Załącznik
do Zarządzenia Nr 370/16
Burmistrza Brus
z dnia 24 sierpnia 2016 r.

URZĄD MIEJSKI W BRUSACH

WYDZIAŁ ORGANIZACYJNO - PRAWNY

ZATWIERDZAM
BURMISTRZ
dr inż. Witold Ossowski
.....

Polityka Bezpieczeństwa Informacji w Urzędzie Miejskim w Brusach

Opracował:
INSPEKTOR
mgr inż. Adam Mochoł

Brusy, sierpień 2016 roku

Spis treści

I. Podstawa prawna

Na podstawie § 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) oraz § 20 rozporządzenia 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 (t.j. z 14 stycznia 2016 r., Dz. U. z 2012r., poz. 113) ustala się „Politykę Bezpieczeństwa Informacji w Urzędzie Miejskim w Brusach", zwaną dalej „Polityką Bezpieczeństwa".

II. Wstęp.

1. Regulacje zawarte w niniejszym dokumencie dotyczą wszystkich informacji przetwarzanych w Urzędzie Miejskim w Brusach w sposób elektroniczny oraz tradycyjny – papierowy ze szczególnym uwzględnieniem danych osobowych oraz innych informacji prawnie chronionych.

2. Kierownictwo Urzędu świadome jest zagrożeń związanych z przetwarzaniem przez Urząd dużej liczby informacji w tym szczególnie chronionych danych osobowych, oraz wynikających z tego zagrożeń związanych z dynamicznym rozwojem metod i technik przetwarzania tych danych w systemach informatycznych oraz sieciach telekomunikacyjnych. Dlatego kierownictwo Urzędu deklaruje zamiar:
    1) doskonalenia systemu zarządzania bezpieczeństwem informacji aby zapewnić poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność,
    2) stosowania odpowiednich środków informatycznych, technicznych i organizacyjnych zapewniające ochronę przetwarzanych informacji ze szczególnym uwzględnieniem danych osobowych a w szczególności ich zabezpieczeniem przed:
        - udostępnieniem osobom nieupoważnionym;
        - przetwarzaniem z naruszeniem ustawy;
        - zmianą, utratą, uszkodzeniem lub zniszczeniem.

3) podejmowania wszystkich działań niezbędnych dla ochrony praw i usprawiedliwionych interesów jednostki związanych z bezpieczeństwem informacji a w szczególności jej danych osobowych, w tym zapewnienia aby dane te były:
   - przetwarzane zgodnie z prawem,
   - przetwarzane wyłącznie w celu realizacji ustawowych zadań,
   - zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,
   - merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,
   - przechowywane w postaci umożliwiającej identyfikacje osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.
4) stałego podnoszenia świadomości oraz kwalifikacji osób przetwarzających informacje w Urzędzie w zakresie problematyki bezpieczeństwa tych informacji,
5) traktowania obowiązków osób zatrudnionych przy przetwarzaniu informacji wynikających z niniejszego dokumentu jako należących do kategorii podstawowych obowiązków pracowniczych oraz stanowczego egzekwowania ich wykonania przez zatrudnione osoby,
6) doskonalenia i rozwijania organizacyjnych, technicznych oraz informatycznych środków ochrony informacji ze szczególnym uwzględnieniem danych osobowych, przetwarzanych zarówno metodami tradycyjnymi jak i elektronicznymi tak, aby skutecznie zapobiegać zagrożeniom związanym z:
   - infekcjami wirusów i innego niebezpiecznego oprogramowania mogącego przyczynić się do nieautoryzowanego przejęcia zasobów komputera lub danych przetwarzanych sieciowo,
   - spamem, wprowadzającym nieład informacyjny mogącym stanowić potencjalne zagrożenie dla informatycznych zasobów Urzędu,
   - dostępem do stron internetowych, które zaopatrzone są w skrypty pozwalające wykradać zasoby komputera,
   - lekceważeniem zasad ochrony danych polegającym na pozostawianiu pomieszczenia lub stanowiska pracy bez ich zabezpieczenia,
   - brakiem świadomości niebezpieczeństwa dopuszczania osób postronnych do swojego stanowiska pracy,

