podstawie art. 31 ustawy z dnia 8 marca 1990r. o samorządzie gminnym (jedn. tekst Dz. U. z 2001r. Nr 142 poz. 1591r. z późn. zm.) oraz Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. 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)

**z a r z ą d z a m**

**co następuje;**

§ 1

W celu jednolitego sposobu prowadzenia i zakresu dokumentacji dotyczącej przetwarzania danych osobowych – wprowadzam Politykę Bezpieczeństwa – stanowiącą załącznik Nr 1 do zarządzenia.

§ 2

Dla określenia środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych osobowych – ustalam Instrukcję Zarządzania Systemami Informatycznymi – stanowiąca załącznik Nr 2 do zarządzenia.

§ 3

W celu realizacji wprowadzonej Polityki Bezpieczeństwa oraz ustalonej Instrukcji Zarządzania Systemami Informatycznymi wyznaczam na;
1) Administratora Bezpieczeństwa Informacji - Pana Gerarda Szydłaka
2) Administratora Systemu Informatycznego - Pana Macieja Dygonia

§ 4

Traci moc Zarządzenie Nr 86/99 Burmistrza Miasta Sanoka z dnia 29.10.1999r. w sprawie określenia warunków organizacyjnych i technicznych gromadzenia, przechowywania i przetwarzania informacji niejawnych.

§ 5

Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ
mgr Wojciech Blecharczyk

RADCA PRAWNY
mgr Alicja Filip

12-08-2011

*Załącznik Nr 1*
*do Zarządzenia Nr 105/2011 BMS*
*z dnia 16 sierpnia 2011r.*

# Polityka bezpieczeństwa

**Gmina Miasta Sanok**
**ul. Rynek 1**
**38-500 Sanok**

## Spis treści:

## 1. Definicje

- Zbiór danych osobowych - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

- Administrator danych osobowych - zadania administratora danych osobowych wykonuje Burmistrz Gminy Miasta Sanoka.

- Administrator bezpieczeństwa informacji - osoba wyznaczona przez administratora danych osobowych, odpowiedzialna za bezpieczeństwo danych osobowych przetwarzanych we wskazanych systemach informatycznych.

- Administrator systemu informatycznego - osoba odpowiedzialna za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego do przetwarzania danych osobowych w Gminie Miasta Sanoka (UM), (może to być administrator sieci lokalnej, systemu operacyjnego, bazy danych itp.).

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

- Stacja robocza – stacjonarny lub przenośny komputer wchodzący w skład systemu informatycznego umożliwiający użytkownikom systemu dostęp do danych osobowych znajdujących się w systemie.

- Bezpieczeństwo systemu informatycznego - wdrożenie przez administratora danych osobowych lub osobę przez niego uprawnioną środków organizacyjnych i technicznych w celu zabezpieczenia oraz ochrony danych przed dostępem, modyfikacją, ujawnieniem, pozyskaniem lub zniszczeniem.

- Przetwarzanie danych osobowych - wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie.

- Osoba upoważniona - osoba posiadająca upoważnienie wydane przez administratora danych osobowych (lub osobę uprawnioną przez niego) i dopuszczona jako użytkownik do przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej w zakresie wskazanym w upoważnieniu.

- Użytkownik systemu - osoba posiadająca uprawnienia do przetwarzania danych osobowych w systemie informatycznym.

- Osoba uprawniona - osoba posiadająca upoważnienie wydane przez administratora danych osobowych do wykonywania w jego imieniu określonych czynności.

- Ustawa – ustawa z dnia 29 sierpnia 1997 r. o ochronie danych (Dz. U. z 2002 r. Nr 101, poz. 926, z pózn. zm.)

- Rozporządzenie - 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.

## 2. Zasady ogólne

- Ochrona danych osobowych przetwarzanych w Urzędzie Miasta obowiązuje wszystkie osoby, które mają dostęp do informacji zbieranych, przetwarzanych oraz przechowywanych w UM, bez względu na zajmowane stanowisko, oraz miejsce wykonywania jak również charakter stosunku pracy.
- Osoby mające dostęp do danych osobowych są zobligowane do stosowania niezbędnych środków zapobiegających ujawnieniu tych danych osobom nieupoważnionym.
- Zachowanie tajemnicy obowiązuje zarówno podczas trwania stosunku pracy jak i po jego ustaniu.
- Burmistrz Miasta jest odpowiedzialny za tworzenie, wdrażanie, administrację i interpretację polityki bezpieczeństwa informacji, standardów, zaleceń oraz procedur w pełnym zakresie systemu przetwarzania danych osobowych w UM.
- Polecenia osób delegowanych wyznaczonych przez Burmistrza Miasta do działań związanych z ochroną w zakresie ochrony informacji i bezpieczeństwa systemu informatycznego muszą być bezwzględnie wykonywane przez wszystkich pracowników i użytkowników systemu.

## 3. Zabezpieczenie dostępu do danych osobowych

Przetwarzanie danych osobowych może odbywać się wyłącznie w obszarach do tego celu przeznaczonych. Wykaz pomieszczeń, w których dopuszczalne jest przetwarzanie danych osobowych stanowi **załącznik nr 1** do niniejszej instrukcji.

W szczególnych przypadkach możliwe jest przetwarzanie danych osobowych poza wyznaczonym obszarem (np. na komputerach przenośnych) jednak wymaga to zgody indywidualnej administratora bezpieczeństwa informacji. Szczegółowe zasady przetwarzania danych osobowych na komputerach przenośnych opisano w punkcie 9 niniejszej instrukcji.

Dostęp do pomieszczeń, w których przetwarzane są dane osobowe oraz do pomieszczeń, w których znajdują się serwery baz danych lub przechowywane są kopie zapasowe mogą mieć wyłącznie osoby, które posiadają do tego upoważnienie.

Przetwarzać dane osobowe może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych.

Wydanie upoważnienia następuje na wniosek przełożonego pracownika, który otrzymuje upoważnienie. Wniosek o wydanie upoważnienia składany jest w formie pisemnej do Administratora bezpieczeństwa.

Szczegółowe zasady sposobu składania wniosku zawiera **„Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danychosobowych".**

## 4. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.

Aktualny wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych stanowi **załącznik nr 2** do niniejszej instrukcji.

Załącznik ten powinien być aktualizowany po wprowadzeniu do przetwarzania nowych zbiorów danych osobowych lub nowych programów, które je obsługują.

