ZARZĄDZENIE NR 25/BOIN/10
BURMISTRZA MIASTA CHEŁMŻY
z dnia 15 lutego 2010 r.

w sprawie ustalenia polityki bezpieczeństwa przetwarzania danych osobowych i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta Chełmży.

Na podstawie art. 33 ust. 1 i 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2001 r. Nr 142, poz. 1591, z 2002 r. Nr 23, poz. 220, Nr 62, poz. 558, Nr 113, poz. 984, Nr 153, poz. 1271 i Nr 214, poz. 1806, z 2003 r. Nr 80, poz. 717 i Nr 162, poz. 1568, z 2004r. Nr 102, poz. 1055, Nr 116, poz. 1203 i Nr 167, poz. 1759, z 2005 r. Nr 172, poz. 1441 i Nr 175, poz. 1457, z 2006 r. Nr 17, poz. 128 i Nr 181, poz. 1337, z 2007 r. Nr 48, poz. 327, Nr 138, poz. 974 i Nr 173, poz. 1218, z 2008 r. Nr 180, poz. 1111 i Nr 223, poz. 1458 oraz z 2009r. Nr 52, poz. 420 i Nr 157, poz. 1241), art. 3 ust. 1, art. 7 pkt. 4, art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. nr 101, poz. 926 i Nr 153 poz. 1271, z 2004 Nr 25, poz. 219 i Nr 33, poz. 285, z 2006r. Nr 104, poz. 708 i 711 oraz z 2007r. Nr 165, poz. 1170 i Nr 176, poz. 1238), § 3, 4 i 5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. nr 100 poz. 1024) oraz § 3 rozporządzenia Rady Ministrów z dnia 11 października 2005 r. w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz. U. nr 212 poz. 1766) zarządzam, co następuje:

§ 1. Ustalam politykę bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miasta Chełmży, stanowiącą Załącznik nr 1 do niniejszego zarządzenia.

§ 2. Ustalam instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta Chełmży stanowiącą Załącznik nr 2 do niniejszego zarządzenia.

§ 3. Na Administratora Bezpieczeństwa Informacji wyznaczam Pełnomocnika ds. ochrony informacji niejawnych, natomiast na Administratora Systemu Informatycznego wyznaczam p. Jarosława Smyczyńskiego zatrudnionego w Urzędzie Miasta Chełmży na stanowisku ds. informatyzacji i komputeryzacji.

§ 4. Administrator Bezpieczeństwa Informacji odpowiada za ochronę danych osobowych w Urzędzie Miasta Chełmży, a w szczególności za aktualizację, realizację i przestrzeganie polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miasta Chełmży.

§ 5. Administrator Systemu Informatycznego Urzędu Miasta Chełmży odpowiada za ochronę danych w systemach informatycznych oraz za aktualizację, realizację i przestrzeganie instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

§ 6. Zobowiązuję kierowników komórek organizacyjnych Urzędu Miasta do bezpośredniego nadzoru przestrzegania zasad zawartych w niniejszym zarządzeniu i ścisłej współpracy z Administratorem Bezpieczeństwa Informacji.

§ 7. Przypadki naruszeń zasad zawartych w niniejszym zarządzeniu lub zaistnienie pojedynczego rażącego naruszenia zasad bezpieczeństwa w stosunku do ochrony danych osobowych i systemów informatycznych w Urzędzie Miasta Chełmży zgłaszane są Administratorowi danych osobowych i stanowią podstawę wszczęcia postępowania dyscyplinarnego w stosunku do osób winnych naruszeń.

§ 8. Przed rozpoczęciem pracy w systemie informatycznym lub dopuszczeniem do przetwarzaniu danych osobowych każdy pracownik Urzędzie Miasta Chełmży zobowiązany jest do zapoznania się z niniejszym zarządzeniem oraz do stosowania zasad w nim opisanych.

§ 9. Tracą moc:
1) Zarządzenie nr 46/BOIN/04 Burmistrza Miasta Chełmży z dnia 20 kwietnia 2004r. w sprawie ochrony danych osobowych w Urzędzie Miasta Chełmży;
2) Zarządzenie nr 138/BOIN/04 Burmistrza Miasta Chełmży z dnia 17 listopada 2004 r. w sprawie ochrony danych osobowych w systemach informatycznych Urzędu Miasta Chełmży.

§ 10. Zarządzenie wchodzi w życie z dniem wydania.

Burmistrz Miasta

(-) mgr Jerzy Czerwiński

Załącznik nr 1
do zarządzenia nr 25/BOIN/10
Burmistrza Miasta Chełmży
z dnia 15.02.2010 r.

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH W URZĘDZIE MIASTA CHEŁMŻY

I. Obszar przetwarzania danych osobowych.

Obszar przetwarzania danych osobowych w Urzędzie Miasta Chełmży obejmuje 2 budynki:

1) Główny ratusz:

pomieszczenia nr :
- 2 – Wydział Organizacyjny - sekretariat;
- 5 - Wydział Finansowo – Księgowy – stanowiska ds.: opłat i podatków lokalnych, księgowości podatkowej;
- 6 – Wydział Finansowo – Księgowy – stanowisko ds. obsługi kasy;
- 9– Wydział Finansowo – Księgowy - stanowiska ds.: płac i zasiłków, rozliczeń świadczeń społecznych;
- 11 i 11a - Wydział Spraw Społecznych i Obywatelskich - Urząd stanu cywilnego;
- 12 i 12a - Wydział Organizacyjny – stanowisko ds. obsługi Rady Miejskiej;
- kancelaria tajna.

2) Mały ratusz:

pomieszczenia nr :
- 13 i 13a – Wydział Spraw Społecznych i Obywatelskich – stanowiska: ds. ewidencji ludności, ds. ewidencji działalności gospodarczej, dowodów tożsamości;
- 14 – Wydział Organizacyjny – stanowisko ds. kadr i szkolenia;
- 18 i 18a – Wydział Gospodarki Miejskiej – stanowiska ds.: obrotu mieniem komunalnym, geodezji i gospodarki nieruchomościami, mieszkaniowych i dodatków mieszkaniowych, planowania przestrzennego, architektoniczno-budowlanych, drogownictwa, gospodarki komunalnej i ochrony środowiska;
- 19 - Wydział Spraw Społecznych i Obywatelskich – stanowisko ds. obronnych i obrony cywilnej
- serwerownia.

