Załącznik do zarzadzenia
Nr 86..Burmistrza Pyrzyc z dnia 13.marca

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

I. Cel instrukcji

Instrukcja określa sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji. Instrukcja ma charakter uniwersalny i precyzuje zagadnienia zarządzania wszystkimi systemami informatycznymi znajdującymi się w Urzędzie Miejskim w Pyrzycach.

II. Definicje

ADO – Administrator Danych Osobowych (Burmistrz)

ASI – Administrator Systemów Informatycznych

LAS – Lokalny Administrator Systemu (Informatycy)

ABI – Administrator Bezpieczeństwa Informacji

Urząd – Urząd Miejski w Pyrzycach

Ustawa – Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

Instrukcja- Instrukcja zarządzania systemem informatycznym służacym do przetwarzania danych

III. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym.

1. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych jest zobowiązany z zapoznaniem się z:

a) Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych,

b) Polityką bezpieczeństwa systemów informatycznych do przetwarzania danych osobowych w Urzędzie Miejskim w Pyrzycach,

c) Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Pyrzycach,

oraz powinien posiadać upoważnienie do przetwarzania danych osobowych.

2. Zapoznanie się z Ustawą, Polityką bezpieczeństwa oraz niniejszą Instrukcją pracownik potwierdza własnoręcznym podpisem na oświadczeniu, którego wzór stanowi **Załącznik nr 3** do Instrukcji

3. Dostęp do systemu informatycznego służącego do przetwarzania danych osobowych może uzyskać wyłącznie osoba upoważniona przez ADO, zgodnie z Polityką bezpieczeństwa.
4. ASI na podstawie wniosku o nadanie uprawnień w systemie informatycznym, którego wzór stanowi **załącznik nr 1**, przyznaje uprawnienia w zakresie dostępu do systemu informatycznego, po akceptacji przez ABI.
5. ASI prowadzi i aktualizuje ewidencje, której wzór stanowi **załącznik nr 2**, osób upoważnionych do pracy w systemie informatycznym na którym przetwarzane są dane osobowe.
6. LAS ma takie same prawa jak ASI oraz zastępuje go w razie nieobecności.
7. Rejestracja użytkownika, polega na nadaniu unikalnego identyfikatora i przydzieleniu hasła oraz wprowadzeniu tych danych do bazy użytkowników systemu.
8. Wyrejestrowanie użytkownika z systemu informatycznego dokonuje ASI, po akceptacji ABI, na podstawie wniosku o nadanie uprawnień w systemie informatycznym, którego wzór stanowi **załącznik nr 1**, który przełożony użytkownika przekłada ASI z podaniem daty oraz przyczyny odebrania uprawnień.
9. Wyrejestrowanie, o którym mowa w pkt. 1, może mieć charakter czasowy lub trwały.
10. Wyrejestrowanie następuje przez:

a) zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe),
b) usunięcie danych użytkownika z bazy użytkowników systemu (wyrejestrowanie trwałe).

11. Przyczyną czasowego wyrejestrowania użytkownika z systemu informatycznego jest:

a) zawieszenie użytkownika w pełnieniu obowiązków służbowych,
b) wszczęcie postępowania dyscyplinarnego względem użytkownika,
c) wypowiedzenie użytkownikowi umowy o pracę

12. Informacje pisemną o zawieszeniu użytkownika w pełnieniu obowiązków służbowych, postępowaniu dyscyplinarnym względem użytkownika, wypowiedzeniu użytkownikowi umowy o pracę, przekazuje pracownik Kadr do ABI z chwilą ich zaistnienia.
13. Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy użytkownika.
14. Identyfikator osoby, która utraciła dostęp do systemu informatycznego należy niezwłocznie wyrejestrować oraz unieważnić hasło.