- atakami z sieci mającymi na celu opóźnienie lub uniemożliwienie dostępu do danych,
- działaniami mającymi na celu zaburzenie integralności danych, w celu uniemożliwienia ich przetwarzania lub osiągnięcia korzyści,
- kradzieżą sprzętu lub nośników z danymi,
- przekazywaniem sprzętu z danymi do serwisu,
- innymi zagrożeniami mogącym wystąpić w przyszłości w związku z rozwojem technik i metod przetwarzania danych.

Jednocześnie kierownictwo Urzędu zamierza doskonalić i rozwijać nowoczesne metody przetwarzania informacji.

3. W celu zapewnienia bezpieczeństwa informacji w Urzędzie dopuszcza się monitorowanie pracowników w szczególności w zakresie dostępu do stron internetowych oraz danych przesyłanych ze służbowych kont pocztowych.

III. Przepisy ogólne.

1. W Urzędzie Miejskim w Brusach przetwarzane są informacje (dane), w tym dane osobowe i inne prawnie chronione, służące do realizacji zadań wynikających z przepisów prawa. Dane te są przetwarzane i składowane zarówno w postaci dokumentów papierowych jak i w formie elektronicznej.

2. Administratorem danych w Urzędzie Miejskim w Brusach jest Burmistrz Brus.

3. W imieniu Burmistrza Brus funkcję Administratora danych przetwarzanych w komórce organizacyjnej Urzędu pełni kierownik danej komórki. Administrator odpowiada za przetwarzanie danych (zbieranie, utrwalanie, przechowywanie opracowywanie, zmienianie, udostępnianie i usuwanie) zgodnie z obowiązującymi przepisami szczegółowymi. Jeżeli przepisy odrębnych ustaw, które odnoszą się do przetwarzania danych, przewidują dalej idącą ich ochronę, niż wynika to z niniejszej ustawy, stosuje się przepisy tych ustaw.
4. Funkcję Administratora Bezpieczeństwa Informacji pełni osoba wyznaczona przez Burmistrza Brus.

5. Decyzję o udostępnieniu danych innemu podmiotowi podejmuje każdorazowo administrator danych przetwarzanych w komórce organizacyjnej, tj. kierownik komórki organizacyjnej

6. Zasady, działania, kompetencje i zakresy odpowiedzialności opisane w Polityce Bezpieczeństwa obowiązują wszystkich pracowników Urzędu Miejskiego w Brusach.

7. Za bezpieczeństwo informacji odpowiedzialny jest każdy pracownik Urzędu Miejskiego w Brusach. Pracownicy zobowiązani są do stosowania zapisów niniejszego dokumentu, przestrzegania zasad dotyczących ochrony danych przed zniszczeniem i nieuprawnionym dostępem, informowania Administratora Bezpieczeństwa Informacji o zaobserwowanych nieprawidłowościach przy przetwarzaniu danych oraz zachowania w tajemnicy wszystkich danych prawnie chronionych w trakcie zatrudnienia i po jego ustaniu.

8. Polityka Bezpieczeństwa będzie weryfikowana i dostosowywana do zmian w technologii informatycznej oraz zmian obowiązujących przepisów.

IV. Infrastruktura systemu informacyjnego.

1. Obszar przetwarzania danych obejmuje budynek będący siedzibą Urzędu Miejskiego w Brusach przy ul. Na Zaborach 1.

2. Dane przetwarzane są w ekranowanej sieci komputerowej kategorii 5 lub wyższej, wszystkie komputery w sieci zasilane są z dedykowanej sieci elektrycznej. Połączenia sieciowe realizowane są za pomocą przełączników sieciowych o przepustowości 10/100/1000 Mb/s. Dane przetwarzane są na serwerach z systemami operacyjnymi Windows 2003/2008 Server oraz Linux. Wszystkie komputery, serwery i urządzenia sieciowe zasilane są przez centralny zasilacz awaryjny. Część informacji przetwarzana jest na komputerach przenośnych użytkowanych przez pracowników. Pomieszczenie serwerowni jest zabezpieczone przed przegrzaniem przez dwa klimatyzatory naścienne.

V. Cel Polityki Bezpieczeństwa.

1. Celem Polityki Bezpieczeństwa jest określenie zasad i reguł postępowania w zakresie zabezpieczenia danych ze szczególnym uwzględnieniem danych osobowych i innych prawnie chronionych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy o ochronie danych osobowych oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

2. Polityka Bezpieczeństwa reguluje sposób zarządzania, ochrony i przepływu informacji wewnątrz Urzędu w taki sposób, aby zapewnić odpowiednią ochronę zasobów informacyjnych i utrzymać ciągłość działania systemów informatycznych niezbędnych do realizacji zadań a przez to chronić wizerunek Urzędu Miejskiego w Brusach.

3. Polityka Bezpieczeństwa odnosi się nie tylko do systemów informatycznych, ale także do informacji (danych) przetwarzanych w postaci papierowej (kartoteki, wydruki i inne).

4. Polityka Bezpieczeństwa ma na celu zapewnienie zgodności sposobu przetwarzania danych ze szczególnym uwzględnieniem danych osobowych i innych prawnie chronionych, z wymogami określonymi w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. 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), rozporządzeniu 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 (t.j. z 14 stycznia 2016 r., Dz. U. z 2012r., poz. 113).

5. Prawidłowe zarządzanie zasobami informacyjnymi wymaga właściwej identyfikacji tych zasobów oraz miejsca i sposobu ich przechowywania, a także określenia struktury zbiorów i przepływu danych pomiędzy poszczególnymi systemami i zbiorami.
6. Informacje te zostały określone w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Brusach stanowiącym załącznik nr 2 do zarządzenia Nr 350/16 Burmistrza Brus z dnia 18 lipca

2016 roku w sprawie realizacji zasad bezpieczeństwa i ochrony danych osobowych przetwarzanych w Urzędzie Miejskim w Brusach .

VI. Analiza zagrożeń.

W wyniku przeprowadzonej analizy zagrożeń ustalono, że należy liczyć się z następującym ryzykiem:

1) utraty danych na skutek awarii zasilania, sprzętu komputerowego, sieci komputerowej, klęsk żywiołowych,
2) włamania do sieci wewnętrznej w celu zniszczenia lub skopiowania danych,
3) zniszczenia danych, zablokowanie możliwości pracy na komputerze lub w całej sieci przez wirusy komputerowe,
4) kradzieży sprzętu komputerowego, dokumentów lub kopii zapasowych,
5) dostępu do danych w tym: zniszczenie, modyfikacja lub odczyt danych przez osoby nieuprawnione,
6) kradzież, zniszczenie lub modyfikacja danych wynikające z niedostatecznej wiedzy lub celowego działania przez osoby upoważnione do ich przetwarzania,
7) udostępnienia danych osobom nieuprawnionym.

Sposób przeciwdziałania zidentyfikowanym zagrożeniom określony został w kolejnych punktach niniejszego dokumentu.

VII. Poziom Bezpieczeństwa.

W całym obszarze przetwarzania danych w Urzędzie Miejskim w Brusach obowiązuje wysoki poziom bezpieczeństwa

VIII. Zabezpieczenia fizyczne.

W Urzędzie Miejskim w Brusach stosuje się następujące zabezpieczenia fizyczne wszystkich pomieszczeń objętych obszarem przetwarzania danych:

1) wszystkie pomieszczenia podczas nieobecności uprawnionego pracownika są zamykane na klucz,
2) obiekt objęty są całodobowym monitoringiem wizyjnym,
3) pomieszczenia są wyposażone w alarm antywłamaniowy jako dodatkowe zabezpieczenie,
4) pomieszczenia wyposażone są w szafy oraz biurka zamykane kluczami,
5) pomieszczenia serwerowni wyposażone są w czujniki temperatury oraz dymu, połączone z systemem alarmowym.

IX. Zabezpieczenia organizacyjne.

W Urzędzie Miejskim w Brusach zastosowano następujące środki organizacyjne:

1) został wyznaczony Administrator Bezpieczeństwa Informacji,
2) dane osobowe są przetwarzane przez osoby posiadające upoważnienie,
3) prowadzi się ewidencję osób upoważnionych do przetwarzania danych osobowych,
4) pracownicy zobowiązani są do realizacji ustawy w zakresie ochrony danych osobowych w ramach wykonywanych obowiązków,
5) przeprowadzane są okresowe szkolenia z zakresu ochrony danych osobowych.

X. Bezpieczeństwo systemów informatycznych.

1. Zabezpieczenie informatyczne dostępu do danych.

Dostęp do danych przetwarzanych w postaci elektronicznej możliwy jest po wielostopniowym uwierzytelnieniu użytkownika:

1) dostęp do systemu operacyjnego wymaga pełnego uwierzytelnienia użytkownika (login i hasło),

2) dostęp do systemów w których przetwarzane są dane (ze szczególnym uwzględnieniem danych osobowych i innych danych prawnie chronionych), wymaga pełnego uwierzytelnienia użytkownika (login i hasło).

Wyjątek stanowią zasoby dyskowe niezawierające danych osobowych lub innych prawnie chronionych, a służące do udostępniania aplikacji w sieci Urzędu Miejskiego.

2. Zasady przyznawania dostępu do danych.

W celu zapewnienia bezpieczeństwa i wyeliminowania zagrożeń związanych z nieuprawnionym dostępem do danych, do przetwarzania uprawnione są jedynie osoby posiadające pisemne upoważnienie oraz podpisane oświadczenie o zachowaniu poufności tych danych - załączniki nr 3 i 4 do Polityki Bezpieczeństwa w Urzędzie Miejskim w Brusach. Polityka Bezpieczeństwa jest załącznikiem nr 1 do zarządzenia Nr 350/16 Burmistrza Brus z dnia 18 lipca 2016 roku w sprawie realizacji zasad bezpieczeństwa i ochrony danych osobowych przetwarzanych w Urzędzie Miejskim w Brusach. Ewidencję upoważnień prowadzi Administrator Bezpieczeństwa Informacji - ABI.

3. Zasady przyznawania uprawnień do przetwarzania danych w systemach informatycznych

Zasady określają procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności opisane w §1 II części szczegółowej Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Brusach.

4. Zasady tworzenia i postępowania z hasłami w systemach informatycznych

Zasady zostały opisane w §2 II części szczegółowej Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Brusach jako stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem.

XI. Bezpieczeństwo komunikacji.

1. Ze względu na wagę posiadanych danych i ich bezpieczeństwo stosuje się zasadę separacji lokalnej sieci wewnętrznej Urzędu od sieci INTERNET za pomocą sprzętowej zapory wysokiej klasy, posiadającej funkcje blokowania portów, wykrywania wirusów, filtrowania treści oraz mechanizm wykrywania i zapobiegania włamaniom. Dodatkowo cała poczta elektroniczna przychodząca do urzędu jest filtrowana pod kątem zawartości wirusów oraz niepożądanych treści (spamu) przez system antyspamowy.

2. W przypadku konieczności przesyłania danych osobowych lub innych danych prawnie chronionych przy użyciu sieci INTERNET należy stosować metody zabezpieczenia tych danych poprzez ich szyfrowanie lub kompresję z użyciem hasła spełniającego warunki określone w §2 II części szczegółowej Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Brusach. Hasło należy przekazać uprawnionemu odbiorcy danych inną metodą niż przesyłane dane. Pracownicy obsługi informatycznej udostępniają program umożliwiający szyfrowanie plików i nośników danych.