## 5. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi.

Aktualny opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi stanowi **załącznik nr 3** do niniejszej instrukcji.

W przypadku istnienia więcej niż jednego zbioru danych dla każdego zbioru powinien zostać sporządzony odrębny załącznik do niniejszego dokumentu opatrzony odpowiednio numerem 3a, 3b itd.

Każdy załącznik powinien być aktualizowany po wprowadzeniu istotnych zmian w strukturze bazy danych, którą opisuje. W przypadku systemów, które są rozbudowywane wprowadzone zmiany rejestruje się (aktualizując odpowiedni załącznik) nie rzadziej niż co 2 miesiące.

## 6. Sposób przepływu danych pomiędzy poszczególnymi systemami

Aktualny opis sposobu przepływu danych pomiędzy poszczególnymi systemami stanowi **załącznik nr 4** do niniejszej instrukcji..

W przypadku istnienia wymiany danych pomiędzy więcej niż dwoma zbiorami danych dla każdej pary zbiorów wymieniających dane powinien zostać sporządzony odrębny załącznik do niniejszego dokumentu opatrzony odpowiednio numerem 4a, 4b itd.

Każdy załącznik powinien być aktualizowany po wprowadzeniu istotnych zmian w sposobie lub zakresie wymiany danych, którą opisuje. W przypadku systemów, które są rozbudowywane wprowadzone zmiany rejestruje się (aktualizując odpowiedni załącznik) nie rzadziej niż co 2 miesiące.

## 7. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

*a) Zasady ogólne:*

- Przetwarzać dane osobowe w systemach informatycznych może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych. Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora (konto użytkownika) i właściwego hasła.
- Wykaz kont użytkowników jest w posiadaniu Administratora Systemu Informatycznego
- Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi. Użytkownik odpowiedzialny jest za wszystkie czynności wykonane przy użyciu identyfikatora, którym się posługuje lub posługiwał.
- 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.

*b) Środki organizacyjne*

- Wprowadzenie instrukcji dla pracowników zatrudnionych przy przetwarzaniu danych osobowych.
- Powołanie Administratora Bezpieczeństwa Informacji, Administratorów Systemu Informatycznego i/lub Administratorów Bazy Danych, odpowiedzialnych za działania organizacyjne i środki techniczne zapewniające odpowiedni poziom bezpieczeństwa danych osobowych.
- Prowadzenie ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych. Wykaz osób posiadających upoważnienia o których mowa prowadzony jest w Wydziale Organizacyjnym.
- wykaz identyfikatorów
- Kontrola dostępu do pomieszczeń, w których przetwarzane są dane osobowe oraz ścisła kontrola dostępu do pomieszczeń, w których znajdują się serwery.
- Zgodne z **„Instrukcją zarządzania systemem"** tworzenie kopii archiwalnych baz danych zawierających dane osobowe.
- Bardzo dokładne testowanie modyfikacji oprogramowania przed wdrożeniem go do użytku operacyjnego zarówno pod kątem poprawności działania jak i podatności na „ataki" z zewnątrz..

*c) Sposób postępowania w zakresie komunikacji w sieci komputerowej*

Dane osobowe są przesyłane w sieci informatycznej dedykowanej do obsługi systemu informatycznego przetwarzającego te dane (intranet). Sieć ta jest odseparowana od pozostałej infrastruktury teleinformatycznej poprzez fizyczne rozdzielenie infrastruktury ethernetowej.
Ponadto, cały ruch do sieci intranet przechodzi przez dedykowane urządzenie pełniące rolę zapory ogniowej (firewall) i skanera AV, gdzie jest filtrowany i translowany na lokalną klasę adresów. Dodatkowo serwery sieci lokalnej chronione są przez własne zapory ogniowe (firewall) uniemożliwiające nieautoryzowany dostęp do danych znajdujących się na tych serwerach.
Stacje robocze w dedykowanej sieci do obsługi danych osobowych znajdują się wewnątrz sieci niedostępnej z internetu.

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

- Zatwierdzenia w formie pisemnej lub w formie elektronicznej przez administratora bezpieczeństwa informacji celu wysłania danych osobowych,
- zastosowanie mechanizmów szyfrowania danych osobowych,

W przypadku stosowania mechanizmów kryptograficznych administrator bezpieczeństwa informacji określa wymagania w zakresie materiału kryptograficznego stosowanego do ochrony danych osobowych. Jeżeli nie określi on innych wymagań stosuje się:

- przy szyfrowaniu symetrycznym algorytm AES z kluczem 256 bitów,
- przy szyfrowaniu asymetrycznym algorytm RSA z kluczem 1024 bity,
- funkcję skrótu SHA-1.

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

W przypadku wystąpienia uzasadnionego podejrzenia przechwycenia kluczy kryptograficznych lub dostania się ich w niepowołane ręce pracownik zobowiązany jest poinformować o tym fakcie administratora bezpieczeństwa informacji lub osoby przez niego uprawnione zgodnie z wytycznymi opisanymi w rozdziale **„Zasady postępowania w przypadku naruszenia ochrony danych osobowych"**.

*d) Zasady postępowania w przypadku naruszenia ochrony danych osobowych*

Każdy pracownik biorący udział w przetwarzaniu danych osobowych w systemie informatycznym jest odpowiedzialny za bezpieczeństwo tych danych. W szczególności osoba, która zauważyła zdarzenie mogące być przyczyną naruszenia ochrony danych osobowych lub mogące spowodować naruszenie bezpieczeństwa danych, zobowiązana jest do natychmiastowego poinformowania administratora bezpieczeństwa informacji lub administratora systemu informatycznego.

