Załącznik Nr 1

ZATWIERDZAM **do Zarządzenia Nr 1492/2016**

Prezydenta Miasta Radomia

Prezydenta Miasta Radomia **z dnia 30 czerwca 2016 r.**

POLITYKA BEZPIECZEŃSTWA INFORMACJI I OCHRONY DANYCH OSOBOWYCH W URZĘDZIE MIEJSKIM W RADOMIU

Spis treści polityki:

Rozdział 1

Postanowienia ogólne

§ 1

Znaczenie bezpieczeństwa danych osobowych i systemów informatycznych służących do przetwarzania danych osobowych jest bezsporne dla realizacji celów Urzędu Miejskiego w Radomiu. Działania podejmowane przez Urząd Miejski w Radomiu zmierzają do zapewnienia bezpieczeństwa przetwarzania danych osobowych i posiadanych zasobów informatycznych. Polityka Bezpieczeństwa Informacji i Ochrony Danych Osobowych w Urzędzie Miejskim w Radomiu uwzględnia wymagania dotyczące zarządzania bezpieczeństwem informacji, zawarte w normie PN-ISO/IEC 17799:2007 oraz w poniższych dokumentach:

a. Ustawa z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. 2016 r., poz. 922 j.t.),

b. 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,

c. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych,

d. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz. U. z 2015, poz. 745),

e. Rozporządzenie Ministra Administracji i Cyfryzacji z 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz. U. z 2015, poz. 719),

f. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji (Dz. U. 2014, poz. 1934).

W celu udokumentowania powyższych działań przyjęto zarządzeniem nr 1492/2016 Prezydenta Miasta Radomia z dnia 30 czerwca 2016 r. niniejszą Politykę Bezpieczeństwa Informacji i Ochrony Danych Osobowych w Urzędzie Miejskim w Radomiu. Zasady postępowania, obowiązki oraz zakresy odpowiedzialności opisane w Polityce Bezpieczeństwa obowiązują wszystkich pracowników Urzędu przetwarzających dane osobowe.

§ 2

Ilekroć mowa w niniejszym dokumencie o:

1. Administratorze Danych Osobowych – 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,
- przeglądy, konserwację,

- 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 **-** odpowiedzialnych za prowadzony przez podległą komórkę zbiór danych osobowych, a w szczególności za przestrzeganie zasad określonych art. 26 UODO.

5. **Dyrektorach/Kierownikach komórek organizacyjnych –** są to osoby odpowiedzialne 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 wyznaczoną 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 – osoba upoważniona do przetwarzania danych osobowych w systemie informatycznym.

9. 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.

10. Systemie informatycznym - system w rozumieniu art. 7 pkt 2a Ustawy.

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

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

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

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

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

16. Zarządzenie Prezydenta Miasta Radomia w sprawie wdrożenia dokumentacji przetwarzania i ochrony danych osobowych w Urzędzie Miejskimi w Radomiu, zwane dalej Zarządzeniem.

§ 3

1. Administrator Danych Osobowych może upoważnić osoby zatrudnione w Urzędzie do wykonywania określonych czynności, znajdujących się w zakresie zadań Administratora.
2. Kontrola prawidłowości wykonywania czynności, o których mowa w ust. 1, należy do Administratora Danych Osobowych.

Rozdział 2

Deklaracja intencji, cele i zakres polityki bezpieczeństwa.

§ 4

W Urzędzie Miejskim w Radomiu przetwarzane są informacje stanowiące dane osobowe w rozumieniu art. 6 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2016 r. poz. 922). Administrator Danych Osobowych wyraża pełne zaangażowanie dla zapewnienia bezpieczeństwa przetwarzanych danych osobowych oraz wsparcie dla przedsięwzięć technicznych i organizacyjnych związanych z ochroną danych osobowych. Dla skutecznej realizacji Polityki, Administrator Danych Osobowych zapewnia:

1. Odpowiednie do zagrożeń i kategorii danych objętych ochroną, środki techniczne i rozwiązania organizacyjne.
2. Szkolenie w zakresie przetwarzania danych osobowych i sposobów ochrony.
3. Kontrole i nadzór nad przetwarzaniem i zabezpieczeniem danych osobowych.

§ 5

1. Polityka określa podstawowe zasady bezpieczeństwa danych osobowych i zarządzania bezpieczeństwem systemów służących do przetwarzania tych danych.
2. Polityka dotyczy wszystkich danych osobowych, przetwarzanych w komórkach organizacyjnych Urzędu Miejskiego w Radomiu, niezależnie od formy ich przetwarzania (zbiory tradycyjne, zbiory w systemach informatycznych) oraz od tego czyi dane są lub mogą być przetwarzane w zbiorach.
3. Polityka ma zastosowanie wobec wszystkich komórek organizacyjnych Urzędu Miejskiego w Radomiu.

§ 6

Celem Polityki Bezpieczeństwa jest realizacja postanowień § 4 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 100, poz.1024)
1. Cele Polityki realizowane są poprzez zapewnienie danymi osobowym następujących cech:
b) poufność – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom,
c) integralność – właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
d) rozliczalność – właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
2. Za podmiot nieupoważniony uważa się podmiot, który nie otrzymał zgody Administratora Danych na udostępnienie mu danych osobowych oraz osobę nie posiadającą upoważnienia

do przetwarzania danych osobowych nadanego przez Administratora w trybie art. 37 Ustawy.

§ 7

Zasady określone przez dokumenty Polityki Bezpieczeństwa Informacji i Ochrony Danych Osobowych mają zastosowanie do systemu ochrony informacji Urzędu Miejskiego w Radomiu a w szczególności do:

a. informacji zawierających dane osobowe, których Administratorem jest Prezydent Miasta Radomia lub przetwarzanych dla realizacji zadań zleconych administracji, a których administratorem są organy centralne administracji rządowej lub samorządowej.

b. istniejących obecnie informacji (w formie papierowej i elektronicznej) lub wdrażanych w przyszłości systemów informatycznych, w których przetwarzane są lub będą dane osobowe,

c. wszystkich nośników magnetycznych, optycznych, flash lub papierowych, na których są lub będą znajdować się informacje zawierające dane osobowe,

d. budynków i pomieszczeń, w których są lub będą przetwarzane dane osobowe,

e. wszystkich pracowników Urzędu Miejskiego (zgodnie z przepisami Kodeksu Pracy), jak również stażystów i innych osób mających dostęp do informacji zawierających dane osobowe. Wprowadzona Polityka Bezpieczeństwa podlega ciągłemu doskonaleniu zgodnie z wymaganiami Normy PN-ISO/IEC 17799:2007.

Rozdział 3

Zakres odpowiedzialności poszczególnych stanowisk/komórek organizacyjnych Urzędu oraz osób upoważnionych przez Administratora danych.

§ 8

Zarządzanie bezpieczeństwem danych osobowych jest procesem ciągłym, realizowanym przy współdziałaniu Administratora Danych Osobowych, Administratora Bezpieczeństwa Informacji, Administratorów Systemów Informatycznych z Lokalnymi Administratorami Danych Osobowych, Dyrektorami / Kierownikami Komórek organizacyjnych i osobami upoważnionymi do przetwarzania danych osobowych oraz użytkownikami systemów.

