Załącznik nr 2
do Zarządzenia nr 118/2011
Burmistrza Miasta Nowe Miasto Lub.
z dnia 28 lipca 2011r.

INSTRUKCJA

zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

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

Nadawanie uprawnień.

1. Bezpośredni przełożony w uzgodnieniu z Administratorem Danych Osobowych określa wymagane dla pracownika uprawnienia do zbiorów danych osobowych.
2. Administrator danych analizuje te wymagania i podejmuje decyzję o nadaniu uprawnień we wnioskowanym zakresie, ograniczeniu nadania uprawnień bądź odmowie nadania uprawnień.
3. Polega na wprowadzeniu osoby do ewidencji osób upoważnionych do przetwarzania danych osobowych.
4. Odnotowaniu informacji o nadanych uprawnieniach do ewidencji osób upoważnionych do przetwarzania danych osobowych na podstawie pisemnego upoważnienia, który określa załącznik nr 6 do polityki bezpieczeństwa dokonuje Administrator Bezpieczeństwa Informacji.
5. Ewidencję osób upoważnionych do przetwarzania danych osobowych prowadzi Administrator Bezpieczeństwa Informacji wg wzoru, który stanowi załącznik nr 7 do polityki bezpieczeństwa.
6. Rejestracji uprawnień do przetwarzania danych osobowych w systemie informatycznym dokonuje Administrator Bezpieczeństwa Informacji, lub osoba przez niego upoważniona.

Odbieranie uprawnień.

1. Odbieranie uprawnień może odbyć się:

a) w przypadku zmiany zakresu obowiązków pracownika,
b) w przypadku zmiany stanowiska pracy,
c) w przypadku rozwiązania umowy o pracę,
d) w przypadku naruszenia zasad ochrony danych osobowych pracownika

2. Uprawnienie do przetwarzania danych osobowych odbiera Administrator Bezpieczeństwa Informacji w uzgodnieniu z bezpośrednim przełożonym pracownika.

3. Wpis informacji o odebranych uprawnieniach do ewidencji osób upoważnionych do przetwarzania danych osobowych na podstawie pisemnego upoważnienia, którego wzór stanowi załącznik nr 7 do Polityki Bezpieczeństwa, dokonuje Administrator Bezpieczeństwa Informacji.
4. Rejestracji odebrania uprawnień administrator bezpieczeństwa informacji dokonuje niezwłocznie.
5. Identyfikator byłego użytkownika nie może być powtórnie nadawany innej osobie.

II Stosowane metody i środki uwierzytelniające oraz procedury związane z ich zarządzaniem i użytkowaniem

1. W systemie informatycznym służącym do przetwarzania danych osobowych stosuje się mechanizm kontroli dostępu do tych danych poprzez wprowadzenie identyfikatora i dokonanie uwierzytelnienia za pomocą hasła.
2. Użytkownik systemu informatycznego posiada niepowtarzalny identyfikator oraz pierwsze hasło dostępu nadane przez Administratora Bezpieczeństwa Informacji.
3. Hasło dostępu użytkownika systemu informatycznego musi zawierać: co najmniej 8 znaków, małe i wielkie litery oraz cyfry lub znaki specjalne.
4. Hasło dostępu użytkownika systemu informatycznego nie może być takie samo jak jego identyfikator.
5. Użytkownik systemu informatycznego ma obowiązek zmieniać swoje hasło dostępu, nie rzadziej niż co 30 dni.
6. Użytkownikowi systemu informatycznego nie wolno zapisywać hasła dostępu na nośnikach informacji.
7. Użytkownik systemu informatycznego jest zobowiązany do utrzymania w tajemnicy hasła dostępu, również po upływie jego ważności.
8. Hasło dostępu przy wpisywaniu go w systemie informatycznym nie może być wyświetlane na ekranie monitora.
9. W przypadku kompromitacji hasła, niezwłocznie jest ono zmieniane przez użytkownika lub Administratora Bezpieczeństwa Informacji.

III Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu

1. Administrator Danych Osobowych, ustala czas pracy systemu. Na pracę poza

godzinami funkcjonowania urzędu pracownik musi posiadać pisemną zgodę kierownika komórki, administratora danych osobowych, w formie upoważnienia jednorazowego lub stałego.

2. Rozpoczęcie pracy z systemem informatycznym odbywa się poprzez wprowadzenie identyfikatora i uwierzytelnienie się poprzez hasło, które w trakcie wpisywania go do systemu informatycznego nie może być widoczne.