O naruszeniu ochrony danych osobowych mogą świadczyć następujące symptomy:

- brak możliwości uruchomienia przez użytkownika aplikacji pozwalającej na dostęp do danych osobowych,
- brak możliwości zalogowania się do tej aplikacji,
- ograniczone, w stosunku do normalnej sytuacji, uprawnienia użytkownika w aplikacji (na przykład brak możliwości wykonania pewnych operacji normalnie dostępnych użytkownikowi) lub uprawnienia poszerzone w stosunku do normalnej sytuacji,
- inny wygląd lub działanie aplikacji niż zazwyczaj,
- inny zakres danych dostępny dla użytkownika – dużo więcej lub dużo mniej danych,
- znaczne spowolnienie działania systemu informatycznego,
- pojawienie się niestandardowych komunikatów generowanych przez system informatyczny,

- ślady włamania lub prób włamania do obszaru, w którym przetwarzane są dane osobowe,
- ślady włamania lub prób włamania do pomieszczeń, w których odbywa się przetwarzanie danych osobowych, w szczególności do serwerowni oraz do pomieszczeń, w których przechowywane są nośniki kopii zapasowych,
- włamanie lub próby włamania do szafek, w których przechowywane są – w postaci elektronicznej lub papierowej – nośniki danych osobowych,
- zagubienie bądź kradzież nośnika danych osobowych,
- zagubienie bądź kradzież nośnika materiału kryptograficznego (karty mikroprocesorowej, dyskietki itp.),
- kradzież sprzętu informatycznego, w którym przechowywane są dane osobowe,
- informacja z systemu antywirusowego o zainfekowaniu systemu informatycznego wirusami,
- fizyczne zniszczenie lub podejrzenie zniszczenia elementów systemu informatycznego przetwarzającego dane osobowe na skutek przypadkowych lub celowych działań albo zaistnienia działania siły wyższej,
- podejrzenie nieautoryzowanej modyfikacji danych osobowych przetwarzanych w systemie informatycznym.

W wypadku wystąpienia powyższych symptomów, jak również innych objawów, które zdaniem pracownika mogą wskazywać na zagrożenie bezpieczeństwa danych osobowych, należy natychmiast powiadomić administratora bezpieczeństwa informacji lub administratora systemu informatycznego. 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 administrator bezpieczeństwa informacji, jest ona zobowiązana poinformować o tym fakcie administratora bezpieczeństwa informacji.

Po otrzymaniu zgłoszenia o wystąpieniu symptomów wskazujących na możliwość zaistnienia w UM naruszenia bezpieczeństwa danych osobowych administrator bezpieczeństwa informacji, we współpracy z administratorem systemu informatycznego, jest zobowiązany do podjęcia kroków w celu:

- wyjaśnienia zdarzenia, a w szczególności czy miało miejsce naruszenie ochrony danych osobowych,
- wyjaśnienia przyczyn naruszenia bezpieczeństwa danych osobowych i zebranie ewentualnych dowodów, a w szczególności, gdy zdarzenie było związane z celowym działaniem pracownika bądź osób trzecich,
- zabezpieczenia systemu informatycznego przed dalszym rozprzestrzenianiem się zagrożenia,
- usunięcia skutków incydentu i przywróceniu pierwotnego stanu systemu informatycznego (to jest stanu sprzed incydentu).

Administrator bezpieczeństwa informacji we współpracy z administratorem systemu informatycznego podejmuje działania zmierzające do wyjaśnienia zgłoszonego zdarzenia:

- przeprowadzenia analizy poprawności funkcjonowania systemu informatycznego,
- przeprowadzenie analizy danych osobowych przetwarzanych w systemie informatycznym,

- zabezpieczenie danych przetwarzanych w systemie informatycznym, w szczególności danych konfiguracyjnych tego systemu.

Administrator bezpieczeństwa informacji określa na podstawie zebranych informacji przyczyny zaistnienia incydentu. Jeżeli incydent był spowodowany celowym działaniem, jest on zobowiązany do pisemnego powiadomienia administratora danych osobowych w UM, który może poinformować organy uprawnione do ścigania przestępstw o fakcie celowego naruszenia bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym.

System informatyczny, którego prawidłowe działanie zostało odtworzone powinien zostać poddany szczegółowej obserwacji w celu stwierdzenia całkowitego usunięcia symptomów incydentu. Administrator bezpieczeństwa informacji prowadzi ewidencję interwencji związanej z zaistniałymi incydentami w zakresie bezpieczeństwa danych osobowych. Ewidencja taka obejmuje następujące informacje:

- imię i nazwisko osoby zgłaszającej incydent,
- imię i nazwisko osoby przyjmującej zgłoszenie incydentu,
- datę zgłoszenia incydentu,
- przeprowadzone działania wyjaśniające przyczyny zaistnienia incydentu,
- wyniki przeprowadzonych działań,
- podjęte akcje naprawcze i ich skuteczność.

Administrator bezpieczeństwa informacji odpowiedzialny jest za przeprowadzenie przynajmniej raz w roku analizy zaistniałych incydentów w celu:

- określenia skuteczności podejmowanych działań wyjaśniających i naprawczych,
- określenie wymaganych działań zwiększających bezpieczeństwo systemu informatycznego i minimalizujących ryzyko zaistnienia incydentów,
- określenie potrzeb w zakresie szkoleń administratorów systemu i użytkowników systemu informatycznego przetwarzającego dane osobowe.

## 8. Zasady korzystania z komputerów przenośnych, na których są przetwarzane dane osobowe

Przetwarzanie danych osobowych na komputerach przenośnych powinno być ograniczone do niezbędnych przypadków. Przetwarzanie danych osobowych przy użyciu komputerów przenośnych może odbywać się wyłącznie za zgodą administratora danych osobowych w UM i za wiedzą administratora bezpieczeństwa informacji. Zakres danych przetwarzanych na komputerze przenośnym oraz zakres uprawnień do przetwarzanych danych ustala przełożony pracownika za wiedzą administratora bezpieczeństwa informacji.

Osoba korzystająca z komputera przenośnego w celu przetwarzania danych osobowych zobowiązana jest do zwrócenia szczególnej uwagi na zabezpieczenie przetwarzanych informacji, zwłaszcza przed dostępem do nich osób nieupoważnionych oraz przed zniszczeniem.
Użytkownik komputera przenośnego zobowiązany jest do:

- transportu komputera w sposób minimalizujący ryzyko kradzieży lub zniszczenia, a w szczególności:

- do transportowania komputera w bagażu podręcznym,
- do nie pozostawiania komputera w samochodzie, przechowalni bagażu, itp,

- zaleca się przenoszenie komputera w torbie przeznaczonej do przenoszenia komputerów przenośnych.
- 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,
- nie zezwalania osobom nieupoważnionym do korzystania z komputera przenośnego, na którym przetwarzane są dane osobowe,
- zabezpieczania komputera przenośnego hasłem,
- blokowania dostępu do komputera przenośnego w przypadku gdy nie jest on wykorzystywany przez pracownika,
- kopiowania danych osobowych przetwarzanych na komputerze przenośnym do systemu informatycznego w celu umożliwienia wykonania kopii awaryjnej tych danych,
- umożliwienia, poprzez podłączenie komputera do sieci informatycznej UM aktualizacji wzorców wirusów w programie antywirusowym,
- utrzymania konfiguracji oprogramowania systemowego w sposób wymuszający korzystanie z haseł,
- wykorzystywania haseł odpowiedniej jakości zgodnie z wytycznymi dotyczącymi tworzenia haseł w systemie informatycznym przetwarzającym dane osobowe,
- zmiany haseł zgodnie z wymaganiami dla systemu informatycznego przetwarzającego dane osobowe.

