

Instrukcja
Zarządzania Systemem Informatycznym
służącym do przetwarzania danych osobowych
w Urzędzie Miasta i Gminy w Kazimierzy Wielkiej

§ 1

Instrukcja określa:

- 1) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osób odpowiedzialnych za te czynności;
- 2) stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;
- 3) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;
- 4) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi służących do ich przetwarzania;
- 5) sposób, miejsce i okres przechowywania:
 - a) elektronicznych nośników informacji zawierających dane osobowe,
 - b) kopii zapasowych określonych w pkt 4;
- 6) sposób zabezpieczenia systemu informatycznego przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego;
- 7) sposób odnotowania informacji o udostępnionych danych osobowych;
- 8) zasady wykonywania przeglądów i konserwacji systemu oraz nośników informacji służących do przetwarzania danych;
- 9) zasady użytkowania sieci komputerowej.

§ 2

Ilekcroć w instrukcji jest mowa o:

- 1) zbiorze danych - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów;

2) systemie informatycznym - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

3) Administratorze Danych Osobowych - rozumie się przez to Burmistrza Miasta i Gminy w Kazimierzy Wielkiej;

4) Administratorze Bezpieczeństwa Informacji – rozumie się osobę lub osoby upoważnione i odpowiedzialne za przestrzeganie ustawy o ochronie danych osobowych;

5) Administratorze Systemu Informatycznego – rozumie się przez to osobę lub osoby upoważnione przez Administratora Danych Osobowych do administrowania i zarządzania systemem informatycznym w Urzędzie Miasta i Gminy w Kazimierzy Wielkiej;

6) identyfikatorze użytkownika - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;

7) hasło - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;

8) publicznej sieci telekomunikacyjnej – rozumie się przez to sieć telekomunikacyjną wykorzystywaną głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych;

9) Urządzie – rozumie się przez to Urząd Miasta i Gminy w Kazimierzy Wielkiej;

§ 3

1. Do obsługi systemu informatycznego służącego do przetwarzania danych osobowych, może być dopuszczona wyłącznie osoba posiadająca upoważnienie wydane przez Burmistrza Miasta i Gminy w Kazimierzy Wielkiej. Upoważnienie to zawiera nazwę zbioru danych oraz zakres uprawnień użytkownika do przetwarzania danych osobowych.

2. Ewidencję upoważnień, o których mowa w ust. 1, prowadzi Administrator Bezpieczeństwa Informacji.

§ 4

1. Upoważnienie, o którym mowa w § 3 ust. 1, stanowi podstawę do rejestracji użytkownika systemu informatycznego.

2. Administrator Systemu Informatycznego rejestruje osobę w systemie na wniosek Administratora Bezpieczeństwa Informacji.

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

4. Dla każdego użytkownika systemu informatycznego, który przetwarza dane osobowe, Administrator Systemu Informatycznego ustala niepowtarzalny identyfikator i hasło.

5. Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego, nie powinien być przydzielany innej osobie.

6. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych, należy niezwłocznie wyrejestrować z systemu informatycznego, unieważnić jej hasło, oraz podjąć inne stosowne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych. O utracie uprawnień Administrator Bezpieczeństwa Informacji niezwłocznie informuje Administratora Systemu Informatycznego.

7. Administrator Systemu Informatycznego przekazując użytkownikowi identyfikator i hasło przeprowadza szkolenie użytkownika z zakresu pracy w systemie informatycznym oraz bezpieczeństwa danych w systemie informatycznym.

8. Administrator Systemu Informatycznego prowadzi ewidencję użytkowników systemu informatycznego.

Ewidencja użytkowników powinna zawierać:

- 1) nazwisko i imię;
- 2) identyfikator użytkownika;
- 3) stanowisko;
- 4) wydział, w którym użytkownik jest zatrudniony;
- 5) wskazanie zbiorów danych, do których użytkownik ma prawo dostępu;
- 6) zakres uprawnień do systemu informatycznego;
- 7) datę przyznania uprawnień;
- 8) datę wyrejestrowania użytkownika z systemu informatycznego w przypadku, gdy upoważnienie traci ważność.

