**Zarządzenie Nr 355/2013**
**Burmistrza Gminy Kozienice**
z dnia 06.11.2013

w sprawie wprowadzenia w Urzędzie miejskim w Kozienicach Polityki Bezpieczeństwa Informacji i Instrukcji Zarządzania Systemem Informatycznym dotyczących ochrony danych osobowych w Urzędzie Miejskim w Kozienicach

Na podstawie art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych ( tj. Dz.U. z 2002 r. Nr 101 poz. 926 z późn. zmianami) oraz § 3, 4 i § 5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024 ) - zarządza się co następuje:

§ 1

1. Wprowadza się do użytku służbowego „Politykę bezpieczeństwa informacji w Urzędzie Miejskim w Kozienicach" w brzmieniu zgodnie z Załącznikiem Nr 1 do zarządzenia.
2. Wprowadza się do użytku służbowego „Instrukcję Zarządzania Systemem Informatycznym w brzmieniu stanowiącym załącznik nr 2 do zarządzenia.

§ 2

Pracownicy, zapoznanie się z zarządzeniem, potwierdzą własnoręcznym podpisem na stosownej liście.

§ 3

Traci moc zarządzenie nr 12 Burmistrza Gminy Kozienice z dnia 29.12.2006 r. w sprawie wprowadzenia „Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miejskim w Kozienicach.

§ 4

Zarządzenie wchodzi w życie z dniem podjęcia.

**Burmistrz Gminy Kozienice**

**dr inż. Tomasz Śmietanka**

ZATWIERDZAM

Burmistrz Gminy Kozienice

*dr inż. Tomasz Śmietanka*

Załącznik nr 1
do zarządzenia Nr 355/2013
Burmistrza Gminy Kozienice
z dnia 06.11.2013 r.

# POLITYKA

## bezpieczeństwa informacji

## w Urzędzie Miejskim w Kozienicach

Spis treści:

## Rozdział 1

## Postanowienia ogólne

§ 1

1. „Polityka bezpieczeństwa systemu informatycznego w Urzędzie Miejskim w Kozienicach", zwana dalej **Polityką**, opracowana została zgodnie z wymogami określonymi w § 3 i 4 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku 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 2004 r. nr 100, poz. 1024 ).
2. Polityka określa :
   a) obszar przetwarzania danych osobowych,
   b) wykaz zbiorów danych osobowych,
   c) opis struktury danych osobowych
   d) sposób przepływu danych pomiędzy poszczególnymi systemami
   e) określenie środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.
3. Niniejsza Polityka, jest wewnętrznym dokumentem wydanym przez Burmistrza Gminy Kozienice i przeznaczona jest dla osób zatrudnionych przy przetwarzaniu danych osobowych.
4. Przestrzeganie postanowień niniejszej Polityki służyć ma wykrywaniu i właściwemu reagowaniu na przypadki naruszenia ochrony danych osobowych w Urzędzie Miejskim w Kozienicach.

§ 2

Określenia i skróty użyte w Polityce oznaczają:

1. **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. 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.
2. **Zbiór danych** – to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
3. **Administrator Danych Osobowych** – Burmistrz Gminy Kozienice, zwany dalej **Administratorem.**
4. **Administrator Bezpieczeństwa Informacji**, zwany dalej **ABI** – osoba wyznaczona przez Administratora lub osobę upoważnioną, odpowiedzialna za bezpieczeństwo danych osobowych, w tym w szczególności za przeciwdziałanie dostępowi osób trzecich do systemów oraz podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w tych systemach i odpowiedzialna za sprawność, konserwacje oraz wdrażanie technicznych zabezpieczeń systemów informatycznych, w których przetwarzane są dane osobowe w zbiorach Urzędu Miejskiego w Kozienicach.
5. **Administrator Systemu Informatycznego** – zwany dalej **ASI** – osoba administrująca serwerami i innymi urządzeniami służącymi przetwarzaniu danych.
6. **Użytkownik systemu**, zwany dalej **użytkownikiem** – osoba posiadająca upoważnienie wydane przez Administratora lub osobę upoważnioną przez niego i dopuszczona w zakresie w nim wskazanym, jako użytkownik do przetwarzania danych osobowych w systemie informatycznym Urzędu Miejskiego w Kozienicach.

7. **System informatyczny,** zwany dalej **systemem** to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
8. **Zabezpieczenie systemu informatycznego** – wdrożenie przez Administratora stosownych środków organizacyjnych i technicznych w celu zabezpieczenia zasobów oraz ochrony danych przed dostępem, modyfikacją ujawnieniem, pozyskaniem lub zniszczeniem przez osobę trzecią.
9. **Przetwarzanie danych osobowych** – wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, udostępnianie i usuwanie, a zwlaszcza tych, które są wykonywane w systemach informatycznych.
10. **Osoba trzecia** – to każda osoba nieupoważniona i przez to nieuprawniona do dostępu do danych osobowych zbiorów będących w posiadaniu Administratora. Osoba trzecią jest również osoba posiadająca upoważnienie wydane przez Administratora podejmująca czynności w zakresie przekraczającym ramy tego upoważnienia.
11. **Zewnętrzny nośnik danych** – to urządzenie, na którym możliwe jest fizyczne zapisanie różnego rodzaju informacji, jej przenoszenie między komputerami, i z którego możliwe jest późniejsze odczytanie tej informacji. Nośniki pamięci w tej kategorii obejmują m.in.: dyskietki, dyski zewnętrzne, pamięci flash, telefony komórkowe, aparaty fotograficzne iphony, ipody, urządzenia mp3, mp4, karty pamięci, płyty CD, DVD, Blue Ray, smartphon`y, palmtopy, laptopy. notebook`i, netbook`i itp.
12. **Laptop / notebook** - to mały, przenośny komputer osobisty, zbudowany jako pojedyncze niewielkie, zamykane urządzenie, w których znajdują się wszystkie podzespoły wewnętrzne (procesor, pamięć, itd.), wybrane wejścia dla nośników, urządzenia komunikacji z użytkownikiem oraz system operacyjny.
13. **Netbook** - mały komputer przenośny typu notebook, zazwyczaj lżejszy od tradycyjnego laptopa przeznaczony do przeglądania Internetu, wideorozmów, aplikacji online oraz prac biurowych w podróży itp. posiadający system operacyjny.

