Zarządzenie 260/2013

w sprawie ustalenia instrukcji zarządzania systemem informatycznym w Urzędzie Miejskim w Choroszczy.

ZARZĄDZENIE NR 260/2013

Burmistrza Choroszczy z dnia 29.10.2013 r.

w sprawie ustalenia instrukcji zarządzania systemem informatycznym w Urzędzie Miejskim w Choroszczy.

Na podstawie § 3 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) zarządzam, co następuje:

§ 1

Ustala się „Instrukcję zarządzania systemem informatycznym w Urzędzie Miejskim w Choroszczy" zwaną dalej „Instrukcją" która stanowi załącznik do niniejszego zarządzenia.

§ 2

Zobowiązuje się pracowników Urzędu Miejskiego w Choroszczy do stosowania zasad określonych w „Instrukcji".

§ 3

Wykonanie niniejszego zarządzenia powierzam Administratorowi Bezpieczeństwa Informacji.

§ 4

Zarządzenie wchodzi w życie z dniem podpisania.

Załącznik
do Zarządzenia nr 260/2013 Burmistrza Choroszczy
z 29.10.2013 r.

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych
w Urzędzie Miejskim w Choroszczy

ROZDZIAŁ I Postanowienia ogólne

§ 1

1. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwana dalej „Instrukcją", określa sposób zarządzania systemem informatycznym, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji, a także zasady i tryb postępowania Administratora Danych oraz osób przez niego upoważnionych przy przetwarzaniu danych osobowych.
2. Instrukcja została opracowana zgodnie z wymogami określonymi w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r., Nr 101, poz. 926 ze zm.) oraz 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).
3. Podstawowym celem zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych jest zapewnienie jak najwyższego standardu bezpieczeństwa tych danych. Za priorytet uznano zagwarantowanie zgromadzonym danym osobowym, przez cały okres ich przetwarzania, charakteru poufnego wraz z zachowaniem ich integralności oraz integralności systemu informatycznego.

§ 2

Instrukcja określa stosowane procedury i warunki zarządzania systemem informatycznym oraz kartotekami, zapewniające ochronę przetwarzanych danych osobowych, odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.

§ 3

1. Ilekroć w Instrukcji jest mowa o:

1) zbiorze danych - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnym według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie

niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,

2) przetwarzaniu danych - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowanie, zmienianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,

3) systemie informatycznym - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,

4) kartotece - rozumie się przez to zewidencjonowany, usystematyzowany zbiór wykazów, skoroszytów, wydruków komputerowych i innej dokumentacji gromadzonej w formie papierowej, zawierającej dane osobowe,

5) Administratorze Danych - rozumie się przez to Urząd Miejski wChoroszczy

6) Administratorze Bezpieczeństwa Informacji — osoba nadzorująca przestrzeganie zasad przetwarzania i ochrony danych osobowych

7) osobie odpowiedzialnej za prawidłowe funkcjonowanie sprzętu oprogramowania i jego konserwację - rozumie się przez to informatyka odpowiedzialnego za powyższe zadania wyznaczone przez Burmistrza, zwanego dalej „Informatykiem",

8) Komórce organizacyjnej - rozumie się przez to każdą wydzieloną organizacyjnie ifunkcjonalnie komórkę wewnętrznie zgodnie z regulaminem organizacyjnym,

9) użytkowniku - rozumie się przez to osobę wyznaczoną przez Burmistrza lub osobę przezniego upoważnioną, uprawnioną do bezpośredniego dostępu do danych osobowych przetwarzanych w systemie informatycznym oraz kartotekach, posiadającą ustalonyidentyfikator i hasło,

10) Pomieszczeniach - rozumie się przez to budynek , pomieszczenia lub części pomieszczeńokreślonych przez Administratora Danych, tworzące obszar, w którym przetwarzane są dane z użyciem stacjonarnego sprzętu komputerowego oraz gromadzenie w kartotekach.