3) Budynek przy ul. Hallera 19:

- Wydział Gospodarki Miejskiej – stanowisko ds. dodatków mieszkaniowych
- Wydział Spraw Społecznych i Obywatelskich – stanowisko ds. pomocy materialnej dla uczniów.

Dla zabezpieczenia dostępu do obszaru, w którym przetwarzane są dane osobowe, budynki i pomieszczenia są ochraniane w sposób określony w „Planie ochrony informacji niejawnych UM Chełmży".

II. Zbiory danych osobowych.

1.Na zbiory danych osobowych składają się:

1) dane w formie dokumentacji papierowej (wykazy, listy, korespondencja, wnioski, deklaracje, wydruki komputerowe, itp.),
2) dane w systemach informatycznych oraz ich nośniki.

2. Wykaz wszystkich zbiorów danych osobowych prowadzony przez Administratora Bezpieczeństwa Informacji stanowi ***Załącznik Nr 1*** do niniejszego dokumentu.

3. Kierownicy komórek organizacyjnych Urzędu Miasta Chełmży prowadzących zbiory danych osobowych lub zakładający takie zbiory zobowiązani są na bieżąco zgłaszać Administratorowi Bezpieczeństwa Informacji:

1) zamiar założenia zbioru,
2) rozpoczęcie pracy ze zbiorem,
3) znaczącą modyfikacji lub zmianę sposobu wykorzystywania zbioru,
4) zaprzestanie eksploatacji zbioru,
5) konieczność likwidacji i sposób likwidacji zbioru.

4. Kierownicy komórek organizacyjnych Urzędu Miasta Chełmży, zobowiązani są do przekazywania Administratorowi Bezpieczeństwa Informacji wypełnionego formularza zgłoszenia zbioru danych osobowych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych, którego wzór określono w załączniku 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).

5. Administrator Bezpieczeństwa Informacji przekazuje zgłoszenia zbiorów danych osobowych Generalnemu Inspektorowi Ochrony Danych Osobowych oraz prowadzi ewidencję zgłoszonych zbiorów po ich rejestracji.

III. Opis struktury zbiorów danych osobowych.

1. Administrator Bezpieczeństwa informatycznego prowadzi opisy struktur zbiorów danych osobowych w systemach informatycznych oraz przepływu danych pomiędzy systemami do ich obsługi według wzoru stanowiącego ***Załącznik Nr 2*** do niniejszego dokumentu.

2. Kierownicy komórek organizacyjnych Urzędu prowadzących własne autonomiczne informatyczne zbiory danych osobowych są zobowiązani do przekazywania na bieżąco Administratorowi Bezpieczeństwa Informatycznego informacji o strukturach tych zbiorów.

IV. Zasady zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

1. Należy zachowywać szczególną staranność w celu ochrony danych oraz wykrywać i właściwie reagować na przypadki naruszenia zabezpieczeń danych osobowych lub systemów informatycznych.

2. Zbiory danych osobowych mogą być przekazywane na zewnątrz wyłącznie za zgodą Administratora Bezpieczeństwa Informacji.

3. W celu zapewnienia integralności i rozliczalności oraz poufności danych osobowych, w Urzędzie Miasta Chełmży zostały ustalone zostają następujące zasady ochrony danych:

A. Ogólne zasady ochrony:

1) Osoby nieuprawnione mogą przebywać w pomieszczeniach tworzących obszar, w którym przetwarzane są dane osobowe wyłącznie w obecności osoby w nim pracującej i zatrudnionej przy przetwarzaniu danych lub w obecności kierownika komórki organizacyjnej albo za pisemnym upoważnieniem Administratora Bezpieczeństwa Informacji.

2) Dokumenty w formie papierowej zawierające dane osobowe należy przechowywać w sposób uniemożliwiający osobom postronnym wgląd w te dane.

3) Każdy zbędny dokument w formie papierowej lub każdy informatyczny nośnik danych zawierające dane osobowe przeznaczony do zniszczenia powinien być likwidowany w sposób uniemożliwiający jego odczytanie.

4) Do przebywania w pomieszczeniach serwerowni upoważnieni są tylko administratorzy systemów oraz w ich obecności osoby upoważnione do kontroli. Przebywanie w pomieszczeniach serwerowni osób nieuprawnionych dopuszczalne jest tylko w obecności administratorów systemu lub za pisemnym upoważnieniem Administratora Bezpieczeństwa Informacji.

5) W przypadku przebywania osób postronnych w pomieszczeniach tworzących obszar, w którym przetwarzane są dane osobowe, monitory komputerowych stanowisk pracy powinny być ustawiane lub wyposażane w sposób uniemożliwiający wgląd w dane osobowe.

6) Zabrania się przenoszenia danych osobowych na zewnętrzne informatyczne nośniki danych (np. karty pamięci, dyskietki, płyty, dyski twarde, itp.) i przechowywania na nich zbiorów danych osobowych bez zastosowania środków ochrony kryptograficznej. Ograniczenie to nie dotyczy kopii zapasowych wykonywanych przez administratorów systemów i przechowywanych w sejfach.

7) Dane osobowe mogą być udostępniane osobom lub podmiotom uprawnionym tylko na pisemny umotywowany wniosek. Wniosek powinien zawierać uzasadnienie faktyczne i prawne oraz być podpisany przez upoważnioną osobę. Kierownicy komórek organizacyjnych Urzędu prowadzący określone zasoby danych rozpatrują wniosek na podstawie przepisów prawa oraz prowadzą odpowiednie rejestry dotyczące danych udostępnionych.

8) Sposób postępowania pracowników Urzędu Miejskiego w Chełmży w przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych opisany jest w ***Załączniku nr*** 3 do niniejszego dokumentu.

9) Fakty naruszenia bezpieczeństwa systemów informatycznych powinny być zgłaszane Administratorowi Bezpieczeństwa Informatycznego w formie notatki służbowej sporządzonej lub potwierdzonej przez kierownika komórki organizacyjnej, w której naruszenie nastąpiło lub zostało zaobserwowane.

