Luty 2015 r.

załącznik nr 2 do ZARZĄDZENIA Nr 30/2015 Burmistrza Miasta Pieszyce z dnia 18 lutego 2015r. w sprawie wprowadzenia ,,Polityki Bezpieczeństwa Informacji i ochrony danych osobowych" oraz ,,Instrukcji Zarządzania Systemem Informatycznym"

Instrukcja zarządzania systemem informatycznym Urzędu Miejskiego w PIESZYCACH

BURMISTRZ
Dorota Konieczna-Enözel

18.02.2015

Załączniki

1. Wstęp

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych Urzędu Miejskiego w Pieszycach określa zasady, tryb postępowania i zalecenia Administratora Danych, ktore muszą być stosowane przez osoby przez niego upoważnione do przetwarzania danych osobowych w systemach informatycznych.

Instrukcja została opracowana zgodnie z wymogami § 5 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).

Podstawowymi celami zabezpieczeń systemów informatycznych służących do przetwarzania danych osobowych, jest zapewnienie jak najwyższego poziomu bezpieczeństwa przetwarzanych danych osobowych w systemach informatycznych.

Instrukcja ta jest zatwierdzona przez Administratora danych Osobowych i przyjęta do stosowania jako obowiązujący dokument.

2. Definicje

Urząd Miasta i Gminy - identyfikuje się jako samorządową jednostkę budżetową;

służba informatyczna urzędu - rozumie się przez to informatyków zatrudnionych w urzędzie;

system informatyczny urzędu - sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych;

serwer - to jednostka centralna, komputer zarządzający systemem informatycznym urzędu;

Stacja robocza – stacjonarny lub przenośny komputer wchodzący w skład systemu informatycznego umożliwiający użytkownikom systemu dostęp do danych osobowych znajdujących się w systemie.

sieć lokalna – połączenie systemów informatycznych urzędu wyłącznie dla własnych potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych

dane –dane będące w posiadaniu urzędu w postaci elektronicznej lub w innej formie, będące w zbiorach urzędu, wykorzystywane przez Urząd lub osoby trzecie, a niezbędne do wykonywania zadań Urzędu;

dane osobowe –informacje o osobie fizycznej dotyczące tożsamości tej osoby (w tym personalia umożliwiające jej identyfikację);

dane wrażliwe - dane określone w artykule 27 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. nr 101, poz. 926 z późniejszymi zmianami), a więc dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym;

zbiór danych osobowych - każdy posiadający strukturę zestaw danych osobowych, dostępnych wg określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony czy podzielony funkcjonalnie.

przetwarzanie danych - operacje wykonywane na danych osobowych, takie jak: zbieranie, wprowadzanie do systemu urzędu, przechowywanie, opracowywanie, zmienianie, usuwanie i udostępnianie;

zabezpieczenie systemu informatycznego – zespól stosowanych środków technicznych i fizycznych w celu zabezpieczenia zasobów oraz ochrony danych osobowych przed ujawnieniem, zniszczeniem i utratą, a także nieuprawnionym dostępem i przetwarzaniem.

Administrator Danych Osobowych (ADO) - osoba pełniącą funkcje i posiadającą zakres uprawnień w rozumieniu ustawy o ochronie danych osobowych oraz pełniącą nadzór nad realizacją obowiązków wynikających z Polityki Bezpieczeństwa w Urzędzie;

Administrator Bezpieczeństwa Informacji (ABI) - osoba, której Administrator Danych Osobowych powierzył pełnienie obowiązków Administratora Bezpieczeństwa Informacji w odniesieniu do systemu nadzoru nad informacją (aktywami) w odniesieniu do systemów informatycznych;

Administrator Systemów Informatycznych (ASI) - osoba, której Administrator Danych Osobowych powierzył pełnienie obowiązków Administratora Systemów Informatycznych w odniesieniu do systemu nadzoru nad informacją (aktywami) funkcjonującą w systemach informatycznych;

użytkownik systemu – osoba upoważniona do przetwarzania danych osobowych w systemie informatycznym urzędu. Użytkownikiem może być prcownik urzędu, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilnoprawnej, osoba odbywająca staż w urzędzie, praktykę studencką lub wolontariusz.

identyfikator użytkownika - ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w wyznaczonych przez administratora danych osobowych obszarach systemu informatycznego urzędu;

hasło - co najmniej 8-znakowy ciąg znaków literowych, cyfrowych, zawierający duże i małe litery oraz znaki specjalne, znany jedynie osobie uprawnionej do pracy w systemie informatycznym, Administratorowi Danych Osobowych oraz Administratorowi Bezpieczeństwa Informacji;

serwisant - firma lub pracownik firmy zajmującej się sprzedażą, instalacją, naprawą i konserwacją sprzętu komputerowego;

3. Poziom bezpieczeństwa

W Urzędzie Miejskim w Pieszycach obowiązuje wysoki poziom bezpieczeństwa systemu informatycznego z uwagi na to, że jest on połączony z siecią publiczną (z internetem) - paragraf 6, ust. 4 rozporządzenie Ministra z dnia 29 kwietnia 2004 r.

4. Bezpieczna eksploatacja sprzętu i oprogramowania

Przy przetwarzaniu danych należy zachować wymogi bezpieczeństwa danych, ich ochrony przed utratą i kradzieżą.

Tryb pracy na poszczególnych stacjach roboczych.