ROZDZIAŁ II

Procedury nadawania uprawnień do przetwarzania danych i rejestrowanie tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności

§ 4

1. Do przetwarzania danych osobowych przy użyciu systemu informatycznego dopuszczane są osoby na podstawie indywidualnego upoważnienia na dostęp do przetwarzania danych osobowych wydawanego przez Administratora Danych Osobowych na wniosek kierowników referatów. Każdy użytkownik dopuszczony do przetwarzania danych osobowych posiada stosowne upoważnienie. Wzór upoważnienia dostępu do danych osobowych i do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych określa załącznik Nr 1 do Instrukcji.
2. Każdy użytkownik posiada indywidualny identyfikator umożliwiający logowanie do tych aplikacji, z którymi może pracować.
3. Identyfikator umożliwia wykonywanie czynności zgodnie z zakresem powierzonychobowiązków, które wyznaczają poziom uprawnień.
4. Postanowienia ust. 2 nie dotyczy użytkowników, którzy mają dostępwyłącznie do danych osobowych gromadzonych w kartotekach.

§ 5

. Użytkownicy systemu przetwarzającego dane osobowe przed przystąpieniem do

przetwarzania danych osobowych w systemie informatycznym, zobowiązani są zapoznać

się z:

1) Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 Nr 101,

poz. 926 z poźn. zm.).

) Polityką bezpieczeństwa przetwarzania danych osobowych Urzędu Miejskiego w Choroszczy.

) Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Choroszczy.

. Użytkownicy przed dopuszczeniem do obsługi systemu informatycznego, w którym

rzetwarzane są dane osobowe powinni podlegać przeszkoleniu w zakresie obsługi sprzętu informatycznego, oprogramowania systemowego oraz oprogramowania do obsługi aplikacji, którą będą wykorzystywali.

§ 6

1. Każdy użytkownik zobowiązany jest do zachowania tajemnicy własnych haseł, także poupływie ich ważności.
2. Osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować wtajemnicy te dane oraz sposoby ich zabezpieczenia.

§ 7

1. Ewidencję osób upoważnionych do przetwarzania danych osobowych prowadzi Administrator Bezpieczeństwa Informacji. Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych określa załącznik Nr 2 do Instrukcji.

2. Ewidencja zawiera:

a) imię i nazwisko użytkownika,

b) datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych,

c) identyfikator użytkownika.

3. Postanowienia ust. 2 lit. c) nie dotyczą użytkowników, którzy mają dostęp wyłącznie dodanych osobowych gromadzonych w kartotekach.
4. Ewidencja użytkowników może być prowadzona w systemie informatycznym.

§ 8

1. Zmiany dotyczące użytkownika, takie jak:

a) zmiana imienia lub nazwiska,

b) zmiana zakresu upoważnienia podlegają niezwłocznemu odnotowaniu w ewidencji, o której mowa w § 7 ust. 2 Instrukcji.

2. Zmiany dotyczące użytkownika, takie jak:

1) rozwiązanie umowy,

2) utrata upoważnienia do dostępu do danych osobowych,

3) zmiana zakresu obowiązków służbowych skutkująca ustaniem upoważnienia powoduje wyrejestrowanie użytkownika przez Administratora Bezpieczeństwa Informacji z ewidencji, o której mowa w § 7 ust. 2 Instrukcji. Zablokowanie identyfikatora i unieważnienie hasła tego użytkownika dokonuje Informatyk.

3. Kierownicy komórek organizacyjnych oraz pracownik odpowiedzialny za sprawy personalne odpowiadają za natychmiastowe zgłoszenie do Administratora Bezpieczeństwa Informacji użytkowników,którzy utracili uprawnienia do dostępu do danych osobowych, celem zablokowania im dostępu do systemu informatycznego poprzez zablokowanie identyfikatora i wyrejestrowanie z ewidencji, o której mowa w § 5 ust. 2 Instrukcji.

ROZDZIAŁ III

Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzeniem i użytkowaniem

§ 9

1. Identyfikatory i hasła są sposobem zagwarantowania rozliczalności, poufności i integralności danych osobowych przetwarzanych w systemach informatycznych. Służą do weryfikowania tożsamości Użytkownika, uzyskania dostępu do określonych zasobów, kont

uprzywilejowanych lub uruchomienia określonej funkcjonalności.

2. Mając na uwadze zagwarantowanie wysokiego poziomu bezpieczeństwa przetwarzania

danych osobowych wszyscy Użytkownicy przy uwierzytelnianiu do systemów informatycznych powinni stosować się do poniższych zasad:

1) Identyfikator, który utracił ważność nie może być ponownie przydzielony innemu

Użytkownikowi.