10) Osoby upoważnione do przetwarzania danych osobowych podlegają szkoleniu w zakresie obowiązujących przepisów o ochronie danych osobowych, procedur przetwarzania danych oraz informowane o podstawowych zagrożeniach związanych z przetwarzaniem danych w systemach informatycznych Urzędu Miasta Chełmży.

B. Środki ochrony programowo-sprzętowej.

1) Każdy użytkownik komputerowego stanowiska pracy posiada własny unikalny identyfikator i hasło dostępu do systemu operacyjnego i środowiska sieciowego. Dla systemów informatycznych, w których zawarte są dane osobowe ustalone są dodatkowe identyfikatory i hasła dostępu. Szczegółowe zasady posługiwania się hasłami określono w „Instrukcji zarządzania systemem informatycznym przetwarzającym dane osobowe Urzędu Miasta Chełmży".

2) Stosuje się mechanizmy powodujące konieczność okresowej zmiany haseł stosowanych przez użytkowników - w cyklach nie dłuższych niż 30 dni.

3) Komputerowe stanowiska pracy powinny być zabezpieczane przed nieuprawnionym dostępem poprzez stosowanie wygaszania ekranu i wymuszanie powtórnego logowania w przypadku dłuższej ich nieaktywności.

4) Serwery muszą być wyposażone w urządzenia do podtrzymywania napięcia na wypadek zaniku zasilania z sieci.

5) Lokalna sieć komputerowa (LAN) Urzędu Miasta w razie konieczności wyjścia do Internetu (sieci WAN) chroniona jest dedykowanymi urządzeniami informatycznymi.

6) W celu ochrony danych przed zniszczeniem należy wykonywać kopie zapasowe właściwe dla danego systemu informatycznego. Kopie te nie powinny być przechowywane w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych eksploatowane na bieżąco.

7) Komputerowe stanowiska pracy zabezpieczane są przed skutkami działania szkodliwego oprogramowania.

8) Zakazuje się przechowywania zbiorów danych osobowych na komputerach przenośnych, które są wykorzystywane poza siedzibą Urzędu Miasta Chełmży.

Załącznik nr 1
do „Polityki bezpieczeństwa przetwarzania danych sobowych w Urzędzie Miasta Chełmży”

WYKAZ ZBIORÓW DANYCH OSOBOWYCH PRZETWARZANYCH W URZĘDZIE MIASTA CHEŁMŻY

Lp.	Nazwa zbioru danych osobowych	Nr rej/zgłoszenia Nr księgi GIODO	Autor oprogramowania	Wydział merytoryczny
1	2	3	5	6
1.	ZBIOR DANYCH OSOBOWYCH URZĘDU MIEJSKIEGO W CHELMŻY W WYDZIALE SPRAW OBYWATELSKICH I SPOLECZNYCH NA STANOWISKU PRACY DS.EWIDENCJI DZIALALNOSCI GOSPODARCZEJ I WYDAWANIA ZEZWOLEN NA SPRZEDAZ NAPOJOW ALKOHOLOWYCH	000360/1999 059367	Zakład Systemów Informatycznych SIGID Poznań	Wydział Spraw Społecznych i obywatelskich
2.	ZBIOR DANYCH OSOBOWYCH URZĘDU MIEJSKIEGO W CHELMŻY W WYDZIALE GOSPODARKI MIEJSKIEJ NA STANOWISKU PRACY DS. OBORTU MIENIEM KOMUNALNYM	001359/1999 002478	Pracownia komputerowa TADANA	Wydział Gospodarki Miejskiej
3.	ZBIOR DANYCH OSOBOWYCH URZĘDU MIEJSKIEGO W CHELMZY W WYDZIALE GOSPODARKI MIEJSKIEJ NA STANOWISKU PRACY DS. GEODEZJI I GOSPODARKI NIERUCHOMOSCI	001360/1999 001762		Wydział Gospodarki Miejskiej
4.	ZBIÓR DANYCH OSOBOWYCH URZĘDU MIEJSKIEGO W CHEŁMŻY W WYDZIALE GOSPODARKI MIEJSKIEJ NA STANOWISKU PRACY DS. MIESZKANIOWYCH I DODATKÓW MIESZKANIOWYCH	001361/1999 002701	Zakład Systemów Informatycznych SIGID Poznań	Wydział Gospodarki Miejskiej
5.	ZBIOR DANYCH OSOBOWYCH URZĘDU MIEJSKIEGO W CHELMZY W WYDZIALE GOSPODARKI MIEJSKIEJ NA STANOWISKU PRACY DS. PLANOWANIA PRZESTRZENNEGO	001362/1999 001761	Brak oprogramowania w formie papierowej	Wydział Gospodarki Miejskiej
6.	ZBIOR DANYCH OSOBOWYCH URZĘDU MIEJSKIEGO W CHEŁMŻY W WYDZIALE GOSPODARKI MEJSKIEJ NA STANOWISKU PRACY DS. ADMINISTRACJI ARCHTEKTONICZNO - BUDOWLANEJ	001364/1999 002479	Brak oprogramowania w formie papierowej	Wydział Gospodarki Miejskiej

1	2	3	5	6
7.	ZBIOR DANYCH OSOBOWYCH URZĘDU MIEJSKIEGO W CHEŁMŻY W WYDZIALE GOSPODARKI MIEJSKIEJ	002155/1999 015646 001665/2000 015645 001666/2000 015647		Wydział Gospodarki Miejskiej
8.	ZBIOR DANYCH OSOBOWYCH URZĘDU MIEJSKIEGO W CHEŁMŻY W WYDZIALE FINANSOWO -KSIĘGOWYM	002156/1999 015644	Zakład Systemów Informatycznych SIGID Poznań	Wydział Finansowo-Księgowy
9.	ZBIOR DANYCH OSOBOWYCH URZĘDU MIEJSKIEGO W CHEŁMŻY W WYDZIALE GOSPODARKI MIEJSKIEJ NA STANOWISKU PRACY DS. DROGOWNICTWA	002157/1999 004751	Brak oprogramowania w formie papierowej	Wydział Gospodarki Miejskiej
10.	ZBIOR DANYCH OSOBOWYCH URZĘDU MIEJSKIEGO W CHEŁMŻY W WYDZIALE GOSPODARKI MIEJSKIEJ NA STANOWISKU PRACY DS. GOSPODARKI KOMUNALNEJ I OCHRONY SRODOWISKA	002164/1999 004749	Brak oprogramowania w formie papierowej	\Wydział Gospodarki Miejskiej
11.	ZBIOR DANYCH OSOBOWYCH URZĘDU MIEJSKIEGO W CHEŁMŻY W WYDZIALE SPRAW SPOLECZNYCH I OBYWATELSKICH NA STANOWISKU PRACY DS. EWIDENCJI LUDNOSCI	002165/1999 051297	ARAM Sp. z .o.o. Warszawa	Wydział Spraw Społecznych i obywatelskich
12.	ZBIOR DANYCH OSOBOWYCH URZĘDU MIEJSKIEGO W CHEŁMŻY W WYDZIALE GOSPODARKI MIEJSKIEJ NA STANOWISKU PRACY DS. MIESZKANIOWYCH I DODATKOW MIESZKANIOWYCH	002166/1999 051298	Zakład Systemów Informatycznych SIGID Poznań	\Wydział Gospodarki Miejskiej