3. Po uwierzytelnieniu użytkownik sprawdza poprawność działania aplikacji. W przypadku stwierdzenia niezgodności w działaniu aplikacji powiadamia Administratora Bezpieczeństwa Informacji, który podejmuje odpowiednie działania.

4. Zawieszenie pracy polega na zakończeniu realizowanych transakcji - jeśli takowe są w trakcie - oraz zamknięciu aplikacji.

5. Zakończenie pracy odbywa poprzez:

a) zakończenie realizowanych transakcji - jeśli takowe są w trakcie,

b) zamknięcie aplikacji służącej do przetwarzania danych osobowych,

c) wyłączeniu komputera,

c) zabezpieczenia dokumentów i nośników przenośnych zawierających dane osobowe zgodnie z obowiązującymi zasadami,

d) zabezpieczenia obszaru, w którym przetwarzane są dane osobowe przed dostępem osób nieupoważnionych zgodnie z obowiązującymi zasadami.

IV Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.

1. Za sporządzanie i bezpieczeństwo kopii odpowiedzialny jest Administrator Bezpieczeństwa Informacji lub osoba przez niego upoważniona.

2. Kopii zapasowych danych osobowych należy dokonywać poprzez kopiowanie całej bazy danych.

3. Kopie zapasowe danych osobowych wykonuje się codziennie w dni robocze na dysku twardym serwera, a raz na miesiąc jedna kopia jest zgrywana na dwa nośniki CD lub DVD.

4. Kopie zapasowe danych osobowych dysku serwera sporządza się programem Cobian Backup, zaś na nośniki CD bądź DVD kopie sporządzane są programem Nero.

5. Kopie zapasowe danych osobowych, umieszcza się w katalogu, którego nazwą fragmentem nazwy jest data utworzenia tej kopii.

6. Nośniki CD lub DVD oznaczone są adnotacją, jakiego okresu dotyczą.
7. W czasie tworzenia kopii zapasowych danych osobowych użytkownicy systemów nie mogą pracować z systemami przetwarzającymi dane osobowe.
8. Kopie zapasowe danych osobowych może tworzyć jedynie Administrator Bezpieczeństwa Informacji, lub osoba przez niego upoważniona,
9. Kopie zapasowe programów i narzędzi programowych służących do przetwarzania danych osobowych wykonywane są przez Administratora Bezpieczeństwa Informacji lub osobę przez niego upoważnioną.
10. Kopie zapasowe programów i narzędzi programowych służących do przetwarzania danych osobowych wykonuje się programem „Nero" na 2 nośnikach CD lub DVD.
11. Kopie zapasowe programów i narzędzi programowych służących do przetwarzania danych osobowych oznacza się wg przeznaczenia, datą oraz nazwą aplikacji czy bazy.
12. Kopie zapasowe programów i narzędzi programowych służących do przetwarzania danych osobowych sporządza się niezwłocznie po instalacji nowego oprogramowania lub jego aktualizacji.
13. Kopie zapasowe sprawdza się pod kątem ich dalszej przydatności do odtworzenia danych poprzez weryfikację w systemie służącym do ich sporządzania.

V Sposób, miejsce i okres przechowywania kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

1. Kopie zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania przechowywane są w pojemniku w szafie metalowej w pomieszczeniu biura nr 5.
2. Pomieszczenie, o którym mowa w pkt. 1 jest wyposażone w następujące zabezpieczenia:
a) drzwi stalowe typu kasy pancernej wyposażone w skomplikowany system zamkowy zamykany na dwa klucze,
b) posiada okratowane okno, które zabezpieczone jest przed obserwacją z zewnątrz poprzez wmontowaną okiennicę obitą blachą,
3. Kopie zapasowe danych osobowych składowane na dysku serwera, zabezpieczone są konsolą serwera, zabezpieczoną hasłem.

4. Kopie zapasowe zbiorów danych przechowywane są przez okres ich przydatności, o ile odrębne przepisy nie stanowią inaczej. Po upływie okresu przydatności kopie usuwa się, a w przypadku nośników CD lub DVD niszczy fizycznie.
5. Kopie zapasowe programów i narzędzi programowych służących do przetwarzania danych osobowych przechowywane są przez okres użytkowania tych programów. Po tym okresie niszczy się je fizycznie poprzez wykorzystanie niszczarki lub innego urządzenia do tego celu przeznaczonego.