## Rozdział 2

## Obszar, w którym przetwarzane są dane osobowe.

§ 3

1. W Urzędzie Miejskim w Kozienicach określa się obszar, w którym przetwarzane są dane osobowe w sposób tradycyjny – ręczny i z użyciem stacjonarnego sprzętu komputerowego obejmujący pomieszczenia w budynku Urzędu Miejskiego w Kozienicach ul. Parkowa 5 pokoje na parterze, I i II piętrze budynku Urzędu Miejskiego w Kozienicach. Budynek USC przy ul Parkowej 5C, w którym znajduje się biuro Rady miejskiej oraz Urząd Stanu Cywilnego.
2. Przebywanie wewnątrz obszaru, w którym są przetwarzane dane osób nieuprawnionych jest możliwe tylko w obecności użytkownika i za zgodą przełożonego.
3. Pomieszczenia, w których przetwarzane są dane, powinny być zamykane na czas nieobecności użytkowników, w sposób uniemożliwiający do nich dostęp osób trzecich.
4. Otwarcie pomieszczeń przez osobę, która rozpoczyna pracę jako pierwsza oraz zamknięcie przez osobę, która ostatnia opuszcza pomieszczenie, odbywa się za pomocą odkodowania i zakodowania systemu alarmowego (dotyczy to pomieszczeń monitorowanych).

§ 4

Zabezpieczenie systemu informatycznego, w zakresie nieuwzględnionym w niniejszej Polityce, reguluje „Instrukcja zarządzania systemem informatycznym, określająca procedury

przetwarzania danych osobowych w Urzędzie Miejskim w Kozienicach"(Załącznik nr 2 do zarządzenia).

## Rozdział 3

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

§ 5

1. Wykaz zbiorów danych osobowych przetwarzanych w Urzędzie Miejskim w Kozienicach zawiera załącznik (druk nr 3) do niniejszej Polityki.
2. Zgodnie z stosownymi ustawami do ww. zbiorów przetwarzane są dane wymienione w art. 27 ustawy o ochronie danych osobowych na poziomie podwyższonym.

## Rozdział 4

## Kontrola przestrzegania zasad zabezpieczenia systemu ochrony danych osobowych

§ 6

1. Do przetwarzania danych, zgodnie z art. 37 ustawy są dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych na wniosek przełożonego (Druk Nr 1) do załącznika nr 1.
2. Upoważnienie może być wydane po podpisaniu przez osobę ubiegającą się o dostęp oświadczenia (Druk Nr 2) do załącznika nr 1 dotyczącego zapoznania się z przepisami o ochronie danych osobowych i zobowiązania do zachowania w tajemnicy informacji związanych z ich przetwarzaniem.
3. Upoważnienia przechowuje się w aktach osobowych pracowników.
4. Ewidencję osób upoważnionych (Druk Nr 3) do załącznika nr 1 prowadzi ABI, na podstawie informacji otrzymanych od inspektora ds kadr.
5. Ewidencja zawiera nazwę zbioru danych, nazwisko i imię osoby upoważnionej, nr pokoju, identyfikator (przy przetwarzaniu w systemie informatycznym), data nadania upoważnienia, zakres upoważnienia, data wygaśnięcia / cofnięcia upoważnienia , uwagi.

§ 7

1. Codzienną kontrolę w zakresie ochrony danych osobowych sprawuje użytkownik.
2. Nadzór nad przestrzeganiem zasad ochrony danych osobowych w komórce organizacyjnej sprawuje bezpośredni kierownik komórki.
3. ABI sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych, przetwarzanych w systemach informatycznych i określonych niniejszą Polityką, oraz dokonuje kontroli i oceny funkcjonowania mechanizmów technicznych zabezpieczeń systemów, w których przetwarzane są dane osobowe.
4. Czynności o których mowa w ustępie 3, Administrator na wniosek ABI może zlecić innemu pracownikowi.

## Rozdział 5

## Postępowanie w przypadku naruszenia zabezpieczenia systemu ochrony danych osobowych

§ 8

1. Naruszenie ochrony danych osobowych, może być spowodowane:
   a) niewłaściwym oddziaływaniem czynników zewnętrznych, takich jak: temperatura otoczenia, wilgotność, pole elektromagnetyczne, wirusy komputerowe, skutki powodzi, pożaru, itp.;

b) niekontrolowanym działaniem osób trzecich, powodującym zaklócenia systemu podczas włamania, niewłaściwym działaniem zespołów serwisowych, przetwarzaniem danych osobowych bez uprawnień;

c) umyślnym lub nieumyślnym działaniem, a nawet zaniechaniem działania użytkowników przetwarzających dane osobowe lub osób odpowiedzialnych za ich ochronę.

d) niewłaściwym używaniem urządzeń takich jak laptop, notebook, netbook, mp3, mp4, smartphon, itp. umożliwiających zapisywanie, przenoszenie i odczytywanie danych.