Załącznik nr 2
do „Polityki bezpieczeństwa przetwarzania danych sobowych w Urzędzie Miasta Chełmży

OPISY STRUKTUR ZBIORÓW DANYCH OSOBOWYCH W SYSTEMACH INFORMATYCZNYCH ORAZ SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY SYSTEMAMI DO ICH OBSŁUGI

Lp.	Nazwa zbioru	Opis zbioru	Zawartość pól informacyjnych	Sposób przepływu danych pomiędzy systemami
1	2	3	4	5
1.	Komputerowy System Rejestracji Stanu Cywilnego	Program do obsługi USC	Pola wymagane przez odpowiednie ustawy dotyczące prowadzonego zbioru	Brak powiązania z innymi systemami
2.	Ewidencja i Naliczanie Dodatków Mieszkaniowych	Program do obsługi dodatków mieszkaniowych	Pola wymagane przez odpowiednie ustawy dotyczące prowadzonego zbioru	Umożliwia eksport danych do pliku w celu wczytania list wypłat do systemu – home-banking.
3.	Ewidencja Działalności Gospodarczej	Program do obsługi ewidencji działalności gospodarczej	Pola wymagane przez odpowiednie ustawy dotyczące prowadzonego zbioru	Brak powiązania z innymi systemami
4.	Ewidencja i Rozliczanie Sprzedaży kredytowej	Program do obsługi sprzedaży kredytowej	Pola wymagane przez odpowiednie ustawy dotyczące prowadzonego zbioru	Powoązany z programem kasa
5.	Ewidencja Opłat za Wieczyste Użytkowanie	Program do obsługi wieczystego użytkowania	Pola wymagane przez odpowiednie ustawy dotyczące prowadzonego zbioru	Powiązany z programem kasa
6.	Ewidencja Opłat Dzierżawnych	Program do obsługi opłat dzierżawnych	Pola wymagane przez odpowiednie ustawy dotyczące prowadzonego zbioru	Powiązany z programem kasa
7.	Ewidencja i drukowanie faktur	Program do ewidencji i drukowania faktur	Pola wymagane przez odpowiednie ustawy dotyczące prowadzonego zbioru	Brak powiązania z innymi systemami

1	2	3	4	5
8.	Program obsługi kasy	Program do obsługi kasy	Pola wymagane przez odpowiednie ustawy dotyczące prowadzonego zbioru	Program powiązany z systemem podatkowym UM
9.	Program obsługi mandatów kredytowych	Program obsługi mandatów kredytowych	Pola wymagane przez odpowiednie ustawy dotyczące prowadzonego zbioru	
10.	Podatek od nieruchomości dla osób fizycznych	Program do obsługi podatków	Pola wymagane przez odpowiednie ustawy dotyczące prowadzonego zbioru	Powiązany z programem kasa
11.	Podatek od nieruchomości dla osób prawnych	Program do obsługi podatków	Pola wymagane przez odpowiednie ustawy dotyczące prowadzonego zbioru	Powiązany z programem kasa
12.	Kadry i płace Urzędu i oświaty	Program do obsługi kadr i płac	Pola wymagane przez odpowiednie ustawy dotyczące prowadzonego zbioru	Umożliwia eksport danych do pliku w celu wczytania list wypłat do systemu – home-banking.
13.	Podatek od środków transportowych	Program do obsługi podatków	Pola wymagane przez odpowiednie ustawy dotyczące prowadzonego zbioru	Powiązany z programem kasa
14.	Ewidencja i drukowanie poleceń przelewów	Program do obsługi przelewów	Pola wymagane przez odpowiednie ustawy dotyczące prowadzonego zbioru	Umożliwia eksport danych do pliku w celu wczytania list wypłat do systemu – home-banking.
15.	Podatek rolny/leśny/ nieruch. dla osób fizycznych	Program do obsługi podatków	Pola wymagane przez odpowiednie ustawy dotyczące prowadzonego zbioru	Powiązany z programem kasa
16.	Podatek rolny/leśny/ nieruch. Dla osób prawnych	Program do obsługi podatków	Pola wymagane przez odpowiednie ustawy dotyczące prowadzonego zbioru	Powiązany z programem kasa
17.	System Ewidencji Ludności z Modułem Rejestr Wyborców	Program do obsługi ewidencji ludności	Pola wymagane przez odpowiednie ustawy dotyczące prowadzonego zbioru	

Załącznik nr 3
do „Polityki bezpieczeństwa przetwarzania danych sobowych w Urzędzie Miasta Chełmży”

SPOSÓB POSTĘPOWANIA PRACOWNIKÓW URZĘDU MIASTA CHEŁMŻY W PRZYPADKU STWIERDZENIA NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

1. Naruszenie bezpieczeństwa danych osobowych może zostać stwierdzone na podstawie oceny:

a) stanu urządzeń technicznych,
b) zawartości zbiorów danych osobowych,
c) sposobu działania systemu informatycznego za pomocą którego odbywa się dostęp do danych osobowych,
d) metod pracy i sposobu obiegu dokumentów.