IV. Metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem

1. W systemie stosuje się uwierzytelnianie dwustopniowe: na poziomie dostępu do sieci lokalnej oraz dostępu do aplikacji.
2. Identyfikator składa się co najmniej z sześciu znaków, w skład których wchodzi nazwisko użytkownika, gdzie pierwsza litera nazwiska jest pisana dużymi literami, kolejne litery nazwiska pisane małymi literami oraz w przypadku zaistniałej konieczności stosowane są inne znaki. W identyfikatorze pomija się polskie znaki diaktryczne.
3. Identyfikator użytkownika w aplikacji (jeśli aplikacja na to pozwala), powinien być tożsamy z tym, jaki jest mu przydzielany w sieci lokalnej.
4. Identyfikator użytkownika nie powinien być zmieniany bez wyraźniej przyczyny, a po wyrejestrowaniu użytkownika z systemu nie powinien być przyznawany innemu użytkownikowi.
5. Kierownicy wydziałów zobowiązani są pisemnie informować ABI o każdej zmianie dotyczącej podległych im pracowników, która ma wpływ na zakres posiadanych uprawnień w systemie informatycznym.
6. Do uwierzytelniania użytkownika w systemie informatycznym stosowany jest mechanizm haseł.
7. Bezpośredni dostęp do systemu informatycznego może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.
8. Hasła generuje Informatyk. Hasło i identyfikator użytkownika jest przekazywane w formie ustnej.

9. Hasło użytkownika powinno być zmieniane nie rzadziej niż co 30 dni. Wprowadzone hasło powinno różnić się od co najmniej trzech ostatnio stosowanych.
10. Hasło jest zmieniane przez użytkownika.
11. Pracownicy są odpowiedzialni za zachowanie poufności hasła. W wypadku gdy istnieje podejrzenie że osoba nieuprawniona uzyskała dostęp do hasła należy powiadomić Informatyka w celu zmiany hasła.
12. Hasło powinno składać się z niepowtarzalnego ciągu co najmniej 8 znaków, zawierać małe i wielkie litery oraz cyfry i znaki specjalne o ile system informatyczny na to pozwala. Hasło powinno różnić się od identyfikatora, imienia oraz nazwiska użytkownika.
13. Nie należy korzystać z opcji zapamiętywania hasła w systemie.
14. Hasła do systemu przechowywane są w zamkniętej kopercie w szafie ognioodpornej w pomieszczeniu serwerowni, do którego dostęp mają wyłącznie Burmistrz, zastępca Burmistrza, Informatycy oraz ABI.

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

1. Rozpoczęcie pracy w systemie informatycznym obejmuje włączenie komputera, a następnie wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione.
2. W przypadku braku możliwości wpisania indywidualnego identyfikatora lub/i hasła, bądź braku dostępu do określonych zasobów systemu oraz w razie podejrzenia naruszenia bezpieczeństwa systemu należy poinformować Informatyka.
3. W przypadku konieczności opuszczenia stanowiska pracy użytkownik zobowiązany jest do wylogowania się z komputera (opcja „Wyloguj" z menu „Start" lub kombinacja klawiszy „klawisz z logo Windows i klawisz L"). Wznowienie pracy wymaga ponownego wpisania hasła użytkownika.
4. Należy uniemożliwić podgląd danych osobowych na ekranach komputerów przez osoby nieupoważnione poprzez odpowiednie ustawienie ekranów (ustawienie monitora powinno uniemożliwić podgląd).
5. Zakończenie pracy w systemie informatycznym obejmuje prawidłowe zamknięcie uruchomionych aplikacji oraz wylogowanie się z systemu i wyłączenie komputera.
6. Obowiązuje bezwzględny zakaz robienia kopii danych które zawierają dane osobowe i wynoszenia ich poza Urząd na jakichkolwiek zewnętrznych nośnikach danych bez uprzedniej zgody ADO, z wyjątkiem

sytuacji, w których jest to niezbędne ze względu na rodzaj realizowanego zadnia.