§ 5

1. Dane osobowe przetwarzane są w Urzędzie Miasta i Gminy w Kazimierzy Wielkiej za pomocą komputerów stacjonarnych.

2. Hasło użytkownika powinno mieć minimum 8 znaków i być zmieniane co 30 dni. Administrator Systemu Informatycznego zmienia hasła lub wymusza w systemie zmianę haseł użytkowników.

3. Hasło nie może być zapisywane w miejscu dostępnym dla osób nieuprawnionych. Użytkownik nie może udostępnić identyfikatora, hasła i stanowiska roboczego osobom nieuprawnionym.

4. Hasło użytkownika, umożliwiające dostęp do systemu informatycznego, utrzymuje się w tajemnicy, również po upływie jego ważności.

5. Zapasowe hasła Administratora Systemu Informatycznego powinny znajdować w zabezpieczonej kopercie w sejfie Urzędu.

6. Pojedyncze komputery, na których dane osobowe służą do edycji powinny być zabezpieczone hasłem. Pracownicy zatrudnieni przy ich obsłudze nie mogą zezwalać na użytkowanie komputera osobom nieupoważnionym.

§ 6

1. Użytkownik wyłącza sprzęt komputerowy i niezwłocznie powiadamia Administratora Systemu Informatycznego o braku możliwości zalogowania się na swoje konto oraz o podejrzeniu fizycznej ingerencji w przetwarzane dane lub użytkowane narzędzia programowe lub sprzętowe.

2. Po potwierdzeniu przez Administratora Systemu Informatycznego fizycznej nieuprawnionej ingerencji w przetwarzane dane lub użytkowane narzędzia programowe lub sprzętowe użytkownik:

1) niezwłocznie powiadamia o tym Administratora Bezpieczeństwa Informacji lub osobę zastępującą Administratora Bezpieczeństwa Informacji, a w przypadku ich nieobecności – bezpośrednio Administratora Danych Osobowych;

2) sporządza notatkę służbową z opisem sytuacji wskazującej na naruszenie zabezpieczeń systemu informatycznego i przekazuje ją Administratorowi Bezpieczeństwa Informacji.

3. Administrator Bezpieczeństwa Informacji po zbadaniu zdarzenia z ust. 1 przygotowuje informację o przyczynach, przebiegu i wnioskach ze zdarzenia oraz przekazuje ją Administratorowi Danych Osobowych.

§ 7

Dane osobowe są przetwarzane z użyciem systemu informatycznego w godzinach pracy Urzędu Miasta i Gminy w Kazimierzy Wielkiej; poza tymi godzinami wyłącznie w uzasadnionych przypadkach, po uzyskaniu pisemnej zgody Administratora Bezpieczeństwa Informacji, z zachowaniem warunków określonych w Regulaminie Pracy Urzędu.

§ 8

1. Ekran monitorów stanowisk, na których przetwarzane są dane osobowe, powinny być automatycznie wyłączone po upływie ustalonego czasu nieaktywności użytkownika.

2. W pomieszczeniach, gdzie przebywają osoby, które nie posiadają upoważnień, o których mowa w § 3 ust. 1, monitory stanowisk na których przetwarzane są dane osobowe powinny być ustawione w taki sposób, aby uniemożliwić tym osobom wgląd w dane.

3. Użytkownik ma obowiązek wylogowania się z systemu przy rozpoczęciu dłuższej nieobecności na stanowisku pracy lub zakończeniu tej pracy. Stanowisko komputerowe z uruchomionym systemem nie może pozostać bez kontroli pracującego na nim pracownika.