Administrator bezpieczeństwa informacji zobowiązany jest do podjęcia działań mających na celu zabezpieczenie komputerów przenośnych, w szczególności aby:

- dokonano konfiguracji oprogramowania na komputerach przenośnych w sposób wymuszający korzystanie z haseł, wykorzystywanie haseł odpowiedniej jakości zgodnie z wytycznymi dotyczącymi tworzenia haseł w systemie informatycznym przetwarzającym dane osobowe oraz wymuszającym okresową zmianę haseł zgodnie z wymaganiami dla systemu informatycznego przetwarzającego dane osobowe,
- zabezpieczono dane osobowe przetwarzane na komputerach przenośnych poprzez zastosowanie oprogramowania szyfrującego te dane. Dostęp do danych jest możliwy wyłącznie po podaniu tego hasła,
- dokonano instalacji i konfiguracji oprogramowania antywirusowego na komputerze przenośnym,
- przeprowadzono aktualizację wzorców wirusów zgodnie z zasadami zarządzania programem antywirusowym.

Administrator bezpieczeństwa informacji jest odpowiedzialny za prowadzenie ewidencji komputerów przenośnych wykorzystywanych do przetwarzania danych osobowych, w szczególności ewidencja obejmuje:

- typ i numer seryjny komputera przenośnego,
- imię i nazwisko osoby będącej użytkownikiem komputera,
- oprogramowanie zainstalowane na komputerze,
- rodzaj i zakres danych osobowych przetwarzanych na komputerze przenośnym.

W razie zgubienia lub kradzieży pracownik zobowiązany jest do natychmiastowego powiadomienia administratora bezpieczeństwa informacji lub osoby uprawnionej zgodnie z zasadami informowania o naruszeniu ochrony danych osobowych.

## 9. Przetwarzanie danych osobowych powierzonych UM przez inne podmioty.

Możliwe jest przetwarzanie danych osobowych w UM powierzonych przez inny podmiot (Zleceniodawcę). W takim przypadku, przetwarzanie danych osobowych odbywa się na podstawie umowy pomiędzy UM a Zleceniodawcą zawartej w formie pisemnej.

Umowa ta musi zawierać ściśle określony zakres przetwarzanych danych. Przetwarzanie danych możliwe jest tylko w ustalonym przez umowę zakresie.

Powierzone dane podlegają ochronie na takich samych zasadach jak dane będące własnością UM, chyba, że umowa określi inne zasady ochrony danych osobowych. W szczególności może dotyczyć to nadawania uprawnień do przetwarzania danych osobowych.

Dostęp do powierzonych danych osobowych z sieci zewnętrznej (np. siedziby Zleceniodawcy) musi odbywać się z zachowaniem odpowiednich zabezpieczeń. Dostęp do danych musi być chroniony identyfikatorem oraz hasłem, a połączenie sieciowe realizujące dostęp do danych musi być odpowiednio szyfrowane.

Załączniki wymienione w niniejszej instrukcji i wprowadzane w nich zmiany aktualizacyjne nie wymagają akceptacji w formie pisemnej, przez Administratora Danych Osobowych.

BURMISTRZ
mgr Wojciech Blecharczyk

*Załącznik Nr 2*
*do Zarządzenia Nr 105/2011 BMS*
*z dnia 16 sierpnia 2011r.*

# Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych



**Gmina Miasta Sanok**
**ul. Rynek 1**
**38-500 Sanok**

## Spis treści






**Gmina Miasta Sanok**
**ul. Rynek 1**
**38-500 Sanok**

## 1. Definicje

- **Zbiór danych osobowych** - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
- **Administrator danych osobowych** - zadania administratora danych osobowych wykonuje Burmistrz Gminy Miasta Sanoka.
- **Administrator bezpieczeństwa informacji** - osoba wyznaczona przez administratora danych osobowych, odpowiedzialna za bezpieczeństwo danych osobowych przetwarzanych we wskazanych systemach informatycznych.
- **Administrator systemu informatycznego** - osoba odpowiedzialna za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego do przetwarzania danych osobowych w UM (może to być administrator sieci lokalnej, systemu operacyjnego, bazy danych itp.).
- **System informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
- Stacja robocza – stacjonarny lub przenośny komputer wchodzący w skład systemu informatycznego umożliwiający użytkownikom systemu dostęp do danych osobowych znajdujących się w systemie.
- **Bezpieczeństwo systemu informatycznego** - wdrożenie przez administratora danych osobowych lub osobę przez niego uprawnioną środków organizacyjnych i technicznych w celu zabezpieczenia oraz ochrony danych przed dostępem, modyfikacją, ujawnieniem, pozyskaniem lub zniszczeniem.
- **Przetwarzanie danych osobowych** - wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie.
- **Osoba upoważniona** - osoba posiadająca upoważnienie wydane przez administratora danych osobowych (lub osobę uprawnioną przez niego) i dopuszczona jako użytkownik do przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej w zakresie wskazanym w upoważnieniu (listę osób upoważnionych do przetwarzania danych osobowych posiada administrator bezpieczeństwa informacji).
- **Użytkownik systemu** - osoba posiadająca uprawnienia do przetwarzania danych osobowych w systemie informatycznym.
- **Osoba uprawniona** - osoba posiadająca upoważnienie wydane przez administratora danych osobowych do wykonywania w jego imieniu określonych czynności.
- **Ustawa** – ustawa z dnia 29 sierpnia 1997 r. o ochronie danych.
- **Rozporządzenie** - 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.

## 2. Informacje ogólne

Niniejsza instrukcja dotyczy każdego zbioru danych osobowych przetwarzanego w UM zarówno w formie elektronicznej jak i papierowej.