7. Obowiązuje bezwzględny zakaz modernizacji (aktualizacji) sprzętu oraz oprogramowania przez użytkowników na stacji roboczej. Wszelkie zmiany dokonywane są przez Informatyka lub pod jego nadzorem stosując instrukcję użytkownika systemu , programu, urządzenia itp.
8. W przypadku wystąpienia usterek w pracy komputerów lub błędów w oprogramowaniu, a także w przypadku ręcznej aktualizacji oprogramowania należy zgłosić ten fakt informatykowi.
9. Przy przetwarzaniu danych osobowych na komputerach przenośnych obowiązują procedury jak podczas pracy na komputerach stacjonarnych. Dodatkowo:

   a) obowiązuje bezwzględny zakaz używania komputerów przenośnych przez osoby inne niż użytkownicy, którym zostały one przydzielone,
   b) użytkownicy, którym zostały przydzielone komputery przenośne, powinny chronić je przed uszkodzeniem, kradzieżą oraz dostępem osób postronnych oraz zachować szczególną ostrożność podczas ich transportu.

VI. Procedury tworzenia, przechowywania i niszczenia kopii zapasowych

1. Kopie zapasowe tworzy się:

a) codziennie – całościowe kopie w przypadku programów SIGID, PB_ewid, PB_usc, MIENIE na taśmach magnetycznych, oraz dodatkowo dwa razy w tygodniu na płytach DVD,
b) raz w tygodniu – całościowa kopia w przypadku Elektronicznego Obiegu Dokumentów na taśmach magnetycznych,
c) kwartalnie – całościowa kopia w przypadku programu SUMPRO na zewnętrznym dysku twardym,
d) kwartalnie – całościowe kopie w przypadku pozostałych programów na płytach CD/DVD.

2. W przypadku lokalnego przetwarzania danych osobowych na stacjach roboczych użytkownicy zobowiązani są do centralnego przechowywania kopii danych, tak aby możliwe było zabezpieczenie ich dostępności poprzez wykonywanie kopii zapasowych.
3. Nad poprawnym wykonaniem kopii zapasowych nadzór sprawuje informatyk.

4. Wybrane kopie wykonywane są po zakończeniu pracy wszystkich użytkowników w sieci komputerowej.
5. W przypadku wykonywania zabezpieczeń długoterminowych na taśmach magnetycznych, dyskach zewnętrznych lub płytach CD/DVD, nośniki te należy dwa razy w roku sprawdzać pod kątem ich dalszej przydatności. Polega to na odtworzeniu danych w warunkach testowych i sprawdzeniu, czy jest możliwość odczytania danych.
6. Kopie zapasowe przetrzymuje się w zamykanej na klucz szafie ognioodpornej w pomieszczeniu innym niż serwerownia do czasu stwierdzenia utraty przedmiotu ich przydatności. Dostęp do kopii zapasowych mają jedynie Burmistrz, zastępca Burmistrza, Informatycy, oraz ABI.
7. Po zakończeniu eksploatacji lub uszkodzeniu nośników danych służących do sporządzania kopii zapasowych dokonuje się fizycznego ich zniszczenia w sposób uniemożliwiający odczyt danych.

VII. Procedura używania, przechowywania i niszczenia elektronicznych nośników informacji zawierających dane osobowe.

1. Elektroniczne zewnętrzne nośniki informacji tj. dyskietki, taśmy magnetyczne, dyski magnetyczne (twarde), dyski optyczne (CD/DVD), pamięci zewnętrzne podpinane do komputera za pomocą złącza USB np. typu Pendrive, na których są przechowywane dane osobowe mogą być używane w wyjątkowych sytuacjach związanych z realizacją określonych zadań za zgodą ABI oraz nie mogą być wynoszone poza siedzibę Urzędu.
2. Elektroniczne zewnętrzne nośniki informacji zawierające dane osobowe należy przechowywać w miejscach zabezpieczających je przed nieuprawnionym przechwyceniem, uszkodzeniem lub zniszczeniem zgodnie z wymogami przewidzianymi dla danych osobowych, w formie tradycyjnej (papierowej) w Polityce bezpieczeństwa.
3. Zabrania się przetwarzania całych zbiorów danych osobowych na elektronicznych zewnętrznych nośnikach informacji a także przesyłanie ich pocztą elektroniczną. Dozwolone jest jedynie przetwarzanie oraz przesyłanie ich jednostkowych danych osobowych w postaci zaszyfrowanej.
4. W przypadku posługiwania się elektronicznymi nośnikami informacji pochodzącymi od podmiotów z zewnątrz, użytkownik zobowiązany jest do sprawdzenia programem antywirusowym dany nośnik w celu weryfikacji czy nie zawiera on zagrożenia w postaci wirusów oraz innego złośliwego oprogramowania.