Wszystkie osoby przetwarzające dane osobowe zobowiązane są do:

1. Przetwarzania danych osobowych zgodnie z obowiązującymi przepisami.
2. Postępowania zgodnie z ustaloną przez Administratora Danych Osobowych:

- ,,Polityką Bezpieczeństwa Informacji i Ochrony Danych Osobowych”
- ,,Instrukcją zarządzania systemem informatycznymi w tym do przetwarzania danych osobowych”.

3. W przypadku naruszenia przepisów lub zasad postępowania osoba upoważniona, użytkownik podlega odpowiedzialności służbowej i karnej.

§ 9

Administrator Danych Osobowych (ADO)

Administratorem Danych Osobowych jest Prezydent Miasta Radomia.

Odpowiedzialność ADO polega na:

1) realizacji ustawy o ochronie danych osobowych w zakresie dotyczącym Administratora Danych.

2) określaniu rodzaju informacji przetwarzanych w Urzędzie Miejskim w Radomiu.

3) określaniu własności informacji (własna czy innego podmiotu),

§ 10

Administrator Bezpieczeństwa Informacji (ABI)

Administratora Bezpieczeństwa Informacji powołuje Administrator Danych Osobowych. ABI współpracuje z Administratorem Danych Osobowych pod kątem bezpieczeństwa. Pracę ABI koordynuje i nadzoruje Sekretarz Miasta Radomia.

ABI odpowiedzialny jest za:

1) nadzór i kontrolę zasad ochrony zastosowanych przez Administratora Danych Osobowych w tym stosowania ,,Polityki Bezpieczeństwa Informacji i Ochrony Danych Osobowych", ,,Instrukcji zarządzania systemem informatycznymi w tym do przetwarzania danych osobowych"

2) przeprowadzanie kontroli/sprawdzeń komórek organizacyjnych Urzędu w zakresie określonym w ,,Regulaminie kontroli wewnętrznej" oraz w ustawie o ochronie danych osobowych,

3) przygotowanie upoważnień dostępu do danych osobowych - osobom dopuszczonym przez Administratora Danych Osobowych do przetwarzania danych osobowych,

4) powiadomienie Administratora Systemu Informatycznego o konieczności utworzenia identyfikatora użytkownika w systemie,

5) powiadomienie Administratora Systemu Informatycznego o zmianie uprawnień dostępu użytkownika do systemu,

6) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,

7) prowadzenie ewidencji zbiorów danych osobowych zarejestrowanych u Generalnego Inspektora Ochrony Danych Osobowych jak i zbiorów zarejestrowanych przez Administratora Bezpieczeństwa Informacji w Urzędzie Miejskim w Radomiu,
8) prowadzenie wykazu obszarów przetwarzania danych osobowych w Urzędzie Miejskim w Radomiu,
9) przygotowanie projektów dokumentów bezpieczeństwa danych osobowych,
10) sprawdzanie przygotowanych przez Lokalnych Administratorów Danych Osobowych, zgłoszeń zbiorów danych osobowych do rejestracji Generalnemu Inspektorowi Danych Osobowych jak i do rejestracji przez Administratora Bezpieczeństwa Informacji,
11) szkolenia osób dopuszczonych do danej grupy danych osobowych, w tym zaznajomienie i przeszkolenie pracowników zatrudnionych przy przetwarzaniu danych osobowych z przepisami ustawy o ochronie danych osobowych i przepisami zawartymi w wewnętrznych aktach normatywnych,
12) opiniowanie umówi dotyczących udostępnienia lub powierzenia danych podmiotom zewnętrznym lub osobom, które nie są pracownikami Urzędu.

Praca Administratora Bezpieczeństwa Informacji jest nadzorowana pod względem bezpieczeństwa przez Administratora Danych Osobowych – Prezydenta Miasta Radomia.

§ 11

1. **Biuro Administracyjno – Gospodarcze** realizuje czynności techniczne związane z zapewnieniem skutecznej ochrony fizycznej danym osobowym przetwarzanym w Urzędzie.
2. Do zadań Kierownika Biura Administracyjno - Gospodarczego należy zapewnienie technicznego zabezpieczenia i wyposażenia pomieszczeń i obiektów, które tworzą obszary przetwarzania danych ze szczególnym uwzględnieniem zadań określonych w § 37 ust. 2 lit. c) – e) „Polityki Bezpieczeństwa Informacji i Ochrony Danych Osobowych”.

3. Czynności, o których mowa w ust. 2, wykonuje się na wniosek ABI lub właściwego Kierownika komórki organizacyjnej Urzędu.

§ 12

1. **Wydział Teleinformatyczny** oraz Biuro ds. Systemów i Projektów Oświatowych Współfinansowanych przez UE realizuje czynności techniczne związane z zapewnieniem bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych.
2. Do zadań kierowników w/w komórek w szczególności należy:
a) wyznaczenie ASI w Urzędzie i określenie dla nich zadań w odniesieniu do poszczególnych systemów informatycznych - uwzględniając wielkość zbiorów i typologię systemów oraz nadzorowanie ich działalności;
b) dostosowywanie systemów do wymogów prawa;
c) w porozumieniu z Administratorem Bezpieczeństwa Informacji, planowanie i wdrażanie rozwiązań systemowych i technicznych elementów bezpieczeństwa danych przetwarzanych w systemach;
d) zapewnienie sprzętu i oprogramowania systemów, odpowiadających normom przewidzianym dla poziomów bezpieczeństwa przetwarzania danych w systemach;
e) nadzorowanie technicznego zabezpieczania i odpowiedniego wyposażenia pomieszczeń, w których znajdują się serwery;
f) prowadzenie ewidencji i wykazów, o których mowa w § 34 pkt 4 - 8 i pkt 11 – 13 niniejszej polityki.

§ 13

Administrator Systemu Informatycznego (ASI)

Rolę ASI dla poszczególnych systemów informatycznych pełni pracownik lub pracownicy Wydziału Teleinformatycznego lub Biura ds. Systemów i Projektów Oświatowych Współfinansowanych przez UE.

ASI odpowiedzialny jest (-ni są) za:

1) bieżący nadzór oraz zapewnianie optymalnej ciągłości działania systemu informatycznego, opracowanie procedur określających zarządzanie systemem informatycznymi przetwarzającym dane osobowe,

2) zabezpieczenie systemów przetwarzania danych osobowych zgłoszonych ASI, w zależności od kategorii przetwarzanych w tym systemie danych,

3) dokonywanie okresowej analizy ryzyka dla poszczególnych systemów informatycznych wykorzystywanych do przetwarzania danych osobowych (co najmniej raz w roku),

4) zapewnienie poufności, integralności, dostępności i rozliczalności danych w związku z wykonywanymi zadaniami,

5) reagowanie bez zbędnej zwłoki w przypadku naruszenia bądź powstania zagrożenia bezpieczeństwa danych osobowych,

6) przeciwdziałanie próbom naruszenia bezpieczeństwa danych osobowych,

7) analizę raportów wszelkich zdarzeń w tym incydentów związanych z bezpieczeństwem systemów przetwarzania danych,

8) zgodność wszystkich wdrażanych systemów przetwarzania danych osobowych z ustawą oraz z niniejszą ,,Polityką Bezpieczeństwa Informacji i Ochrony Danych Osobowych" i ,,Instrukcją zarządzania systemem informatycznymi w tym do przetwarzania danych osobowych",