1. Rozpoczęcie pracy na stacji roboczej, następuje po włączeniu napięcia w listwie separującej napięcie, włączeniu urządzenia UPS i komputera, a następnie wprowadzeniu indywidualnego, znanego tylko użytkownikowi identyfikatora i hasła.
2. W pomieszczeniu, w którym przetwarzane są dane osobowe, mogą znajdować się osoby postronne tylko za zgodą i w towarzystwie użytkownika danych osobowych, Administratora Danych Osobowych lub Administratora Systemów Informatycznych.
3. Przed osobami postronnymi należy chronić ekrany komputerów (ustawienie monitora powinno uniemożliwiać podgląd), wydruki leżące na biurkach oraz w otwartych szafach.
4. Stacje robocze wyposażone są we włączające się, po max. 30 minutach od przerwania pracy, wygaszacze ekranu lub też w systemy wylogowania użytkownika. Wznowienie wyświetlenia następuje dopiero po wprowadzeniu odpowiedniego hasła do systemu operacyjnego stacji roboczej lub systemu informatycznego aktualnie użytkowanego.

5. W przypadku opuszczenia stanowiska pracy, użytkownik obowiązany jest aktywizować wygaszacz ekranu lub w inny sposób zablokować stację roboczą.
6. Obowiązuje zakaz robienia kopii zbiorów danych przez użytkownika stacji roboczej. Całe zbiory danych kopiowane są tylko przez Administratora Systemów Informatycznych lub automatycznie przez system, z zachowaniem procedur ochrony danych osobowych.
7. Jednostkowe dane mogą być kopiowane na nośniki magnetyczne, optyczne i inne po ich zaszyfrowaniu i przechowywane w zamkniętych na klucz szafach. Po ustaniu przydatności tych kopii dane należy trwale skasować lub fizycznie zniszczyć nośniki, na których są przechowywane.
8. Jednostkowe dane mogą być przekazywane pocztą elektroniczną pomiędzy komputerami Urzędu , a komputerami przenośnymi używanymi przez upoważnionych pracowników Urzędu Miejskiego w Pieszycach tylko po ich zaszyfrowaniu.
9. Wypisy ze zbiorów danych udostępniane zgodnie z art. 7 ust. 6 ustawy o ochronie danych osobowych można przesyłać pocztą elektroniczną tylko w postaci zaszyfrowanej.
10. Obowiązuje zakaz wynoszenia, na jakichkolwiek nośnikach, całych zbiorów danych oraz szerokich z nich wypisów, nawet w postaci zaszyfrowanej. W przypadku uzasadnionej konieczności wynoszenia zbiorów danych (aktywów) poza obręb Urzędu wymagana jest pisemna zgoda Starosty oraz konieczność zarejestrowania tego faktu w rejestrze stwierdzającym fakt pobrania danych i ich zakresu oraz w rejestrze zwrotu zbioru.
11. Zakończenie pracy na stacji roboczej następuje po wprowadzeniu danych tego dnia, przetwarzanych w odpowiednie obszary serwera, a następnie prawidłowym wylogowaniu się użytkownika i wyłączeniu komputera oraz odcięciu napięcia w UPS lub listwie.
12. Przed opuszczeniem pokoju należy:
    - zniszczyć w niszczarce lub schować do zamykanych na klucz szaf wszelkie wykonane wydruki zawierające dane osobowe,
    - schować do zamykanych na klucz szaf wszelkie akta zawierające dane osobowe,
    - umieścić klucze do szaf w ustalonym, przeznaczonym do tego miejscu,
    - zamknąć okna,
13. Opuszczając pokój należy zamknąć za sobą drzwi na klucz. Klucz do pokoju przechowywany jest w metalowej szafce, w sekretariacie. Jeśli niemożliwe jest umieszczenie wszystkich dokumentów zawierających dane osobowe w zamykanych szafach, należy powiadomić o tym ABI, który zgłasza jednorazową rezygnację z wykonania usługi sprzątania. W takim przypadku także należy zostawić klucz w metalowej szafce, w sekretariacie.

Tryb pracy na komputerach przenośnych.

1. Na ile to możliwe, przy przetwarzaniu danych osobowych na komputerach przenośnych, obowiązują wymogi dotyczące pracy na komputerach stacjonarnych.
2. Komputery przenośne użytkownicy, którym zostały one powierzone, powinni chronić przed uszkodzeniem, kradzieżą i dostępem osób postronnych, szczególną ostrożność należy zachować podczas ich transportu.
3. Obowiązuje zakaz używania komputerów przenośnych przez osoby inne niż użytkownicy, którym zostały one powierzone.
4. Praca na komputerze przenośnym możliwa jest po wprowadzeniu indywidualnego identyfikatora i osobistego hasła. System automatycznie wymusza systematyczną zmianę hasła przez Administratora Systemów Informatycznych lub użytkownika.
5. Pliki zawierające dane osobowe przechowywane na komputerach przenośnych są zaszyfrowane i opatrzone hasłem dostępu.
6. Obowiązuje zakaz przetwarzania na komputerach przenośnych całych zbiorów danych lub szerokich z nich wypisów, nawet w postaci zaszyfrowanej.
7. Użytkownicy danych przetwarzanych na komputerach przenośnych obowiązani są raz na kwartał do wprowadzania ich w określone miejsca na serwerze (wprowadzania do systemu informatycznego Urzędu Miejskiego w Pieszycach), a następnie do nadpisywania tych danych w pamięci powierzonych komputerów przenośnych.
8. Obowiązuje zakaz samodzielnej modernizacji oprogramowania i sprzętu w powierzonych komputerach przenośnych. Wszelkie zmiany mogą być dokonywane tylko pod nadzorem Administratora Systemów Informatycznych, stosownie do wymagań niniejszej instrukcji. W razie wystąpienia usterek w pracy komputerów przenośnych lub w razie wystąpienia konieczności aktualizacji ich oprogramowania, należy zgłosić to Administratorowi Systemów Informatycznych.
9. Komputery przenośne wyposażone są w odpowiednie programy ochrony antywirusowej, których aktualizację sugeruje automatycznie system.
10. Użytkowanie nośników danych typu dyski zewnętrzne lub typu pendrive wymaga zgody Starosty i stosowania urządzeń z koniecznością hasłowania i szyfrowania zapisu danych.