2. W przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych należy bezzwłocznie:

a) powiadomić bezpośredniego przełożonego lub Administratora Bezpieczeństwa Informacji,
b) jeśli naruszenie dotyczy systemu informatycznego - zablokować dostęp do systemu dla użytkowników oraz osób nieupoważnionych,
c) podjąć działania dla zminimalizowania lub wyeliminowania powstałego zagrożenia, zabezpieczyć dowody umożliwiające ustalenie przyczyn i skutków naruszenia ochrony danych.

3. Przełożony pracownika lub Administrator Bezpieczeństwa Informacji przejmują nadzór nad pracą w systemie na stanowisku, na którym stwierdzono naruszenie bezpieczeństwa danych. Jednocześnie, do czasu wyjaśnienia sprawy pracownik jest odsunięty od pracy na tym stanowisku.

4. Administrator Bezpieczeństwa Informacji lub upoważniona przez niego osoba podejmuje czynności wyjaśniające w zakresie, co najmniej:

a) przyczyn i okoliczności naruszenia bezpieczeństwa danych osobowych,
b) osób winnych naruszenia bezpieczeństwa danych osobowych,
c) skutków naruszenia bezpieczeństwa danych osobowych.

5. Administrator Bezpieczeństwa Informacji zobowiązany jest do powiadomienia o naruszeniu bezpieczeństwa danych osobowych Administratora Danych Osobowych, który podejmuje decyzję o wykonaniu czynności zmierzających do przywrócenia poprawnej pracy systemu oraz o ponownym przystąpieniu do pracy w systemie.

6. Administrator Bezpieczeństwa Informacji zobowiązany jest do sporządzenia pisemnego raportu na temat naruszenia bezpieczeństwa danych osobowych, który przedstawia Administratorowi Danych Osobowych. Raport ten zawiera co najmniej:

a) czas i miejsce wystąpienia naruszenia,
b) zakres ujawnionych lub zmienionych danych,
c) przyczynę ujawnienia lub zmiany, osoby odpowiedzialne oraz dowody winy,
d) sposób przywrócenia stanu właściwego,
e) rozwiązania mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.

7. Za naruszenie ochrony danych osobowych stosuje się kary przewidziane przepisami prawa. Niezależnie od tego Administrator Danych Osobowych może stosować kary porządkowe.

Załącznik nr 2
do zarządzenia nr 25/BOIN/10
Burmistrza Miasta Chełmży
z dnia 15.02.2010 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM PRZETWARZAJĄCYM DANE OSOBOWE W URZĘDZIE MIASTA CHEŁMŻY

Niniejsza instrukcja stanowi podstawę do określenia sposobu zarządzania systemem informatycznym przetwarzającym dane osobowe.

I. PODSTAWOWE DEFINICJE I ZASADY OGÓLNE.

1. Definicje.

Ilekroć mowa jest o:

- administratorze danych – należy przez to rozumieć Burmistrza Chełmży;

- użytkowniku - należy przez to rozumieć pracownika korzystającego z systemu informatycznego na indywidualnym komputerowym stanowisku pracy;

- systemie informatycznym – należy przez to rozumieć - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

- administratorze systemu informatycznego - należy przez to rozumieć - osobę wyznaczoną przez Burmistrza Chełmży, odpowiedzialną za przestrzeganie zasad i wymagań bezpieczeństwa systemów i sieci teleinformatycznych;

- administratorze bezpieczeństwa informacji - należy przez to rozumieć- osobę wyznaczoną przez Burmistrza Chełmży, nadzorującą przestrzeganie zasad ochrony przetwarzania danych osobowych w Urzędzie Miasta Chełmży(UM).

2. Zasady ogólne.

1) Burmistrz Miasta Chełmży wprowadza instrukcję i upoważnia Administratora systemu informatycznego do nadzorowania wdrożenia sposobu administrowania i zarządzania środkami informatycznymi wspomagającymi procesy przetwarzania informacji stanowiących dane osobowe w rozumieniu ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych wraz z późniejszymi zmianami.

2) Administrator systemu informatycznego odpowiada za korygowanie niniejszej instrukcji w przypadku uzasadnionych zmian w przepisach prawnych dotyczących przetwarzania danych osobowych w systemach informatycznych, jak również zmian organizacyjno - funkcjonalnych zachodzących w UM.

3) Administrator systemu informatycznego publikuje zatwierdzony dokument. Kierownicy jednostek organizacyjnych są zobowiązani zapoznać swoich podwładnych z niniejszą instrukcją. Aktualna wersja niniejszej instrukcji jest podstawą szkoleń poświęconych zagadnieniu ochrony danych osobowych w UM, związanych z nadawaniem pracownikom uprawnień do korzystania z systemu informatycznego przetwarzającego dane osobowe.

4) Instrukcja zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Urzędzie Miasta Chełmży określa:

- procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym;
- stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;
- procedury rozpoczęcia, zawieszenia i zakończenia pracy;
- procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;
- sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych;
- metody i częstotliwość sprawdzania obecności wirusów komputerowych oraz sposoby ich usuwania;
- sposób dokonywania przeglądów i konserwacji systemu i zbioru danych osobowych;
- sposób postępowania w zakresie komunikacji w sieci komputerowej.

II. PROCEDURY NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH I REJESTROWANIA TYCH UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM.

1. Systemy informatyczne służące do przetwarzania danych osobowych powinny być obsługiwane tylko przez osoby upoważnione. Wzór upoważnienia do przetwarzania danych osobowych określono w ***Załączniku nr 2*** do niniejszej instrukcji. Systemy informatyczne zabezpieczane są przed dostępem osób nieuprawnionych mechanizmami identyfikacji każdego użytkownika poprzez jego identyfikator i hasło oraz ustalaniem zakresu prawa dostępu.

2. Administrator systemu przyznaje uprawnienia dostępowe na podstawie indywidualnego pisemnego zgłoszenia użytkownika dokonanego przez kierownika komórki organizacyjnej UM, zaakceptowanego przez Administratora Danych lub upoważnionego przez niego Administratora Bezpieczeństwa Informacji. Wzór formularza zgłoszenia użytkownika stanowi ***Załącznik 1*** do niniejszego dokumentu. Na podstawie zgłoszenia Administrator Systemu przekazuje użytkownikowi ustnie lub pisemnie identyfikator użytkownika w systemie oraz hasło inicjujące.