9) instalacje i konfiguracje oprogramowania i sprzętu typu „stand-alone", sieciowego i serwerowego używanego do przetwarzania danych osobowych,

10) konfigurację i administrację oprogramowaniem systemowymi i sieciowym zabezpieczającym dane osobowe przed nieupoważnionymi dostępem,

11) nadzór nad czynnościami związanymi ze sprawdzaniem systemu pod kątem obecności szkodliwego oprogramowania,

12) nadzór nad systemem komunikacji w sieci komputerowej oraz przesyłaniem danych za pośrednictwem urządzeń teletransmisji,

13) nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe,

14) współpracę z dostawcami usługi i sprzętu komputerowego (sieciowego i serwerowego) wraz z weryfikacją zapisów dotyczących ochrony danych osobowych,

15) przyznawanie, na wniosek Kierownika komórki organizacyjnej za zgodą Administratora Danych i zatwierdzeniu przez Administratora Bezpieczeństwa Informacji, ściśle określonych praw dostępu do danych osobowych w danymi systemie,

16) świadczenie pomocy technicznej w ramach oprogramowania a także serwis sprzętu komputerowego będącego na stanie Urzędu Miejskiego w Radomiu służącego do przetwarzania danych osobowych,

17) diagnozowanie i usuwanie awarii sprzętu komputerowego oraz realizacje umów z firmami świadczącymi usługi pogwarancyjnej naprawy sprzętu komputerowego,

18) wykonywanie i zarządzanie kopiami awaryjnymi oprogramowania systemowego (w tym danych osobowych oraz zasobów umożliwiających ich przetwarzanie) i sieciowego,

19) wykonywanie i przechowywanie opisów struktur zbiorów danych osobowych wskazujących zawartość poszczególnych pól informacyjnych i powiązań miedzy nimi - zgodnie z § 4 pkt 3 rozporządzenia. Opis ten może być przedstawiony w postaci formalnej, w postaci graficznej pokazującej istniejące powiązania pomiędzy obiektami, jak również w formie opisu tekstowego,

20) wykonywanie i przechowywanie schematów przepływu danych pomiędzy systemami informatycznymi zastosowanymi w celu przetwarzania danych osobowych ze wskazaniem zakresu przesyłanych danych, podmiotu lub kategorii podmiotów, do których są one

przekazywane oraz ogólnych informacji na temat sposobów ich przesyłania (Internet, poczta elektroniczna, inne rozwiązania), które mogą decydować o rodzaju narzędzi niezbędnych do zapewnienia ich bezpieczeństwa podczas teletransmisji,

21) nadzór nad wdrożeniem i zarządzanie aplikacjami (przeglądanie, nadawanie i odbieranie uprawnień użytkownikom, itp.), w których przetwarza się dane osobowe,

22) prowadzenie rejestru użytkowników systemu (rejestr powinien zawierać: imię i nazwisko osoby, wydział, stanowisko, nr upoważnienia, nazwę zbioru danych osobowych oraz czas trwania dostępu),

23) prowadzenie ewidencji sprzętu i oprogramowania służącego do przetwarzania danych osobowych w zbiorach,

24) prowadzenie rejestru incydentów,

25) zgłaszanie do Administratora Danych Osobowych zmiany oprogramowania służącego do przetwarzania danych w zbiorach,

26) zatwierdzanie wniosków zgłoszeń do rejestracji zbiorów danych osobowych w części E i F,

27) umożliwienie przeprowadzenia kontroli systemu informatycznego przez służby Biura Generalnego Inspektora Ochrony Danych Osobowych.

Praca Administratora Systemu Informatycznego jest nadzorowana pod względem bezpieczeństwa przez Dyrektora Wydziału Teleinformatycznego, lub Kierownika Biura ds. Systemów i Projektów Oświatowych Współfinansowanych przez UE, Administratora Danych i Administratora Bezpieczeństwa Informacji.

§ 14

Lokalny Administrator Danych Osobowych (LADO)

Rolę LADO pełnią Dyrektorzy / Kierownicy (Wydziałów, Biur, Zespołów), w których prowadzone są zbiory danych osobowych i którzy posiadają stosowne pełnomocnictwo Administratora Danych Osobowych

LADO odpowiedzialni są za:

1) zapewnienie by dane osobowe w prowadzonych zbiorach były:

- przetwarzane zgodnie z prawem,
- zbierane dla oznaczonych, zgodnych z prawem celów,
- merytorycznie poprawne i adekwatne w stosunku do celów w jakich są przetwarzane,
- przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą,

2) zapewnienie poufności, integralności i dostępności danych osobowych przetwarzanych w podległym Wydziale,

3) określanie miejsca i czasu przetwarzania, przechowywania, tworzenia i niszczenia informacji zawierających dane osobowe,

4) określenie budynków, pomieszczeń, lub części pomieszczeń tworzących obszar w którym przetwarzane są dane osobowe oraz zgłaszanie zmiany obszarów przetwarzania do Administratora Bezpieczeństwa Informacji oraz Administratora Systemu Informatycznego (załącznik nr 3),

5) stosowanie zabezpieczeń fizycznych i logicznych danych osobowych przetwarzanych tradycyjnie oraz w formie elektronicznej,

6) ewidencjonowanie zbiorów danych osobowych prowadzonych w podległej komórce organizacyjnej Urzędu,

7) określenie i uzgadnianie rodzaju programu oraz wymagań sprzętowych niezbędnych do realizacji zadań w danym Wydziale z Administratorem Systemu Informatycznego,

8) określanie, które osoby i na jakich prawach mają dostęp do danych informacji,

9) ewidencjonowanie osób upoważnionych do przetwarzania danych osobowych w podległej komórce organizacyjnej,

10) określenie czasu rozpoczęcia i zakończenia pracy użytkowników,

11) zapewnienie użytkownikowi stanowiska pracy zgodnie z powierzonymi obowiązkami,

12) powiadomienie Administratora Bezpieczeństwa Informacji i Administratora Systemu Informatycznego o konieczności założenia zbiorów danych na lokalnych stacjach

komputerowych oraz w formie manualnej przed rozpoczęciem przetwarzania danych w zbiorze,

13) przygotowanie (w części A-D) zgłoszenia rejestracji zbiorów danych do Generalnego Inspektora Ochrony Danych Osobowych lub zgłoszenia do Administratora Bezpieczeństwa Informacji (zbiory nierejestrowe) jeżeli mają one charakter danych osobowych,

14) zgłaszanie zmian informacji, o których mowa w art. 41 ust. 1 Ustawy do ABI oraz przygotowanie wniosku aktualizacyjnego zbioru do GIODO lub wniosku do ABI (w przypadku gdy zmiany te dotyczą zbioru nie podlegającego rejestracji przez GIODO),

15) w przypadku nabycia oprogramowania od podmiotów zewnętrznych w trybie innym niż przewidziano w niniejszej polityce oraz instrukcji - LADO jest zobowiązany przed instalacją zgłosić program do Administratora Systemu Informatycznego celem sprawdzenia legalności i bezpieczeństwa oprogramowania oraz zaewidencjonowania w Rejestrze, o którymi mowa w § 34 pkt 5. LADO powiadamia także Administratora Bezpieczeństwa Informacji jeżeli program będzie wykorzystywany do przetwarzania danych osobowych w zbiorze,