Aktualny wykaz przetwarzanych zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, ich lokalizacją i sposobem dostępu znajduje się w **załączniku nr 2** do dokumentu **„Polityka bezpieczeństwa"**.

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

Przetwarzać dane osobowe w systemach informatycznych może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych (wzór upoważnienia stanowi **załącznik nr 1** do niniejszej instrukcji).

Wydanie upoważnienia oraz rejestracja użytkownika systemu informatycznego przetwarzającego dane osobowe następuje na wniosek przełożonego użytkownika lub koordynatora zadania, na rzecz którego będą wykonywane czynności związane z przetwarzaniem danych osobowych.

W formie pisemnej składa on wniosek do Administratora Bezpieczeństwa Informacji odpowiedniego dla zakresu danych o wydanie upoważnienia do przetwarzania danych osobowych. Wniosek ten powinien zawierać:

- imię i nazwisko pracownika, któremu upoważnienie zostanie nadane,
- nazwę zbioru danych osobowych oraz nazwę systemu informatycznego, do którego użytkownik będzie miał dostęp,
- zakres upoważnienia do przetwarzania danych osobowych,
- datę, z jaką upoważnienie ma być nadane,
- okres ważności upoważnienia.

Oryginał upoważnienia zostaje przekazany pracownikowi za potwierdzeniem odbioru, kopia zostaje dołączona do akt osobowych pracownika, ewidencji wydanych upoważnień oraz przekazana do wiadomości przełożonego pracownika.

Identyfikator i hasło do systemu informatycznego przetwarzającego dane osobowe są przydzielane użytkownikowi tylko w przypadku, gdy posiada on pisemne upoważnienie do przetwarzania danych osobowych wydane przez administratora danych osobowych lub osobę przez niego uprawnioną.

Za przydzielenie i wygenerowanie identyfikatora i hasła użytkownikowi, który pierwszy raz będzie korzystał z systemu informatycznego, odpowiada administrator odpowiedniego systemu informatycznego (czynności te wykonuje na pisemny lub przesłany drogą elektroniczną wniosek administratora bezpieczeństwa informacji).

Wyrejestrowanie użytkownika z systemu informatycznego może nastąpić na wniosek administratora danych osobowych, przełożonego użytkownika lub koordynatora zadania, na rzecz którego były wykonywane czynności związane z przetwarzaniem danych osobowych.

Pisemny wniosek o wyrejestrowanie użytkownika systemu należy złożyć do Administratora bezpieczeństwa informacji. Wyrejestrowanie użytkownika z systemu realizuje administrator odpowiedniego systemu informatycznego na pisemny lub przesłany drogą elektroniczną wniosek administratora bezpieczeństwa informacji.

Administrator bezpieczeństwa informacji jest zobowiązany do prowadzenia ewidencji pracowników upoważnionych do przetwarzania danych osobowych w UM. Zgodnie z art. 39 ust. 1 ustawy taka ewidencja zawiera:

- imię i nazwisko osoby upoważnionej,
- datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych,
- nazwa systemu informatycznego, którego dotyczy upoważnienie,
- identyfikator nadany w systemie.

## 4. Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.

Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi. Użytkownik odpowiedzialny jest za wszystkie czynności wykonane przy użyciu identyfikatora, którym się posługuje lub posługiwał.

- identyfikator składa się minimalnie z pięciu znaków, znaki identyfikatora nie są rozdzielone spacjami ani znakami interpunkcyjnymi, identyfikator nie zawiera polskich liter,
- identyfikator wpisuje się do ewidencji, prowadzonej przez administratora bezpieczeństwa informacji, wraz z imieniem i nazwiskiem użytkownika oraz nazwami systemów informatycznych, do których użytkownik uzyskał dostęp i wprowadzany jest przez administratorów systemów informatycznych do właściwych systemów,
- identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego nie może być przydzielany innej osobie.

System informatyczny przetwarzający dane osobowe jest skonfigurowany w sposób wymagający bezpieczne zarządzanie hasłami użytkowników:

- hasło przydzielone użytkownikowi musi być zmienione po pierwszym udanym zalogowaniu się do systemu informatycznego przetwarzającego dane osobowe,
- hasła są zmieniane przez użytkownika,
- system informatyczny wyposażony jest w mechanizmy wymuszające zmianę hasła po upływie 45 dni od dnia ostatniej zmiany hasła,
- system informatyczny wyposażony jest w mechanizm pozwalający na wymuszenie jakości hasła, w szczególności hasło powinno składać z co najmniej 8 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.

Osoby uprawnione do wykonywania prac administracyjnych w systemie informatycznym posiadają własne konta administracyjne, do których mają przydzielone hasło. Zasady zarządzania hasłami są analogiczne, jak w przypadku haseł użytkowników.

Nazwy i hasła użytkowników posiadających uprawnienia administratorów systemów informatycznych powinny być przechowywane w zamkniętej szafie, do której dostęp jest w pełni kontrolowany, przy czym dostęp do szafy mają wyłącznie uprawnione osoby.

Nazwy użytkowników oraz hasła powinny być przechowywane w opieczętowanej i opatrzonej podpisem administratorów systemu kopercie. W przypadku konieczności awaryjnego użycia nazw i haseł tych użytkowników konieczny jest wpis ilustrujący zaistniała sytuację w „Dzienniku haseł" znajdującym się w szafie wraz z kopertą, w której znajdują się hasła.

Wpis powinien zawierać następujące informacje:

- imię i nazwisko oraz stanowisko osoby upoważnionej udostępniającej dostęp do szafy, w której znajdują się hasła,
- imię i nazwisko oraz stanowisko osoby, która pobiera nazwy użytkowników i hasła,
- krótki opis sytuacji, która zmusiła do awaryjnego wykorzystania haseł.

O konieczności i okolicznościach awaryjnego użycia nazw i haseł musi niezwłocznie zostać powiadomiony administrator bezpieczeństwa informacji.

## 5. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu.

Przed rozpoczęciem pracy, w trakcie rozpoczynania pracy z systemem informatycznym oraz w trakcie pracy każdy pracownik obowiązany jest do zwrócenia bacznej uwagi, czy nie wystąpiły symptomy mogące świadczyć o naruszeniu ochrony danych osobowych.