2. Za naruszenie ochrony danych osobowych uważa się w szczególności:

a) brak możliwości fizycznego dostępu do danych np. zagubiony klucz do pomieszczenia, lub mebli biurowych, w których przechowywane są dokumenty, zniszczona szafa z dokumentami, brak nośników informacji, zalane pomieszczenie, brak sprzętu komputerowego itp.;

b) brak dostępu do zawartości zbioru danych – zbiór istnieje lecz nie można go otworzyć;

c) zmienioną zawartość zbioru, niepoprawną treść, postać, data, różnicę w danych itp.;

d) próbę lub fakt nieuprawnionego dostępu do zbioru danych lub pomieszczenia w którym jest przetwarzany np. zmiana ułożenia kolejności dokumentów, otwarte drzwi lub meble biurowe, nietypowe ustawienie sprzętu lub pojawienie się nowych dokumentów;

e) różnicę funkcjonowania systemu, a w szczególności wyświetlania komunikatów i informacji o błędach oraz nieprawidłowościach w wykonywaniu operacji;

f) zniszczenie lub próby zniszczenia, w sposób nieautoryzowany danych ze zbioru lub danych systemowych;

g) zmianę lub utratę danych zapisanych na kopiach awaryjnych lub zapisach archiwalnych;

h) nieskuteczne niszczenie nośników informacji zawierających dane osobowe (dyskietki, nośniki optyczne, wydruki papierowe), umożliwiające ponowny ich odczyt przez osoby nieuprawnione;

i) próba nielegalnego logowania się do systemu lub włamania do systemu;

j) zmienione oprogramowanie systemu, stwierdzone przez użytkownika po przerwie w przetwarzaniu danych.

3. Niniejszą Politykę stosuje się także w przypadku stwierdzenia, że stan pomieszczeń i szaf, bądź mebli biurowych, w których przechowuje się dokumentację lub zawartości tej dokumentacji wzbudzają podejrzenie, że dostęp do nich mogły mieć osoby trzecie.

§ 9

W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenie systemu ochrony, o których mowa w § 8 niniejszej Polityki, użytkownik zobowiązany jest do bezzwłocznego powiadomienia o tym fakcie przełożonego oraz ABI lub osobę upoważnioną przez ABI.

§ 10

1. Użytkownik do momentu przybycia ABI, lub osoby przez niego upoważnionej powinien:

a) zabezpieczyć dostęp do pomieszczenia lub urządzenia;

b) powstrzymać się od rozpoczęcia lub kontynuowania jakichkolwiek czynności mogących spowodować zatarcie śladów, bądź dowodów naruszenia ochrony;

c) zatrzymać pracę na komputerze, na którym zaistniało naruszenie ochrony oraz nie uruchamiać innych urządzeń, które mogą mieć związek z naruszeniem ochrony;

d) podjąć, stosownie do zaistniałej sytuacji działania, które zapobiegną ewentualnej utracie danych osobowych.

§ 11

1. ABI po otrzymaniu informacji o naruszeniu lub próbie naruszenia zabezpieczenia systemu przetwarzającego dane osobowe, podejmuje działania zmierzające do usunięcia powstałego zagrożenia.
2. Po przybyciu na miejsce, o którym mowa w ust. 1, ABI realizuje czynności w kolejności:
   a) ocenia sytuację, uwzględniając stan pomieszczenia, w którym przetwarzane są dane, stan urządzenia i zbioru oraz identyfikuje zakres negatywnych następstw naruszenia ochrony danych osobowych;
   b) wysłuchuje relacji użytkownika lub osoby, która dokonała powiadomienia;
   c) podejmuje działania mające na celu ustalenie sprawcy, miejsca, czasu i sposobu dokonania naruszenia ochrony;
   d) w zależności od zakresu naruszenia ochrony podejmuje decyzje o dalszym postępowaniu, wydając użytkownikowi stosowne polecenia i wskazówki do obsługi urządzeń;
   e) biorąc pod uwagę skalę oraz skutki naruszenia ochrony, ABI decyduje o powołaniu doraźnego zespołu i powiadomieniu o zdarzeniu Administratora lub osobę upoważnioną przez niego.

§ 12

1. ABI z przebiegu zdarzenia sporządza notatkę służbową, która obejmuje:
   a) dane osoby stwierdzającej naruszenie ochrony;
   b) datę, godzinę i miejsce naruszenia ochrony;
   c) rodzaj naruszenia ochrony;
   d) czas powiadomienia o zdarzeniu;
   e) opis podjętych czynności;
   f) wnioski do realizacji.
2. Notatkę o której mowa w ust. 1, ABI przekazuje Administratorowi lub osobie upoważnionej przez niego.

§ 13

Zgodę na ponowne uruchomienie komputera lub innych urządzeń oraz kontynuowanie przetwarzania danych, wyraża ABI lub osoba przez niego upoważniona.

§ 14

Dokonywanie zmian w miejscu naruszenia ochrony bez zgody, o której mowa w § 13 jest dopuszczalne tylko w przypadku konieczności ratowania osób, mienia albo zapobieżenia powstaniu innego niebezpieczeństwa.

§ 15

W przypadku powołania doraźnego zespołu, o którym mowa w § 11, pracą jego kieruje ABI.

1. Zespół z przeprowadzonych czynności sporządza protokół, w którym ujmuje skalę stwierdzonych naruszeń ochrony, przyczyny ich powstania oraz skutki jakie wpłynęły lub wpłynąć mogą na stan zabezpieczenia i ochrony danych osobowych.
2. Protokół zawierać powinien wnioski określające zakres działań organizacyjnych i technicznych, zapobiegających w przyszłości naruszeniom ochrony danych osobowych.
3. Protokół przekazywany jest Administratorowi lub osobie upoważnionej przez niego w celu akceptacji wniosków i zaleceń usprawniających zabezpieczenia ochrony danych.