16) w przypadku oprogramowania wykorzystywanego do przetwarzania danych osobowych, o którym mowa w pkt 15 LADO ma obowiązek uzyskać, od podmiotu od którego otrzymał oprogramowanie, opis struktury zbioru,

17) powiadamianie bez zbędnej zwłoki ASI i ABI w przypadku naruszenia bądź powstania zagrożenia bezpieczeństwa danych osobowych,

18) przeszkolenie podległych pracowników dopuszczonych do przetwarzania danych osobowych w zakresie bezpieczeństwa danych osobowych,

19) w porozumieniu z ABI rozpatrywanie skargi i wniosków dotyczących przetwarzania i ochrony danych osobowych,

20) wskazywanie osoby wykonującej w komórce organizacyjnej czynności administracyjne związane z przetwarzaniem i ochroną danych osobowych,

21) przygotowanie umów dotyczących udostępniania lub powierzenia przetwarzania danych osobom i podmiotom zewnętrznymi zgodnie z art. 31 Ustawy.

Praca Lokalnych Administratorów Danych Osobowych jest nadzorowana pod względem bezpieczeństwa przez Administratora Danych Osobowych i Administratora Bezpieczeństwa Informacji. Lokalni Administratorzy Danych Osobowych realizując zadania w imieniu Administratora Danych współpracują z: Administratorem Bezpieczeństwa Informacji, Kierownikiem Biura Administracyjno – Gospodarczego, Dyrektorem Wydziału Teleinformatycznego, Kierownikiem Biura ds. Systemów i Projektów Oświatowych Współfinansowanych przez UE oraz innymi osobami upoważnionymi przez Administratora.

§ 15

Użytkownik (U)

Rolę Użytkownika Systemu pełni osoba upoważniona do przetwarzania danych osobowych.

1) Do obsługi systemu komputerowego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych, są dopuszczeni wyłącznie pracownicy, stażyści i inne osoby - posiadający upoważnienie wydane przez Administratora Danych lub upoważnioną przez niego osobę.

2) Bezpośredni dostęp do danych osobowych użytkownik ma dopiero po podaniu identyfikatora i właściwego hasła.

3) Użytkownik zmienia hasło z częstotliwością nie rzadszą niż 30 dni.

4) Pracownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu.

5) Użytkownik zamyka system, aplikację, program po zakończeniu pracy, stanowisko komputerowe z uruchomionymi systemem, programem nie może pozostać bez kontroli pracującego na nimi użytkownika.

6) Osoby dopuszczone do obsługi programu komputerowego obowiązane są do zachowania tajemnicy co do sposobu dostępu do danych osobowych i ich merytorycznej treści, a także sposobu zabezpieczeń. Obowiązek ten istnieje również po ustaniu zatrudnienia.

7) Wszelkie wydruki zawierające dane osobowe oraz zewnętrzne nośniki danych, na których znajdują się dane osobowe powinny być przechowywane w miejscu uniemożliwiającymi ich odczyt przez osoby nieuprawnione, zaś po upływie czasu ich przydatności powinny być niszczone w taki sposób by uniemożliwić odczytanie danych.
8) Osoby fizyczne oraz inne podmioty wykonujące umowy na rzecz Gminy Miasta Radomia powinny posiadać aktualne upoważnienia wydane przez Administratora Danych zezwalające na korzystanie ze zbiorów danych.
9) Użytkownik ma obowiązek:
- ścisłego przestrzegania zakresu nadanego upoważnienia,
- przetwarzania i ochrony danych osobowych zgodnie z przepisami,
- powiadamiać Administratora Bezpieczeństwa Informacji oraz Administratora Systemu Informatycznego o sytuacjach nadzwyczajnych i wszelkiego rodzaju różnicach w funkcjonowaniu programu, systemu i tylko w porozumieniu z wymienionymi osobami może zostać wezwany do konsultacji autor programu lub przedstawicieli autora (firmy, od której zostało oprogramowanie zakupione).
Praca Użytkownika jest nadzorowana pod względem bezpieczeństwa przez Kierowników Komórek Organizacyjnych, Administratora Systemu Informatycznego oraz Administratora Bezpieczeństwa Informacji.

§ 16

1. Osoby upoważnione przez Administratora do podpisywania umów z osobami lub podmiotami, o których mowa w § 1 ust. 2 „Instrukcji zarządzania systemem informatycznymi w tym do przetwarzania danych osobowych" stanowiącej załącznik nr 2 do Zarządzenia, zobowiązane są do umieszczania postanowień umownych, gwarantujących bezpieczeństwo i ochronę danych osobowych w formie oświadczenia, którego treść określa wzór nr 4 do niniejszej Polityki Bezpieczeństwa Informacji i Ochrony Danych Osobowych.

2. Postanowienia, o których mowa w ust. 1, dotyczą udostępniania lub powierzenia danych do przetwarzania i zawierają:

a) określenie przedmiotu i celu umowy,

b) zobowiązanie zleceniobiorcy do zapewnienia bezpieczeństwa i właściwej ochrony przetwarzanych danych osobowych,

c) zobowiązanie zleceniobiorcy do przestrzegania procedur ochrony danych osobowych,

d) oświadczenie zleceniobiorcy dotyczące dostosowania systemów informatycznych wykorzystywanych w procesie przetwarzania danych osobowych do wymogów rozporządzenia Ministra Sprawi Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r,

e) zapewnienie zleceniodawcy nadzoru i kontroli nad przetwarzaniem i ochroną danych osobowych,

f) określenie kar umownych za nieprzestrzeganie zapisów umownych,

g) możliwość rozwiązania umowy w trybie natychmiastowymi w przypadku stwierdzenia omijania przez zleceniobiorcę przepisów dotyczących bezpieczeństwa i ochrony przetwarzanych danych osobowych.

Rozdział 4

Ogólne zasady przetwarzania danych osobowych.

§ 17

1. Dane osobowe są przetwarzane w Urzędzie w celu realizacji zadań określonych przepisami prawa.

2. Cel, o którym mowa w ust. 1, należy osiągać przy zachowaniu szczególnej staranności w realizacji przedsięwzięć dotyczących ochrony interesów osób, których dane dotyczą.

§ 18

1. Zasadą obowiązującą w Urzędzie jest zachowanie przez użytkowników w tajemnicy wszelkich informacji dotyczących danych osobowych oraz sposobów ich zabezpieczania.
2. Możliwość wystąpienia zagrożeń bezpieczeństwa danych przetwarzanych w systemach lub kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych nakłada na użytkowników i ich przełożonych obowiązek zapewnienia danym skutecznej ochrony.
3. Przesyłanie danych osobowych za pomocą urządzeń telekomunikacyjnych lub transmisji danych w sieci publicznej wymaga wykorzystania odpowiednich urządzeń i przedsięwzięć zapewniających poufność, integralność, dostępność, autentyczność, niezaprzeczalność i niezawodność danych.
4. Kopiowanie danych osobowych oraz wykonywanie wydruków jest zabronione, chyba że konieczność ich sporządzania wynika z nałożonych na użytkownika obowiązków i dozwolona jest przepisami prawa.
5. Do przetwarzania danych osobowych mogą służyć wyłącznie systemy informatyczne lub zewnętrzne nośniki danych będące własnością Urzędu Miejskiego w Radomiu, które odnotowane zostały w stosownej ewidencji, o której mowa w § 34 niniejszej polityki.