Szczegółowy opis takich symptomów oraz sposób postępowania w przypadku ich wykrycia został opisany w dokumencie „Polityka bezpieczeństwa" punkt 7d.

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.

Maksymalna ilość prób wprowadzenia hasła przy logowaniu się do systemu wynosi trzy. Po przekroczeniu tej liczby prób logowania system blokuje dostęp do zbioru danych na poziomie danego użytkownika. Odblokowania konta może dokonać administrator systemu informatycznego w porozumieniu z administratorem bezpieczeństwa informacji. Użytkownik informuje administratora bezpieczeństwa informacji o zablokowaniu dostępu do zbioru danych.

W przypadku bezczynności użytkownika na stacji roboczej przez okres dłuższy niż 30 minut automatycznie włączany jest wygaszacz ekranu. Wygaszacze ekranu powinny być zaopatrzone w hasła zbudowane analogicznie do haseł używanych przez użytkownika przy logowaniu. Hasło powinno składać się z co najmniej 8 znaków, powinno zawierać małe i wielkie litery oraz cyfry lub znaki specjalne oraz być zmieniane nie rzadziej niż co 45 dni.

Zmianę użytkownika stacji roboczej każdorazowo musi poprzedzać wylogowanie się poprzedniego użytkownika. Niedopuszczalne jest, aby dwóch lub większa ilość użytkowników wykorzystywała wspólnie jedno konto użytkownika.

W przypadku, gdy przerwa w pracy na stacji roboczej trwa dłużej niż 60 minut użytkownik obowiązany jest wylogować się z aplikacji i systemu stacji roboczej, na której pracuje oraz sprawdzić czy nie zostały pozostawione bez zamknięcia nośniki informacji zawierające dane osobowe.

W pomieszczeniach, w których przetwarzane są dane i w których jednocześnie mogą przebywać osoby postronne, monitory stanowisk dostępu do danych powinny być ustawione w taki sposób, żeby uniemożliwić tym osobom wgląd w dane.

Zakończenie pracy użytkownika w systemie informatycznym obejmuje wylogowanie się użytkownika z aplikacji.

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

Dane osobowe przetwarzane w systemie informatycznym podlegają zabezpieczeniu poprzez tworzenie kopii zapasowych. Za proces tworzenia kopii zapasowych odpowiada administrator systemu informatycznego lub osoba specjalnie do tego celu wyznaczona.

W przypadku lokalnego przetwarzania danych osobowych na stacjach roboczych użytkownicy systemu informatycznego zobowiązani są do centralnego przechowywania kopii danych, tak aby możliwe było zabezpieczenie ich dostępności poprzez wykonanie kopii zapasowych. Przez centralne przechowywanie kopii danych rozumie się cotygodniowe przegranie zbioru danych na specjalnie wydzielony do tego celu obszar dysku na serwerze. W przypadku, gdy z przyczyn technicznych jest to niemożliwe użytkownicy systemu są zobowiązani do sporządzania kopii zapasowych baz danych na nośniku wymiennym i centralne ich przechowywanie w miejscu wskazanym przez administratora bezpieczeństwa informacji.

Kopie zapasowe informacji przechowywanych w systemie informatycznym przetwarzającym dane osobowe tworzone są w następujący sposób:

- kopia zapasowa aplikacji przetwarzającej dane osobowe – pełna kopia wykonywana jest po wprowadzeniu zmian do aplikacji, kopie umieszczone są na nośnikach wymiennych, kopia przechowywana jest w zamkniętej szafie,
- kopia zapasowa danych osobowych przetwarzanych przez aplikację (pełna kopia) wykonywana jest codziennie na dysku lokalnym komputera wybranego przez administratora systemu informatycznego (komputerem tym nie może być serwer baz danych),
- raz w tygodniu, na nośniku wymiennym, tworzona jest kopia zawierająca kopie zapasową danych osobowych z każdego dnia ostatniego tygodnia, kopia ta przechowywana jest w zamkniętej szafie, w innym pomieszczeniu niż znajdują się serwery danych,
- zbiorcze (tygodniowe) kopie przechowywane są przez okres dwóch tygodni, po tym terminie stare kopie są niszczone poprzez nadpisywanie ich przez bardziej aktualne lub fizyczne zniszczenie nośnika z kopią,

- raz w miesiącu, pomiędzy 1 a 5 każdego miesiąca, tworzona jest kopia zapasowa danych osobowych, która przekazywana jest do przechowywania przy zachowaniu odpowiednich zabezpieczeń, w innym budynku niż ten, w którym znajdują się serwery, przechowywane są tam kopie z 3 ostatnich miesięcy,
- kopia zapasowa danych konfiguracyjnych systemu informatycznego przetwarzającego dane osobowe, w tym uprawnień użytkowników systemu – pełna kopia wykonywana jest każdorazowo po wprowadzeniu istotnych zmian w konfiguracji lub aktualizacji systemów lecz nie rzadziej niż raz na 3 miesiące i przechowywana jest w zamkniętej szafie.

Do tworzenia kopii zapasowych wykorzystywane są dedykowane do tego celu urządzenia wchodzące w skład systemu informatycznego na nośnikach wymiennych adekwatnych do rodzaju urządzenia.

W przypadku przechowywania kopii zapasowych przez okres dłuższy niż pół roku, wszystkie kopie zapasowe zbiorów danych osobowych, aplikacji przetwarzających dane osobowe oraz danych konfiguracyjnych systemu informatycznego przetwarzającego dane osobowe, których to dotyczy muszą być okresowo (co najmniej raz na pół roku) sprawdzane pod względem ich dalszej przydatności. Czynności te wykonuje administrator systemu informatycznego. Z przeprowadzonego testu administrator systemu sporządza krótką notatkę uwzględniającą datę testu oraz jego rezultat (kopię notatki przekazuje administratorowi bezpieczeństwa informacji). Nośniki kopii zapasowych, które zostały wycofane z użycia, jeżeli jest to możliwe, należy pozbawić zapisanych danych za pomocą specjalnego oprogramowania do bezpiecznego usuwania zapisanych danych. W przeciwnym wypadku podlegają fizycznemu zniszczeniu z wykorzystaniem metod adekwatnych do typu nośnika, w sposób uniemożliwiający odczytanie zapisanych na nich danych.