3. System informatyczny przetwarzający dane osobowe wykorzystuje mechanizm haseł jako narzędzie umożliwiające bezpieczne uwierzytelnienie. Administrator Systemu przydziela login i hasło tymczasowemu użytkownikowi, który pierwszy raz korzysta z systemu informatycznego.
Identyfikator składa się z nazwiska i pierwszej litery imienia (Elektroniczny obieg dokumentów, logowanie do systemu Windows dla komputerów podłączonych do publicznej sieci informatycznej) lub numeru PESEL (systemy finansowo – księgowe, logowanie do systemu Windows dla komputerów nie podłączonych do publicznej sieci informatycznej).

4. W przypadku zbieżności nadawanego identyfikatora z identyfikatorem wcześniej zarejestrowanego użytkownika administrator systemu, za zgodą Administratora Bezpieczeństwa Informacji, nadaje inny identyfikator odstępując od zasady określonej w ust. 3.

5. W identyfikatorze pomija się polskie znaki diakrytyczne.

6. Rejestracja użytkownika systemu informatycznego przetwarzającego dane osobowe następuje na wniosek przełożonego pracownika po zatwierdzeniu przez Administratora bezpieczeństwa informatycznego i jest wykonywana przez administratora systemu.

7. Administrator systemu po zarejestrowaniu użytkownika w systemie i uzupełnia jego zgłoszenie o następujące dane:

- datę rejestracji użytkownika,
- nazwisko i imię osoby rejestrującej,
- zakres odpowiedzialności (roli) w systemie informatycznym,

przekazują kopię zgłoszenia użytkownika do Wydziału Organizacyjnego w celu jej załączenia do akt osobowych. Oryginały formularzy zgłoszenia użytkownika pozostają u Administratora systemu.

8. Wyrejestrowanie lub zmiana uprawnień użytkownika następuje na wniosek przełożonego danego pracownika przez Administratora systemu informatycznego.

9. Wyrejestrowanie, o którym mowa w ust. 8, może mieć charakter czasowy lub trwały. Wyrejestrowanie następuje poprzez:

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

10. Przyczyną czasowego wyrejestrowania użytkownika z systemu informatycznego może być :

a) nieobecność w pracy trwająca dłużej niż 30 dni kalendarzowych,
b) zawieszenie w pełnieniu obowiązków służbowych,
c) zwolnienie z pełnienia obowiązków służbowych.

11. W przypadku odejścia z pracy użytkownika systemu Administrator systemu informatycznego dokonuje zablokowania identyfikatorów takiego użytkownika na podstawie przedstawionej mu karty obiegowej pracownika. oraz odnotowuje odebranie uprawnień na oryginale formularza zgłoszenia użytkownika.

12. Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy pracownika.

13. Użytkownik po otrzymaniu loginu i hasła ma przydzielone odpowiednie uprawnienia do pracy w systemie komputerowym.

14. Loginy i hasła administratora systemu są znane tylko Administratorowi systemu informatycznego.

III. STOSOWANE METODY I ŚRODKI UWIERZYTELNIENIA ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM.

1. Hasła generuje Administrator systemu informatycznego. Hasło i login użytkownika wraz z dodatkowymi informacjami jest przekazywane w formie ustnej lub papierowej (drukowanej w zamkniętej kopercie, które po przeczytaniu zostaje

zniszczone w odpowiednim urządzeniu niszczącym). Hasło nie może być przekazywane przez osoby trzecie.

2. Hasło tymczasowe przydzielone użytkownikowi logującemu się po raz pierwszy do systemu musi być zmienione po udanym zalogowaniu się do systemu informatycznego przetwarzającego dane osobowe.

3. Hasła są zmieniane przez użytkowników.

4. System informatyczny wyposażony jest w mechanizmy wymuszające zmianę hasła po upływie 30 dni od dnia ostatniej zmiany hasła.

5. System informatyczny wyposażony jest w mechanizm pozwalający na wymuszenie jakości hasła.

6. Hasło składa się z co najmniej ośmiu znaków, zawiera co najmniej jedną literę wielką, jedną cyfrę i jeden znak specjalny (zgodnie z Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. (Dz.U. z 2004 Nr 100, poz. 1024). Wprowadzone hasło różni się od co najmniej trzech ostatnio stosowanych, przy czym system informatyczny jest wyposażony w mechanizmy pozwalające na wymuszenie wymaganych różnic.

7. Oprócz identyfikatorów i haseł obowiązujących w systemach informatycznych, każde komputerowe stanowisko pracy zabezpiecza się dodatkowo przez hasło dostępu do komputera.

8. Użytkownicy systemów zobowiązani są do niezwłocznej zmiany przekazanego im hasła inicjującego w systemie informatycznym a następnie, o ile system nie wymusi tego automatycznie, do jego zmiany co najmniej raz na 30 dni.

9. Zabronione jest udostępnianie innym osobom własnych haseł i identyfikatorów oraz wykonywania jakichkolwiek operacji w systemach informatycznych przy wykorzystaniu innych niż własne haseł i identyfikatorów.

10. Każdy użytkownik odpowiada za poufność swojego hasła i ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła.

11. Hasło Administratora systemu informatycznego przechowywane jest w zamkniętej kopercie w sejfie ognioodpornym do którego ma dostęp tylko Burmistrz Miasta.

IV. PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I

ZAKOŃCZENIA PRACY.

1. Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione.

2. Użytkownik powinien powiadomić inspektora bezpieczeństwa teleinformatycznego lub inne osoby przez niego upoważnione zgodnie z Instrukcją postępowania w sytuacji naruszenia ochrony danych osobowych, jeżeli:

a) wygląd, zakres danych lub sposób działania aplikacji odbiega od stanu normalnego,
b) pewne opcje, dostępne użytkownikowi w normalnej sytuacji, przestały być dostępne lub też pewne opcje, niedostępne użytkownikowi w normalnej sytuacji, stały się dostępne.

3. W przypadku odejścia pracownika od stanowiska komputerowego obowiązany jest on zamknąć wszystkie programy oraz włączyć tzw. wygaszacz ekranu odblokowywany hasłem.

4. Zakończenie pracy użytkownika w systemie informatycznym obejmuje wylogowanie się użytkownika z aplikacji oraz wyłączenie komputera .