§ 19

1. Przetwarzanie danych osobowych może być wykonywane wyłącznie przez osoby, które spełniają wymagania zawarte w art. 37 Ustawy.
2. Procedury nadawania (wycofywania) w Urzędzie upoważnień do przetwarzania danych osobowych:
a) Kierownik Komórki Organizacyjnej, w ciągu 7 dni od chwili zatrudnienia pracownika, występuje do Administratora Danych z wnioskiem o wydanie upoważnienia do przetwarzania danych osobowych w zbiorze dla pracownika – wzór wniosku o nadanie upoważnienia określa załącznik nr 1. Wniosek powinien zawierać: nazwisko i imię,

zajmowane stanowisko, nazwę zbioru, nazwę systemu informatycznego zakres upoważnienia oraz termin obowiązywania.

b) Administrator Danych udziela zezwolenia na dostęp do danych osobowych.

c) Na podstawie zaakceptowanego wniosku Administrator Bezpieczeństwa Informacji przygotowuje stosowne upoważnienie, wzór upoważnienia - załącznik nr 2, określając numer rejestrowy i identyfikator dostępu do zbioru. Identyfikator dostępu jest przekazany Administratorowi Systemu Informatycznego. Kopia wniosku w formie papierowej przechowywana jest przez Administratora Bezpieczeństwa Informacji.

d) Upoważnienie po podpisaniu przez osobę upoważnioną wraz z oświadczeniem o zachowaniu w tajemnicy zasad przetwarzania danych oraz sposobów ich zabezpieczania, obejmującej także okres po ustaniu stosunku pracy, zostaje skierowane do realizacji do Dyrektora/Kierownika komórki organizacyjnej oraz do Administratora Systemu Informatycznego – w przypadku przetwarzania danych w systemie informatycznym. W przypadku upoważnienia do dostępu do danych osobowych wyłącznie w formie tradycyjnej, upoważnienie zostaje przekazane do Dyrektora/Kierownika komórki organizacyjnej wnioskującego o upoważnienie podległego pracownika.

e) Administrator Systemu Informatycznego zakłada konto użytkownika w systemie informatycznym o wskazanym identyfikatorze zabezpieczone hasłem tymczasowym, którego zmiana jest wymuszona przy pierwszym zalogowaniu użytkownika zgodnie z zasadami panującymi w Urzędzie Miejskim w Radomiu i szczegółowymi instrukcjami dla danej aplikacji / programu.

f) Jeden egzemplarz upoważnienia o przyznanie lub modyfikację praw dostępu jest przechowywany przez Administratora Systemu Informatycznego.

g) Kierownik Komórki Organizacyjnej, w ciągui7 dni od przeniesienia pracownika do innej komórki organizacyjnej, jest zobowiązany złożyć wniosek do Administratora Danych o unieważnienie upoważnienia temu pracownikowi.

h) W przypadku otrzymania przez Administratora Bezpieczeństwa Informacji wniosku o zablokowanie konta użytkownika, jest on zobowiązany w trybie natychmiastowym odznaczyć ten fakt w ewidencji.

i) Konto zostaje zablokowane przez Administratora Systemu Informatycznego na wniosek Kierownika Komórki Organizacyjnej po akceptacji Administratora Danych i Administratora Bezpieczeństwa Informacji. Konto użytkownika jest blokowane zgodnie ze szczegółowymi instrukcjami operacyjnymi specyficznymi dla danej aplikacji lub systemu.

j) W przypadku rozwiązania umowy o pracę cofnięcie upoważnień następuje na podstawie karty obiegowej.

k) Centralna ewidencja osób upoważnionych do przetwarzania zbiorów danych osobowych jest prowadzona przez Administratora Bezpieczeństwa Informacji.

3. Polityka zawiera także załączniki, które stanowią:

a) druk nr 1 – wzór wniosku przełożonego o nadanie (pozbawienie) lub zmianę upoważnienia do przetwarzania danych osobowych.

b) druk nr 2 – wzór upoważnienia do przetwarzania danych osobowych wraz z oświadczeniem o zachowaniu w poufności danych i sposobów ich zabezpieczeń.

c) druk nr 3 - wzór zgłoszenia (zmiany) obszaru przetwarzania danych osobowych.

d) druk nr 4 – wzór oświadczenia użytkownika zewnętrznego.

4. Kopie upoważnień przechowuje Administrator Bezpieczeństwa Informacji.

5. Kierownik/Dyrektor komórki organizacyjnej ma obowiązek realizacji procedur, o których mowa w ust. 2.

6. ABI prowadzi kontrolę realizacji obowiązku, o którym mowa w ust. 1.

§ 20

1. Budynki, pomieszczenia lub ich część, w których przetwarzane są dane osobowe tworzą obszary przetwarzania danych osobowych w Urzędzie. Przebywanie osób nieuprawnionych w tych obszarach jest ograniczone i odbywać się może tylko w obecności użytkowników.

2. Administrator zapewnia ochronę obszarów przetwarzania danych osobowych w Urzędzie, według zasad określonych w niniejszej „Polityce Bezpieczeństwa Informacji i Ochrony Danych Osobowych”.
3. Do obszarów podlegających szczególnej ochronie Administrator zalicza serwerownie oraz pomieszczenia, w których przetwarzane są dane sensytywne.

Rozdział 5

Obszary przetwarzania danych.

§ 21

1. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe w Urzędzie jest prowadzony przez Administratora Bezpieczeństwa Informacji.
2. Za obszar przetwarzania danych uznaje się obszar, w którym wykonywana jest choćby jedna z czynności wymienionych w art. 7 pkt. 2 Ustawy.

§ 22

Dyrektorzy/Kierownicy Wydziałów/Biur Urzędu, zobowiązani są do niezwłocznego przekazywania do Administratora Bezpieczeństwa Informacji o lokalizacji miejsc przetwarzania danych osobowych.

Rozdział 6

Procedury tworzenia, rejestrowania i dokonywania zmian w przetwarzaniu danych osobowych w zbiorach.

§ 23

1. Tworzy się zbiory danych osobowych przez nadanie danym osobowymi odpowiedniej struktury, dostępnej według określonych kryteriów, niezależnie od tego, czy zestaw danych jest rozproszony lub podzielony funkcjonalnie.
2. Przetwarzanie danych osobowych może odbywać się:
a) w zbiorach ewidencyjnych papierowych, w rozumieniu art. 2 ust. 2 pkt 1) Ustawy,
b) w systemach informatycznych, w rozumieniu art. 2 ust. 2 pkt 2) Ustawy.
3. Zgodnie z potrzebami realizacji zadań służbowych, Lokalni Administratorzy Danych Osobowych tworzą zbiory lub wnioskują o ich wycofanie (zmianę), według następujących reguł:
a) nazwa zbioru powinna odzwierciedlać cel przetwarzania danych i być zgodna z nazewnictwem stosowanymi w przepisach prawa,
b) należy wskazać podstawy prawne do przetwarzania danych,
c) należy określić sposób i miejsca przetwarzania danych oraz użytkowników,
d) należy przekazać informację ABI w celu określenia poziomu bezpieczeństwa systemu, w którym przetwarzane są dane,
e) należy przekazać informację do ASI celem zabezpieczenia systemu zgodnie z określonym poziomem bezpieczeństwa,
f) należy zapewnić ochronę danym osobowym.