## 7. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych, o których mowa w § 5 pkt 4 rozporządzenia

Nośniki danych zarówno w postaci elektronicznej, jak i papierowej powinny być zabezpieczone przed dostępem osób nieuprawnionych, nieautoryzowaną modyfikacją i zniszczeniem. Dane osobowe mogą być zapisywane na nośnikach przenośnych w przypadku tworzenia kopii zapasowych lub gdy istnieje konieczność przeniesienia tych danych w postaci elektronicznej, a wykorzystanie do tego celu sieci informatycznej jest nieuzasadnione, niemożliwe lub zbyt niebezpieczne.

Nośniki danych osobowych oraz wydruki powinny być przechowywane w zamkniętych szafach wewnątrz obszaru przeznaczonego do przetwarzania danych osobowych i nie powinny być bez uzasadnionej przyczyny wynoszone poza ten obszar. Przekazywanie nośników danych osobowych i wydruków poza lokalizację budynków UM powinno odbywać się za wiedzą administratora bezpieczeństwa informacji.

W przypadku, gdy nośnik danych osobowych nie jest dłużej potrzebny, należy przeprowadzić zniszczenie nośnika lub usunięcie danych z nośnika zgodnie ze wskazówkami umieszczonymi w punkcie 5. Jeżeli wydruk danych osobowych nie jest dłużej potrzebny, należy przeprowadzić zniszczenie wydruku przy użyciu niszczarki dokumentów.

W przypadku, gdy kopia zapasowa nie jest dłużej potrzebna, należy przeprowadzić jej zniszczenie lub usunięcie danych z nośnika, na którym się ona zgodnie ze wskazówkami umieszczonymi w punkcie 5.

## 8. Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III załącznika do rozporządzenia.

W związku z tym, że system informatyczny narażony jest na działanie oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do tego systemu konieczne jest podjęcie odpowiednich środków ochronnych.

Można wyróżnić następujące rodzaje występujących tu zagrożeń:

- nieuprawniony dostęp bezpośrednio do bazy danych,
- uszkodzenie kodu aplikacji umożliwiającej dostęp do bazy danych w taki sposób, że przetwarzane dane osobowe ulegną zafałszowaniu lub zniszczeniu,
- przechwycenie danych podczas transmisji w przypadku rozproszonego przetwarzania danych z wykorzystaniem ogólnodostępnej sieci Internet,
- przechwycenie danych z aplikacji umożliwiającej dostęp do bazy danych na stacji roboczej wykorzystywanej do przetwarzania danych osobowych przez wyspecjalizowany program szpiegowski i nielegalne przesłanie tych danych poza miejsce przetwarzania danych,
- uszkodzenie lub zafałszowanie danych osobowych przez wirus komputerowy zakłócający pracę aplikacji umożliwiającej dostęp do bazy danych na stacji roboczej wykorzystywanej do przetwarzania danych osobowych.

W celu przeciwdziałania wymienionym zagrożeniom system informatyczny musi posiadać następujące zabezpieczenia:

- fizyczne odseparowanie serwera bazy danych od sieci zewnętrznej,
- autoryzacja użytkowników przy zachowaniu odpowiedniego poziomu komplikacji haseł dostępu,
- stosowanie rygorystycznego systemu autoryzacji dostępu do wszystkich serwerów, na których znajdują się elementy aplikacji umożliwiających przetwarzanie danych osobowych,
- stosowaniu aplikacji w postaci skompilowanej i nie umieszczenie kodu źródłowego aplikacji na powszechnie dostępnych serwerach,
- stosowanie szyfrowanej transmisji danych przy zastosowaniu odpowiedniej długości klucza szyfrującego,
- stosowanie odpowiedniej ochrony antywirusowej na stacjach roboczych wykorzystywanych
- do przetwarzania danych osobowych.

Potencjalnymi źródłami przedostawania się programów szpiegowskich oraz wirusów komputerowych na stacje robocze są:

- załączniki do poczty elektronicznej,
- przeglądane strony internetowe,

- pliki i aplikacje pochodzące z nośników wymiennych uruchamiane i odczytywane na stacji roboczej.

W celu zapewnienia ochrony antywirusowej administrator systemu informatycznego przetwarzającego dane osobowe, lub osoba specjalnie do tego celu wyznaczona, jest odpowiedzialny za zarządzanie systemem wykrywającym i usuwającym wirusy.

System antywirusowy powinien być skonfigurowany w następujący sposób:
- rezydentny monitor antywirusowy (uruchomiony w pamięci operacyjnej stacji roboczej) powinien być stale włączony,
- antywirusowy skaner ruchu internetowego powinien być stale włączony,
- monitor zapewniający ochronę przed wirusami makr w dokumentach MS Office lub innych powinien być stale włączony,
- skaner poczty elektronicznej powinien być stale włączony.

Systemy antywirusowe zainstalowane na stacjach roboczych powinny być skonfigurowane w sposób następujący:
- zablokowanie możliwości ingerencji użytkownika w ustawienia oprogramowania antywirusowego,
- możliwość centralnego uaktualnienia wzorców wirusów.

System antywirusowy powinien być aktualizowany na podstawie materiałów publikowanych przez producenta oprogramowania.

Użytkownicy systemu informatycznego zobowiązani są do następujących działań:
- skanowania zawartości dysków stacji roboczej pracującej w systemie informatycznym pod względem potencjalnie niebezpiecznych kodów – przynajmniej 2 razy w tygodniu,
- skanowania zawartości nośników wymiennych odczytywanych na stacji roboczej pracującej w systemie informatycznym pod względem potencjalnie niebezpiecznych kodów – przy każdym odczycie,
- skanowanie informacji przesyłanych do systemu informatycznego pod kątem pojawienia się niebezpiecznych kodów – na bieżąco.

W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy administrator systemu informatycznego lub inny wyznaczony pracownik powinien podjąć działania zmierzające do usunięcia zagrożenia. W szczególności działania te mogą obejmować:
- usunięcie zainfekowanych plików, o ile jest to akceptowalne ze względu na prawidłowe funkcjonowanie systemu informatycznego,
- odtworzenie plików z kopii zapasowych po uprzednim sprawdzeniu, czy dane zapisane na kopiach nie są zainfekowane,
- samodzielną ingerencję w zawartość pliku – w zależności od posiadanych kwalifikacji lub skonsultowanie się z zewnętrznymi ekspertami.