5. Po wyłączeniu komputera użytkownik powinien wyłączyć także zasilacz awaryjny UPS.

V. PROCEDURY TWORZENIA KOPII ZAPASOWYCH ZBIORÓW DANYCH ORAZ PROGRAMÓW I NARZĘDZI PROGRAMOWYCH SŁUŻĄCYCH DO ICH PRZETWARZANIA.

1.Dane osobowe przetwarzane w systemie informatycznym podlegają zabezpieczeniu poprzez tworzenie kopii awaryjnych. Za proces tworzenia kopii awaryjnych odpowiada Administrator systemu informatycznego.

2.W przypadku lokalnego przetwarzania danych osobowych na stacjach roboczych użytkownicy systemu informatycznego zobowiązani są do wykonywania kopii z lokalnego dysku twardego na dysk sieciowy. Niestosowanie się do tego wymagania stanowi wykroczenie przeciwko zasadom ochrony informacji i może skutkować konsekwencjami służbowymi.

3. Kopie awaryjne informacji przechowywanych w systemie informatycznym przetwarzającym dane osobowe (serwer) tworzone są w następujący sposób:

a) kopia awaryjna danych osobowych przetwarzanych przez aplikację wykonywana jest codziennie w dni robocze i umieszczana na nośniku.

b) kopie są przechowywane w innym budynku niż ten w którym jest serwer.

c) kopia awaryjna danych konfiguracyjnych systemu informatycznego przetwarzającego dane osobowe, w tym uprawnień użytkowników systemu ,wykonywana jest raz na kwartał.

d) do tworzenia kopii awaryjnych wykorzystywane są przeznaczone do tego celu urządzenia wchodzące w skład systemu informatycznego.

e) wszelkie kopie awaryjne mogą być sporządzane automatycznie lub wywoływane w sposób ręczny; za sporządzanie kopii zapasowych na stanowiskach pracy , które nie są podłączone do wewnętrznej sieci LAN jest odpowiedzialny użytkownik systemu informatycznego.

f) Administrator systemu informatycznego dokonuje zakupów nośników kopii awaryjnych.

4. Administrator systemu informatycznego wykonuje testy odtworzeniowe kopii awaryjnych. W tym celu zabezpiecza on platformę sprzętowo-programową pozwalającą na ich przeprowadzenie. Testy przeprowadzane są raz na pół roku i obejmują sprawdzenie możliwości odtworzenia przechowywanych danych osobowych oraz danych konfiguracyjnych. Po ich wykonaniu administrator systemu informatycznego sporządza protokół potwierdzający wykonanie testów, który jest zatwierdzany przez Administratora bezpieczeństwa informacji.

5. Negatywne wyniki testu lub zaistnienie problemów w trakcie odtwarzania danych może stać się podstawą do zmiany sposobu tworzenia kopii awaryjnych w urzędzie lub zmiany technologii wykorzystywanej do tworzenia kopii (urządzenia, nośniki). W przypadku wystąpienia negatywnych wyników lub problemów Administrator systemu informatycznego przeprowadza analizy przyczyn i podejmuje działania w celu zmniejszenia ryzyka utraty danych poprzez brak możliwości odtworzenia kopii.

6. Nośniki kopii awaryjnych, które zostały wycofane z użycia, podlegają zniszczeniu po usunięciu danych osobowych, w odpowiednim urządzeniu niszczącym przez administrator systemu informatycznego w obecności kierownika kancelarii tajnej zgodnie z obowiązującymi przepisami.

VI. SPOSÓB, MIEJSCE I OKRES PRZECHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE ORAZ KOPII ZAPASOWYCH.

1. Nośniki danych osobowych postaci elektronicznej winny być zabezpieczone przed dostępem osób nieupoważnionych, nieautoryzowaną modyfikacją i zniszczeniem.

2. Dane osobowe mogą być zapisywane na nośnikach przenośnych w przypadku tworzenia kopii awaryjnych lub gdy istnieje konieczność przeniesienia tych danych w postaci elektronicznej.

3. Nośniki danych osobowych przechowuje się w zamkniętych szafkach wewnątrz obszaru przeznaczonego do przetwarzania danych osobowych i nie powinny być bez uzasadnionej potrzeby wynoszone poza ten obszar.

4. Przekazywanie nośników danych osobowych poza obręb UM może odbywać się za wiedzą i zgodą Administratora bezpieczeństwa informatycznego.

5. W przypadku gdy nośnik danych osobowych nie jest dłużej potrzebny, należy przeprowadzić zniszczenie nośnika albo usunięcie danych z nośnika zgodnie ze szczegółowymi wytycznymi.

6. W zależności od rodzaju przechowywanych informacji Administrator danych osobowych określa wymagany czas przechowywania nośników danych osobowych, wydruków, jak również danych osobowych w systemie informatycznym.

VII. METODA I CZĘSTOTLIWOŚĆ SPRAWDZANIA OBECNOŚCI WIRUSÓW KOMPUTEROWYCH ORAZ METODA ICH USUWANIA.

1. Użytkownicy rozpoczynają pracę w systemie informatycznym uwierzytelniając się poprzez swoje indywidualne identyfikatory i hasła.

2. Każdy zewnętrzny nośnik danych, z którego informacja jest wprowadzana do komputera musi najpierw zostać sprawdzony systemem ochrony antywirusowej.

W przypadkach niejednoznacznych należy przekazać nośnik do sprawdzenia przez informatyka.

3. Użytkownicy stanowisk komputerowych używanych do wprowadzania informacji z zewnętrznych nośników danych lub poczty elektronicznej zobowiązani są do cyklicznego, nie rzadziej niż cotygodniowego, sprawdzania systemem ochrony antywirusowej stanu dysków i pamięci komputera.

4. Administrator systemu informatycznego zapewnia ochronę antywirusową, zarządza systemem wykrywającym i usuwającym wirusy oraz inne niebezpieczne kody. System antywirusowy jest skonfigurowany w następujący sposób:

a) skanowanie dysków zawierających potencjalnie niebezpieczne kody odbywa się automatycznie po włączeniu komputera w tle działania aplikacji,

b) skanowanie informacji przesyłanych do systemu informatycznego pod kątem pojawienia się niebezpiecznych kodów odbywa się na bieżąco.