5. Elektroniczne zewnętrzne nośniki informacji zawierające dane osobowe:

a) jednorazowego użytku tj. płyty CD-R, DVD-R, na których znajdują się nieaktualne lub zbędne dane niszczy się w sposób fizyczny uniemożliwiający odczyt danych,
b) wielorazowego użytku tj. płyty CD-RW, DVD-RW, dyski twarde, pendrive, dyskietki itp., na których znajdują się nieaktualne lub zbędne dane można wykorzystać ponownie po usunięciu ich zawartości w sposób uniemożliwiający ich odzyskanie,
c) wielorazowego użytku które nie nadają się do ponownego wykorzystania, niszczy się w sposób fizyczny uniemożliwiający odczyt danych.

VIII. Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego oraz wirusami komputerowymi.

1. W Urzędzie wszystkie stanowiska komputerowe połączone są siecią wewnętrzną oraz z siecią publiczną Internet.
2. Z uwagi na wysokie ryzyko infekcji wirusami oraz innym złośliwym oprogramowaniem wszystkie stanowiska komputerowe mają zainstalowany program antywirusowy. Dodatkowo na styku sieci publicznej i sieci wewnętrznej znajduje się specjalne urządzenie sprzętowe typu Firewall, które chroni sieć wewnętrzną przed zagrożeniami z sieci publicznej.
3. Sprawdzanie obecności wirusów oraz innego złośliwego oprogramowania odbywa się za pomocą programu antywirusowego, sprawującego ciągły nadzór (ciągła praca w tle) nad pracą systemu informatycznego jego zasobami oraz stacjami roboczymi oraz serwerami.
4. Informatyk zapewnia aktualizacje definicji wirusów programu antywirusowego oraz jest odpowiedzialny za zarządzanie tym oprogramowaniem. System antywirusowy jest aktualizowany na podstawie materiałów publikowanych przez producenta oprogramowania.
5. Użytkownicy mogą korzystać z zewnętrznych nośników informacji jedynie po sprawdzeniu danego nośnika programem antywirusowym zaraz po podłączeniu go do stacji roboczej.
6. Użytkownik jest zobligowany niezwłocznie powiadomić Informatyka:

a) w razie komunikatów o zagrożeniu wysyłanych przez program antywirusowy,
b) w razie stwierdzenia nieprawidłowości w funkcjonowaniu sprzętu lub oprogramowania.

7. W przypadku wykrycia wirusów lub innego złośliwego oprogramowania i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy Informatyk podejmuje działania zmierzające do usunięcia zagrożenia. W szczególności działania te mogą obejmować:

   a) usunięcie zainfekowanych plików, o ile jest to akceptowalne ze względu na prawidłowe funkcjonowanie systemu informatycznego,
   b) odtworzeniu plików z kopii zapasowych po uprzednim sprawdzeniu, czy dane zapisane na kopiach nie zostały zainfekowane,
   c) samodzielną ingerencję w zawartość pliku, w zależności od posiadanego oprogramowania.

IX. Kontrola nad wprowadzeniem, dalszym przetwarzaniem i udostępnianiem danych osobowych.

1. System informatyczny umożliwia:

   a) przypisanie wprowadzonych danych użytkownikowi (identyfikatorowi użytkownika), który te dane wprowadza do systemu,
   b) sygnalizację wygaśnięcia czasu obowiązywania hasła dostępu do systemu,
   c) sporządzenie i wydrukowanie dla każdej osoby, której dane są przetwarzane w systemie, raportu zwierającego datę pierwszego wprowadzenia danych do systemu oraz identyfikator użytkownika wprowadzającego te dane.