§ 16

W przypadku stwierdzenia:

1. błędu użytkownika systemu – ABI przeprowadza dodatkowe szkolenie osób zatrudnionych przy przetwarzaniu danych w komórce organizacyjnej;
2. uaktywnienia wirusa – należy zgłosić ASI, który ustali źródło jego pochodzenia oraz uaktualni zabezpieczenia antywirusowe;
3. zaniedbania ze strony użytkownika – należy w stosunku do niego zastosować konsekwencje wynikające z właściwych przepisów prawa;
4. włamania, w celu nielegalnego pozyskania danych – należy dokonać szczegółowej analizy wdrożonych środków zabezpieczenia i zapewnić skuteczniejszą ochronę;
5. złego stanu urządzenia lub złego działania programu – należy niezwłocznie powiadomić ASI i przeprowadzić kontrolę czynności serwisowo-programowych.

## Rozdział 6

## Postanowienia końcowe

§ 17

1. Każdy użytkownik przetwarzający dane osobowe w zbiorach Urzędu Miejskiego w Kozienicach zobowiązany jest zapoznać się z niniejszą Polityką i stosować przepisy w niej zawarte na swoim stanowisku pracy.
2. Nadużycie przez użytkownika postanowień niniejszej Polityki może stanowić podstawę do pociągnięcia go do odpowiedzialności dyscyplinarnej, odszkodowawczej lub karnej, w trybie i na zasadach przewidzianych przepisami prawa.

§ 18

W sprawach nie uregulowanych niniejszą Polityką zastosowanie znajdują przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.) i rozporządzenia 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 2004 r. Nr 100, poz. 1024).

ZATWIERDZAM

Burmistrz Gminy Kozienice
dr inż. Tomasz Śmietanka

Załącznik nr 2
do zarządzenia Nr 355/2013
Burmistrza Gminy Kozienice
z dnia .06.11.2013r.

# INSTRUKCJA

## zarządzania systemem informatycznym w Urzędzie Miejskim w Kozienicach

Spis treści:

## Rozdział 1

## Postanowienia ogólne.

§ 1

Niniejsza „Instrukcja zarządzania systemem informatycznym w Urzędzie Miejskim w Kozienicach", zwana dalej **Instrukcją**, jest dokumentem wewnętrznym wydanym przez Burmistrza Gminy Kozienice i ma zastosowanie do przetwarzania danych osobowych w systemach informatycznych Urzędu Miejskiego w Kozienicach, zwanego dalej **Urzędem**, w celu bezpiecznego ich wykorzystywania.

§ 2

1. Instrukcja określa ogólne zasady i tryb postępowania Administratora Danych, osób wyznaczonych przez niego oraz wszystkich użytkowników, przetwarzających dane osobowe w systemach informatycznych Urzędu.
2. Instrukcja została opracowana zgodnie z wymogami § 3, 4 i 5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100 poz. 1024)

§ 3

Określenia i skróty użyte w § 2 Polityki (załącznik nr 1) stosuje się odpowiednio:

§ 4

1. Administrator na wniosek ABI może zlecić innej zatrudnionej osobie wykonywanie określonych czynności, leżących w zakresie jego obowiązków.
2. Kontrola prawidłowości wykonywania czynności o których mowa w ust. 1 należy do ABI.
3. Inna osoba, o której mowa w ust. 1 niezwłocznie informuje ABI o podjętych przez siebie czynnościach.

## Rozdział 2

## Przydział haseł i identyfikatorów dla użytkowników.

§ 5

Systemy, w których przetwarza się dane osobowe w zbiorach Urzędu muszą być wyposażone w mechanizmy uwierzytelnienia użytkownika oraz kontroli dostępu do nich osób.

§ 6

1. ABI prowadzi wykaz identyfikatorów (login).
2. Hasła dostępu opracowuje się indywidualnie dla każdego uprawnionego użytkownika systemu i natychmiast zmienia w przypadku podejrzenia lub stwierdzenia ujawnienia ich osobom trzecim.
3. Każdy użytkownik sam ustala dla siebie hasła dostępu do systemu, zawierające minimum osiem znaków w poziomie podstawowym i dwanaście znaków w poziomie podwyższonym.
4. Wykaz, o którym mowa w ust. 1 może być otworzony tylko w przypadku zaistnienia sytuacji szczególnych przez przełożonego użytkownika w obecności ABI.
5. Hasła dostępu zapisywane są na ekranie monitora w formie niejawnej i mogą być znane tylko użytkownikowi. Hasła dostępu nie mogą powtarzać się w danym roku.
6. Hasła obowiązują 30 dni i zmienia je użytkownik w pierwszy roboczy dzień każdego miesiąca lub wg wymagań aplikacji systemowych.
7. Osobą odpowiedzialną za techniczny sposób ustalania, przechowywania i wprowadzania haseł jest ABI, który określa w tym zakresie szczegółowe zasady w swoich wytycznych.

§ 7

1. Identyfikatory dla użytkowników przydziela ABI. Identyfikator po wylogowaniu danej osoby z systemu, nie może być przydzielony innemu użytkownikowi.
2. Identyfikator wpisuje się do „Ewidencji osób upoważnionych do przetwarzania danych osobowych", o której mowa w § 6 ust. 1 Polityki.