4. Wydruki zawierające dane osobowe należy przechowywać w miejscu uniemożliwiającym ich odczytanie przez osoby nieuprawnione. Wydruki nieprzydatne należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

§ 9

1. Przebywanie osób nieuprawnionych do dostępu do danych osobowych w pomieszczeniach znajdujących się na obszarze, w którym są przetwarzane dane osobowe, jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu tych danych.

2. Pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane na czas nieobecności w nich osób zatrudnionych w sposób uniemożliwiający dostęp do nich osób trzecich.

§ 10

1. Zbiory danych w systemie informatycznym są zabezpieczane przed utratą lub uszkodzeniem za pomocą:

1) urządzeń zabezpieczających przed awarią zasilania lub zakłóceniami w sieci zasilającej;

2) sporządzania kopii zapasowych zbiorów danych (kopie całościowe).

2. Kopie zapasowe baz danych zainstalowanych na serwerach Urzędu – wykonuje się codziennie na dysku lokalnym, CDRW lub taśmie. W przypadku kopii na dysku lokalnym raz na 30 dni wykonuje się CDR, DVDR.

3. Za wykonywanie kopii, o których mowa w ust. 2, odpowiedzialny jest Administrator Systemu Informatycznego. W przypadku zbiorów danych przetwarzanych lokalnie (przetwarzanie rozproszone) za wykonanie bieżących kopii zapasowych zbiorów danych odpowiedzialny jest użytkownik wyznaczony do wykonania tego zadania przez swojego przełożonego.

4. Administrator Systemu Informatycznego nie ma obowiązku sporządzania kopii zapasowej, jeżeli w danym dniu nie wykonano zapisu zmieniającego bazę danych.

5. Kopie zapasowe zbiorów danych należy okresowo sprawdzać pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu. Nośniki danych po ustaniu ich użyteczności należy pozbawiać danych lub niszczyć w sposób uniemożliwiający ich odczyt.

6. Kopie zapasowe miesięczne wykonywane na dyskietkach, płytach CD, DVD lub taśmach należy przechowywać w kasie pancерnej Urzędu. Kopie baz danych nie powinny być przechowywane w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych wykorzystywane na bieżąco. Kopie zapasowe przechowuje się w pomieszczeniach zabezpieczonych przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem.

7. Kopie miesięczne przechowuje się przez okres 3 miesięcy. W przypadku danych księgowych okres przechowywania danych wynosi 5 lat.

§ 11

1. W związku z istnieniem zagrożenia dla zbiorów danych ze strony wirusów komputerowych oraz oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego, konieczna jest ochrona sieci komputerowej i stanowisk komputerowych. Wirusy komputerowe oraz wyżej wymienione oprogramowanie mogą pojawić się w Urzędzie poprzez:

- 1) Internet;
- 2) oprogramowanie przenoszone dyskietskami.

2. Przeciwdziałanie zagrożeniom ze strony wirusów komputerowych:

1) serwery, programy i zbiory danych zainstalowane na serwerach, nośniki informacji będące w bezpośrednim użytkowaniu przez Administratora Systemu Informatycznego winny być sprawdzane przez Administratora Systemu Informatycznego na obecność wirusów komputerowych co najmniej raz w tygodniu lub w razie potrzeby częściej;

2) komputer z dostępem do Internetu musi być zabezpieczony za pomocą oprogramowania antywirusowego. Użytkownik komputera, w którym jest zainstalowany program antywirusowy zobowiązany jest do sprawdzenia komputera raz w tygodniu na obecność wirusów komputerowych oraz co 3 dni do dokonania aktualizacji bazy wirusów tego programu w przypadku, gdy aktualizacja automatyczna nie działa.

3. Przeciwdziałanie zagrożeniom, które są związane z połączeniem sieci lokalnej z publiczną:

1) serwer i inne urządzenia wykorzystywane w realizacji dostępu do Internetu posiadają oprogramowanie i mechanizmy zabezpieczające przed nieautoryzowanym dostępem do sieci lokalnej;

2) Administrator Systemu Informatycznego monitoruje na bieżąco stan bezpieczeństwa, analizuje logi pod kątem naruszenia zabezpieczeń; raz na tydzień dokonuje szczegółowej analizy stanu zabezpieczeń.