2) Hasło początkowe, które jest przydzielane przez Informatyka, powinno umożliwiać Użytkownikowi zarejestrowanie się w systemiei powinno być natychmiast zmienione przez Użytkownika.

3) Użytkownicy powinny wybierać hasła dobrej jakości.

4) Hasła nie mogą być takie same jak identyfikator Użytkownika oraz nie mogą być zapisywane w systemach w postaci jawnej.

5) Użytkownik nie powinien przechowywać haseł w widocznych miejscach, nie powinien

umieszczać haseł w żadnych automatycznych procesach logowania (skryptach, makrach lub pod klawiszami funkcyjnymi).

6) Użytkownicy są odpowiedzialni za wszelkie działania w systemach informatycznych

prowadzone z użyciem ich identyfikatora i hasła.

7) Informatyk jest odpowiedzialny za okresowe sprawdzanie, usuwanie lub blokowanie zbędnych identyfikatorów Użytkowników oraz kont w systemach, za które są odpowiedzialni.

§ 10

1. Użytkownik jest zobowiązany zmieniać hasło, w którego posiadaniu się znajduje:

a) systematycznie, co 30 dni chyba że stacje robocze sąwyposażone w system wymuszania zmiany hasła co 30 dni.

b) w przypadku ujawnienia lub podejrzenia ujawnienia hasła.

2. W przypadku braku dostępu do konta chronionego hasłem, w którego posiadaniu się

znajduje, Użytkownik zobowiązany jest wystąpić o zmianę hasła do Informatyka, w sytuacji:

1) Zapomnienia/zgubienia hasła.

2) Wygaśnięcia ważności hasła.

3) Zablokowania konta spowodowanego nieprawidłowym wprowadzeniem hasła.

ROZDZIAŁ IV

Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemów

§ 11

Przed przystąpieniem do pracy z systemem informatycznym lub kartotekami, użytkownikobowiązany jest dokonać sprawdzenia stanu urządzeń komputerowych oraz dokonać oględzin swojego stanowiska pracy, w tym zwrócić szczególną uwagę, czy nie zaszły okoliczności wskazujące na naruszenie poufności danych osobowych.

§ 12

W przypadku stwierdzenia bądź podejrzenia, iż miało miejsce naruszenia systemu, użytkownik obowiązany jest postępować zgodnie z zasadami określonymi w Polityce bezpieczeństwa.

§ 13

Przed opuszczeniem stanowiska pracy, użytkownik obowiązany jest:

1) wylogować się z systemu informatycznego lub,

2) zablokować system ręcznie lub,

3) poczekać, aż zaktywizuje się blokowany hasłem wygaszasz ekranu.

§ 14

Kończąc pracę należy:

1) wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy,

2) zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się dane osobowe.

ROZDZIAŁ V

Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służącychdo ich przetwarzania

§ 15

1. Kopie zapasowe zbiorów danych osobowych oraz programów i narzędzi programowych

służących do ich przetwarzania powinny być wykonywane na bieżąco przez Informatyka.

2. Kopie zapasowe powinny być tworzone na nośnikach magnetycznych, odpowiednio

opisanych, oznakowanych i ewidencjonowanych.

3. Kopie zapasowe należy opisywać w sposób umożliwiający szybką i jednoznaczną

identyfikację zawartych w nich danych.

4. Informatyk odpowiedzialny za tworzenie kopi zapasowych, zobowiązany jest przestrzegać terminów sporządzania kopii zapasowych oraz okresowo dokonywać kontroli możliwości odtworzenia danych zapisanych na tych kopiach, pod kątem ewentualnej przydatności w sytuacji awarii systemu.

5. Kopie zapasowe powinny być tworzone w bezpiecznym systemie archiwizacji, który powinien zapewniać ograniczony dostęp fizyczny do nośników oraz przyznanie uprawnień dostępu tylko wyznaczonemu imiennie Informatykowi oraz Administratorowi Bezpieczeństwa Informacji.

6. Dane z kopii zapasowych powinny być odtwarzane wyłącznie przez Informatyka.

7. Kopie zapasowe, które uległy uszkodzeniu powinny podlegać natychmiastowemu

zniszczeniu.

8. Niszczenia kopii zapasowych, na nośnikach magnetycznych dokonuje Informatyk

lub inna upoważniona przez Kierownictwo osoba.

9. Proces niszczenia kopii zapasowych powinien odbywać się komisyjnie i powinien być dokumentowany.

§ 16

Zbiory danych osobowych oraz programy i narzędzia programowe, służące do ichprzetwarzania, zapisywane na nośnikach zewnętrznych (streamer, dyski: wymienne, magnetyczne, optyczne) tworzące kopie zapasowe kolejnych okresów, powinny być odpowiednio oznakowane i przechowywane w wyznaczonych odpowiednio zabezpieczonych pomieszczeniach.

ROZDZIAŁ VI

Sposób, miejsce i okres przechowywaniaelektronicznych nośników informacji zawierających dane osobowe i kopii zapasowych

§ 17

1. Zbiory danych osobowych przetwarzane w systemie informatycznym są przechowywane na serwerzebądź na osobnych komputerach zapisywanych na dyskach twardych obsługującym system informatyczny Administratora Danych Osobowych, przy czym dane przetwarzane w systemie informatycznym na stacjach roboczych są niezwłocznie umieszczane w odpowiednich miejscach na serwerze.

2. Kopie bezpieczeństwa komputerowych zbiorów danych osobowych umieszczanych na serwerze wykonywane są automatycznie w każdym dniuroboczym o określonej stałej porze a raz w tygodniu są one przenoszone na zewnętrzny dysk twardy. Kopie zbiorów danych osobowych znajdujących się na osobnych komputerach wykonywane są ręcznie. Kopie systemów informatycznych są wykonywane całościowo po stronie serwera, które znajdują się na zewnętrznych dyskach twardych.

3. Nad poprawnym wykonywaniem kopii bezpieczeństwa nadzór sprawuje Informatyk.

4. W celu zapewnienia poprawności wykonywanych kopii bezpieczeństwa Informatyk, co najmniej raz w miesiącu, poddaje testowi cyklicznie wybraną kopię. Próba polega na odtworzeniu danych w warunkach testowych i sprawdzeniu, czy jest możliwość ich odczytania.

5. Kopie bezpieczeństwa przechowuje się przez okres co najmniej 30 dni, w szafie w pomieszczeniu innym niż serwerownia. Dostęp do kopii bezpieczeństwa posiada Administrator Bezpieczeństwa Informacji, Informatyk lub inny upoważniony pracownik Urzędu.

6. Po zakończeniu eksploatacji lub uszkodzeniu zewnętrznych nośników danych służących do

sporządzania kopii zapasowych dokonuje się fizycznego ich zniszczenia w sposób uniemożliwiających ich odczytanie.

§ 1 8

1. Elektroniczne zewnętrzne nośniki informacji mogą być używane przez Użytkowników w wyjątkowych sytuacjach związanych z realizacją określonych zadań, a w innych przypadkach wyłącznie za zgodą Administratora Bezpieczeństwa Informacji.

2. W przypadku posługiwania się elektronicznymi nośnikami informacji pochodzącymi od podmiotu zewnętrznego, użytkownik jest zobowiązany do uprzedniego sprawdzenia go programem antywirusowym w celu wyeliminowania ewentualnych zagrożeń.

3. Użytkownikowi zakazuje się przetwarzania zbiorów danych osobowych w całości na elektronicznych zewnętrznych nośnikach informacji oraz ich przesyłania pocztą elektroniczną, nawet w postaci zaszyfrowanej. Dopuszczalne jest przetwarzanie jedynie jednostkowych danych osobowych.

4. Nośniki informacji jednorazowego użytku takie jak płyty CD-R, DVD-R, zawierające nieaktualne lub zbędne kopie danych likwiduje się poprzez fizyczne zniszczenie w taki sposób, by nie można było odczytać ich zawartości.

5. Nośniki informacji wielorazowego użytku, takie jak dyski twarde, pendrive, płyty CD-RW, DVD-RW, dyskietki, itp., zawierające nieaktualne lub zbędne kopie danych, można wykorzystać ponownie po uprzednim usunięciu ich zawartości w sposób uniemożliwiający ich odzyskanie.

6. Nośniki informacji wielorazowego użytku nienadające się do ponownego użycia, a mogące

zawierać dane osobowe, niszczy się fizycznie w taki sposób, by nie można było odczytać ich

zawartości.

§ 19

1. Wymienne nośniki elektroniczne, o ile nie są Użytkowane, powinny być przechowywane w

zamykanych szafkach.

2. Nośniki zawierające kopie zapasowe powinny być przechowywane w innym pomieszczeniu niż to, w którym umieszczony jest serwer przetwarzający dane osobowe.

3. Kopie zapasowe powinny być przechowywane w odpowiednio zabezpieczonej szafie, do której dostęp mogą mieć wyłącznie osoby upoważnione.

§ 20

1. Kartoteka przekazywana jest do archiwum zgodnie z procedurami archiwizacji dokumentów

2. Likwidacji zbiorów archiwalnych dokonuje się przy użyciu niszczarki do papieru lub winny sposób zapewniający skuteczne ich usunięcie.

§ 21

Decyzję o likwidacji zbiorów danych osobowych, przetwarzanych w kartotekach orazsystemach informatycznych podejmuje właściciel zasobów danych osobowych informując Administratora Bezpieczeństwa Informacji.

§ 22

Dla udokumentowania czynności dokonywanych w celu likwidacji zbiorów danych osobowych, Administrator Bezpieczeństwa Informacji lub osoba przez niego upoważniona sporządza protokół, w którym zamieszcza następujące informacje:

1) datę dokonania likwidacji,

2) przedmiot likwidacji (nośniki, kartoteka)

3) przedmiot czasowy likwidowanych zbiorów danych osobowych,

4) podpisy osób dokonujących i obecnych przy likwidacji zbiorów danych osobowych.

ROZDZIAŁ VII

Zabezpieczenia systemu informatycznego

§ 23

1. System informatyczny zabezpiecza się przed:

1) działaniem, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego,

2) utratą danych spowodowaną:

a) działaniem nieautoryzowanym,

b) awarią zasilania lub zakłóceniami w sieci zasilającej.

§ 24

1. Informatyk odpowiada za niezwłoczne instalowanie na sprzęcie oprogramowania zabezpieczającego system informatyczny.

2. Program antywirusowy należy instalować również na komputerach przenośnych.

§ 25

1. Kontrola antywirusowa jest przeprowadzana na wszystkich nośnikach magnetycznych i optycznych, służących zarówno do przetwarzania danych osobowych w systemie informatycznym, jak i do celów instalacyjnych,

2. Na stacjach roboczych oprogramowanie antywirusowe powinno być aktywne cały czas i powinno dokonywać sprawdzenia każdego otwieranego lub uruchamianego pliku.

§ 26

Użytkownicy są zobowiązani do dokonywania kontroli antywirusowej wszystkich nośnikówmagnetycznych lub optycznych przychodzących z zewnątrz oraz okresowo nośników własnych.

§ 27

1. W razie stwierdzenia zainfekowania systemu, użytkownik obowiązany jest poinformować niezwłocznie o tym fakcie Informatyka.

2. Informatyk usuwa wirusy, jeśli automatycznie nie dokonał tego program antywirusowy.

2. Po usunięciu wirusa Informatyk sprawdza system informatyczny oraz przywraca go do pełnej sprawności i funkcjonalności.

3. Administrator Bezpieczeństwa Informacji sporządza raport wystąpieniu wirusa. Raport winien zawierać następujące informacje:

1) nazwę wirusa

2) datę wykrycia i usunięcia wirusa

3) miejsce zainfekowania

§ 28

W razie niemożności usunięcia wirusa, Informatyk za zgodą Administratora Bezpieczeństwa Informacji, korzysta z usług zewnętrznych specjalistów w tej dziedzinie.

§ 29

1. Przy przetwarzaniu danych osobowych zakwalifikowanych do poziomu bezpieczeństwawysokiego system informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionych dostępem.

2. W przypadku zastosowania logicznych zabezpieczeń , o których mowa w ust. 1, obejmujeona:

1) kontrolę przepływu informacji pomiędzy systemem informatycznym a siecią publiczną

2) kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego

3. Wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej stosuje się środki ochrony kryptograficznej.

ROZDZIAŁ IX

Wymagania dotyczące sprzętu i oprogramowania

§ 30

1. Sprzęt obsługujący zbiór danych osobowych składa się z komputerów stacjonarnych klasy PC.

2. Komputery przenośne mogą być używane do przetwarzania danych osobowych po odpowiednim ich zabezpieczeniu.

3. Użytkownik korzystający z komputera przenośnego jest zobowiązany do zachowaniaszczególnej ostrożności podczas jego transportu, przechowywania i użytkowania. Nie może udostępnić komputera osobom nieupoważnionym oraz zobowiązany jest do stosowania środków ochrony kryptograficznej wobec przetwarzania danych osobowych.