XII. Bezpieczeństwo danych.

1. Zabezpieczenie serwerów.

1) Serwery, na których przetwarzane są dane znajdują się w wydzielonych zabezpieczonych i klimatyzowanych pomieszczeniach, dodatkowo zabezpieczonych systemem alarmowym. Dostęp do pomieszczeń posiada tylko i wyłączenie informatyk Urzędu.
2) Wszystkie serwery są podłączone do centralnego zasilacza awaryjnego.
3) Wszystkie serwery wyposażone są w system antywirusowy posiadający funkcje automatycznej aktualizacji bazy wirusów oraz bieżącego skanowania każdego uruchomionego programu i otwieranego pliku.

2. Zasady dotyczące sporządzania kopii zapasowych.

Dane zabezpiecza się przed utratą lub uszkodzeniem w przypadku awarii zasilania, sprzętu lub sieci komputerowej poprzez tworzenie kopii zapasowych. Metody sporządzania

i przechowywania kopii zapasowych ujęte są w §4 II części szczegółowej Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Brusach jako procedury tworzenia oraz przechowywania kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.

3. Zasilanie komputerów i sieci.

Sprzęt komputerowy w tym serwery, stanowiska robocze, drukarki, urządzenia peryferyjne i sieciowe są zasilane z wydzielonej sieci elektrycznej odpowiednio zabezpieczonej. Niedopuszczalne jest używanie sieci komputerowej do podłączania innych urządzeń, zwłaszcza urządzeń dużej mocy (czajniki, urządzenia grzewcze).

XIII. Bezpieczeństwo zmian i rozwoju systemów.

1. Przy zakupie nowych systemów informatycznych, ich wymianie lub modernizacji należy zwrócić szczególną uwagę na ich zgodność z wdrożoną w Urzędzie Polityką Bezpieczeństwa.
2. Przeglądy i konserwacje systemu i zbioru danych dokonywane są przez informatyka Urzędu lub w przypadku uzasadnionej potrzeby przez osoby posiadające odpowiednie kwalifikacje w tym zakresie pod nadzorem pracownika uprawnionego do przetwarzania danych.

XIV. Pozostałe zasady bezpieczeństwa.

1. Wszystkie komputery wyposażone są w system antywirusowy posiadający funkcje automatycznej aktualizacji bazy wirusów, bieżącego skanowania każdego uruchomionego programu i otwieranego pliku oraz centralnego zarządzania za pomocą konsoli administracyjnej z monitorowaniem zagrożeń.

2. Sposób przeprowadzenia napraw i konserwacji sprzętu komputerowego określa §7 II części szczegółowej Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Brusach jako procedury

wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

3. Użytkownik komputera każdorazowo sprawdza otrzymane z zewnątrz płyty CD/DVD, pamięci zewnętrzne Pendrive a także wszystkie otrzymane lub skopiowane za pomocą internetu pliki za pomocą programu antywirusowego.

4. Dyski, płyty CD/DVD lub inne nośniki informatyczne zawierające dane przeznaczone do likwidacji, użytkownik pozbawia zapisu tych danych a gdy jest to niemożliwe uszkadza w sposób uniemożliwiający odczytanie.

5. Wydruki zawierające dane przeznaczone do usunięcia użytkownik niszczy w stopniu uniemożliwiającym ich odczytanie.

6. Monitory w pomieszczeniach, w których przebywają osoby postronne użytkownicy ustawiają w sposób uniemożliwiający tym osobom wgląd do danych.

7. Ekran monitora powinien być automatycznie wygaszany po upływie max. 10 minut od momentu zaprzestania pracy, a powtórne jego wyświetlenie możliwe po podaniu hasła. Za stosowanie wygaszaczy odpowiedzialni są użytkownicy komputera.