§ 8

1. Użytkownik ponosi odpowiedzialność za czynności wykonywane w systemie przy użyciu identyfikatora i hasła, którymi się posługuje lub posługiwał.
2. Użytkownik zobowiązany jest do utrzymania haseł dostępu w tajemnicy, a w szczególności do dołożenia starań, w celu uniemożliwienia zapoznania się z nimi osób trzecich, nawet po ustaniu ich ważności.

## Rozdział 3

## Rejestrowanie i wyrejestrowywanie użytkowników.

§ 9

1. Rejestracji i wyrejestrowania użytkowników z systemu na wniosek dokonuje ABI na podstawie informacji uzyskanej od inspektora ds. kadr, wprowadzając dane do ewidencji, o której mowa § 7 ust.
2. Jakakolwiek zmiana informacji wyszczególnionych w ewidencji podlega natychmiastowemu odnotowaniu.

§ 10

1. Zarejestrowanie użytkownika w systemie następuje po otrzymaniu upoważnienia do przetwarzania danych osobowych, o którym mowa w § 6 Polityki
2. Z chwilą zarejestrowania w systemie użytkownik jest informowany przez ABI o ustalonym dla niego identyfikatorze i obowiązku posługiwania się hasłem dostępu.

§ 11

1. Użytkownika wyrejestrowuje się z systemu na wniosek przełożonego - po utracie uprawnień dostępu do przetwarzania danych, co może mieć miejsce w sytuacjach:
   a) ustania zatrudnienia użytkownika u Administratora;
   b) zmiany zakresu obowiązków użytkownika.
2. Rozwiązanie umowy o pracę powoduje utratę dostępu do przetwarzania danych i natychmiastowe wyrejestrowanie użytkownika z systemu, wykreślenie identyfikatora z ewidencji oraz unieważnienie jego hasła. Identyfikatory, które utraciły ważność, odnotowuje ABI.
3. Pracownik ds. kadrowych zobowiązany jest do przekazywania informacji ABI w przypadku zaistnienia okoliczności, o których mowa w ust. 1 i 2.

## Rozdział 4

## Procedury rozpoczęcia i zakończenia pracy w systemie.

§ 12

1. Użytkownik rozpoczynający pracę zobowiązany jest przestrzegać procedur, które mają na celu sprawdzenie zabezpieczenia pomieszczenia, w którym przetwarzane są dane osobowe, swojego stanowiska pracy oraz stanu sprzętu komputerowego, a w szczególności:
   a) przed wejściem do pomieszczenia sprawdzić czy na drzwiach i zamkach nie ma widocznych śladów prób niepowołanego ich otwierania;
   b) sprawdzić stan okien i krat oraz ocenić czy w pomieszczeniu nie ma znaków wskazujących na pobyt w nim osób nieuprawnionych;
   c) sprawdzić stan sprzętu informatycznego oraz zamknięcie szaf i biurek;
   d) po włączeniu komputera ocenić jakość jego pracy i stwierdzić zmiany.

2. Użytkownik przed przystąpieniem do przetwarzania danych powinien zalogować się w systemie, posługując się swoim identyfikatorem i hasłem:
   a) maksymalna ilość prób wprowadzenia hasła do systemu wynosi 3;
   b) po przekroczeniu liczby prób logowania system blokuje dostęp do zbioru danych na poziomie użytkownika. Użytkownik powinien poinformować o tym zdarzeniu ABI, który podejmuje stosowne czynności;
   c) po zalogowaniu się należy ocenić pracę systemu i stan zbioru danych.
3. Użytkownik w czasie pracy powinien stosować przedsięwzięcia zapewniające bezpieczeństwo przetwarzania danych osobowych w systemie:
   a) ustawić ekrany monitorów w pomieszczeniach tak, aby uniemożliwiać podgląd osób nieuprawnionych;
   b) dopilnować aby w pomieszczeniach, stanowiących obszar przetwarzania danych osobowych przebywały osoby trzecie, tylko za zgodą przełożonych i w obecności osób uprawnionych;
   c) stosować urządzenia zabezpieczające przed utratą danych, spowodowaną awarią zasilania lub zakłóceniami w sieci elektrycznej. Potrzeby w tym zakresie zgłaszają ASI - przełożeni użytkownika;
   d) stosować wygaszacze ekranów, które włączają się po upływie 3 minut bezczynności komputera,
   e) stosować automatyczne wyłączanie dysku lub wylogowanie się z systemu w przypadku, kiedy przerwa w pracy trwa dłużej niż 30 minut.
4. Po zakończeniu pracy użytkownik powinien przestrzegać następujących zasad:
   a) wylogować się z systemu i zaczekać na jego wyłączenie się;
   b) sprawdzić czy nie zostały pozostawione bez nadzoru nośniki informacji;
   c) upewnić się, że szafy i biurka z dokumentacją są zamknięte;
   d) wyłączyć odbiorniki energii elektrycznej, zamknąć pomieszczenie i klucze oddać na portiernię.
5. Po godzinach pracy Administrator zapewnia monitorowanie i fizyczną ochronę pomieszczeń, w których przetwarzane są dane osobowe.

§ 13

Pomieszczenia, w których przetwarzane są dane osobowe w zbiorach zarejestrowanych u generalnego Inspektora Ochrony Danych Osobowych oraz zbiorach danych personalnych i finansowych - pracowników zatrudnionych przez Administratora, są zabezpieczone przed dostępem osób trzecich.