§ 31

1. Sieć komputerowa służąca do przetwarzania danych osobowych powinna mieć zapewnione prawidłowe zasilenie energetyczne gwarantujące właściwe i zgodne z wymaganiami producenta działanie sprzętu komputerowego.

2. Sieć komputerowa powinna być podłączona do zasilania zapasowego (zasilanie dwustronne, agregat prądotwórczy lub UPS). Oprogramowanie powinno zapewnić bezpieczne wyłączenie systemu informatycznego, po dokonaniu operacji zamknięcia wpracujących aplikacjach i oprogramowaniu systemowym.

3. Serwer sieci powinien być zasilany przez UPS o odpowiednich parametrach, pozwalających na podtrzymanie napięcia przez ok. min. 15 minut oraz wykonanie, bezpiecznego wyłączenia serwera, tak by przed zanikiem zostały prawidłowo zakończoneoperacje rozpoczęte na zbiorze danych osobowych.

4. Zasilaczem awaryjnym powinny być zabezpieczone wszystkie stacje robocze.

§ 32

1. Infrastruktura techniczna związana z siecią komputerową i jej zasilaniem (rozdzielnie elektryczne, skrzynki z bezpiecznikami) powinna być zabezpieczona przed dostępem osób nieupoważnionych.

§ 33

1. Dane osobowe przesyłane na nośnikach magnetycznych i optycznych oraz za pomocą systemów teleinformatycznych powinny być zabezpieczone w sposób uniemożliwiający dostęp do nich osób nieupoważnionych.

2. Dane osobowe przesyłane po łączach telekomunikacyjnych wewnątrz danej sieci powinnybyć dodatkowo zabezpieczone w sposób uniemożliwiający dostęp do danej sieci LAN z innej sieci.

3. Dane osobowe przesyłane po łączach telekomunikacyjnych na zewnątrz powinny być wmiarę możliwości technicznych szyfrowane za pomocą algorytmu kryptograficznego.

§ 34

1. Stacje robocze powinny być wyposażone w wygaszacze zabezpieczone hasłem, które aktywują się automatycznie po upływie określonego czasu od ostatniego użycia komputera.

2. Ekrany monitorów, powinny być ustawione w taki sposób, żeby uniemożliwić odczyt wyświetlanych informacji osobom nieupoważnionym.

3. Za spełnienie obowiązku określonego w ust. 2 odpowiadają użytkownicy i kierownicykomórek organizacyjnych.

ROZDZIAŁ X

Procedury wykonywania przeglądów i konserwacji

§ 35

1. Bieżących oraz okresowych przeglądów, napraw i konserwacji systemów oraz nośnikówinformacji służących do przetwarzania danych osobowych, niewymagających angażowania zewnętrznych firm serwisowych, dokonuje Informatyk.

2. Przeglądów i konserwacji zbiorów danych osobowych dokonują użytkownicy, zgodnie zindywidualnymi zakresami upoważnień i odpowiedzialności.

§ 36

W przypadku gdy jest konieczne dokonanie przeglądów, konserwacji i napraw, wymagające zaangażowania firm zewnętrznych, są wykonywane za wiedzą Administratora Bezpieczeństwa Informacji przez uprawnionych przedstawicieli tych firm pod nadzorem Informatyka lub upoważnionego użytkownika w miarę możliwości bez dostępu do rzeczywistych danych osobowych. W takim przypadku należy zawrzeć z podmiotem dokonującym w/w czynności umowę powierzenia danych w rozumieniu art. 31 ustawy o ochronie danych osobowych.

§ 37

1. W przypadku, gdy zaistnieje potrzeba wymiany sprzętu komputerowegosłużącego do przetwarzania lub przechowywania danych osobowych należy usunąć dane, w sposób uniemożliwiający ich odzyskanie.

§ 38

Nadzór nad instalowaniem, sprawnym funkcjonowaniem i wymianą uszkodzonych urządzeń oraz ich likwidacją sprawuje Informatyk.