System informatyczny przetwarzający dane osobowe powinien posiadać mechanizmy pozwalające na zabezpieczenie ich przed utratą lub wystąpieniem zafałszowania w wyniku awarii

zasilania lub zakłóceń w sieci zasilającej. W związku z tym system informatyczny powinien być wyposażony w co najmniej:

- filtry zabezpieczające stacje robocze przed skutkami przepięcia,
- zasilacze awaryjne serwerów baz danych, serwerów aplikacji oraz urządzeń pamięci masowej pozwalające na bezpieczne zamkniecie aplikacji przetwarzających dane osobowe w sposób umożliwiający poprawne zapisanie przetwarzanych danych.

## 9. Sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4 rozporządzenia

System informatyczny przetwarzający dane osobowe musi posiadać mechanizm uwierzytelniający użytkownika, wykorzystujący identyfikator i hasło. Powinien także posiadać mechanizmy pozwalające na określenie uprawnień użytkownika do korzystania z przetwarzanych informacji (np. prawo do odczytu danych, modyfikacji istniejących danych, tworzenia nowych danych, usuwania danych).

System informatyczny przetwarzający dane osobowe musi posiadać mechanizmy pozwalające na odnotowanie faktu wykonania operacji na danych. W szczególności zapis ten powinien obejmować:

- rozpoczęcie i zakończenie pracy przez użytkownika systemu,
- operacje wykonywane na przetwarzanych danych, a w szczególności ich dodanie, modyfikację oraz usunięcie,
- przesyłanie za pośrednictwem systemu danych osobowych przetwarzanych w systemie informatycznym innym podmiotom nie będącym właścicielem ani współwłaścicielem systemu,
- nieudane próby dostępu do systemu informatycznego przetwarzającego dane osobowe oraz nieudane próby wykonania operacji na danych osobowych,
- błędy w działaniu systemu informatycznego podczas pracy danego użytkownika.

Zapis działań użytkownika uwzględnia:

- identyfikator użytkownika,
- datę i czas, w którym zdarzenie miało miejsce,
- rodzaj zdarzenia,
- określenie informacji, których zdarzenie dotyczy (identyfikatory rekordów).

W ramach możliwości technicznych system informatyczny powinien posiadać mechanizmy pozwalające na automatyczne powiadomienie administratora bezpieczeństwa informacji lub osoby przez niego uprawnionej o zaistnieniu zdarzenia krytycznego (mogącego mieć krytyczne znaczenie dla bezpieczeństwa przetwarzanych danych osobowych).

Ponadto system informatyczny powinien zapewnić zapis faktu przekazania danych osobowych z uwzględnieniem:

- identyfikatora osoby, której dane dotyczą,
- osoby przesyłającej dane,
- odbiorcy danych,
- zakresu przekazanych danych osobowych,

- daty operacji,
- sposobu przekazania danych.

## 10. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych

Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe muszą uwzględniać wymagany poziom zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych.

Prace serwisowe na terenie UM prowadzone w tym zakresie mogą być wykonywane wyłącznie przez pracowników UM lub przez upoważnionych przedstawicieli wykonawców zewnętrznych w obecności pracowników UM.

W szczególnych przypadkach prac serwisowych przy przetwarzaniu danych osobowych, pracownicy serwisu zobowiązani są do posiadania stosownego upoważnienia lub zaświadczenia.

Przed rozpoczęciem prac serwisowych przez osoby spoza UM konieczne jest potwierdzenie tożsamości serwisantów.

Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:

- likwidacji — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,
- przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie,
- naprawy — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

## 11. Dokumenty powiązane z „Instrukcją zarządzania systemami informatycznymi"

- ewidencja upoważnień do przetwarzania danych osobowych
- ewidencja identyfikatorów z określonym dostępem do systemów przetwarzania danych osobowych
- dziennik systemowy obsługi sprzętu komputerowego i systemów do przetwarzania danych osobowych

BURMISTRZ
mgr Wojciech Blecharczyk



**Gmina Miasta Sanok**
**ul. Rynek 1**
**38-500 Sanok**

## Załącznik nr 1

**Wykaz pomieszczeń, w których dopuszczalne jest przetwarzanie danych osobowych**

1. Budynek Gminy Miasta Sanok, ul. Rynek 1, 38-500 Sanok:
   - pomieszczenia o nr: 1, 7, 17, 18, 19, 20, 21, 23, 24-1, 24-2, 24-3, 24-4, 26, 29, 30, 31, 34, 61, 50a, 50b, 51, 53.
2. Budynek Stanu Cywilnego, ul. Rynek 16, 38-500 Sanok:
   - pomieszczenia o nr: 2, 3, 4.
3. Biuro Stypendiów Socjalnych, ul. Rynek 16, 38-500 Sanok:
   - pomieszczenia o nr: 5
4. Punkt informacyjny ds. alkoholowych: ul. Sobieskiego 1, 38-500 Sanok
   - pomieszczenia o nr: 101

## Załącznik nr 2

**Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.**

| L.p. | Nazwa zbioru | Nazwa programu |
|---|---|---|
| 1 | Ewidencja Ludności, Rejestr Wyborców (ELUD) | ELUD+, WYB+ |
| 2 | Naliczanie Podatków od Gruntów i Nieruchomości (POGRUN) | POGRUN+ |
| 3 | Windykacja Podatkowa, Obsługa Kasy (WIP) | WIP+, KASA+ |
| 4 | Księgowość Organu i Jednostki Budżetowej (FKB) | FKB+ |
| 5 | Kadry – Płace (PLACE) | KADRY+, PŁACE+ |
| 6 | Rejestr Działalności Gospodarczej (EPOD) | EPOD+ |
| 7 | Rejestr Koncesji Alkoholowych (ALK) | ALK+ |
| 8 | Naliczanie Podatku od Środków Transportu (POST) | POST+ |
| 9 | Rejestr Faktur (FAKT) | FAKTURA+ |
| 10 | Ewidencji Gruntów i Mienia Komunalnego (DOS - baza DBASE) | EGRUN |
| 11 | przekazywanie dokumentów ubezpieczeniowych drogą elektroniczną (urzadmiasta, oswiata) | PŁATNIK |
| 12 | elektroniczny obieg dokumentów (el-Dok) | el-Dok |
| 13 | Rejestr Urzędu Stanu Cywilnego (pb_usc) | PB_USC |
| 14 | Kadry-Płace (Place_Optivum) | VULCAN |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |