Załącznik Nr 2

ZATWIERDZAM

do Zarządzenia Nr 1492/2016

Prezydenta Miasta Radomia

Prezydenta Miasta Radomia

z dnia 30 czerwca 2016 r

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM W TYM DO PRZETWARZANIA DANYCH OSOBOWYCH W URZĘDZIE MIEJSKIM W RADOMIU

Spis treści instrukcji:

Rozdział 1. Postanowienia ogólne.

Rozdział 2. Procedury zarządzania i kontroli dostępu do systemów informatycznych.

Rozdział 3. Zasady posługiwania się hasłami (złożoność, okresowość wymiany, sposób przekazywania użytkownikowi).

Rozdział 4. Aplikacje i usługi zabronione.

Rozdział 5. Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie informatycznym.

Rozdział 6. Zasady i sposób odnotowania w systemie informacji o udostępnieniu danych osobowych,

funkcjonalność systemu.

Rozdział 7. Zasady komunikacji w sieci teleinformatycznej

Rozdział 8. Konserwacja i naprawa systemu informatycznego w tym przetwarzającego dane osobowe

Rozdział 9. Procedura postępowania w sytuacji naruszenia ochrony danych osobowych.

Rozdział 10. Procedura zarządzania zmianą w systemach informatycznych.

Rozdział 11. Procedura rejestracji działań dokonywanych na krytycznych systemach informatycznych.

Rozdział 12. Zasady ochrony antywirusowej.

Rozdział 13. Procedura zarządzania kopiami zapasowymi.

Rozdział 14. Zasady zarządzania komputerami przenośnymi.

Rozdział 15. Postanowienia końcowe.

Rozdział I

Postanowienia ogólne.

§ 1

1. Niniejsza ,,Instrukcja zarządzania systemem informatycznym w tym do przetwarzania danych osobowych", zwana dalej Instrukcją, obejmuje swoim zakresem wszystkie osoby biorące udział w procesie przetwarzania danych osobowych w Wydziałach, Biurach Urzędu Miejskiego w Radomiu, w szczególności zaś osoby pełniące funkcje:

a) administratora bezpieczeństwa informacji,

b) administratorów systemów informatycznych,

c) lokalnych administratorów danych osobowych,

d) dyrektorów/kierowników komórek organizacyjnych Urzędu,

e) inne osoby wskazane przez administratora danych osobowych.

2. Instrukcja ma zastosowanie także do podmiotów zewnętrznych i osób fizycznych, które współpracują z Urzędem i na podstawie przepisów współuczestniczą w procesie przetwarzania danych osobowych, a w szczególności:

a) podmioty, którym na podstawie przepisów udostępniono dane osobowe,

b) podmioty, którym na podstawie umowy przekazano lub udostępniono dane osobowe do przetwarzania,

c) przedsiębiorcy świadczący usługi związane z konserwacją systemu informatycznego,

d) inne osoby, niebędące pracownikami Urzędu, wykonujące prace na podstawie stosunków cywilnoprawnych.

§ 2

Instrukcja została opracowana zgodnie z wymogami § 5 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. Nr 101 poz. 926 z 2002 r., z póź. zm, Dz. U. Nr 100, poz. 1024).

§ 3

Definicje ilekroć w instrukcji jest mowa o:

1. Administratorze Danych – rozumie się przez to Prezydenta Miasta Radomia.

2. Administratorze Bezpieczeństwa Informacji – należy przez to rozumieć pracownika wyznaczonego przez Prezydenta Miasta oraz podlegającego bezpośrednio pod Prezydenta Miasta Radomia w rozumieniu art. 36a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r., poz. 922) zwanej dalej Ustawą.

3. Administratorze Systemu Informatycznego – należy przez to rozumieć pracownika lub pracowników Wydziału Teleinformatycznego oraz Biura ds. Systemów i Projektów Oświatowych Współfinansowanych przez UE w zakresie Zintegrowanego Systemu Zarządzania Oświatą odpowiedzialnych za funkcjonowanie:

- infrastruktury informatycznej Urzędu Miejskiego w Radomiu, na którą składa się cały sprzęt informatyczny oraz oprogramowanie,
- za ich przeglądy, konserwację,
- za stosowanie technicznych i organizacyjnych środków bezpieczeństwa w systemach informatycznych.

4. Lokalnych Administratorach Danych Osobowych należy przez to rozumieć Dyrektorów/Kierowników Komórek Organizacyjnych Urzędu Miejskiego w Radomiu posiadających stosowne pełnomocnictwo udzielone przez Administratora Danych Osobowych **–** odpowiedzialnych za prowadzony przez podległą komórkę zbiór danych osobowych, a w szczególności za przestrzeganie zasad określonych art. 26 UODO.

5. Dyrektorach/Kierownikach komórek organizacyjnych - odpowiedzialni za przestrzeganie zasad przetwarzania i ochrony danych osobowych przez podległych pracowników przetwarzających dane osobowe w podległych komórkach organizacyjnych

6. Osobie upoważnionej - osoba posiadająca upoważnienie nadane przez Administratora Danych Osobowych lub osobę wyznaczona przez niego i uprawniona do przetwarzania danych osobowych w zakresie wskazanym w upoważnieniu.

7. Przetwarzaniu danych – należy przez to rozumieć jakiekolwiek operacje wykonywane na danych w rozumieniu art. 7 pkt 2 Ustawy

8. Użytkowniku systemu – osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.

9. Systemie informatycznym, zwanym dalej systemem w rozumieniu art. 7 pkt 2a Ustawy

10. Ustawa – rozumiana jako ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2016 poz.922)

11. Urzędzie – należy przez to rozumieć Urząd Miejski w Radomiu.

12. Użytkowniku zewnętrznym - należy przez to rozumieć osobę nie będącą pracownikiem lub stażystą Urzędu, posiadającą uprawnienia do przetwarzania informacji w związku z wykonywaniem czynności na rzecz Urzędu.

13. Uwierzytelnieniu – należy przez to rozumieć identyfikację użytkownika za pomocą identyfikatora oraz hasła potwierdzająca jego uprawnienia.

14. Indywidualne stanowisko komputerowe – komputer stacjonarny, na którym przetwarzane są dane osobowe w zbiorze bez połączenia do sieci teleinformatycznej.

15. Zabezpieczeniu danych w systemie, zwanym dalej zabezpieczeniem – czynności wykonywane w rozumieniu art. 7 pkt 2b Ustawy.

16. Wewnętrzna sieć teleinformatyczna – sieć Administratora, łącząca co najmniej dwa indywidualne stanowiska komputerowe, umożliwiająca użytkownikom określony dostęp do danych osobowych.

17. Dane sensytywne – dane w rozumieniu art. 27 Ustawy, podlegające szczególnej ochronie.

18. Polityce Bezpieczeństwa – należy przez to rozumieć dokumentację opisującą sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych odpowiednie do zagrożeń oraz kategorii danych osobowych, rozumianą także jako zestaw praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji danych osobowych w Urzędzie Miejskim w Radomiu.

19. Krytyczne systemy informatyczne – systemy, których działanie ma wpływ na świadczone usługi. Awaria może spowodować spadek jakości świadczonych usług a nawet przerwanie wykonywania usług, konsekwencje prawne, finansowe lub wpływa na wizerunek Urzędu.

20. Szczegółowych instrukcjach operacyjnych – należy przez to rozumieć instrukcje i procedury określające pracę poszczególnych systemów.

21. Środowisku testowym – należy przez to rozumieć odrębną wyizolowaną część systemu informatycznego, w której dokonuje się sprawdzenia poprawności działania oprogramowania i sprzętu komputerowego, w środowisku identycznym jak produkcyjne.

22. Bazach sygnatur wirusów – należy przez to rozumieć bazy wirusów z którymi porównywane są sprawdzane obiekty i w przypadku stwierdzenia zgodności podejmowane są ustalone działania.

23. Instrukcji – należy przez to rozumieć „Instrukcję Zarządzania Systemem Informatycznym w tym do przetwarzania danych osobowych.”.

24. Serwisancie – należy przez to rozumieć upoważnionego pracownika firmy świadczącej usługi w zakresie naprawy i konserwacji sprzętu i oprogramowania

25. Zbiór danych – zbiór w rozumieniu art. 7 pkt 1 Ustawy.

Rozdział 2

Procedury zarządzania i kontroli dostępu do systemów informatycznych.

§ 4

Potrzebę dostępu pracowników do programów komputerowych, danych, usług sieciowych – określa kierownik macierzystej komórki organizacyjnej. Administrator Systemu Informatycznego przed nadaniem stosownych uprawnień dostępu pracownikowi dokonuje przeglądu i przygotowania jego stanowiska komputerowego.

Do przetwarzania danych osobowych mogą służyć wyłącznie systemy informatyczne i zewnętrzne nośniki danych będące własnością Urzędu Miejskiego w Radomiu, które odnotowane zostały w stosownej ewidencji o której mowa w § 34 ,,Polityki Bezpieczeństwa Informacji i Ochrony Danych Osobowych”

§ 5

Zasady przyznawania dostępu do systemów informatycznych i usług sieciowych.

1. Do przetwarzania danych osobowych w systemach informatycznych mogą mieć dostęp wyłącznie osoby posiadające upoważnienie nadane przez Administratora lub osobę przez niego upoważnioną.

2. Procedury nadawania / cofania upoważnień do danych osobowych zawarte zostały w § 19

,,Polityka Bezpieczeństwa Informacji i Ochrony Danych Osobowych”

3. Procedura nadawania upoważnień do przetwarzania innych danych:

a) Przyznanie dostępu do innych danych i usług zawartych w systemach informatycznych wymaga złożenia wniosku kierownika komórki organizacyjnej do Administratora Systemu Informatycznego.

b) Wniosek powinien zawierać: imię i nazwisko osoby, której mają być udostępnione dane lub usługa, datę, nazwę programu/usługi, proponowany zakres uprawnień. Na podstawie złożonego wniosku ASI nadaje uprawnienia do przetwarzania informacji lub dostęp do usług w systemach informatycznych po uprzednim przeglądzie i przygotowaniu stanowiska komputerowego.

c) **ASI** przechowuje złożone wnioski i prowadzi rejestr osób posiadających uprawnienia do danych i usług w systemach informatycznych.

d) Kierownik komórki organizacyjnej, w ciągu 7 dni od zwolnienia, przeniesienia użytkownika do innej komórki organizacyjnej lub w przypadku innej uzasadnionej okoliczności, jest zobowiązany złożyć wniosek do ASI o odebranie uprawnień temu użytkownikowi.

e) ASI bez zbędnej zwłoki cofa uprawnienia dostępu do danych lub usługi w systemie informatycznym.

Rozdział 3

Zasady posługiwania się hasłami (złożoność, okresowość wymiany, sposób przekazywania użytkownikowi)

§ 6

Uwierzytelnienie użytkownika w systemie informatycznym następuje za pomocą identyfikatorów i haseł.

W systemie informatycznym zastosowano uwierzytelnianie w zakresie:

- dostępu do systemu operacyjnego,
- dostępu do aplikacji.

Dodatkowo zastosowano zabezpieczenie w postaci hasła dostępu do uruchomienia komputera.

§ 7

Komputery stacjonarne oraz komputery przenośne posiadające dostęp do sieci publicznej (Internet) poprzez inną niż sieć komputerowa Urzędu, mogą służyć do przetwarzania danych osobowych w zbiorach tylko za zgodą Administratora Danych Osobowych i po akceptacji Administratora Bezpieczeństwa Informacji.

W systemie informatycznym stosowane są zabezpieczenia systemów informatycznych na poziomach:

- podstawowym,
- podwyższonym,
- wysokim.

1. Poziom podstawowy:

a) Dostęp do komputera powinien być zabezpieczony hasłem uruchomieniowym.

b) Po założenia konta Administrator Systemu Informatycznego przekazuje użytkownikowi:

- identyfikator,
- hasło dostępu.

c) Niezwłocznie po otrzymaniu identyfikatora i hasła, o którym mowa w postanowieniu poprzednim, jednak nie później niż do końca dnia roboczego, w którymi to nastąpiło, użytkownik zmienia to hasło.

d) Hasła uprawniające do korzystania z aplikacji użytkownik wpisuje osobiście. Hasła nie są wyświetlane na ekranie monitora.

e) Hasła dostępu użytkownika do systemu tworzone są zgodnie z instrukcjami operacyjnymi specyficznymi dla poszczególnych systemów oraz aplikacji. Każde hasło powinno składać się z co najmniej 6 znaków, w tym jednej cyfry bądź znaków specjalnych.

f) Tworząc hasło nie należy używać: imion swoich lub często spotykanych, rzeczowników pospolitych, cyfr tylko na początku lub końcu hasła, nazw związanych z miejscem umieszczenia konta. Tworząc hasło zaleca się stosowanie: cyfr wewnątrz hasła, słów nie występujących często w języku potocznym.

g) Użytkownik zobowiązany jest do zachowania haseł w tajemnicy. Hasło nie może być zapisywane w miejscu dostępnym dla osób nieuprawnionych.

h) Użytkownik ma obowiązek zmieniać hasła nie rzadziej niż raz na 30 dni także w przypadku gdy zmiana ta nie jest wymuszana komunikatem.

i) Hasła w stosunku, do których zaistniało podejrzenie o ich ujawnieniu podlegają bezzwłocznej zmianie. Sytuację taką należy zgłosić do Administratora Systemu Informatycznego i Administratora Bezpieczeństwa Informacji.

j) W celu zabezpieczenia awaryjnego dostępu do systemu przetwarzającego dane, aktualne hasła do sieciowych systemów operacyjnych są tworzone przez Administratora Systemu Informatycznego i deponowane w sejfie.

k) Sposób generowania i przekazywania haseł gwarantuje, że są one znane wyłącznie użytkownikowi końcowemu.

l) Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie jest przydzielany innym osobom.

m) System informatyczny służący do przetwarzania danych osobowych zabezpieczony jest programem antywirusowym.

n) Serwery baz danych służące do przetwarzania danych osobowych zabezpieczony jest przed awarią zasilania.

o) Dane osobowe przetwarzane w systemie zabezpieczone są przez wykonanie kopii zapasowych zbiorów danych i programów służących do przetwarzania danych przez Administratora Systemu Informatycznego.

p) Kopie przechowywane są w sejfie w pomieszczeniach Administratora Systemu Informatycznego.

r) Dane osobowe w komputerach przenośnych chronione są za pomocą technik kryptograficznych.

2. **Na poziomie podwyższonym** stosuje się środki wymagane dla poziomu podstawowego i dodatkowo:

a) hasła składające się co najmniej z 8 znaków i zawierające małe i duże litery oraz cyfry lub znaki specjalne

b) urządzenia nośniki zawierające dane osobowe o których mowa w art. 27 ust. 1 ustawy, przekazywane poza obszar bezpieczeństwa, zabezpieczone są w sposób zapewniający poufność i integralność tych danych

3. Na poziomie wysokim stosowane są środki wskazane w pkt 1 i 2 i dodatkowo

a) system informatyczny służący do przetwarzania danych osobowych jest chroniony przed

zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń przed nieuprawnionym dostępem,

b) w przypadku stosowania logicznych zabezpieczeń, o których mowa w lit a) obejmują one:

- kontrolę przepływu informacji pomiędzy systemem informatycznym Administratora Danych a siecią publiczną,
- kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego Administratora Danych,

c) Administrator Danych stosuje środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelniania, które są przesyłane w sieci publicznej.

Rozdział 4.

Aplikacje i usługi zabronione

§ 8

Użytkownikowi zabrania się:

1. Wykorzystywania sieci komputerowej w celach innych niż wyznaczone przez Prezydenta Miasta Radomia (Administratora Danych).
2. Podłączania jakichkolwiek urządzeń do dedykowanej elektrycznej sieci komputerowej.
3. Ingerowania w bazy danych narzędziami innymi niż przeznaczona do tego aplikacja.
4. Ingerowania w sprzęt komputerowy.
5. Tłumaczenia, przystosowywania, zmiany układu lub jakichkolwiek innych zmian w programie komputerowym nie przeznaczonych dla użytkownika.
6. Instalowania i używania programów komputerowych (posiadających lub nie posiadających licencji) bez zgody Administratora Systemu Informatycznego.
7. Przechowywania jakichkolwiek plików łamiących ustawę o ochronie praw autorskich i prawach pokrewnych (nielegalnych plików mp3, plików video itp.)
8. Trwałego lub czasowego kopiowania programów komputerowych w całości lub w części jakimikolwiek środkami i w jakiejkolwiek formie.
9. Niezgodnym z licencją publicznego udostępniania programów komputerowych lub ich kopii dla osób postronnych.

10. Przenoszenia programów komputerowych z własnego stanowiska roboczego na inne stanowisko.
11. Używania oprogramowania, które posiada sfałszowane znaki firmowe lub nie posiada w ogóle znaków firmowych, etykiet, oryginalnych nośników, dokumentacji łącznie z elektroniczną.
12. Udostępniania osobom postronnym programów komputerowych Urzędu lub możliwość dostępu do zasobów sieci wewnętrznej oraz Internetu.
13. Wykorzystywania oprogramowania lub materiałów ściągniętych z Internetu do rozprowadzania bez licencji lub wyraźnego upoważnienia autora.
14. Używania nośników udostępnianych przez osoby postronne (nie będącymi pracownikami Urzędu) i podejrzanych o zainfekowanie wirusem. W razie podejrzenia o zainfekowanie wirusem nośnika danych (dyskietki, CD/DVD lub dysku twardego) użytkownik ma obowiązek niezwłocznie poinformować o tym Administratora Systemu Informatycznego.
15. Używania oprogramowania w większym zakresie niż pozwala na to umowa licencyjna.

Rozdział 5.

Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie informatycznym

§ 9

1. Rozpoczynając pracę na komputerze użytkownik podaje wszystkie wymagane, własne identyfikatory i hasła w sposób uniemożliwiający ich ujawnienie innym osobom.
2. Użytkownik zobowiązany jest uwierzytelniać się w systemie informatycznym wyłącznie na podstawie własnego identyfikatora i hasła.
3. Ustawienie monitora powinno uniemożliwiać podgląd osobom nieuprawnionym szczególnie w procesie obsługi klienta.
4. W przypadku opuszczenia stanowiska pracy, użytkownik systemu obowiązany jest zaktywizować wygaszacz ekranu z opcją ponownego uwierzytelnienia się w systemie lub w inny sposób zablokować stację roboczą, w szczególności poprzez wylogowanie się z systemu.

5. Po zakończeniu pracy użytkownik powinien prawidłowo wylogować się z systemu, wyłączyć komputer a także schować wszelkie elektroniczne nośniki informacji zawierające dane w sposób uniemożliwiający dostęp osobom nieupoważnionym.
6. Do obsługi systemu komputerowego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych, użytkownik może być dopuszczony wyłącznie posiadając upoważnienie wydane przez Administratora Danych.

Rozdział 6.

Zasady i sposób odnotowania w systemie informacji o udostępnieniu danych osobowych, funkcjonalność systemów.

§ 10

1. Dane osobowe z eksploatowanych systemów mogą być udostępniane wyłącznie osobom upoważnionym.
2. Udostępnianie danych osobowych, w jakiejkolwiek postaci, jednostkom nieuprawnionym wymaga pisemnego upoważnienia Administratora Danych.
3. Udostępnianie danych osobowych nie może być realizowane drogą telefoniczną.
4. Udostępnienie danych osobowych może nastąpić wyłącznie po przedstawieniu wniosku, którego wzór stanowi **Załącznik Nr 2.1**
5. System informatyczny służący do przetwarzania danych osobowych powinien zapewniać dla każdej osoby, której dane osobowe są przetwarzane w tym systemie — z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie — automatyczne odnotowywanie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych, informacji o dacie pierwszego wprowadzenia danych do systemu oraz o identyfikatorze osoby wprowadzającej dane.
6. W przypadku zbierania danych osobowych od osoby, której dane nie dotyczą należy zapewnić w systemie informatycznym odnotowywanie informacji o źródle pochodzenia danych. Proces ten nie musi odbywać się automatycznie.

7. Dla każdego systemu służącego do przetwarzania danych osobowych, z którego udostępniane są dane osobowe odbiorcom danych, należy zapewnić odnotowanie komu, kiedy i w jakim zakresie dane osobowe zostały udostępnione, chyba, że dane pochodzą z jawnego zbioru danych osobowych.

8. W przypadku zgłoszenia sprzeciwu, o którym mowa w art. 32 ust 1 pkt. 8 Ustawy, wobec przetwarzania danych osobowych należy zapewniać odnotowywanie tej informacji.

9. Należy zapewnić dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym sporządzenie i wydrukowanie:

1) zestawień zakresu i treści przetwarzanych na jej temat danych osobowych,

2) zestawienia zawierającego informacje wymagane w § 7 ust. 1 Rozporządzenia.

10. W przypadku przetwarzania danych osobowych, w co najmniej dwóch systemach, wymagania, o których mowa w § 7 ust. 1 pkt 4 Rozporządzenia, mogą być realizowane w jednej z nich lub w odrębnym systemie informatycznym przeznaczonym do tego celu.

11. Treść ostatecznego rozstrzygnięcia indywidualnej sprawy osoby, której dane dotyczą, nie może być wyłącznie wynikiem operacji na danych osobowych, prowadzonych w aplikacji lub systemie informatycznym.

12. Zabronione jest nadawanie ukrytych znaczeń elementom numerów porządkowych w aplikacjach ewidencjonujących osoby fizyczne.

13. Kierownicy komórek organizacyjnych prowadzą rejestry udostępnionych danych osobowych zawierające co najmniej: datę udostępnienia, podstawę, zakres udostępnionych informacji oraz osobę lub instytucję, dla której dane udostępniono.

Załącznik 2.1.

WNIOSEK

O UDOSTĘPNIENIE DANYCH ZE ZBIORU DANYCH OSOBOWYCH

1. Wniosek do Prezydenta Miasta Radomia

2. Wnioskodawca

……

……

(nazwa firmy i jej siedziba albo imię , nazwisko i adres zamieszkania wnioskodawcy, ew. NIP oraz nr REGON)

3. Podstawa prawna upoważniająca do pozyskania danych albo wskazanie wiarygodnie uzasadnionej potrzeby posiadania danych w przypadku osób innych niż wymienione w art. 29 ust 1 ustawy o ochronie danych osobowych:

……

……

4. Wskazanie przeznaczenia dla udostępnionych danych:

……

……

5. Oznaczenie lub nazwa zbioru, z którego mają być udostępniane dane:

……

……

6. Zakres żądanych informacji ze zbioru:

……

……

10. Informacje umożliwiające wyszukanie w zbiorze żądanych danych:

……

……

……

(Data i podpis wnioskodawcy)

Rozdział 7

Zasady komunikacji w sieci teleinformatycznej

§ 11

1. Przesyłanie danych osobowych drogą teletransmisji powinno odbywać się wyłącznie przy wykorzystaniu wymaganych zabezpieczeń logicznych chroniących przed nieuprawnionym dostępem, w szczególności takich jak ochrona kryptograficzna.
2. Pliki zawierające dane osobowe mogą się znajdować jedynie na serwerach, gdzie podlegają ochronie zapewnianej przez mechanizmy bezpieczeństwa systemu operacyjnego.
3. Wyłącznie w sytuacjach wyjątkowych dopuszcza się przetwarzanie danych osobowych w plikach (MS Word, MS Excel) na stacjach roboczych użytkowników, poza bazą danych, znajdującą się w określonym systemie informatycznym.
4. Zgodę na przetwarzanie danych w sytuacjach określonych w ust. 3 wydają lokalni administratorzy danych osobowych.
5. Dopuszcza się wykorzystywanie sieci opartych na falach radiowych (WiFi) w budynkach Urzędu Miejskiego w Radomiu. Sieci te nie mogą być wykorzystywane do przekazu informacji zawierających dane osobowe.
6. Wszystkie połączenia zewnętrzne do systemu informatycznego powinny być monitorowane a logi połączeń archiwizowane w trybie ciągłym i bezterminowym.
7. System informatyczny służący do przetwarzania danych osobowych, Administrator Systemu Informatycznego powinien chronić przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.
8. Zabezpieczenia logiczne, o których mowa w ust. 7 powyżej, obejmują:
a) kontrolę przepływu informacji pomiędzy systemem informatycznym a siecią publiczną.
b) kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego.
9. Kontrola powinna być nadzorowana przez Administratorów Systemów, a jej wynik powinien być dokumentowany w „Rejestrze zdarzeń i incydentów”.

10. Zdalne uruchamianie komend systemowych ze stacji roboczych znajdujących się w lokalizacjach nie należących do Urzędu jest możliwe, po prawidłowym logowaniu się użytkownika i zastosowaniu „silnego" uwierzytelnienia.

Rozdział 8.

Konserwacja i naprawa systemu informatycznego w tym przetwarzającego dane osobowe

§ 12

1. Prace dotyczące przeglądów, konserwacji i napraw wymagające zaangażowania firm zewnętrznych, są wykonywane przez uprawnionych przedstawicieli tych firm pod nadzorem Administratora Systemu Informatycznego.
2. W wypadku konieczności dostępu do danych osobowych przez serwisantów firm niezwiązanych z Urzędem umowami zawierającymi klauzule dotyczące ochrony powierzonych danych, podpisują oni specjalny dokument (**Druk Nr 4** do Polityki Bezpieczeństwa Informacji i Ochrony Danych Osobowych) o zachowaniu poufności (zgodnie z Art. 39 pkt. 2 ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997r.). Administrator Systemu Informatycznego ma obowiązek poinformować Administratora Bezpieczeństwa Informacji o zaistniałej sytuacji.

3. Urządzenia komputerowe, dyski twarde lub inne informatyczne nośniki danych, przeznaczone do naprawy, Administrator Systemu Informatycznego pozbawia przed naprawą zapisu danych osobowych lub nadzoruje ich naprawę w Urzędzie.
4. Serwery i wyznaczone stacje robocze są chronione przed zanikiem zasilania poprzez zastosowanie zasilaczy awaryjnych. Konserwację i testowanie zasilaczy awaryjnych wykonuje się zgodnie z planem zaakceptowanym przez Dyrektora Wydziału Teleinformatycznego.
5. Zgłoszenia nieprawidłowego funkcjonowania sprzętu/oprogramowania bądź innych problemów informatycznych odbywają się przez elektroniczny system zgłoszeń serwisowych „Helpdesk”. W sytuacjach, gdy nie jest to technicznie możliwe dopuszcza się zgłoszenia np. telefoniczne, osobiste lub pisemne. Instrukcję użytkowania sytemu „Helpdesk” ustala Dyrektor Wydziału Teleinformatycznego.

Rozdział 9

Procedura postępowania w sytuacji naruszenia ochrony danych osobowych

§ 13

Na fakt naruszenia zabezpieczeń systemu informatycznego mogą wskazywać:

1. stan stacji roboczej (np. brak zasilania, problemy z uruchomieniem, zdjęta obudowa),
2. wszelkiego rodzaju różnice w funkcjonowaniu systemu, programu (np. komunikaty informujące o błędach, brak dostępu do funkcji programu, nieprawidłowości w wykonywanych operacjach),
3. różnice w zawartości zbioru danych osobowych (np. brak lub nadmiar danych),
4. jakość komunikacji w sieci teleinformatycznej (gwałtowne opóźnienia lub przyśpieszenia wykonywanych czynności) ,
5. inne sytuacje nadzwyczajne.

§ 14

W przypadku, stwierdzenia naruszenia zabezpieczeń systemu informatycznego należy niezwłocznie powiadomić Administratora Systemu Informatycznego oraz Administratora Bezpieczeństwa Informacji. Przetwarzanie i udostępnianie danych osobowych przez osoby nieuprawnione oraz ich modyfikacja, uszkodzenie lub zniszczenie podlega sankcjom cywilnym i karnym (także wtedy, gdy sprawca działa nieumyślnie).

Rozdział 10

Procedura zarządzania zmianą w systemach informatycznych

§ 15

1. W celu zapewnienia prawidłowego funkcjonowania Urzędu, systemy informatyczne podlegają zmianom. Zmiany w systemach informatycznych Urzędu mogą dotyczyć oprogramowania lub sprzętu.
2. Aby zapewnić odpowiednie bezpieczeństwo i poziom usług zmiany muszą być wykonywane jedynie przez osoby do tego powołane – Administratora Systemu Informatycznego lub Serwisanta.
3. W przypadku zmian dokonywanych przez Serwisanta, wszelkie czynności muszą być nadzorowane i kontrolowane przez Administratora Systemu Informatycznego.
4. W zależności od wpływu na funkcjonowanie Urzędu zmiany dzielimy na znaczące i niewielkie.
5. Zmiana znacząca obejmuje:
a. strukturę baz danych;
b. wersję oprogramowania użytkowego i systemów sieciowych;
c. zmiany w plikach konfiguracyjnych;
d. topologię sieci komputerowej (rozbudowa, okablowanie, zmiana urządzeń aktywnych);
e. konfigurację sprzętu i oprogramowania odpowiedzialnego za ochronę przed szkodliwym oprogramowaniem (wirusy, robaki sieciowe, konie trojańskie, bomby logiczne itp.);
f. sposób archiwizacji danych;
g. inne nie opisane powyżej zmiany w zbiorach i systemach przetwarzających dane osobowe.
6. W przypadku zmiany znaczącej przygotowywany jest plan zmiany zawierający: daty i czasy zmian, osoby odpowiedzialne, wykonanie kopii zapasowych, czynności do wykonania, sposób testowania zmiany. Plan zmiany akceptuje kierownik Wydziału Teleinformatycznego (**Załącznik 2.3.** – Plan zmiany).
7. Dla zmian dotyczących: oprogramowania użytkowego, struktury baz danych, plan zmiany przygotowuje kierownik zainteresowanej komórki organizacyjnej Urzędu, w pozostałych przypadkach Administrator Systemu Informatycznego.

8. Informacje o zmianach znaczących są odnotowywane w Rejestrze działań.

9. Dla zmian znaczących dotyczących systemów operacyjnych w Rejestrze działań powinny się znaleźć informacje o: aktualizowanym oprogramowaniu, aktualizowanych bibliotekach, zmienianych plikach konfiguracyjnych (wersji obecnych i nowych), wpływie zmian na cechy systemu (m.in. bezpieczeństwo, stabilność, wydajność), innych – uznanych za przydatne.

10. W przypadku aktualizacji oprogramowania użytkowego utrzymywana jest kontrola wersji, polegająca na odnotowaniu zmiany w rejestrze działań, zmiany nr wersji w oprogramowaniu.

11. O ile jest to możliwe zmiany są wprowadzane w czasie nie zakłócającym funkcjonowania Urzędu.

12. Po przeprowadzeniu zmiany w systemach aplikacyjnych, poddaje się ją przeglądowi i przetestowaniu, w celu uzyskania pewności, że nie miała ona niekorzystnego wpływu na ich działanie lub bezpieczeństwo.

13. Dla zapewnienia kontroli nowego oprogramowania i ochrony rzeczywistych danych, Administrator Systemu Informatycznego utrzymuje środowisko testowe. Testowanie zmian powinno być najpierw przeprowadzone na środowisku testowym.

14. Czynności, które należy wykonać w celu przeprowadzenia testów zmian muszą opierać się na procedurach testowania dostarczonych przez dostawcę/producenta.

15. Po zakończeniu zmian, zbiór dokumentacji systemu jest aktualizowany.

16. O wprowadzenie zmian w systemach informatycznych mogą wnioskować:

- pracownicy w przypadku zmian sprzętowo-programowych dotyczących stacji roboczych, na których pracują
- kierownicy komórek organizacyjnych w przypadku zmian znaczących.

17. Wniosek powinien zawierać: imię i nazwisko osoby, datę, nazwę i nr ewidencyjny systemu/urządzenia, proponowany zakres i termin zmian. **(Załącznik Nr 2.2.** - Wniosek o wprowadzenie zmiany).

18. Rejestr zgłoszonych wniosków prowadzi Administrator Systemu Informatycznego.

19. Odpowiedzialność za weryfikację przy zmianie (zakupie) oprogramowania użytkowego ponosi:

- Administrator Systemu Informatycznego – pod względem zgodności z istniejącą infrastrukturą informatyczną,
- Kierownik zainteresowanej komórki organizacyjnej – pod względem merytorycznym

- Administrator Bezpieczeństwa Informacji pod względem merytorycznej zgodności z przepisami prawa o ochronie danych osobowych.

20. Wszystkie elementy sprzętu zawierające nośniki przechowujące dane (np. dyski twarde) są sprawdzane przed zbyciem, aby upewnić się, że wszelkie wrażliwe dane i licencjonowane oprogramowanie zostały skutecznie usunięte lub nadpisane.

21. Oprogramowanie jest aktualizowane o poprawki bezpieczeństwa. Na komputerach podłączonych do sieci Internet włączone są funkcje codziennego automatycznego pobierania i instalacji poprawek. Dla programów nie posiadających takiej funkcji lub komputerów nie podłączonych do sieci Internet, konieczność i częstotliwość instalacji poprawek określa Dyrektor Wydziału Teleinformatycznego.

Załącznik Nr 2.2.

Wniosek o Wprowadzenie Zmiany w Systemie Informatycznym

Zmiana: znacząca / niewielka*

Data	
Nazwa komórki organizacyjnej	
Imię i nazwisko osoby wnioskującej	
Nr ewidencyjny urządzenia/systemu*	
Nazwa urządzenia/systemu*	
Proponowany zakres zmiany	
Uzasadnienie zmiany	
Proponowany termin zmiany	
Podpis osoby wnioskującej	

* niepotrzebne skreślić

Załącznik Nr 2.3.

Plan Zmiany

Data opracowania planu zmiany	
Imię i nazwisko osoby odpowiedzialnej	
Nr ewidencyjny urządzenia/systemu*	
Nazwa urządzenia/systemu*	
Data i czas zmiany	
Czynności do wykonania	
Sposób testowania zmiany	
Wykonanie kopii zapasowych	
Podpis osoby akceptującej	

* niepotrzebne skreślić

Rozdział 11

Instrukcja rejestracji działań dokonywanych na krytycznych systemach Informatycznych

§ 15

1. Rejestr działań prowadzi się dla zdarzeń i operacji dokonywanych na krytycznych systemach informatycznych.
2. Rejestr może być prowadzony w formie pisemnej lub elektronicznej.
3. Rejestr powinien zawierać: datę i godzinę wystąpienia błędu lub rozpoczęcia operacji, nazwisko osoby wykonującej czynności, opis błędu, podjęte działania i wykonane czynności, datę zakończenia działań, inne informacje uznane za przydatne.
4. Zapisy w rejestrze działań powinny być pogrupowane w kategorie zdarzeń, w celu większej przejrzystości zapisów.
5. Rejestr powinien zawierać co najmniej następujące kategorie: awarie, nadanie uprawnień, problem z aplikacją, kopie zapasowe, zmiany, test systemu.
6. Nadzór nad procesem prowadzenia rejestracji działań powierza się kierownikowi Wydziału Teleinformatycznego. Dokonuje on przeglądu zapisów w celu zapewnienia, że błędy zostały w zadowalający sposób usunięte a wykonane operacje nie zaburzą prawidłowej pracy systemu.
7. Do prowadzenia rejestru działań i dokonywania w nim wpisów zobowiązany jest Administrator Systemu Informatycznego, wykonujący operacje na krytycznych systemach informatycznych.
8. Rejestr działań przechowywany jest w pomieszczeniach ASI w sposób uniemożliwiający dostęp osobom nieupoważnionym.

Rozdział 12

Zasady ochrony antywirusowej

§ 16

1. Ogólne zasady ochrony antywirusowej.

a) Ochronie antywirusowej podlegają wszystkie komputery pracujące w Urzędzie.

b) Dla komputerów z zainstalowanym systemem operacyjnym (np. MS-DOS) lub o parametrach technicznych uniemożliwiających zastosowanie aktualnego programu antywirusowego dopuszcza się stosowanie oprogramowania antywirusowego odpowiedniego do parametrów komputera.

c) Do ochrony antywirusowej stosuje się licencjonowane oprogramowanie. Licencja powinna obejmować wszystkie stacje podlegające ochronie.

d) Szczegółowy sposób instalacji, konfiguracji i aktualizacji baz sygnatur aktualnego oprogramowania antywirusowego opisuje **Instrukcja operacyjna ochrony antywirusowej**.

2. Odpowiedzialność.

a) Nadzór nad procesem ochrony antywirusowej powierza się Dyrektorowi Wydziału Teleinformatycznego. Wyznacza on i weryfikuje działania pracowników Wydziału j/w odpowiedzialnego za ochronę antywirusową i za aktualizację baz sygnatur wirusów w komputerach podłączonych do sieci Urzędu.

b) W przypadku komputerów nie podłączonych do sieci wewnętrznej, obowiązek aktualizacji baz sygnatur wirusów spoczywa na użytkowniku. Raz w miesiącu zgłasza się do siedziby Wydziału Teleinformatycznego (pok. 52) po nośnik z aktualnymi bazami sygnatur.

c) W przypadku komputerów w wydzielonych odrębnych sieciach, administrowanych przez podmioty zewnętrzne (dowody osobiste, rejestracja pojazdów, prawa jazdy) ochrona antywirusowa spoczywa na podmiotach administrujących tymi komputerami.

3. Instalacja, konfiguracja, aktualizacja baz sygnatur.

a) Jeśli **Instrukcja operacyjna ochrony antywirusowej** nie przewiduje inaczej, Administrator Systemu Informatycznego instaluje program antywirusowy z następującymi opcjami: ochrona plików, ochrona poczty, ochrona WWW, ochrona komunikatorów, zapora sieciowa, blokowanie ataków sieciowych, kontrola systemu i kontrola aplikacji.

b) Instalacji oprogramowania antywirusowego należy dokonywać w sposób pozwalający na centralne zarządzanie oraz monitorowanie stanu stacji roboczych.
c) Na komputerach podłączonych do sieci aktualizacja baz sygnatur może odbywać się poprzez Internet lub z foldera na serwerze lokalnych. Należy tak konfigurować program, aby aktualizacja odbywała się automatycznie.
d) W przypadku komputerów nie podłączonych do sieci aktualizacji baz sygnatur należy dokonywać ręcznie z dostępnego nośnika danych np.: dyskietki, płyty CD-ROM. Aktualizacji należy dokonywać nie rzadziej niż raz w miesiącu.

Rozdział 13

Instrukcja zarządzania kopiami zapasowymi

§ 17

1. Ogólne zasady wykonywania archiwizacji danych.
a) Archiwizacji podlegają informacje w tym dane osobowe oraz programy wykorzystywane do ich przetwarzania na terenie Urzędu.
b) Wykonywanie kopii awaryjnych danych osobowych podlega Administratorowi Systemu Informatycznego.
c) Szczegółowy wykaz archiwizowanych zbiorów przetwarzanych na serwerach, ustala Dyrektor Wydziału Teleinformatycznego w porozumieniu z kierownikami komórek organizacyjnych Urzędu.
d) Szczegółowy wykaz archiwizowanych zbiorów wraz z harmonogramem archiwizacji prowadzony i przechowywany jest przez Administratora Systemu Informatycznego.
2. Odpowiedzialność.
a) Nadzór nad procesem archiwizacji danych przetwarzanych na serwerach znajdujących się w pomieszczeniach powierza się Dyrektorowi Wydziału Teleinformatycznego. Wyznacza on pracowników w/w Wydziału odpowiedzialnych za wykonywanie i przechowywanie kopii zapasowych poszczególnych systemów informatycznych urzędu oraz za testowanie i odtwarzanie danych z kopii zapasowych.

b) W przypadku systemów informatycznych przetwarzanych w Urzędzie, ale znajdujących się na serwerach umieszczonych poza budynkami urzędu i administrowanymi przez podmioty zewnętrzne, odpowiedzialność za wykonywanie kopii zapasowych spoczywa na podmiotach zewnętrznych administrujących te systemy.

§ 18

1. Tworzenie, testowanie i odtwarzanie danych z kopii zapasowych

Kopie bezpieczeństwa systemów w tym do przetwarzania danych osobowych wykonywane są zgodnie z poniższymi zasadami:

a) Kopie bezpieczeństwa wykonuje się na dyskietkach, taśmach magnetycznych, dyskach twardych, płytach CD-ROM/DVD-ROM.
b) Kopie bezpieczeństwa systemów przetwarzających dane osobowe oraz zbiorów przetwarzanych na serwerach wykonuje się codziennie. Kopie innych zbiorów przetwarzanych na komputerach lokalnych z częstotliwością określoną przez Administratora Systemu Informatycznego zgodnie z harmonogramem archiwizacji.
c) Użytkownik podłączony do sieci wewnętrznej posiada dostęp do swojego katalogu roboczego na serwerze. Kopie bezpieczeństwa zapisanych w nim dokumentów, wykonuje się codziennie na koniec pracy.
d) Raz na pół roku wykonuje się kopie wyznaczonych danych na płytach CD-ROM/DVD-ROM.
e) Czas przechowywania kopii dziennych - 1 tydzień, półrocznych - 1 rok

2. Nośniki zawierające kopie bezpieczeństwa są dokładnie opisane. Opis precyzuje zawartość nośnika, oraz datę pierwszego zapisu danych na nim.

3. Jeśli jest to możliwe, kopie bezpieczeństwa wykonywane na taśmach streamera powinny być wykonywane z włączoną funkcją automatycznego sprawdzania pod względem poprawności zapisu danych.

4. Kopie bezpieczeństwa należy okresowo, nie rzadziej jednak niż raz na 6 miesięcy sprawdzać pod kątem ich przydatności do odtworzenia danych w przypadku awarii systemu.

5. Kopie bezpieczeństwa, które uległy uszkodzeniu lub stały się niepotrzebne pozbawia się bezpowrotnie zapisu danych, a w przypadku gdy nie jest to możliwe, niszczy w stopniu uniemożliwiającym ich odczytanie.

6. W celu zabezpieczenia danych, dyski na serwerach pracują w technologii zapewniającej bezpieczne przechowywanie danych (dane są zapisywane jednocześnie na kilku dyskach).

§ 19

1. Zasady przechowywania kopii zapasowych

a) Kopie zapasowe wyznaczonych zbiorów w tym danych osobowych przechowywane są w kasie pancernej w pomieszczeniu innym niż to w którym znajdują się przetwarzane dane.

b) Kopie zapasowe pozostałych zbiorów danych przechowywane są w pomieszczeniu innym niż to w którym znajdują się przetwarzane dane, w sposób uniemożliwiający dostęp osobom nieupoważnionym.