VI Zabezpieczenie przed niebezpiecznym oprogramowaniem

1. Systemy informatyczne zabezpieczone są przed niebezpiecznym oprogramowaniem poprzez stosowanie programów antywirusowych i systemu wykrywania włamań-firewall.
2. Na komputerze, w którym przetwarzane są dane osobowe powinien być zainstalowany program antywirusowy, którego zadaniem jest praca w tle.
3. Należy stosować program antywirusowy, który zabezpiecza przed wirusami i innymi zagrożeniami.
4. Użytkownik systemu zobowiązany jest raz na 2 tygodnie aktualizować definicje wirusów i zagrożeń ze strony producenta oprogramowania.
5. W przypadku wykrycia obecności wirusa komputerowego lub innego zagrożenia należy niezwłocznie powiadomić Administratora Bezpieczeństwa Informacji, który podejmuje odpowiednie działania.
6. System wykrywania włamań oparty jest na rozwiązaniu sprzętowym, który ma za zadanie uwierzytelnianie źródła przychodzących pakietów oraz filtrowania pakietów w oparciu o adres IP i numer portu.
7. System wykrywania włamań podłączony jest do sieci komputerowej LAN na styku jej połączenia z siecią WAN.
8. Ruch pakietów, który przepuszcza firewall jest określony przez Administratora Bezpieczeństwa Informacji lub osobę przez niego upoważnioną.

VII Sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać

urządzenia i systemy informatyczne służące do przetwarzania danych osobowych:

1. Systemy informatyczne służące do przetwarzania danych osobowych spełniają wymogi § 7 ust. 1 pkt 4. cyt. rozporządzenia
2. W przypadku udostępnienia danych osobowych należy ten fakt odnotować w postaci notatki, która musi uwzględniać informacje: komu przekazujemy dane (np. firmie której eksploatujemy oprogramowanie), w jakim celu (np. naprawa struktury danych) i kiedy, (data).

VIII Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do ich przetwarzania.

1. Przeglądu i konserwacji dokonuje Administrator Bezpieczeństwa Informacji, lub osoba przez niego upoważniona.
2. W przypadku przekazania do naprawy komputera z dyskiem lub innym nośnikiem danych osobowych, należy nośnik zdemontować, zabezpieczyć dostęp hasłem lub dokonać naprawy w obecności osoby upoważnionej przez administratora danych, natomiast w przypadku przekazania nośnika innemu podmiotowi dane muszą zostać nieodwracalnie skasowane.
3. Zabronione jest dokonywanie napraw sprzętu komputerowego samodzielnie przez pracowników urzędu.
4. Nośniki informacji przeznaczone do likwidacji zawierające dane osobowe muszą zostać pozbawione przez Administratora Bezpieczeństwa Informacji lub osobę przez niego upoważnioną zapisu tych danych, w sposób uniemożliwiający ich odczytanie.
5. Nośniki informacji przeznaczone do przekazania podmiotowi nieuprawnionemu do przetwarzania danych zawierające dane osobowe, pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie.

Zabrania się:

1) udostępniania stanowisk roboczych oraz istniejących na nich danych (w postaci elektronicznej jak i wydruków) osobom nieupoważnionym,

2) wykorzystywania sieci komputerowej w celach innych niż służbowych,

3) samowolnego instalowania i używania programów komputerowych (posiadających lub nie posiadających licencji),

4) trwałego lub czasowego kopiowania programów komputerowych w całości lub w części jakimikolwiek środkami i w jakiejkolwiek formie,

5) publicznego rozpowszechniania programów komputerowych lub ich kopii,

6) przenoszenia programów komputerowych z własnego stanowiska roboczego na inne stanowisko,

7) udostępniania osobom postronnym programów komputerowych i danych przez możliwość dostępu do zasobów sieci wewnętrznej lub Internetu,

8) wykorzystywania oprogramowania lub materiałów ściąganych z Internetu do masowego rozpowszechniania bez wyraźnego upoważnienia Administratora Bezpieczeństwa Informacji,

9) używania prywatnych skrzynek mailowych działających na innych serwerach niż urzędowy bez uzgodnienia z Administratorem Bezpieczeństwa Informacji,

10) uruchamiania programów otrzymanych pocztą elektroniczną oraz odczytywania listów o wątpliwej treści,

11) kopiowania całości lub części baz danych zawierających dane osobowe na jakichkolwiek nośnikach bez zgody Administratora Danych Osobowych.