2. Odnotowanie informacji, o których mowa w pkt. 1 ppkt. c), następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.
3. Dane osobowe z używanego systemu informatycznego mogą być udostępniane wyłącznie osobom uprawnionym.
4. Dane osobowe nie mogą być udostępniane drogą telefoniczną.
5. W przypadku przesyłania danych osobowych poza sieć przystosowaną do transferu danych osobowych zostają zastosowane szczególne środki w zakresie bezpieczeństwa. Obejmują one:

   a) zatwierdzenie przez ABI informacji w celu wysłania danych,
   b) zastosowanie mechanizmów szyfrowania danych osobowych,
   c) zastosowanie mechanizmów podpisu elektronicznego zabezpieczającego transmisję danych osobowych,
   d) umożliwienie wysyłania danych osobowych tylko z wykorzystaniem określonej aplikacji i tylko przez określonych użytkowników.

X. Procedury wykonywania przeglądów, konserwacji i naprawy systemów oraz elektronicznych nośników informacji służących do przetwarzania danych.

1. Dla zachowania ciągłości pracy i bezpieczeństwa systemów informatycznych przeprowadza się przeglądy, konserwacje, naprawy oraz zmiany (aktualizacje).
2. Wszelkie przeglądy, konserwacje, naprawy oraz zmiany w systemie informatycznym przeprowadzane są przez Informatyka przy zachowaniu odpowiedniego poziomu bezpieczeństwa danych oraz przed dostępem osób nieuprawnionych.
3. Przeglądy, konserwacje, aktualizacje powinny być wykonywane w terminach określonych przez producenta sprzętu, oprogramowania.
4. Nieprawidłowości wykryte podczas tych działań powinny być natychmiastowo usunięte, a przyczyny powstania nieprawidłowości powinny być przeanalizowane. O wykrytych nieprawidłowościach należy zawiadomić ABI.
5. Przeglądy, konserwacje, naprawy i zmiany w systemie informatycznym przez serwisanta prowadzone są pod nadzorem Informatyka, jeżeli jest to możliwe w siedzibie Urzędu z zachowaniem zasad ochrony danych osobowych.
6. Jeżeli jest to konieczne przeglądy, konserwacje, naprawy i zmiany mogą być dokonywane przez serwisanta poza siedzibą Urzędu wyłącznie na podstawie odpowiednich umów zawierających zapisy o powierzeniu przetwarzania danych osobowych lub po uprzednim usunięciu danych w nich przetwarzanych w sposób uniemożliwiający ich odczytanie.

XI. Postępowanie w przypadku stwierdzenia naruszenia bezpieczeństwa systemu informatycznego.

1. Użytkownik systemu informatycznego zobowiązany jest zawiadomić niezwłocznie ABI lub Informatyka o każdym naruszeniu lub podejrzeniu naruszenia bezpieczeństwa systemu, a w szczególności o:

   a) użyciu hasła dostępu i identyfikatora przez inne osoby niż uprawniony do nich użytkownik,

   b) braku reakcji systemu na wprowadzone hasło, bądź możliwości dostępu do systemu bez użycia hasła,

   c) częściowym lub całkowitym braku danych, bądź dostępie do danych na wyższym poziomie niż przyznane uprawnienia,

   d) braku dostępu do właściwej aplikacji, bądź zmianie zakresu dostępu do zasobów serwera,

   e) wykryciu wirusa i innego złośliwego oprogramowania,

   f) zmianie położenia sprzętu komputerowego lub nośników informacji zawierających dane osobowe,

   g) kradzieży sprzętu komputerowego lub nośników informacji zawierających dane osobowe,

   h) zauważeniu śladów usiłowania lub dokonania włamania do pomieszczeń lub zamykanych szaf.

2. Użytkownik systemu do czasu przybycia na miejsce ABI lub Informatyka powinien:

   a) jeżeli istnieje taka możliwość, niezwłocznie podjąć czynności niezbędne do powstrzymania niepożądanych skutków zaistniałego zdarzenia a następnie uwzględnić w działaniu również ustalenie jego przyczyny lub sprawców,

   b) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,

   c) zaniechać – jeżeli to możliwe – dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,

e)przygotować opis incydentu,

f)nie opuszczać bez uzasadnionej przyczyny miejsca zdarzenia do czasu przybycia ABI lub Informatyka.