§ 14

1. W przypadku stwierdzenia przez użytkownika prób niepowołanego naruszenia zabezpieczenia fizycznego pomieszczenia, zmian w systemie bezpieczeństwa systemu lub zauważenia, że stan urządzeń, zawartość zbiorów danych, ujawnione metody pracy lub sposób działania programu mogą wskazywać na naruszenie danych osobowych – postępuje zgodnie z procedurą opisaną w rozdziale 5 § 8 – 16 Polityki (załącznik nr 1).
2. Rozpoczynając pracę użytkownik powinien zwrócić szczególną uwagę na okoliczności, o których mowa w ust. 1 i przypadku ich zaistnienia natychmiast informować ABI i przełożonego.

## Rozdział 5

## Tworzenie i przechowywanie kopii awaryjnych.

§ 15

1. Kopie danych osobowych oraz wszystkich zasobów komputera tworzy i przechowuje użytkownik w porozumieniu z ABI.
2. Kopie zasobów serwera tworzy ASI według harmonogramu.
3. Kopie awaryjne należy tworzyć na odpowiedniej jakości nośnikach dopuszczonych do użytku przez ABI, które należy szczegółowo opisać i przechowywać zgodnie z przepisami.
4. Tryb i harmonogram wykonywania kopii bezpieczeństwa:
   a) zasoby serwera – wykonuje ASI:
      - kopie zawartości serwera wykonywane są w trybie całościowym
      - ASI wykonuje kopie zawartości całego serwera z danymi osobowymi a także z danymi użytkowników na zapasowym serwerze.
      - ASI wykonuje kopie baz danych zawartych na serwerach raz dziennie poza godzinami pracy Urzędu.
      - ASI przechowuje kopie dzienne nie krócej niż 1 miesiąc, miesięczne nie krócej niż pół roku
   b) zasoby użytkownika na stacjach roboczych – wykonuje każdy użytkownik
      - kopie zawartości bazy danych wykonywane są w trybie całościowym
      - Użytkownik wykonuje kopie zapasowe w każdy piątek tygodnia i na koniec miesiąca. Przełożony może polecić codzienne wykonywanie kopii awaryjnych.
      - Użytkownik wykonuje kopie archiwalne na wskazanym katalogu udostępnionym w sieci lokalnej zatwierdzonego i dopuszczonego przez ABI i przechowuje je zgodnie z przepisami, lub wykonuje kopiowanie zawartości na serwer, z którego ABI wykonuje kopię archiwalną wszystkich zasobów serwera.
      - Użytkownik przechowuje kopie dzienne nie krócej niż 1 miesiąc, miesięczne nie krócej niż pół roku.

§ 16

1. Kopiowanie danych osobowych na nośniki informacji oraz robienie wydruków jest zabronione, chyba że istnieje konieczność ich sporządzenia, która wynika z nałożonych na użytkownika obowiązków i dozwolona jest przepisami prawa.
2. Wykorzystywanie nośników informacji lub wydruków w innym celu niż wskazany w ust.1 jest zabronione.
3. Każdy pracownik zobowiązany jest do podpisania oświadczenia o zapoznaniu się z używaniem zewnętrznych nośników danych, które stanowi Druk Nr 1 do załącznika nr 2.

§ 17

1. Czas przechowywania kopii awaryjnych, jeżeli nie stanowią inaczej przepisy prawa, należy ograniczyć do:
   a) codziennych - miesiąc;
   b) miesięcznych – 6 miesięcy.
2. Kopie awaryjne należy przechowywać w innych budynkach, jeśli są do tego warunki, niż zbiory danych osobowych.
3. Kopie awaryjne przechowuje ASI w miejscach wskazanych przez Administratora, zapewniających im odpowiednie warunki bezpieczeństwa.

§ 18

1. Użytkownik i ASI, po upływie dwóch miesięcy, sprawdzają kopie awaryjne i określa ich przydatność do wykorzystania w wypadku awarii systemu.
2. Zdezaktualizowane i uszkodzone kopie awaryjne należy mechanicznie niszczyć w sposób uniemożliwiający ich ponowne użycie.
3. Nie wolno sporządzać wydruków z kopii awaryjnych i innych nośników informacji, które podlegają zniszczeniu.

## Rozdział 6

## Ochrona systemu informatycznego przed wirusami komputerowymi.

§ 19

1. Użytkownik ma obowiązek na bieżąco sprawdzać obecność wirusów komputerowych. Czynność ta powinna być zaprogramowana w systemie, który automatycznie sygnalizuje obecność wirusów, w trakcie włączania systemu lub wprowadzania danych z zewnętrznych nośników informacji.
2. Kontrola antywirusowa systemu obejmować powinna wszystkie nośniki magnetyczne i optyczne, służące zarówno do przetwarzania danych osobowych w systemie, jak i do celów instalacyjnych.
3. Obowiązkiem ASI jest dostarczanie, uaktualnianie i instalowanie nowego oprogramowania antywirusowego.
4. O każdorazowym wykryciu wirusa użytkownik zobowiązany jest niezwłocznie powiadomić ASI, który po jego usunięciu sprawdza system i przywraca go do pełnej funkcjonalności.
5. ASI, po przeprowadzeniu analizy zasad działania wirusa, zobowiązany jest do przekazania Administratorowi informacji, o zaistnieniu takiego zdarzenia.

§ 20

1. Zabrania się użytkownikom wykorzystywania połączenia z Internetem w sieci z dostępem do danych osobowych do ściągania plików, instalacji i korzystania z oprogramowania, na które administrator nie posiada licencji oraz ignorowania komunikatów systemu antywirusowego.

§ 21

1. Każdy użytkownik systemu informatycznego jest monitorowany. Monitorowanie dotyczy poczynań użytkownika na jego stanowisku pracy oraz statystyk odwiedzanych stron internetowych.