§ 24

Lokalni Administratorzy Danych Osobowych oraz Dyrektorzy/Kierownicy Wydziałów/Biur mają obowiązek zgłaszania do Administratora Bezpieczeństwa Informacji aktualnych wykazów zbiorów danych osobowych przetwarzanych przez podległych im pracowników.

§ 25

1. Administrator Danych Osobowych ma obowiązek zgłosić zbiór danych do rejestracji w GIODO, z wyjątkiem przypadków określonych w art. 43 ust. 1 Ustawy.
2. Lokalni Administratorzy mają obowiązek wypełnienia i parafowania wniosku zgłoszenia zbioru do rejestracji - w części od A – D i przesłania go do Administratora Systemu Informatycznego celem wypełnienia i parafowania wniosku w części E - F
3. Administrator Systemu Informatycznego przekazuje wniosek do Administratora Bezpieczeństwa Informacji.
4. Administrator Bezpieczeństwa Informacji po podpisaniu wniosku przez Administratora Danych Osobowych przesyła go do GIODO.
5. Wzór wniosku, o którym mowa w ust. 2, stanowi załącznik do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz.U. Nr 229, poz. 1536).
6. Dane osobowe w zbiorze można przetwarzać po potwierdzeniu przez GIODO jego zarejestrowania.

Rozdział 7

Wykaz zbiorów danych oraz programów zastosowanych do przetwarzania danych osobowych.

§ 26

1. Wykaz zbiorów danych oraz programów zastosowanych do przetwarzania danych jest Prowadzony przez Administratora Bezpieczeństwa Informacji.
2. Administratorzy Systemów Informatycznych zobowiązani są do niezwłocznego przekazywania do Administratora Bezpieczeństwa Informacji wykazu programów zastosowanych do przetwarzania danych osobowych w zbiorach.

Rozdział 8

Struktury zbiorów danych oraz przepływ danych pomiędzy systemami.

§ 27

1. Dane osobowe są przetwarzane przy zastosowaniu systemów informatycznych, w zbiorach ewidencyjnych oraz poza zbiorami.
2. Zbiory danych osobowych zlokalizowane są w przedmiotowych bazach danych umieszczonych na serwerach bazodanowych.
3. Dane osobowe w zbiorach są przetwarzane tylko w aplikacjach (programach) dostosowanych do merytorycznych potrzeb komórek organizacyjnych Urzędu.

§ 28

1. Zawartość pól informacyjnych, występujących w aplikacjach (programach) systemów zastosowanych do przetwarzania danych, musi być zgodna z przepisami prawa, które

uprawniają lub zobowiązują Administratora Danych Osobowych do przetwarzania danych osobowych.
2. Na żądanie Administratora Danych Osobowych lub osoby przez niego upoważnionej, osoby o których mowa w § 8, zobowiązane są wskazać podstawy prawne określające zakres przetwarzanych danych.

§ 29

1. Opisy struktur zbiorów danych wskazujące zawartość poszczególnych pól informacyjnych i powiązania pomiędzy nimi, wykonują ASI na podstawie dokumentacji aplikacji zastosowanych do przetwarzania tych danych.
2. Opisy wykonywane są w postaci wydruków zrzutów ekranowych lub struktur tablic bazy prezentujących zawartość pól informacyjnych i powiązań pomiędzy nimi. W przypadku braku możliwości uzyskania wydruku zrzutu ekranowego ASI sporządzają inne dostępne opisy struktury zbioru.
3. ASI zobowiązani są do prowadzenia i przechowywania opisów struktur zbiorów danych oraz natychmiastowego uaktualniania w przypadku zmian.

§ 30

1. Schematy przepływu danych pomiędzy systemami informatycznymi, zastosowanymi w celu przetwarzania danych osobowych, wykonują ASI, zgodnie z relacjami występującymi w programach służących do przetwarzania danych osobowych.
2. ASI zobowiązani są do prowadzenia i przechowywania schematów oraz natychmiastowego ich uaktualniania w przypadku zmian.

§ 31

1. Przepływ danych pomiędzy systemami zastosowanymi w celu przetwarzania danych osobowych może odbywać się w postaci przepływu jednokierunkowego lub przepływu dwukierunkowego.
2. Przesyłanie danych pomiędzy systemami może odbywać się w sposób automatyczny lub manualny: przy wykorzystaniu funkcji eksportu (importu) danych z wykorzystaniem nośników zewnętrznych (np., CD, DVD, dyski wymienny, PenDrive itp.) lub teletransmisji.

Rozdział 9

Szkolenie oraz prowadzenie dokumentacji z zakresu przetwarzania danych osobowych.

§ 32

1. Każda osoba przed rozpoczęciem przetwarzania danych ma obowiązek zapoznania się z przepisami dotyczącymi bezpieczeństwa przetwarzania i ochrony danych osobowych. Bezpośredni przełożony zobowiązany jest zapoznać podwładnych z tymi przepisami.
2. W przypadku wdrażania w Urzędzie nowych procedur przetwarzania i ochrony danych osobowych, Administrator Bezpieczeństwa Informacji na wniosek LADO, może polecić zorganizowanie dodatkowych szkoleń dla wskazanych przez przełożonych grup użytkowników.
3. Szkolenia, o których mowa w ust. 2, dla Wydziałów / Biur organizuje ABI.

§ 33

Dokumentacja przetwarzania i ochrony danych osobowych w Urzędzie obejmuje:
1. „Politykę Bezpieczeństwa Informacji i Ochrony Danych Osobowych”,

2. „Instrukcję zarządzania systemem informatycznym w tym do przetwarzania danych osobowych”;

§ 34

W procesie przetwarzania i ochrony danych osobowych prowadzi się następujące ewidencje i wykazy:

1. „Centralna ewidencja osób upoważnionych do przetwarzaniu danych osobowych” - prowadzona przez Administratora Bezpieczeństwa Informacji,
2. „Wykaz zbiorów danych osobowych oraz programów zastosowanych do ich przetwarzania” – prowadzona przez Administratora Bezpieczeństwa Informacji,
3. ,,Rejestr zbiorów danych osobowych” – prowadzony przez Administratora Bezpieczeństwa Informacji,
4. ,,Rejestr użytkowników systemu” – prowadzone przez Wydział Teleinformatyczny,
5. ,,Ewidencja sprzętu i oprogramowania służącego do przetwarzania danych osobowych” – prowadzona przez Wydział Teleinformatyczny,
6. ,,Rejestr zdarzeń i incydentów” – prowadzony przez Wydział Teleinformatyczny,
7. ,,Harmonogram archiwizacji danych i programów” – prowadzony przez Wydział Teleinformatyczny,
8. „Wykaz budynków i pomieszczeń lub części pomieszczeń tworzących obszary przetwarzania danych osobowych” – prowadzony przez Administratora Bezpieczeństwa Informacji,
9. „Lokalne ewidencje osób upoważnionych do przetwarzaniu danych osobowych” prowadzone w poszczególnych komórkach organizacyjnych Urzędu Miejskiego w Radomiu,
10. rejestry udostępnionych danych osobowych zawierające co najmniej: datę udostępnienia, podstawę prawną, zakres udostępnionych informacji oraz osobę lub instytucję, której dane udostępniono - prowadzą Kierownicy komórek organizacyjnych,
11. opisy struktur zbiorów danych osobowych wskazujących zawartość poszczególnych pól