ROZDZIAŁ XI

Postanowienia końcowe

§ 39

1. Kierownicy komórek organizacyjnych są obowiązani zapoznać z treścią Instrukcji każdego użytkownika.

2. Użytkownik zobowiązany jest złożyć oświadczenie, o tym, iż został zaznajomiony z przepisami ustawy o ochronie danych osobowych, wydanymi na jej podstawie aktami wykonawczymi, obowiązującą Polityką bezpieczeństwa oraz Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, opracowanymi przez Administratora Danych.

3. Wzór oświadczenia, o którym mowa w ust. 2, określa załącznik Nr 3 do Instrukcjizarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

4. Oświadczenia przechowywane są w aktach personalnych pracownika.

§ 40

1. W sprawach nieuregulowanych w niniejszej Instrukcji mają zastosowanie przepisy ustawy o ochronie danych osobowych oraz wydanych na jej podstawie aktów wykonawczych.
2. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Instrukcji.

Załączniki:

- **załącznik nr 1** — wzór upoważnienia dopuszczeniado przetwarzania danych osobowych
- **załącznik nr 2** - wzór ewidencja osób upoważnionych do przetwarzania danych osobowychw Urzędzie Miejskim w Choroszczy
- **załącznik nr 3 —** wzór oświadczenia o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych

Załącznik Nr 1
do „Instrukcji zarządzania…"
stanowiącej załącznik
do Zarządzenia Nr 260/2013
Burmistrza Choroszczy
z dnia 29.10.2013 r.

W z ó r

Choroszcz, dnia ……

Pan/Pani……

zatrudniony/a

w Urzędzie Miejskim w Choroszczy

na stanowisku

……..

……..

UPOWAŻNIENIE

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.)

u p o w a ż n i a m

Pana/Panią do obsługi systemu informatycznego funkcjonującego w Urzędzie Miejskim w Choroszczy oraz urządzeń wchodzących w jego skład, służących przetwarzaniu danych osobowych, w zakresie niezbędnym do wykonywania obowiązków służbowych, określonych w zakresie obowiązków z dnia ……

Zgodnie z art. 39 ust. 2 ustawy o ochronie danych osobowych, ma Pan/Pani obowiązek zachować w tajemnicy dane osobowe oraz sposoby ich zabezpieczenia.

Niniejsze upoważnienie:

1) zostało wydane na czas ……
2) może być w każdym czasie cofnięte,
3) wygasa z dniem rozwiązania stosunku pracy z upoważnionym pracownikiem.

Otrzymuje:

……..

Do wiadomości:

1) Administrator Bezpieczeństwa Informacji

Załącznik Nr 2
do „Instrukcji zarządzania…"
stanowiącej załącznik
do Zarządzenia Nr 260/2013
Burmistrza Choroszczy
z dnia 29.10.2013 r.

W z ó r

Ewidencja pracowników upoważnionych do przetwarzania danych osobowych w Urzędzie Miejskim w Choroszczy

Imię i nazwisko	Zbiór danych osobowych	Rodzaj systemu	Data upoważnienia (od —do)	Identyfikator

Załącznik Nr 3
do „Instrukcji zarządzania…"
stanowiącej załącznik
do Zarządzenia Nr 260/2013
Burmistrza Choroszczy
z dnia 29.10.2013 r.

……

(miejscowość, data)

……

(imię i nazwisko)

wzór

OŚWIADCZENIE

Oświadczam, iż zostałem/am zapoznany/a z obowiązującymi przepisami dotyczącymi ochrony danych osobowych, w szczególności ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 Nr 101, poz. 926 z poźn. zm.) i wydanych na jej podstawie aktów wykonawczych oraz opracowanych przez Administratora Danych: Polityką bezpieczeństwa oraz Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Jednocześnie zobowiązuje się do ich przestrzegania.

……

(podpis osoby składającej oświadczenie)

INSTRUKCJA ZARZĄDZANIA.docx (50.65 KB)
INSTRUKCJA ZARZĄDZANIA.docx

Metryka strony

Udostępniający: **Urząd Miejski w Choroszczy**
Wytwarzający/odpowiadający: **Dorota Tomicka**
Wprowadzający: **Dorota Tomicka**
Data modyfikacji: **2013-10-29**
Opublikował: **Ewa Łukaszewicz**
Data publikacji: **2013-10-29**