Tychy, 01.08.2005 r.

ZAŁĄCZNIK NR 2

INSTRUKCJA ZARZĄDZANIA

INSTRUKCJA OKREŚLAJĄCA SPOSÓB ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Podstawa prawna

„Instrukcja określająca sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych", zwana dalej „**Instrukcją**", stanowi wykonanie obowiązku, o którym mowa w § 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. z 2004 r. Nr 100, poz. 1024), zwanego dalej „rozporządzeniem".

2. Zakres stosowania

Instrukcja określa zasady zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, a w szczególności: sposób nadawania uprawnień użytkownikowi, sposób przydziału haseł i zasady korzystania z nich, procedury rozpoczęcia, zawieszenia i zakończenie pracy, obowiązki użytkownika, metodę i częstotliwość tworzenia kopii, zasady sprawdzania obecności wirusów komputerowych oraz dokonywania przeglądów i konserwacji systemu.

3. Strefa bezpieczeństwa

Wszystkie pomieszczenia stanowiące obszar przetwarzania danych osobowych, (pomieszczenia, w których przetwarzane są dane) wyposażone są w zamknięcia. W czasie, gdy nie znajdują się w nich osoby upoważnione pomieszczenia są zamykane w

sposób uniemożliwiający wstęp osobom nieupoważnionym. Osoby nieupoważnione mogą przebywać w obszarze przetwarzania danych tylko za zgodą **Administratora Danych Osobowych** lub w obecności osób upoważnionych.

4. Nadawanie uprawnień użytkownikowi

4.1. Uprawnienia w systemie informatycznym są nadawane na podstawie upoważnienia administratora danych.

4.2. Uzyskanie uprawnień następuje na dwóch poziomach:

a) zarejestrowania w sieci komputerowej (założenie konta),
b) nadanie określonych uprawnień dostępu do systemów aplikacyjnych.

4.3. Obowiązuje następująca procedura przyznania uprawnień:

a) o nadanie uprawnień użytkownikowi zwraca się do swojego przełożonego
b) decyzję w zakresie uprawnień podejmuje osoba działająca w imieniu Administratora Danych Osobowych na podstawie wniosku o nadanie upoważnienia do przetwarzania danych osobowych

4.4. Na podstawie decyzji o nadaniu uprawnień administrator systemu nadaje uprawnienia w systemie informatycznym,

4.5 Uprawnienia użytkowników są rejestrowane w systemie informatycznym,. Wszystkie wydane upoważnienia składane w formie pisemnej do Administrator Bezpieczeństwa Informacji są archiwizowane i przechowywane.

4.6 W przypadku zmiany zakresu upoważnienia procedurę określoną w punktach 4.1-4.5 stosuje się odpowiednio

4.7. Stosuje się następującą procedurę wyrejestrowania użytkownika:

1) Bezpośredni przełożony osoby upoważnionej lub dział kadr zawiadamia Administratora Bezpieczeństwa Informacji o konieczności wyrejestrowania użytkownika na postawie wniosku o odwołanie przetwarzania danych osobowych.
2) Administrator Bezpieczeństwa Informacji wydaje administratorowi systemu polecenie wyrejestrowania użytkownika oraz odnotowuje fakt ustania upoważnienia w ewidencji osób upoważnionych.

5. Sposób uwierzytelniania użytkownika i zasady korzystania z haseł

5.1. Każdorazowe uwierzytelnienie użytkownika w systemie następuje po podaniu własnego identyfikatora i hasła. Dodatkowego uwierzytelnienia wymaga dostęp do aplikacji.

5.2. Unikalny identyfikator jest nadawany użytkownikowi podczas rejestracji w systemie informatycznym i pozostaje niezmienny przez cały okres rejestracji.

5.3 Zasady dotyczące identyfikatora:

a) .....
b) .....
c)

5.4 Używanie hasła jest obowiązkowe dla każdego użytkownika, posiadającego identyfikator w systemie.

5.4. W ..... obowiązują następujące zasady korzystania z haseł:

a) .....
b) .....
c) .....

.

5.5. Prawidłowe wykonywanie obowiązków związanych z korzystaniem użytkowników z haseł nadzoruje Administrator Bezpieczeństwa Informacji. Nadzór ten w szczególności polega na obserwacji (monitorowaniu) funkcjonowania mechanizmu uwierzytelniania i przywracania stanu prawidłowego w przypadku nieprawidłowości.

6. Rozpoczęcie, zawieszenie i zakończenie pracy

6.1. Przed przystąpieniem do pracy w systemie informatycznym użytkownik zobowiązany jest sprawdzić urządzenie komputerowe i stanowisko pracy ze zwróceniem uwagi, czy nie zaszły okoliczności wskazujące na naruszenie ochrony danych osobowych.

6.2. Użytkownik rozpoczyna pracę w systemie informatycznym od następujących czynności:

1) włączenia komputera,
2) uwierzytelnienia się („zalogowania” w systemie) za pomocą identyfikatora i hasła,
3) uwierzytelnienie się w systemie aplikacyjnym.

6.3. Niedopuszczalne jest uwierzytelnianie się na hasło i identyfikator innego użytkownika lub praca w systemie informatycznym na koncie innego użytkownika.

6.4. Zawieszenie i zakończenie pracy użytkownika w systemie następuje po „wylogowaniu się” z systemu. Po zakończeniu pracy użytkownik zabezpiecza swoje stanowisko pracy, w szczególności dyskietki, dokumenty i wydruki zawierające dane osobowe, przed dostępem osób nieupoważnionych.