5. Procedura nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności

Przetwarzać dane, w tym dane osobowe w systemach informatycznych może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych (wzór upoważnienia stanowi załącznik do niniejszej instrukcji). Wydanie upoważnienia oraz rejestracja użytkownika systemu informatycznego przetwarzającego dane osobowe następuje na wniosek przełożonego użytkownika lub koordynatora zadania, na rzecz którego będą wykonywane czynności związane z przetwarzaniem danych osobowych. W formie pisemnej składa on wniosek do Administratora Bezpieczeństwa Informacji odpowiedniego dla zakresu danych o wydanie upoważnienia do przetwarzania danych osobowych.

Wniosek ten powinien zawierać:

- imię i nazwisko pracownika urzędu, któremu upoważnienie zostanie nadane,
- nazwę zbioru danych osobowych oraz nazwę systemu informatycznego, do którego użytkownik będzie miał dostęp,
- zakres upoważnienia do przetwarzania danych osobowych,
- datę, z jaką upoważnienie ma być nadane,
- okres ważności upoważnienia.

Oryginał upoważnienia zostaje przekazany pracownikowi za potwierdzeniem odbioru, kopia zostaje dołączona do akt osobowych pracownika oraz przekazana do wiadomości przełożonego pracownika.

Identyfikator i hasło do systemu informatycznego przetwarzającego dane osobowe są przydzielane użytkownikowi tylko w przypadku, gdy posiada on pisemne upoważnienie do przetwarzania danych osobowych wydane przez administratora danych osobowych lub osobę przez niego uprawnioną.

Za przydzielenie i wygenerowanie identyfikatora i hasła użytkownikowi, który pierwszy raz będzie korzystał z systemu informatycznego, odpowiada administrator odpowiedniego systemu informatycznego (czynności te wykonuje na pisemny lub przesłany drogą elektroniczną wniosek Administratora Bezpieczeństwa Informacji).

Wyrejestrowanie użytkownika z systemu informatycznego może nastąpić na wniosek administratora danych osobowych, przełożonego użytkownika lub koordynatora zadania, na rzecz którego były wykonywane czynności związane z przetwarzaniem danych osobowych.
Pisemny wniosek o wyrejestrowanie użytkownika systemu należy złożyć do Administratora Bezpieczeństwa Informacji. Wyrejestrowanie użytkownika z systemu realizuje administrator odpowiedniego systemu informatycznego na pisemny lub przesłany drogą elektroniczną wniosek administratora bezpieczeństwa informacji.

Administrator bezpieczeństwa informacji jest zobowiązany do prowadzenia ewidencji pracowników upoważnionych do przetwarzania danych, w tym danych osobowych, osobowych.

Zgodnie z art. 39 ust. 1 ustawy taka ewidencja zawiera:

- imię i nazwisko osoby upoważnionej,
- datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych,
- nazwa systemu informatycznego, którego dotyczy upoważnienie,
- identyfikator nadany w systemie.

6. Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

(§ 5 pkt 2 rozporządzenia)

Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła. Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi. Użytkownik odpowiedzialny jest za wszystkie czynności wykonane przy użyciu identyfikatora, którym się posługuje lub posługiwał.

- identyfikator składa się minimalnie z siedmiu znaków, znaki identyfikatora nie są rozdzielone spacjami ani znakami interpunkcyjnymi, identyfikator nie zawiera polskich liter,
- identyfikator wpisuje się do ewidencji, prowadzonej przez Administratora Bezpieczeństwa Informacji, wraz z imieniem i nazwiskiem użytkownika oraz nazwami systemów informatycznych, do których użytkownik uzyskał dostęp i wprowadzany jest przez administratorów systemów informatycznych do właściwych systemów,
- identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego nie może być przydzielany innej osobie.

System informatyczny przetwarzający dane osobowe jest konfigurowany w sposób wymagający bezpieczne zarządzanie hasłami użytkowników:

- hasło przydzielone użytkownikowi musi być zmienione po pierwszym udanym zalogowaniu się do systemu informatycznego przetwarzającego dane osobowe,
- hasła są zmieniane przez użytkownika,
- system informatyczny wyposażony jest w mechanizmy wymuszające zmianę hasła po upływie 30 dni od dnia ostatniej zmiany hasła,

- w przypadku gdy system informatyczny nie jest wyposażony w mechanizmy wymuszające zmianę hasła, należy dążyć do uaktualnienia systemu tak aby taki mechanizm posiadał lub zobowiązać pracownika do ręcznej zmiany hasła w terminach wskazanych prawem,
- system informatyczny wyposażony jest w mechanizm pozwalający na wymuszenie jakości hasła, w szczególności hasło powinno składać z co najmniej 8 znaków. Hasło powinno zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.