5. Systemy antywirusowe zainstalowane na stacjach roboczych są skonfigurowane w celu:

- możliwości centralnego uaktualniania wzorców wirusów;
- możliwości centralnego zbierania informacji o wynikach pracy oprogramowania;

- możliwość centralnej konfiguracji oprogramowania.

6. Administrator systemu informatycznego aktualizuje wzorce wirusów. System antywirusowy jest aktualizowany na podstawie materiałów publikowanych przez producenta oprogramowania.

7. W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy Administrator systemu informatycznego podejmuje działania zmierzające do usunięcia zagrożenia. W szczególności działania te mogą obejmować:

a) usunięcie zainfekowanych plików, o ile jest to akceptowalne ze względu na prawidłowe funkcjonowanie systemu informatycznego,

b) odtworzenie plików z kopii awaryjnych po uprzednim sprawdzeniu, czy dane zapisane na kopiach nie są zainfekowane,

c) samodzielną ingerencję w zawartość pliku - w zależności od posiadanych narzędzi i oprogramowania.

VIII. SPOSÓB DOKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMU I ZBIORU DANYCH OSOBOWYCH.

1**.** Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe muszą uwzględniać zachowanie wymaganego poziomu zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych. Prace serwisowe mogą być wykonywane wyłącznie w siedzibie UM. W przypadku uszkodzenia zestawu komputerowego nośnik informacji danych na których są przechowywane dane osobowe zostaje zabezpieczony przez Administratora bezpieczeństwa informatycznego przed dostępem osób nieuprawnionych.

2. Pracownicy winni zgłaszać wszelkie niesprawności systemu informatycznego Administratorowi bezpieczeństwa informatycznego.

3. W przypadku konieczności przeprowadzenia prac serwisowych poza siedzibą urzędu dane z naprawianego urządzenia muszą zostać w sposób trwały usunięte. Od poniższego wymagania możliwe jest odstępstwo jeżeli urządzenie, podczas przechowywania poza siedzibą przedsiębiorstwa, będzie pod stałym nadzorem osoby upoważnionej do dostępu do danych na nim przetwarzanych, wskazanej przez inspektora bezpieczeństwa informacji.

4. Administrator systemu informatycznego wykonuje okresowy przegląd zbioru danych osobowych oraz usuwa dane, których przechowywanie jest dłużej nieuzasadnione.

IX . SPOSÓB POSTĘPOWANIA W ZAKRESIE KOMUNIKACJI W SIECI KOMPUTEROWEJ.

1. Dane osobowe są przesyłane w sieci informatycznej przystosowanej do obsługi systemu informatycznego przetwarzającego te dane. Sieć ta jest odseparowana od pozostałej infrastruktury teleinformatycznej za pomocą zapory ogniowej [firewalla].

2. Administrator systemu informatycznego jest odpowiedzialny za konfigurację zapory [firewalla].

3. W przypadkach gdy nie jest konieczna wymiana informacji pomiędzy siecią a pozostałymi sieciami informatycznymi, zostają one fizycznie odseparowane.

4. Administrator bezpieczeństwa informacji wskazuje rodzaje danych i sposoby transmisji danych, które wymagają szyfrowania i/lub stosowania podpisu elektronicznego.

5. W wypadku przesyłania danych osobowych poza sieć przystosowaną do transferu danych osobowych zostają zastosowane szczególne środki w zakresie bezpieczeństwa.

Obejmują one:

a) zatwierdzenie przez Administratora bezpieczeństwa informacji celu wysłania danych osobowych,

b) zastosowanie mechanizmów szyfrowania danych osobowych,

c) zastosowanie mechanizmów podpisu elektronicznego zabezpieczającego transmisje danych osobowych oraz rejestrację transmisji wysyłania danych osobowych,

d) umożliwienie wysyłania danych osobowych tylko z wykorzystaniem określonej aplikacji i tylko przez określonych użytkowników - odpowiednia konfiguracja aplikacji i zapory ogniowej.

6. W przypadku stosowania mechanizmów kryptograficznych Administrator systemu informatycznego określa minimalne wymagania w zakresie materiału kryptograficznego stosowanego do ochrony danych osobowych.

Jeżeli nie określi on innych wymagań, stosuje się:

- przy szyfrowaniu symetrycznym stosowanie minimum algorytmu typu AES z kluczem 256 bitów;
- przy szyfrowaniu asymetrycznym stosowanie minimum algorytm RSA z kluczem 1024 bity.

7. W wypadku gdy podmiot zewnętrzny, z którym wymieniane są dane osobowe, korzysta z innych mechanizmów kryptograficznych niż stosowane w urzędzie , Administrator bezpieczeństwa informacji może dopuścić zastosowanie tych mechanizmów lub mechanizmów z nimi zgodnych pod warunkiem zapewnienia zbliżonej do obowiązującej ochrony przesyłanych danych osobowych. W tym celu Administrator bezpieczeństwa informacji może przeprowadzić analizę poziomu bezpieczeństwa mechanizmu kryptograficznego oraz zgodności tego mechanizmu z komponentami systemu informatycznego.

9. W Urzędzie Miasta Chełmży klucze kryptograficzne wykorzystywane w kryptografii asymetrycznej są użytkowane przez jeden rok i po tym okresie podlegają wycofaniu i wymianie. Administrator bezpieczeństwa informacji może określić inny (ale nie dłuższy) okres ważności kluczy w kryptografii asymetrycznej, jeśli zabezpieczenie pewnego rodzaju danych osobowych będzie wymagało skrócenia czasu życia kluczy.

10. Klucze kryptograficzne w kryptografii symetrycznej mają charakter sesyjny - generowane są na potrzeby określonej sesji wymiany danych i czas ich życia jest równy czasowi trwania sesji.

11. W przypadku wystąpienia uzasadnionego podejrzenia przechwycenia kluczy kryptograficznych lub dostania się ich w niepowołane ręce pracownik zobowiązany jest poinformować o tym fakcie Administratora bezpieczeństwa informacji lub osoby przez niego upoważnione zgodnie z zasadami opisanymi w „Instrukcji postępowania w przypadku naruszenia ochrony danych osobowych".