6.5. W przypadku dłuższego opuszczenia stanowiska pracy (zawieszenie pracy) użytkownik zobowiązany jest „wylogować się” lub zaktywizować wygaszacz ekranu z opcją ponownego „logowania” się do systemu.

6.6. W przypadku wystąpienia nieprawidłowości w mechanizmie uwierzytelniania („logowaniu się” w systemie) lub stwierdzeniu innej sytuacji naruszenia ochrony danych użytkownik niezwłocznie powiadamia o nich Administratora Bezpieczeństwa Informacji.

7. Tworzenie, przechowywanie, sprawdzanie przydatności i likwidacji kopii zapasowych.

7.1. Kopie zapasowe są tworzone, przechowywane i wykorzystywane z uwzględnieniem następujących zasad:

1) kopie są wykonywana całościowo*/przyrostowo* według następującego harmonogramu:

.....

.....

.....

.....

2) kopie przechowywane są w sejfie w odrębnych pomieszczeniu wskazanym w „Polityce bezpieczeństwa”.

Opcje dodatkowe: *dziennik tworzenia kopii, opis na nośnikach, itp.*

7.2 Kopie są okresowo, przynajmniej raz w kwartale, sprawdzane przez administratora pod kątem ich przydatności do odtworzenia danych, a jeżeli ustanie ich użyteczność są niezwłocznie usuwane.

8. Sposób zabezpieczenia systemu informatycznego przed obecnością wirusów komputerowych i innego oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

8.1. Sprawdzanie obecności wirusów komputerowych dokonywane jest poprzez zainstalowanie programu, który skanuje automatycznie, bez udziału użytkownika, na obecność wirusów wszystkie pliki. Program jest zainstalowany na wszystkich serwerach i stacjach roboczych.

8.2. Po każdej naprawie i konserwacji komputera należy dokonać sprawdzenia pod kątem występowania wirusów i ponownie zainstalować program antywirusowy.

8.3. Elektroniczne nośniki informacji pochodzenia zewnętrznego podlegają sprawdzeniu programem antywirusowym przed rozpoczęciem korzystania z nich.

8.4

.....

.....

9. Sposób realizacji wymogu zapisania w systemie informacji o odbiorcach, którym dane osobowe zostały udostępnione

9.1. Informacja o odbiorcach, którym dane osobowe zostały udostępnione zapisywane są w systemie informatycznym przy danych osobowych, których to udostępnienie dotyczyło.

9.2. Informacja o odbiorcy zapisana w systemie uwzględnia datę i zakres udostępnienia, a także dokładne określenie odbiorcy danych.

9.3. Funkcjonuje odrębny system służący do odnotowywania informacji, o którym mowa w pkt 9.2: .....

Inna opcja:

Informacja o odnotowywaniu udostępnianiu danych dla wszystkich systemów następować będzie w systemie .....

10. Sposób i czas przechowywania nośników informacji, w tym kopii informatycznych i wydruków

10.1. Dokumenty papierowe zawierające dane osobowe oraz nośniki magnetyczne i optyczne z danymi osobowymi przechowywane są wyłącznie w zamykanych szafach. Obowiązek zabezpieczenia nośników spoczywa na osobie upoważnionej wykorzystującej nośnik. Jeżeli w pomieszczeniu, w którym osoba upoważniona wykonuje swoje czynności brak jest zamykanych szaf zwraca się ona do swojego bezpośredniego przełożonego w wskazanie miejsca zabezpieczenia nośnika.

10.3. Wyłącznie osoby upoważnione mogą wykonywać kopii baz danych oraz zapisywać dane na nośnikach magnetycznych i optycznych z danych osobowych.

10.4. Fizyczna likwidacja zniszczonych lub niepotrzebnych magnetycznych i optycznych nośników informatycznych z danymi osobowymi odbywa się w sposób uniemożliwiający

odczyt danych osobowych. Za prawidłowość tego procesu odpowiada Administrator Bezpieczeństwa Informacji.

11.5. Dopuszczalne jest zlecenie/powierzenie niszczenia wszelkich nośników danych osobowych wyspecjalizowanym podmiotom zewnętrznym. Podstawą przekazania danych do zniszczenia innemu podmiotowi powinna być w każdym przypadku umowa zawarta na piśmie.

12. Zasady przeglądów i konserwacji systemu

12.1. Przegląd i konserwacja zbiorów danych dokonywane są poprzez:

a) .....
b) .....
c) .....
.

12.2. Przeglądu i konserwacji dokonują
.....
.....

13. Komunikacja w sieci komputerowej

13.1. W zakresie korzystania z sieci komputerowej w ..... obowiązują następujące zasady:

1) .....
2) .....
3) .....
4) .....
5) .....

14. Obowiązki i odpowiedzialność użytkownika związane z obowiązywaniem instrukcji.

14.1. Użytkownik systemu jest zobowiązany zapoznać się z treścią niniejszej Instrukcji i potwierdzić to stosownym oświadczeniem.

14.2. Naruszenie przez pracownika ..... niniejszej Instrukcji może zostać potraktowane przez pracodawcę, jako naruszenie obowiązków pracowniczych i powodować określoną przepisami Kodeksu pracy odpowiedzialność pracownika.

14.3. Treść niniejszej Instrukcji ma charakter informacji chronionej tajemnicą pracodawcy na zasadzie art. 100 § 2 pkt 4 Kodeksu pracy.

15. Moment wejścia w życie instrukcji

Instrukcja wchodzi w życie z dniem ogłoszenia zarządzenia przez Dyrektora.