Osoby uprawnione do wykonywania prac administracyjnych w systemie informatycznym posiadają własne konta administracyjne, do których mają przydzielone hasło. Zasady zarządzania hasłami są analogiczne, jak w przypadku haseł użytkowników. Nazwy i hasła użytkowników posiadających uprawnienia administratorów systemów informatycznych powinny być przechowywane w zamkniętej szafie, do której dostęp jest w pełni kontrolowany, przy czym dostęp do szafy mają wyłącznie uprawnione osoby. Nazwy użytkowników oraz hasła powinny być przechowywane w opieczętowanej i opatrzonej podpisem administratorów systemu kopercie. W przypadku konieczności awaryjnego użycia nazw i haseł tych użytkowników konieczny jest wpis ilustrujący zaistniała sytuację w „Dzienniku haseł" znajdującym się w szafie wraz z kopertą w której znajdują się hasła. Wpis powinien zawierać następujące informacje:

- imię i nazwisko oraz stanowisko osoby upoważnionej udostępniającej dostęp do szafy, w której znajdują się hasła,
- imię i nazwisko oraz stanowisko osoby, która pobiera nazwy użytkowników i hasła,
- krótki opis sytuacji, która zmusiła do awaryjnego wykorzystania haseł.

O konieczności i okolicznościach awaryjnego użycia nazw i haseł musi niezwłocznie zostać powiadomiony administrator bezpieczeństwa informacji.

7. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu

(§ 5 pkt 3 rozporządzenia)

Rozpoczęcie pracy w systemie

Przed rozpoczęciem pracy, w trakcie rozpoczynania pracy z systemem informatycznym oraz w trakcie pracy każdy pracownik obowiązany jest do zwrócenia bacznej uwagi, czy nie wystąpiły symptomy mogące świadczyć o naruszeniu ochrony danych osobowych. Szczegółowy opis takich symptomów oraz sposób postępowania w przypadku ich wykrycia został opisany w dokumencie „Polityka bezpieczeństwa".

Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione oraz ogólne stwierdzenie poprawności działania systemu.

Maksymalna ilość prób wprowadzenia hasła przy logowaniu się do systemu wynosi trzy. Po przekroczeniu tej liczby prób logowania system blokuje dostęp do zbioru danych na poziomie danego użytkownika. Odblokowania konta może dokonać administrator systemu informatycznego w porozumieniu z administratorem bezpieczeństwa informacji. Użytkownik informuje administratora bezpieczeństwa informacji o zablokowaniu dostępu do zbioru danych.

Zawieszenie pracy

W przypadku bezczynności użytkownika na stacji roboczej przez okres dłuższy niż 30 minut automatycznie włączany jest wygaszasz ekranu. Wygaszacze ekranu powinny być zaopatrzone w hasła zbudowane analogicznie do haseł używanych przez użytkownika przy logowaniu. Hasło powinno składać się z co najmniej 8 znaków, powinno zawierać małe i wielkie litery oraz cyfry lub znaki specjalne oraz być zmieniane nie rzadziej niż co 30 dni.

Zmianę użytkownika stacji roboczej każdorazowo musi poprzedzać wylogowanie się poprzedniego użytkownika. Niedopuszczalne jest aby dwóch lub większa ilość użytkowników wykorzystywała wspólnie jedno konto użytkownika.

W przypadku, gdy przerwa w pracy na stacji roboczej trwa dłużej niż 60 minut użytkownik obowiązany jest wylogować się z aplikacji i systemu stacji roboczej, na której pracuje oraz sprawdzić czy nie zostały pozostawione bez zamknięcia nośniki informacji zawierające dane osobowe. W pomieszczeniach, w których przetwarzane są dane i w których jednocześnie mogą przebywać osoby postronne, monitory stanowisk dostępu do danych powinny być ustawione w taki sposób, żeby uniemożliwić tym osobom wgląd w dane.

Zakończenie pracy w systemie

Przed wyłączeniem komputera należy bezwzględnie zakończyć pracę uruchomionych programów i wykonać zamknięcie systemu. Niedopuszczalne jest wyłączenie komputera przed zamknięciem oprogramowania i zakończeniem pracy w sieci komputerowej. Przed opuszczeniem stanowiska pracy należy upewnić się, że system jest wyłączony.

8. Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania (§ 5 pkt 3 rozporządzenia)

Dane, w tym dane osobowe przetwarzane w systemie informatycznym, podlegają zabezpieczeniu poprzez tworzenie kopii zapasowych. Za proces tworzenia kopii zapasowych odpowiada administrator systemu informatycznego lub osoba specjalnie do tego celu wyznaczona.

W przypadku lokalnego przetwarzania danych osobowych na stacjach roboczych użytkownicy systemu informatycznego zobowiązani są do centralnego przechowywania kopii danych, tak aby możliwe było zabezpieczenie ich dostępności poprzez wykonanie kopii zapasowych. Przez centralne przechowywanie kopii danych rozumie się cotygodniowe przegranie zbioru danych na specjalnie wydzielony do tego celu obszar dysku na serwerze. W przypadku, gdy z przyczyn technicznych jest to niemożliwe użytkownicy systemu są zobowiązani do sporządzania kopii zapasowych baz danych na nośniku wymiennym i centralne ich przechowywanie w miejscu wskazanym przez administratora bezpieczeństwa informacji.

Kopie zapasowe informacji przechowywanych w systemie informatycznym przetwarzającym dane osobowe tworzone są w następujący sposób:

- kopia zapasowa aplikacji przetwarzającej dane osobowe - pełna kopia wykonywana jest po wprowadzeniu zmian do aplikacji, kopie umieszczone są na nośnikach wymiennych, kopia przechowywana jest w zamkniętej szafie,
- kopia zapasowa danych osobowych przetwarzanych przez aplikację (pełna kopia) wykonywana jest codziennie na dysku lokalnym komputera wybranego przez administratora systemu informatycznego (komputerem tym nie może być serwer baz danych),
- raz w tygodniu, na nośniku wymiennym, tworzona jest kopia zawierająca kopie zapasową danych osobowych z każdego dnia ostatniego tygodnia, kopia ta przechowywana jest w zamkniętej szafie, w innym pomieszczeniu niż znajdują się serwery danych,
- zbiorcze (tygodniowe) kopie przechowywane są przez okres dwóch tygodni, po tym terminie stare kopie są niszczone poprzez nadpisywanie ich przez bardziej aktualne,
- raz w miesiącu, pomiędzy 1 a 5 każdego miesiąca, tworzona jest kopia zapasowa danych osobowych, która przekazywana jest do przechowywania przy zachowaniu odpowiednich zabezpieczeń, w innym budynku niż ten, w którym znajdują się serwery, przechowywane są tam kopie z 3 ostatnich miesięcy,
- kopia zapasowa danych konfiguracyjnych systemu informatycznego przetwarzającego dane osobowe, w tym uprawnień użytkowników systemu -

pełna kopia wykonywana jest raz na miesiąc, przechowywana jest w zamkniętej szafie.

Do tworzenia kopii zapasowych wykorzystywane są dedykowane do tego celu urządzenia wchodzące w skład systemu informatycznego na nośnikach wymiennych adekwatnych do rodzaju urządzenia.

W przypadku przechowywania kopii zapasowych przez okres dłuższy niż pół roku, wszystkie kopie zapasowe zbiorów danych osobowych, aplikacji przetwarzających dane osobowe oraz danych konfiguracyjnych systemu informatycznego przetwarzającego dane osobowe, których to dotyczy muszą być okresowo (co najmniej raz na pół roku) sprawdzane pod względem ich dalszej przydatności. Czynności te wykonuje administrator systemu informatycznego. Z przeprowadzonego testu administrator systemu sporządza krótką notatkę uwzględniającą datę testu oraz jego rezultat (kopię notatki przekazuje administratorowi bezpieczeństwa informacji).

- Nośniki kopii zapasowych, które zostały wycofane z użycia, jeżeli jest to możliwe, należy pozbawić zapisanych danych za pomocą specjalnego oprogramowania do bezpiecznego usuwania zapisanych danych. W przeciwnym wypadku podlegają fizycznemu zniszczeniu z wykorzystaniem metod adekwatnych do typu nośnika, w sposób uniemożliwiający odczytanie zapisanych na nich danych, protokolarnie potwierdzonym wobec ABS.

Ponadto:

- Zbiory danych przechowywane są generalnie na serwerze obsługującym system informatyczny Urzędu. Wszelkie dane przetwarzane w pamięci poszczególnych stacji roboczych oraz komputerów przenośnych są niezwłocznie umieszczane w odpowiednich, przydzielonych dla danego użytkownika przez Administratora Systemów Informatycznych miejscach na serwerze lub innych wskazanych i określonych lokalizacjach.
- Zakazuje się przetwarzania danych, w tym danych osobowych na zewnętrznych nośnikach magnetycznych, optycznych i innych oraz ich przesyłania pocztą elektroniczną bez ich uprzedniego zaszyfrowania.
- Zabrania się przetwarzania całych baz danych na nośnikach, o których mowa w ust.2.
- W przypadku posługiwania się nośnikami danych pochodzącymi od podmiotu zewnętrznego, użytkownik jest zobowiązany do sprawdzenia go programem antywirusowym oraz oznakowania.
- Nośniki danych typu pendrive, zewnętrzne dyski twarde musza być spisane, wyraźnie oznakowane oraz stosowane z systemem szyfrowania danych sprzętowo lub programowo oraz posiadać system indywidualnych haseł

niezbędnych do odczytu i zapisu danych. Administrator Systemów informatycznych prowadzi ewidencję nośników przenośnych użytkowanych w systemie informatycznym urzędu oraz jednoznacznie je przypisuje personelowi.

- Nośniki magnetyczne raz użyte do przetwarzania danych osobowych mogą być wykorzystywane do innych celów, tylko po nadpisaniu danych w trybie kasowania formatującego przy zastosowaniu specjalistycznego oprogramowania lub demagnetyzacji. Nośniki na których nie można powtórnie zapisać informacji powinny być niszczone poprzez pocięcie, zgniecenie lub spopielenie.
- Nośniki magnetyczne z zaszyfrowanymi, jednostkowymi danymi osobowymi są – na czas ich użyteczności, przechowywane w zamkniętych na klucz szafach, a po wykorzystaniu dane na nich zawarte są trwale usuwane lub nośniki są niszczone w trybie niniejszej instrukcji.
- Kopie zapasowe programów i aktualizowane kopie systemu informatycznego urzędu przechowywane są w szafie pancernej, stojącej w innym pomieszczeniu niż serwery. Po wygaśnięciu okresu przydatności tychże kopii (zastąpieniu ich przez aktualne wersje lub zakończeniu okresu trwałości), są one trwale kasowane lub nośniki je przechowujące niszczone mechanicznie. Kopie zapasowe są ewidencjonowane przez ASI zgodnie z określonym schematem oznaczenia np.: **Data1/S/T** gdzie

  Data1 - czas utworzenia kopii

  S - oznaczenie systemu, z którego dane zostały zapisane jako kopia zapasowa

  T - typ kopii (pełny, przyrostowy, różnicowy)

Oznaczenie to jest trwale naniesione na nośnik kopii danych i wpisane do rejestru kopii zapasowych. Kopie bieżące wykonuje się na płytach CD, kasetach, streamerach lub dyskach twardych. Kopie roczne wykonujemy na płytach CD/DVD lub kasetach z finalnym okresem trwałości zapisu 5 lat.

- Kopie danych przetwarzanych na serwerze przechowywane są w zamkniętych na klucz szafach, w trybie określonym w procedurze wykonywania kopii zapasowych.
- Ochrona antywirusowa systemu informatycznego urzędu jest realizowana przez oprogramowanie antywirusowe zainstalowane na serwerach, wybranych stacjach roboczych oraz komputerach przenośnych.

- Dostęp do Internetu możliwy jest na wszystkich stacjach roboczych, specjalnie chronionych urządzeniem sprzętowym z wbudowanym programem Firewall i translacją adresów NAT oraz w ograniczonym zakresie na kilku komputerach przenośnych wraz z systemem monitoringu logów i adresów internetowych w zabezpieczonych sieciach urzędu. Zakres, technologię i sposób stosowanych zabezpieczeń określa Administrator Systemów Informatycznych.

9. Procedura sposobu, miejsca i okresu przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych (§ 5 pkt 4 rozporządzenia)

Nośniki danych zarówno w postaci elektronicznej, jak i papierowej powinny być zabezpieczone przed dostępem osób nieuprawnionych, nieautoryzowaną modyfikacją i zniszczeniem. Dane osobowe mogą być zapisywane na nośnikach przenośnych w przypadku tworzenia kopii zapasowych lub gdy istnieje konieczność przeniesienia tych danych w postaci elektronicznej, a wykorzystanie do tego celu sieci informatycznej jest nieuzasadnione, niemożliwe lub zbyt niebezpieczne.

Nośniki danych, w tym danych osobowych oraz wydruki powinny być przechowywane w zamkniętych szafach wewnątrz obszaru przeznaczonego do przetwarzania danych osobowych i nie powinny być bez uzasadnionej przyczyny wynoszone poza ten obszar. Przekazywanie nośników danych osobowych i wydruków poza gmach urzędu powinno odbywać się za wiedzą administratora bezpieczeństwa informacji.

W przypadku, gdy nośnik danych, w tym danych osobowych nie jest dłużej potrzebny, należy przeprowadzić zniszczenie nośnika lub usunięcie danych z nośnika zgodnie ze wskazówkami umieszczonymi w punkcie II.5. Jeżeli wydruk danych, w tym danych osobowych nie jest dłużej potrzebny, należy przeprowadzić zniszczenie wydruku przy użyciu niszczarki dokumentów.

W przypadku, gdy kopia zapasowa nie jest dłużej potrzebna, należy przeprowadzić jej zniszczenie lub usunięcie danych z nośnika, na którym się ona zgodnie ze wskazówkami zwartymi w „Procedurze rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu"

W przypadku dokonania brakowania dokumentów tradycyjnych lub przekazania ich do Archiwum Państwowego, należy odpowiadające im zapisy w bazach danych usunąć lub zabezpieczyć przed ich odczytaniem. Dokonanie brakowania dokumentów tradycyjnych, potwierdzone protokołem brakowania musi być skorelowane z protokołem brakowania (usunięcia) zapisów z baz danych na

serwerach, stacjach roboczych a także z bieżących i archiwalnych kopii bezpieczeństwa.

10. Procedura sposobu zabezpieczenia systemu informatycznego przed działalnością oprogramowania (§ 5 pkt 6 rozporządzenia załącznika do Rozporządzenia 1024 ROZPORZĄDZENIE MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych)

W związku z tym, że system informatyczny narażony jest na działanie oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do tego systemu konieczne jest podjęcie odpowiednich środków ochronnych.

Można wyróżnić następujące rodzaje występujących tu zagrożeń:

- nieuprawniony dostęp bezpośrednio do bazy danych,
- uszkodzenie kodu aplikacji umożliwiającej dostęp do bazy danych w taki sposób, że przetwarzane dane osobowe ulegną zafałszowaniu lub zniszczeniu,
- przechwycenie danych podczas transmisji w przypadku rozproszonego przetwarzania danych z wykorzystaniem ogólnodostępnej sieci Internet,
- przechwycenie danych z aplikacji umożliwiającej dostęp do bazy danych na stacji roboczej wykorzystywanej do przetwarzania danych osobowych przez wyspecjalizowany program szpiegowski i nielegalne przesłanie tych danych poza miejsce przetwarzania danych,
- uszkodzenie lub zafałszowanie danych osobowych przez wirus komputerowy zakłócający pracę aplikacji umożliwiającej dostęp do bazy danych na stacji roboczej wykorzystywanej do przetwarzania danych osobowych.

W celu przeciwdziałania wymienionym zagrożeniom system informatyczny musi posiadać następujące zabezpieczenia:

- fizyczne odseparowanie serwera bazy danych od sieci zewnętrznej,
- autoryzacja użytkowników przy zachowaniu odpowiedniego poziomu komplikacji haseł dostępu,
- stosowanie rygorystycznego systemu autoryzacji dostępu do wszystkich serwerów, na których znajdują się elementy aplikacji umożliwiających

przetwarzanie danych osobowych,

- stosowaniu aplikacji w postaci skompilowanej i nie umieszczenie kodu źródłowego aplikacji na powszechnie dostępnych serwerach,
- stosowanie szyfrowanej transmisji danych przy zastosowaniu odpowiedniej długości klucza szyfrującego,
- stosowanie odpowiedniej ochrony antywirusowej na stacjach roboczych wykorzystywanych do przetwarzania danych osobowych.

Potencjalnymi źródłami przedostawania się programów szpiegowskich oraz wirusów komputerowych na stacje robocze są:

- załączniki do poczty elektronicznej,
- przeglądane strony internetowe,
- pliki i aplikacje pochodzące z nośników wymiennych uruchamiane i odczytywane na stacji roboczej.

W celu zapewnienia ochrony antywirusowej administrator systemu informatycznego przetwarzającego dane osobowe lub osoba specjalnie do tego celu wyznaczona, jest odpowiedzialna za zarządzanie systemem wykrywającym i usuwającym wirusy. System antywirusowy powinien być skonfigurowany w następujący sposób:

- rezydentny monitor antywirusowy (uruchomiony w pamięci operacyjnej stacji roboczej) powinien być stale włączony,
- antywirusowy skaner ruchu internetowego powinien być stale włączony,
- monitor zapewniający ochronę przed wirusami makr w dokumentach MS Office powinien być stale włączony,
- skaner poczty elektronicznej powinien być stale włączony.

Systemy antywirusowe zainstalowane na stacjach roboczych powinny być skonfigurowane w sposób następujący:

- zablokowanie możliwości ingerencji użytkownika w ustawienia oprogramowania antywirusowego,
- możliwość centralnego uaktualnienia wzorców wirusów.

System antywirusowy powinien być aktualizowany na podstawie materiałów publikowanych przez producenta oprogramowania.

Użytkownicy systemu informatycznego zobowiązani są do następujących działań:

- skanowania zawartości dysków stacji roboczej pracującej w systemie informatycznym pod względem potencjalnie niebezpiecznych kodów -

przynajmniej 2 razy w tygodniu,
- skanowania zawartości nośników wymiennych odczytywanych na stacji roboczej pracującejw systemie informatycznym pod względem potencjalnie niebezpiecznych kodów - przy każdym odczycie,
- skanowania informacji przesyłanych do systemu informatycznego pod kątem pojawienia się niebezpiecznych kodów - na bieżąco.

W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy administrator systemu informatycznego lub inny wyznaczony pracownik powinien podjąć działania zmierzające do usunięcia zagrożenia. W szczególności działania te mogą obejmować:

- usunięcie zainfekowanych plików, o ile jest to akceptowalne ze względu na prawidłowe funkcjonowanie systemu informatycznego,
- odtworzenie plików z kopii zapasowych po uprzednim sprawdzeniu, czy dane zapisane na kopiach nie są zainfekowane,
- samodzielną ingerencję w zawartość pliku - w zależności od posiadanych kwalifikacji lub skonsultowanie się z zewnętrznymi ekspertami.

System informatyczny przetwarzający dane osobowe powinien posiadać mechanizmy pozwalające na zabezpieczenie ich przed utratą lub wystąpieniem zafałszowania w wyniku awarii zasilania lub zakłóceń w sieci zasilającej. W związku z tym system informatyczny powinien być wyposażony w co najmniej:

- filtry zabezpieczające stacje robocze przed skutkami przepięcia,
- zasilacze awaryjne serwerów baz danych, serwerów aplikacji oraz urządzeń pamięci masowej pozwalające na bezpieczne zamkniecie aplikacji przetwarzających dane osobowe w sposób umożliwiający poprawne zapisanie przetwarzanych danych.

11. Procedura sposobu realizacji wymogów *o których mowa w w/w rozporządzeniu w § 7 ust. 1 pkt 4*

System informatyczny przetwarzający dane, w tym dane osobowe musi posiadać mechanizm uwierzytelniający użytkownika, wykorzystujący identyfikator i hasło. Powinien także posiadać mechanizmy pozwalające na określenie uprawnień użytkownika do korzystania z przetwarzanych informacji (np. prawo do odczytu danych, modyfikacji istniejących danych, tworzenia nowych danych, usuwania danych).

System informatyczny przetwarzający dane osobowe musi posiadać mechanizmy pozwalające na odnotowanie faktu wykonania operacji na danych. W szczególności zapis ten powinien obejmować:

- rozpoczęcie i zakończenie pracy przez użytkownika systemu,
- operacje wykonywane na przetwarzanych danych, a w szczególności ich dodanie, modyfikację oraz usunięcie,
- przesyłanie za pośrednictwem systemu danych osobowych przetwarzanych w systemie informatycznym innym podmiotom nie będącym właścicielem ani współwłaścicielem systemu,
- nieudane próby dostępu do systemu informatycznego przetwarzającego dane osobowe oraz nieudane próby wykonania operacji na danych osobowych,
- błędy w działaniu systemu informatycznego podczas pracy danego użytkownika.

Zapis działań użytkownika uwzględnia:

- identyfikator użytkownika,
- datę i czas, w którym zdarzenie miało miejsce,
- rodzaj zdarzenia,
- określenie informacji, których zdarzenie dotyczy (identyfikatory rekordów).

W ramach możliwości technicznych system informatyczny powinien posiadać mechanizmy pozwalające na automatyczne powiadomienie administratora bezpieczeństwa informacji lub osoby przez niego uprawnionej o zaistnieniu zdarzenia krytycznego (mogącego mieć krytyczne znaczenie dla bezpieczeństwa przetwarzanych danych osobowych).

Ponadto system informatyczny powinien zapewnić zapis faktu przekazania danych, w tym danych osobowych z uwzględnieniem:

- identyfikatora osoby, której dane dotyczą
- osoby przesyłającej dane,
- odbiorcy danych,
- zakresu przekazanych danych osobowych,
- daty operacji,
- sposobu przekazania danych.

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

(§ 5 pkt 8 rozporządzenia)

Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe muszą uwzględniać wymagany poziom zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych.

Prace serwisowe na terenie urzędu prowadzone w tym zakresie mogą być wykonywane wyłącznie przez pracowników urzędu lub przez upoważnionych przedstawicieli wykonawców zewnętrznych znajdujących się w towarzystwie pracowników urzędu.

Przed rozpoczęciem prac serwisowych przez osoby spoza Urzędu Miejskiego w Pieszycach, a nie będące pracownikami urzędu, konieczne jest potwierdzenie tożsamości serwisantów.

Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane, w tym dane osobowe, przeznaczone do:

- likwidacji — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
- przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
- naprawy — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

Wszelkie prace serwisowe prowadzone na sprzęcie urzędu w jego siedzibie lub w siedzibie serwisu, musi być potwierdzone protokołem opisującym czas, datę rozpoczęcia i zakończenia prac, zakres prac oraz osoby prowadzące prace.

W przypadku prowadzenia prac w trybie zdalnym musi być sporządzony protokół zawierający informacje o czasie trwania prac, ich zakresie, osobie prowadzącej serwis, osobie udostępniającej zdalny dostęp.

Procedura naprawy urządzeń komputerowych z chronionymi danymi w tym z danymi osobowymi

1. Wszelkie naprawy urządzeń komputerowych oraz zmiany w systemie informatycznym Urzędu przeprowadzane są – o ile to możliwe – przez Informatyka Urzędu .
2. Naprawy i zmiany w systemie informatycznym Urzędu Miejskiego w Pieszycach przeprowadzane przez serwisanta nie będącego pracownikiem Urzędu odbywają się pod nadzorem Administratora Systemów Informatycznych – w siedzibie Urzędu lub poza siedzibą Urzędu , po uprzednim nieodwracalnym nadpisaniu danych w nich przetwarzanych lub pod warunkiem sporządzenia umowy powierzenia przetwarzania danych, zgodnie z zatwierdzonym formularzem.
3. Jeśli nośnik danych (dysk, dyskietka, płyta lub inne) zostanie uszkodzony i nie można go odczytać ani usunąć z niego danych, należy go zniszczyć mechanicznie.

13. Procedura postępowania w przypadku stwierdzenia naruszenia bezpieczeństwa systemu informatycznego.

1. Użytkownik zobowiązany jest powiadomić Administratora Systemów Informatycznych lub uprzednio wskazanego przez niego pracownika służb informatycznych Urzędu o każdym naruszeniu lub podejrzeniu naruszenia bezpieczeństwa systemu, a w szczególności o:
   - naruszeniu identyfikatora i hasła (system nie reaguje na hasło lub je ignoruje bądź można przetwarzać dane bez wprowadzenia hasła),
   - częściowym lub całkowitym braku danych,
   - braku dostępu do właściwej aplikacji lub zmianie zakresu wyznaczonego dostępu do zasobów serwera,
   - wykryciu wirusa komputerowego,
   - zauważeniu elektronicznych śladów próby włamania do systemu informatycznego Urzędu,
   - podejrzeniu kradzieży sprzętu komputerowego lub dokumentów zawierających dane osobowe,
   - zmianie położenia sprzętu komputerowego,
   - zauważeniu śladów usiłowania lub dokonania włamania do pomieszczeń lub zamykanych szaf,
2. Do czasu przybycia na miejsce Administratora Systemów Informatycznych należy:
   - niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego zdarzenia, o ile istnieje taka możliwość,
   - następnie uwzględnić w działaniu również ustalenie jego przyczyn i sprawców,

- rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
- zaniechać – o ile to możliwe – dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,
- zastosować się do instrukcji i regulaminów lub dokumentacji aplikacji, jeśli odnoszą się one do zaistniałego przypadku,
- udokumentować w formie dokumentacji urzędowej wstępnie zaistniałe naruszenie,
- nie opuszczać bez uzasadnionej przyczyny miejsca zdarzenia do czasu przybycia Administratora Systemów Informatycznych.

3. Administrator Systemów Informatycznych po otrzymaniu zawiadomienia, o którym mowa w ust.1, powinien niezwłocznie:
   - przeprowadzić postępowanie wyjaśniające, w celu ustalenia okoliczności naruszenia ochrony danych osobowych,
   - podjąć działania chroniące system przed ponownym naruszeniem,
   - w przypadku stwierdzenia faktycznego naruszenia bezpieczeństwa systemu, sporządzić raport naruszenia bezpieczeństwa systemu informatycznego Urzędu Miejskiego w Pieszycach (wg zatwierdzonego wzoru), a następnie niezwłocznie przekazać go do Urzędu Miejskiego w Pieszycach. W dalszym trybie postępowania należy, powiadomić właściwe organy oraz podjąć inne, szczególne czynności zapewniające bezpieczeństwo systemu informatycznego Urzędu , bądź podjąć środki ochrony fizycznej. Decyzję podejmuje Burmistrz Miasta Pieszyce po zapoznaniu się z otrzymanym od Administratora Systemów Informatycznych raportem o zaistniałym incydencie.
4. Administrator Systemów Informatycznych jest zobowiązany do informowania ADO i ABI o awariach systemu informatycznego Urzędu, zauważonych przypadkach naruszenia niniejszej instrukcji przez użytkowników danych, w szczególności o przypadkach posługiwania się przez użytkowników nieautoryzowanymi programami, nieprzestrzegania zasad używania programów antywirusowych, niewłaściwego wykorzystania sprzętu komputerowego lub przetwarzania danych w sposób niezgodny z procedurami ochrony danych osobowych.
5. Administrator Systemów Informatycznych składa raz w roku Administratorowi Danych Osobowych kompleksową analizę zarządzania systemem informatycznym Urzędu Miejskiego w Pieszycach oraz założenia strategii i polityki bezpieczeństwa.