informacyjnych i powiązań miedzy nimi – prowadzone przez Wydział Teleinformatyczny,
12. schematy przepływu danych pomiędzy systemami informatycznymi zastosowanymi w celu przetwarzania danych osobowych. – prowadzone przez Wydział Teleinformatyczny,
13. lokalne ewidencje danych osobowych – prowadzone przez Lokalnych Administratorów Danych,
14. lokalne ewidencje zewnętrznych nośników pamięci wykorzystywanych do przetwarzania danych osobowych - prowadzone przez Kierowników komórek organizacyjnych.
Dokumentacja , o której mowa w § 34 pkt 1 - 15 powinna być aktualizowana zaraz po wystąpieniu zmian.

Rozdział 10

Dostęp zdalny.

§ 35

1. Zastosowane przez Urząd rozwiązania techniczne umożliwiające dostęp zdalny do danych osobowych powinny zapewniać integralność, poufność i rozliczalność przetwarzanych danych osobowych oraz ochronę kryptograficzną wobec danych służących do uwierzytelniania, a przesyłanych publicznymi łączami telekomunikacyjnymi.
2. Nadawanie uprawnień w celu dostępu zdalnego do systemów informatycznych przetwarzających dane osobowe realizowane jest przez Administratora Systemu po spełnieniu wymagań określonych w ust.1 oraz po uzyskaniu akceptacji Administratora Danych Osobowych oraz Administratora Bezpieczeństwa Informacji.
3. Dostęp do systemów informatycznych dla użytkowników zewnętrznych powinien być monitorowany pod kątem bezpieczeństwa przez Administratorów Systemu w celu zapewnienia poufności, rozliczalności i integralności danych osobowych.

Rozdział 11

Organizacja bezpieczeństwa danych osobowych

§ 36

1. Administrator Danych Osobowych zapewnia zastosowanie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.
2. 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 niniejszej polityki lub systemy posiadające zgodę Administratora Danych Osobowych na ich użytkowanie.
3. Osoby, o których mowa w § 8 przeprowadzają okresową analizę ryzyka dla poszczególnych systemów (przynajmniej raz do roku) i na tej podstawie przedstawiają Administratorowi Danych Osobowych oraz Administratorowi Bezpieczeństwa Informacji propozycje dotyczące zastosowania środków technicznych i organizacyjnych (środków ochrony), celem zapewnienia właściwej ochrony przetwarzanym danym.
4. Analiza ryzyka obejmuje:
a) identyfikację występujących zagrożeń dla systemów, zbiorów i baz danych,
b) ocenę dotychczas stosowanej ochrony obszarów przetwarzania danych osobowych,
c) określenie wielkości ryzyka, tj. prawdopodobieństwa, że określone zagrożenie wykorzysta podatność(słabość) zasobu,
d) identyfikację obszarów wymagających szczególnych zabezpieczeń.
5. Zastosowane środki ochrony (techniczne i organizacyjne) powinny być adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych osobowych.

§ 37

1. Środki ochrony, zastosowane przez Administratora dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych, obejmują:

a) środki fizyczne,

b) środki osobowe,

c) środki techniczne.

2. Środki ochrony fizycznej obejmują:

a) lokalizację miejsc przetwarzania danych osobowych w pomieszczeniach o ograniczonym i kontrolowanym dostępie,

b) ustalenie zasad gospodarki kluczami do pomieszczeń i szaf,

c) wyposażenie pomieszczeń, w których przetwarzane są dane osobowe, w zabezpieczone zamkiem drzwi, odpowiednio zabezpieczone okna poniżej I piętra, meble, zamknięcia i niezbędne zabezpieczenia alarmowe,

d) składowanie danych sensytywnych oraz nośników wymiennych i nośników kopii zapasowych, w odpowiednio zabezpieczonych szafach,

e) zastosowanie ochrony p. poż. pomieszczeń, w których przetwarzane są dane osobowe,

f) odpowiednie wyposażenie i zabezpieczenie pomieszczeń serwerowni.

3. Środki ochrony osobowej obejmują:

a) dopuszczenie do przetwarzania danych osobowych wyłącznie osób posiadających upoważnienie nadane przez Administratora lub osobę upoważnioną przez niego,

b) zapoznanie tych osób z zasadami przetwarzania danych osobowych oraz obsługą systemu służącego do ich przetwarzania,

c) odebranie stosownych zobowiązań i oświadczeń, tj. zobowiązania do zachowania w tajemnicy danych i sposobów ich zabezpieczenia oraz oświadczenia o zapoznaniu z treścią przepisów określających zasady postępowania przy przetwarzaniu danych osobowych, a także z dokumentacją przetwarzania i ochrony danych osobowych.

4. Środki ochrony technicznej obejmują:

a) mechanizmy kontroli dostępu do systemów i zasobów,
b) zastosowanie odpowiednich i regularnie aktualizowanych narzędzi ochronnych (programy antywirusowe itp.),
c) regularne tworzenie kopii zapasowych zbiorów danych przetwarzanych w systemach informatycznych,
d) zastosowanie ochrony zasilania.

§ 38

1. Uwzględniając kategorie przetwarzanych danych oraz zagrożenia zidentyfikowane w wyniku przeprowadzonej analizy ryzyka dla poszczególnych systemów, stosuje się następujące poziomy bezpieczeństwa:
a) podstawowy,
b) podwyższony,
c) wysoki.
2. Określenia poziomu bezpieczeństwa systemu informatycznego dla zbiorów dokonuje ABI na wniosek osób o których mowa w § 15.
3. Poziomy bezpieczeństwa systemu informatycznego w odniesieniu do poszczególnych zbiorów odnotowuje się w dokumentacji prowadzonej przez Administratora Bezpieczeństwa Informacji.

§ 39

Systemy informatyczne, którym przypisano poziomy bezpieczeństwa wymienione w § 38 muszą spełniać wymagania wymienione w załączniku do 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 100, poz. 1024).

Rozdział 12

Środki ochrony

(wyłączony z publikacji)

Rozdział 13

Postanowienia Końcowe

§ 49

1. Wszelkie zmiany w „Polityce Bezpieczeństwa Informacji i Ochrony Danych Osobowych" wymagają zatwierdzenia przez Administratora Danych Osobowych.
2. Aktualizacje danych zawartych w załącznikach do „Polityki Bezpieczeństwa Informacji i Ochrony Danych Osobowych" będą dokonywane w miarę potrzeb, jednakże nie rzadziej niż raz do roku.
3. Odpowiedzialność karną za przetwarzanie danych osobowych niezgodnie z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r., poz. 922) oraz przepisami wykonawczymi do tej ustawy określają art. 49-54 ww. ustawy.
4. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z „Polityki Bezpieczeństwa Informacji i Ochrony Danych Osobowych" traktowane są jako ciężkie naruszenie obowiązków pracowniczych. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w „Polityce Bezpieczeństwa Informacji i Ochrony Danych Osobowych", a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także gdy nie zrealizowała stosownego

działania dokumentującego ten przypadek, wszczyna się postępowanie dyscyplinarne.