8. Użytkownik zawieszający pracę lub oddalający się od swojego stanowiska pracy ma obowiązek zakończyć pracę w systemie informatycznym lub uruchomić wygaszacz ekranu zabezpieczony hasłem, aby w ten sposób uniemożliwić nieuprawnionym osobom dostęp do danych.
9. Użytkownik po zakończeniu pracy ma obowiązek:
    1) zakończyć pracę w systemie informatycznym,
    2) wyłączyć komputer,
    3) wyłączyć zasilanie (listwę zasilającą).

10. W przypadku opuszczenia pomieszczeń, w których znajdują się komputery, pomieszczenia te winny być bezwzględnie zamykane na klucz. Przebywanie w obszarze przetwarzania danych osób nieuprawnionych jest dopuszczalne za zgodą Administratora

danych lub w obecności osoby upoważnionej do przetwarzania danych. Niedopuszczalne jest pozostawienie w pomieszczeniu osób postronnych.

11. Wydruki zawierające dane osobowe jak również inne informacje prawnie chronione należy zabezpieczyć przed dostępem osób nieuprawnionych przez ich przechowywanie w zamkniętych szafach.

12. Nośniki (płyty CD/DVD, pamięci zewnętrzne Pendrive i inne) zawierające dane osobowe należy zabezpieczyć przed dostępem osób nieuprawnionych przez ich przechowywanie w zamkniętych szafach.

13. W udostępnionych zasobach sieciowych serwerów (katalog Public) nie wolno przechowywać plików zawierających dane osobowe lub inne dane prawnie chronione.

14. Przekazanie komputerów podmiotom zewnętrznym może odbyć się tylko po trwałym usunięciu danych.

15. W przypadku zbiorów danych osobowych przetwarzanych w postaci plików tekstowych lub arkuszy kalkulacyjnych dane te należy zabezpieczyć hasłem (mechanizm dostępny w pakietach biurowych oraz w archiwizatorach np. 7z).

16. Użytkownik przenośnego sprzętu komputerowego używanego poza obszarem przetwarzania danych zobowiązany jest do prawidłowego zabezpieczenia danych na nim zawartych poprzez zastosowanie mechanizmów zabezpieczania dokumentów hasłami (mechanizm dostępny w pakietach biurowych) lub stosować kompresję danych z zabezpieczeniem hasłem (mechanizm dostępny w archiwizatorach np. 7z). W uzasadnionych przypadkach należy stosować mechanizm szyfrowania dysku, informatyk Urzędu udostępniają program umożliwiający szyfrowanie nośników danych.

17. W sytuacji, gdy stwierdzone zostanie naruszenie zabezpieczenia systemu informatycznego użytkownik zobowiązany jest do:
    1) zawiadomienia o powyższym administratora bezpieczeństwa informacji oraz kierownika komórki organizacyjnej,

2) zablokowania komputera w sposób uniemożliwiający dalszą pracę w systemie,
3) utrzymania sprzętu w taki sposób, aby uniemożliwić do niego dostęp innym osobom.

XV. Znajomość przepisów.

Dla skuteczności Polityki Bezpieczeństwa wymagana jest powszechna znajomość przez pracowników przepisów dotyczących ochrony danych. W przypadku zatrudniania pracownika Wydział Organizacyjny jest zobowiązany wręczyć pracownikowi Politykę Bezpieczeństwa, Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych oraz ustawę o ochronie danych osobowych i przyjąć oświadczenie o zapoznaniu się z ich treścią i przyjęciu do stosowania. Oświadczenie należy przechowywać w aktach osobowych pracownika.

XVI. Konsekwencje nie przestrzegania Polityki Bezpieczeństwa.

Stosowanie zapisów Polityki Bezpieczeństwa Informacji podlega kontroli. Sposób przeprowadzania kontroli określa „Procedura kontroli sprzętu komputerowego i oprogramowania" stanowiąca załącznik nr 5 Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych w Urzędzie Miejskim w Brusach.
Nie stosowanie się do zapisów Polityki Bezpieczeństwa skutkować będzie karami przewidzianymi w Regulaminie Pracy Urzędu Miejskiego w Brusach.