## Rozdział 7

## Przechowywanie nośników informacji, w tym kopii informatycznych i wydruków.

§ 22

1. Nośniki informacji, w tym kopie informatyczne i wydruki komputerowe przechowuje się wyłącznie wówczas, gdy jest to konieczne i dozwolone przepisami prawa.
2. Nośniki informacji, w tym wydruki komputerowe przechowuje się w wyznaczonych pomieszczeniach w szafach i innych meblach biurowych, które posiadają odpowiednie zamknięcia, uniemożliwiające niepowołany dostęp do nich osób trzecich.
3. Pomieszczenia, o których mowa w ust. 2 winny spełniać określone warunki bezpieczeństwa, a w szczególności posiadać:
   a) wewnętrzne ściany, gwarantujące trwałe oddzielenie ich od innych pomieszczeń;
   b) pełne drzwi wejściowe, zaopatrzone w co najmniej jeden zamek (patentowy lub szyfrowy);
   c) odpowiednie zabezpieczenie okien przed dostępem z zewnątrz i obserwacją;

d) oznakowanie wywieszkami zabraniającymi osobom nieuprawnionym wstępu i przebywania w nich.

4. W razie uzasadnionej potrzeby ABI wprowadza dalej idące środki bezpieczeństwa dotyczące przechowywania nośników informacji w szafach i innych meblach biurowych, które winny być:
   a) zaopatrzone w co najmniej jeden zamek o skomplikowanym mechanizmie otwierania, tj. w szczególności zamek patentowy lub szyfrowy;
   b) po zakończeniu pracy zamknięte i opieczętowane.

## Rozdział 8

## Przeglądy i konserwacje systemów oraz zbiorów danych osobowych

§ 23

1. Okresowe przeglądy i konserwacje sprzętu komputerowego, wynikające z eksploatacji, warunków zewnętrznych oraz ważności systemu dla funkcjonowania Urzędu Miejskiego w Kozienicach, wykonuje ASI.
2. Urządzenia, dyski lub inne informatyczne nośniki informacji, przeznaczone do napraw w autoryzowanych firmach zewnętrznych, pozbawia się przed naprawą zapisu danych osobowych albo naprawia się je pod nadzorem ABI.

§ 24

1. Urządzenia, dyski lub inne informatyczne nośniki informacji, zawierające zapis danych osobowych przeznaczone do likwidacji należy pozbawić zapisu, a w przypadku gdy nie jest to możliwe, uszkodzić mechanicznie w sposób uniemożliwiający ich odczytanie.
2. Urządzenia, dyski lub inne informatyczne nośniki informacji, zawierające zapis danych osobowych przeznaczone do przekazania innemu podmiotowi, który nie jest uprawniony do otrzymania takich danych, należy wcześniej pozbawić zapisów danych.
3. Czynności, o których mowa w ust. 1 i 2 wykonuje komisja powołana przez Administratora na wniosek ABI.

## Rozdział 9

## Postępowanie w zakresie komunikacji w sieci komputerowej.

§ 25

1. Komunikacja w sieci komputerowej jest dozwolona tylko po odpowiednim zalogowaniu się i podaniu indywidualnego hasła użytkownika.
2. Wprowadzanie do systemu informacji z zewnątrz jest dopuszczalne tylko przy stwierdzeniu legalności i wiarygodności źródeł informacji i przez użytkownika posiadającego uprawnienia, wynikające z zakresu jego obowiązków.
3. Uprawnienia, o których mowa w ust. 1 wydaje ABI na pisemny wniosek przełożonego użytkownika.
4. Konfiguracja sieci jest wykonywana przez administratora sieci na wniosek ABI.
5. Wszelkie zmiany konfiguracji systemu podlegają ewidencji, którą prowadzi ASI.

§ 26

Pomieszczenie, w którym znajdują się serwery systemów, w miarę możliwości lokalowych i technicznych Administratora, powinno znajdować się na piętrze budynku, posiadać wentylację wymuszoną oraz spełniać warunki zawarte w § 22 ust. 3 i 4.

## Rozdział 10

## Postanowienia końcowe.

§ 27

1. Instalację nowego oprogramowania systemowego oraz oprogramowania użytkowego, gwarantującego bezpieczeństwo przetwarzania danych osobowych wykonuje ASI.
2. ABI prowadzi „Rejestr zbiorów danych osobowych przetwarzanych w systemach informatycznych".
3. Administrator realizuje co najmniej raz w roku szkolenia użytkowników systemów informatycznych, w których przetwarzane są dane osobowe.
4. ABI lub osoba upoważniona przez Administratora na wniosek ABI, dokonuje sprawdzenia sprawności funkcjonowania zabezpieczeń systemów, w których przetwarzane są dane osobowe, nie rzadziej niż raz na 4 miesiące. Z przeprowadzonych kontroli sporządza notatkę służbową, którą przedkłada przełożonemu.

§ 28

1. Każdy pracownik zatrudniony przy przetwarzaniu danych osobowych w systemie, zobowiązany jest zapoznać się z niniejszą Instrukcją i stosować jej przepisy na swoim stanowisku pracy.
2. Nadużycie przez użytkownika postanowień niniejszej Instrukcji, może stanowić podstawę do pociągnięcia go do odpowiedzialności przewidzianej właściwymi przepisami prawa.

§ 29

W sprawach nie uregulowanych niniejszą Instrukcją zastosowanie znajdują przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101 poz. 926 ze zm.) i 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. Nr 100 poz. 1024).