3.Informatyk przyjmujący zawiadomienie jest obowiązany niezwłocznie poinformować ABI o naruszeniu lub podejrzeniu naruszenia bezpieczeństwa systemu.

4.ABI po otrzymaniu zawiadomienia powinien podjąć działania wyjaśniające w celu ustalenia okoliczności naruszenia ochrony danych osobowych, podjąć działania chroniące system przed ponownym naruszeniem, a w przypadku stwierdzenia faktycznego naruszenia bezpieczeństwa systemu sporządzić raport naruszenia bezpieczeństwa systemu informatycznego, a następnie niezwłocznie przekazać jego kopie ADO.

5.ABI w uzgodnieniu z ASI może zarządzić, w razie potrzeby, odłączenie części systemu informatycznego dotkniętej incydentem od pozostałej jego części.

6.ADO po zapoznaniu się z raportem, o którym mowa w pkt. 4, podejmuje decyzję o dalszym trybie postępowania, powiadomieniu właściwych organów oraz podjęciu innych, szczególnych czynności zapewniających bezpieczeństwo systemu informatycznego bądź zastosowaniu środków ochrony fizycznej.

7.ABI i ASI zobowiązani są do informowania ADO o awariach systemu informatycznego, zauważonych przypadkach naruszenia niniejszej instrukcji przez użytkowników, a zwłaszcza o przypadkach posługiwania się przez użytkowników nieautoryzowanymi programami, nieprzestrzegania zasad używania oprogramowania antywirusowego, niewłaściwego wykorzystania sprzętu komputerowego lub przetwarzania danych w sposób niezgodny z procedurami ochrony danych osobowych.

XII Postanowienia końcowe.

1. W przypadkach nie określonych instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych należy stosować postanowienia Polityki bezpieczeństwa, a także instrukcje obsługi i zalecenia producentów aktualnie wykorzystywanych urządzeń i programów oraz umów serwisowych.

Załącznik nr 1 do Instrukcji

Wniosek przełożonego o nadanie uprawnień dla użytkownika w systemie informatycznym.

Nowy użytkownik	Modyfikacja uprawnień	Odebranie uprawnień w systemie

DOTYCZY SYSTEMU:

.....

.....

(nazwa systemu (aplikacji), w którym przetwarzane są dane osobowe)

Imię i nazwisko użytkownika:	**Wydział/Samodzielne stanowisko**	
Posiada upoważnienie do przetwarzania danych osobowych:	TAK	NIE
Opis zakresu uprawnień użytkownika w systemie informatycznym:		
Data zagłoszenia:	Podpis przełożonego Użytkownika systemu:	
Podpis ASI:	Akceptacja ABI:	

Wyżej przedstawiony wniosek wypełnia przełożony pracownika i dostarcza do ASI, oraz ABI.

Załącznik nr 2 do Instrukcji

Ewidencja osób upoważnionych do pracy w systemie informatycznym oraz upoważnionych do przetwarzania danych osobowych

L.p.	Nazwisko, Imię	System/aplikacja	Zakres upoważnienia do przetwarzania danych osobowych	Data nadania uprawnień	Data ustania uprawnień	Identyfikator użytkownika

Załącznik nr 3 do Instrukcji

Pyrzyce, dnia .....

.....
(nazwisko i imię)

.....
(stanowisko)

OŚWIADCZENIE

Oświadczam, iż w związku z wykonywanymi obowiązkami służbowymi, przetwarzam lub mam dostęp do zbiorów, dokumentów, zestawień, kartotek lub systemów informatycznych zawierających dane osobowe i w związku z tym zapoznałem(am) się z:

1. Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych,
2. Polityką bezpieczeństwa systemów informatycznych do przetwarzania danych osobowych w Urzędzie Miejskim w Pyrzycach,
3. Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Pyrzycach,

.....
(podpis pracownika)