2. Kopie awaryjne, które uległy uszkodzeniu lub stały się niepotrzebne pozbawia się zapisu danych, a w przypadku gdy nie jest to możliwe, niszczy w stopniu uniemożliwiającym ich odczytanie.

3. Wydruki ze zbiorów danych osobowych tworzone i używane do celów operacyjnych przez określony czas wykorzystywania przechowywane są w odpowiednio zabezpieczonych szafach lub sejfach.

4. Likwidacji wydruków dokonuje się w sposób uniemożliwiający odczyt danych.

5. Jeżeli dysk twardy jest uszkodzony i nie ma możliwości skasowania z niego danych osobowych Administrator Systemu Informatycznego wymontowuje go z komputera i fizycznie niszczy.

6. Likwidacji zniszczonych lub niepotrzebnych nośników magnetycznych lub optycznych dokonuje się zgodnie z ustaloną przez Administratora Systemu Informatycznego procedurą.

Rozdział 14

Instrukcja zarządzania komputerami przenośnymi

§ 20

Komputery przenośne (laptop, notebook, palmtop) to urządzenia do przetwarzania informacji, których gabaryty umożliwiają ich przenoszenie i pracę mobilną.

Uprawnieni do pracy z wykorzystaniem komputerów przenośnych są pracownicy Urzędu Miejskiego w Radomiu oraz użytkownicy zewnętrzni, którym udostępniono komputer przenośny. Komputery nie będące własnością Urzędu nie mogą być wykorzystywane do przetwarzania danych osobowych.

§ 21

1. Komputery przenośne, które są własnością Urzędu Miejskiego w Radomiu (wraz z zainstalowanym oprogramowaniem) są wpisane do ewidencji środków trwałych i **podlegają tym samym regułom ochrony jak komputery stacjonarne.**
2. Komputer przenośny służy do wykonywania czynności na rzecz Urzędu, sprawowania mandatu radnego lub w związku z wykonywaniem czynności przez organizacje pozarządowe oraz inne podmioty prowadzące działalność pożytku publicznego, współpracujące z Urzędem.
3. Użytkownik zewnętrzny może pracować na komputerze przenośnym udostępnionym do wykonywania czynności na rzecz Urzędu z niezbędnymi uprawnieniami dostępu do wykonania określonej pracy.
4. Użytkownik nie może instalować oraz usuwać oprogramowania, a także uruchamiać aplikacji nie będących aplikacjami zainstalowanymi domyślnie na komputerze przenośnym.
5. Przypadki łamania niniejszych zasad przez użytkowników mogą skutkować odpowiedzialnością materialną i karną zgodnie z obowiązującym prawem.

§ 22

W celu ochrony całego systemu przed włamaniami a także zabezpieczenia dostępu do informacji zlokalizowanych na komputerach przenośnych Administrator Systemu tworzy w systemie operacyjnym użytkownika wraz z hasłem. Zasady przyznawania haseł zawarte są w Rozdziale 6 niniejszej Instrukcji.

§ 23

1. Komputery przenośne, będące własnością Urzędu Miejskiego mogą być używane poza Urzędem tylko w uzasadnionym przypadku za pisemną zgodą Kierownika Komórki Organizacyjnej wpisaną w rejestr przechowywany w podległej mu komórce organizacyjnej. Rejestr, (którego wzór stanowi **załącznik nr 2.4**) powinien zawierać nazwę komórki organizacyjnej, dane pracownika (imię, nazwisko, stanowisko), powód / potrzebę korzystania na zewnątrz Urzędu, datę wraz z godziną pobrania i oddania sprzętu, podpis pracownika pobierającego komputer przenośny, podpis wyrażającego zgodę Kierownika Komórki Organizacyjnej.
2. Komputery przenośne powinny być zabezpieczone podczas transportu oraz przechowywane przed dostępem osób nieuprawnionych.

Rozdział 15

Postanowienia końcowe.

§ 24

1. Kierownicy komórek organizacyjnych oraz wszyscy pracownicy Urzędu są zobowiązani zapoznać się z niniejszymi procedurami oraz złożyć stosowne oświadczenie dotyczące znajomości jej treści.
2. Zgodnie z Zarządzeniem Nr 194/2006 Prezydenta Miasta Radomia z dnia 9 maja 2006 r. w sprawie systemu kontroli wewnętrznej w Urzędzie Miejskim w Radomiu przeprowadzane będą kontrole w poszczególnych komórkach organizacyjnych Urzędu.
3. Pracownik za naruszenie obowiązków, wynikających z niniejszej Instrukcji i przepisów o ochronie danych osobowych ponosi odpowiedzialność przewidzianą w Regulaminie Pracy oraz Kodeksie Pracy (Dz. U. z 1974r. Nr24, poz.141) za naruszenie podstawowych obowiązków pracowniczych.
4. Sprzęt komputerowy oraz oprogramowanie, będące własnością lub w posiadaniu Urzędu Miejskiego w Radomiu, a udostępnione w celu świadczenia pracy lub usług dla Urzędu, jest monitorowane za pomocą urządzenia sieciowego klasy UTM oraz dedykowanych programów

komputerowych. Kontrola o której mowa polega na: monitorowaniu i logowaniu użytkowników sieci komputerowej, kontroli połączeń sieciowych, kontroli wykorzystania zainstalowanego oprogramowania.

5. Użytkownik nie przestrzegający zasad określonych w niniejszej Instrukcji ponosi odpowiedzialność karną z art.49-54 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r., poz. 922) oraz na podstawie art.267 - 269, 287 Kodeksu Karnego (Dz. U. z 1997 r. Nr 88, poz.553).

6. W sprawach nieuregulowanych w Instrukcji mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r., o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922) oraz przepisy aktów wykonawczych wydanych na jej podstawie

Załącznik 2.4

Rejestr Komputerów Przenośnych Używanych Poza Urzędem Miejskim w Radomiu

Data pobrania	
Data zdania	
Nazwa komórki organizacyjnej	
Imię i nazwisko pracownika / stanowisko	
Nr ewidencyjny urządzenia	
Uzasadnienie użycia komputera przenośnego poza Urzędem Miejskim	
Podpis osoby wnioskującej	
Podpis Kierownika Komórki Organizacyjnej	