Urząd Miejski w Kozienicach
26-900 Kozienice, ul. Parkowa 5
tel. (048) 611-71-00
fax: (048) 614-20-48

.....
(pieczęć)

Kozienice, dnia 06.11.2013

**Druk Nr 1**
**do Polityki Bezpieczeństwa**

Na podstawie § 6 ust. 1 Polityki bezpieczeństwa informacji w Urzędzie Miejskim w Kozienicach,

**w n i o s k u j ę o udzielenie (pozbawienie)***

**Pani / Pana /* .....**

dostępu do przetwarzania danych osobowych w Urzędzie Miejskim w Kozienicach **z powodu:** /przyjęcia do pracy, przejścia na inne stanowisko, zwolnienia z pracy/* lub innego (jakiego?):

.....

1. **Nazwa zbioru** .....
   danych osobowych .....
2. **Uprawnienia:** (użytkownika systemu)* - (rozpatrywania wniosków)* z tytułu zajmowanego stanowiska (jakiego?) .....
3. Sposób przetwarzania danych osobowych: papierowy/ informatyczny/*
4. Miejsce przetwarzania (adres siedziby) .....
   danych osobowych (piętro, nr pokoju) .....
5. Wprowadzono poprawki do obowiązków pracownika, dotyczące zakresu przetwarzania danych osobowych i odpowiedzialności za to: **tak/ nie** *
6. Zobowiązano pracownika do podpisania oświadczenia o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych: **tak/ nie***

.....
(kierownik)

* niepotrzebne proszę skreślić

Burmistrz Gminy Kozienice
dr inż. Tomasz Śmietanka

**Druk Nr 2**
**do Polityki Bezpieczeństwa**

.....
(imię i nazwisko stażysty- praktykanta )

.....
(stanowisko )

# O Ś W I A D C Z E N I E

**Oświadczam, że zapoznałem się z przepisami dotyczącymi ochrony danych osobowych i zobowiązuję się do przestrzegania:**

1. Ustawy z dni 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. Dz.U. z 2002 r. Nr 101 poz. 926 z późn. zm.).
2. „Polityki bezpieczeństwa systemu informatycznego w Urzędzie Miejskim w Kozienicach".
3. „Instrukcji zarządzania systemem informatycznym, służącym do przetwarzania danych w Urzędzie Miejskim w Kozienicach

**Jednocześnie w czasie wykonywania swoich obowiązków służbowych zobowiązuję się do:**

a) zapewnienia ochrony danym osobowym przetwarzanym w zbiorach Urzędu Miejskiego w Kozienicach, a w szczególności zapewnienia ich bezpieczeństwa przed udostępnianiem osobom trzecim i nieuprawnionym, zabraniem, uszkodzeniem oraz nieuzasadnioną modyfikacją lub zniszczeniem,
b) zachowaniem w tajemnicy, także po ustaniu stażu - praktyki, wszelkich informacji dotyczących funkcjonowania systemów lub urządzeń służących do przetwarzania danych osobowych w zbiorach Urzędu Miejskiego w Kozienicach,
c) zachowania w tajemnicy hasła dostępu do systemów informatycznych, przetwarzających dane osobowe w Urzędzie Miejskim w Kozienicach, również po upływie jego ważności,
d) natychmiastowego zgłaszania przełożonemu i Administratorowi Bezpieczeństwa Informacji stwierdzenia, na swoim stanowisku pracy, próby lub faktu naruszenia zabezpieczenia fizycznego pomieszczenia, bezpieczeństwa zbioru lub systemu informatycznego, w którym przetwarzane są dane osobowe.

.....
(podpis stażysty-praktykanta )

Kozienice, dnia .....

---

Oświadczenie wypełnia tylko pracownik (również stażysta, praktykant), który wykonując swoje obowiązki służbowe, ma dostęp do przetwarzania danych osobowych. Oświadczenie jest niezbędne do realizacji zapisu art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych .

Burmistrz Gminy Kozienice
dr inż. Tomasz Śmietanka

Kozienice, dnia.....

**Druk Nr 1**
**do Instrukcji**
**zarządzania systemem**
**informatycznym**

# OŚWIADCZENIE

**o zapoznaniu się z zasadami używania zewnętrznych nośników danych**

Zgodnie z Zarządzeniem Burmistrza Gminy Kozienice Nr ..... z dnia ..... r. odnośnie polityki bezpieczeństwa informacji w Urzędzie Miejskim w Kozienicach, oświadczam, iż zapoznałem/łam się z poniższymi zasadami:

1. Zabrania się kopiowania i wynoszenia poza teren budynku Urzędu Miejskiego w Kozienicach na pendrive'y, napędy USB oraz inne urządzenia umożliwiające przenoszenie danych (w tym m.in.: dyskietki, dyski zewnętrzne, telefony komórkowe, iphony, ipody, urządzenia mp3, mp4, karty pamięci, płyty CD, DVD, Blue Ray, smartphon'y, palm topy, laptopy itp.) wszelkich danych poufnych, zastrzeżonych, danych osobowych oraz stanowiących tajemnicę służbową.
2. Wszelkie dane wymienione w pkt. 1 zawarte na urządzeniach zewnętrznych mogą być przetwarzane wyłącznie w Urzędzie Miejskim w Kozienicach na przeznaczonych do tego celu stanowiskach.
3. Za wszelkie awarie oraz za szkody wynikłe z posiadania na urządzeniach zewnętrznych szkodliwego w tym nielegalnego oprogramowania odpowiada pracownik.
4. W przypadku naruszenia zasad polityki bezpieczeństwa użytkownik zostanie m.in. pozbawiony możliwości korzystania z urządzeń zewnętrznych w postaci zablokowania portów USB w jego komputerze.

.....
(podpis pracownika)

Burmistrz Gminy Kozienice
dr inż. Tomasz Śmietanka