§ 12

Użytkownik zapisuje w programie informację o odbiorcach danych osobowych, w rozumieniu art. 7 pkt 6 ustawy o ochronie danych osobowych, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, jeżeli system informatyczny nie jest używany do przetwarzania danych zawartych w zbiorach jawnych.

§ 13

1. Przeglądy i konserwacje systemu i zbiorów danych wykonuje Administrator Systemu Informatycznego na bieżąco, lecz nie rzadziej niż raz w miesiącu. Administrator sprawdza spójność danych, indeksów oraz stan nośników np. dysków twardych.

2. Administrator Systemu Informatycznego okresowo sprawdza możliwość odtworzenia danych z kopii zapasowej.

§ 14

Urządzenia, dyski i inne informatyczne nośniki danych zawierające dane osobowe należy pozbawić tych danych przed ich przekazaniem innemu podmiotowi. Nośniki danych zawierające dane osobowe są likwidowane poprzez uszkodzenie w sposób uniemożliwiający ich odczytanie. Naprawę wymienionych urządzeń należy wykonać pod nadzorem osoby upoważnionej przez Administratora Danych Osobowych lub jeśli jest to możliwe, pozbawić je danych osobowych przed wydaniem ich do naprawy.

§ 15

Korzystającym z systemu informatycznego w Urzędzie zabrania się:

- 1) udostępniania stanowiska pracy oraz istniejących w nich danych osobom nieupoważnionym;
- 2) udostępniania osobom nieuprawnionym programów komputerowych;
- 3) używania oprogramowania w innym zakresie niż pozwala na to umowa licencyjna;
- 4) przenoszenia programów komputerowych, dysków twardej z jednego stanowiska na inne;
- 5) samowolnego instalowania i używania programów komputerowych; programy komputerowe instalowane są przez Administratora Systemu Informatycznego lub za jego zgodą przez inną upoważnioną osobę;
- 6) używania nośników danych udostępnionych przez osoby nieuprawnione;
- 7) używania nośników danych niesprawdzonych, niewiadomego pochodzenia lub niezwiązanych z pracą; w przypadku konieczności użycia niesprawdzonych przenośnych nośników danych, należy te nośniki przeskanować programem antywirusowym; jeżeli program antywirusowy nie jest zainstalowany na danej stacji roboczej należy to zrobić na innym stanowisku;
- 8) wykorzystywania sprzętu komputerowego w celach innych, niż wyznaczone przez Administratora Danych Osobowych.

**Załącznik nr 1 do
Instrukcji Zarządzania
Systemem Informatycznym
stanowiącej załącznik do zarządzenia nr 9/2008
Burmistrza Miasta i Gminy Kazimierza Wielka
z dnia 19 lutego 2008 r.**

.....
(miejsowość, data)

.....
(pieczęć jednostki organizacyjnej)

Nr rej.

Upoważnienie do przetwarzania danych osobowych

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) upoważniam:

.....
(imię i nazwisko)

zatrudnionego na stanowisku.....

W
(oznaczenie jednostki i komórki organizacyjnej)

do przetwarzania danych i obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych.

.....
(podpis i pieczęć administratora danych)

**Załącznik nr 2 do
Instrukcji Zarządzania
Systemem Informatycznym
stanowiącej załącznik do zarządzenia nr 9/2008
Burmistrza Miasta i Gminy Kazimierza Wielka
z dnia 19 lutego 2008 r.**

WZÓR

Ewidencja osób zatrudnionych przy przetwarzaniu danych osobowych

W.....
(oznaczenie jednostki organizacyjnej)

L.p.	Imię i nazwisko	Stanowisko	Komórka organizacyjna	Data przeszkolenia	Nr upoważnienia imiennego*

* dotyczy osób przetwarzających dane w systemie informatycznym