5. Orzeczona kara dyscyplinarna wobec osoby uchylającej się od powiadomienia, nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. z 2016 r., poz 922.) oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
6. Osoby, które zostały zapoznane z Polityką Bezpieczeństwa zobowiązują się do bezwzględnego stosowania zasad w niej zawartych. Upoważnienia do przetwarzania danych osobowych przechowywane są w aktach personalnych pracownika.
7. Wszystkie regulacje określone w „Polityki Bezpieczeństwa Informacji i Ochrony Danych Osobowych" dotyczą przetwarzania danych osobowych w zbiorach prowadzonych w zarówno w formie elektronicznej jak i w formie papierowej.
8. W przypadku konieczności udostępnienia danych osobowych, Administrator Danych Osobowych udostępnia posiadane w zbiorze dane osobowe, osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.
9. Dane osobowe udostępnia się na pisemny wniosek, chyba że przepis innej ustawy stanowi inaczej.
10. Udostępnione dane osobowe można wykorzystywać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
11. Niezależnie od zasad opisanych w „Polityce Bezpieczeństwa Informacji i Ochrony Danych Osobowych" w zakresie bezpieczeństwa mają zastosowanie wszelkie wewnętrzne regulaminy i instrukcje dotyczące bezpieczeństwa ludzi i zasobów informacyjnych oraz indywidualne zakresy zadań osób zatrudnionych przy przetwarzaniu danych osobowych w określonym systemie; dokumenty te nie mogą być sprzeczne z regulacjami określonymi w „Polityce Bezpieczeństwa Informacji i Ochrony Danych Osobowych".

Załącznik Nr 1 do Polityki Bezpieczeństwa Informacji i Ochrony Danych Osobowych

Wzór wniosku o nadanie/zmianę/pozbawienie upoważnienia do przetwarzania danych osobowych

…… Radom, dn. .....

(pieczęć komórki organizacyjnej)

Prezydent

Miasta Radomia

W N I O S E K

Zgodnie z art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U.2016, poz. 922)

wnioskuję o nadanie /pozbawienie/zmianę/*

Pani /Panu/*.....stanowisko służbowe……
upoważnienia do przetwarzania danych osobowych w Urzędzie Miejskim w Radomiu z powodu: /przyjęcia do pracy, przejścia na inne stanowisko, zwolnienia z pracy, zmiany uprawnień, lub innego - jakiego/*:

.....

Upoważnienie wydaje się na okres: /stały/czasowy – do kiedy/*.....

1. Zakres przetwarzania danych osobowych

.....

. /zbieranie, utrwalanie, opracowywanie, wprowadzanie, przechowywanie, zmiana, usuwanie, udostępnianie/*

2. Nazwa zbioru danych osobowych:

.....

3. Sposób przetwarzania danych osobowych: /papierowy/ informatyczny/*
   - jeśli sposób informatyczny to jaki:
     identyfikator :……. ……
     program:……
4. Obszar przetwarzania /adres siedziby/.....
   danych osobowych /piętro, nr pokoju/.....
5. Uprawnienia obejmują przetwarzanie danych sensytywnych /art. 27 Ustawy/
   /tak/nie/*
6. Osoba została zapoznana z przepisami o ochronie danych osobowych:
   /tak/nie/*

……
(przełożony osoby / LADO)

/* niepotrzebne proszę skreślić

Druk Nr 2 do Polityki Bezpieczeństwa Informacji i Ochrony Danych Osobowych

Wzór upoważnienia do przetwarzania danych osobowych

Radom, dn. .....

UPOWAŻNIENIE Nr …./…..

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych

(Dz. U 2016 poz. 922)

Upoważniam

Pana/Panią……..

Stanowisko służbowe……..

Do przetwarzania danych osobowych w zbiorze o nazwie:

……

w zakresie:

……

w systemie tradycyjnym/ informatycznym*

identyfikator…… program…….……

od dnia……. do dnia……

Jednocześnie zobowiązuję Pana/Panią do przestrzegania przepisów dotyczących ochrony danych osobowych zawartych w cytowanej wyżej ustawie z dnia 29 sierpnia 1997 r.

……..

/podpis Administratora Danych Osobowych/

Przyjmuje do wiadomości i przestrzegania,

Zobowiązuje się do zachowania w tajemnicy

tych danych oraz sposobów ich zabezpieczeń

także po ustaniu zatrudnienia

.....

/data i podpis pracownika/

/* niepotrzebne proszę skreśli

Druk Nr 3 do Polityki Bezpieczeństwa Informacji i Ochrony Danych Osobowych - **Wzór zgłoszenia (zmiany) obszaru przetwarzania danych osobowych**

Lp.	Nazwa zbioru	Forma przetwarzania	Dane sensytywne	Obszar przetwarzania	Ilość stanowisk

Forma przetwarzania – należy wskazać formę: elektroniczną, tradycyjną lub elektroniczną i tradycyjną . Nie należy wskazywać formy elektronicznej w przypadku przetwarzania danych w SI ograniczonego do edycji tekstu.

Dane sensytywne – należy wypełnić tak lub nie. Dane sensytywne (wrażliwe) art. 27 ust 1 ustawy z dn. 29.08.1997 r. o ochronie danych osobowych.

Obszar przetwarzania – dot. wszystkich zbiorów niezależnie od formy przetwarzania.

Ilość stanowisk – wypełnić tylko w przypadku zbiorów przetwarzanych w formie elektronicznej lub tradycyjnej i elektronicznej. Należy wskazać ilość stanowisk komputerowych, na których
przetwarzany jest zbiór danych osobowych.

Druk Nr 4 do Polityki Bezpieczeństwa Informacji i Ochrony Danych Osobowych

Radom, dnia ……..

Oświadczenie

1. Zgodnie art. 31 ust 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2016., poz. 922) wykonawca/zleceniobiorca oświadcza, że spełnia wymagania określone w przepisach, o których mowa w art. 39a wyżej cytowanej ustawy.
2. Wykonawca/Zleceniobiorca umowy zobowiązuje się do bezwzględnego zachowania w poufności wszelkich informacji uzyskanych w związku z wykonywaniem umowy, oraz sposobów ich zabezpieczeń, także po zakończeniu realizacji umowy. Obowiązek ten nie dotyczy informacji, co do których Gmina Miasta Radomia / Urząd Miejski w Radomiu - ma nałożony ustawowy obowiązek publikacji lub która stanowi informacje jawną, publiczną opublikowaną przez Gminę Miasta Radomia / Urząd Miejski w Radomiu.
3. W przypadku naruszenia zapisów pkt 1-2 Gmina Miasta Radomia / Urząd Miejski w Radomiu może wypowiedzieć umowę ze skutkiem natychmiastowym.

…… ……. ……

(Data i podpis osoby przyjmującej oświadczenie) (Zleceniobiorca/wykonawca)

(Data i podpis składającego oświadczenie)