

Zarządzenie nr3/10.....
Starosty Powiatu Rybnickiego
z dnia08...lutego....2010v.

Dotyczy zmiany Zarządzenia w sprawie „Ustalenia dokumentacji przyjętych zasad polityki rachunkowości dla Starostwa Powiatowego w Rybniku”

Na podstawie art. 10 ust. 1 i 2 i art. 13 ustawy z dnia 29 września 1994 r. o rachunkowości (j.t.Dz.U. z 2009 r. Nr 152 poz. 1223 z późn.zm.) oraz zgodnie z art. 40 ustawy z 27 sierpnia 2009 r. o finansach publicznych (Dz.U. Nr 157, poz.1240) i §3, §11, §12 i §13 rozporządzenia Ministra Finansów z 28 lipca 2008 r. w sprawie szczególnych zasad rachunkowości oraz planów kont dla budżetu państwa, budżetów jednostek samorządu terytorialnego oraz niektórych jednostek sektora finansów publicznych (Dz.U. Nr 142, poz.1020 z późn.zm.) oraz art.35 ust.2 ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (j.t. Dz.U. z 2001 r. Nr 142 poz.1592 z późn.zm) zarządza się, co następuje:

§ 1

W Zarządzeniu Nr 15/2008 Starosty Powiatu Rybnickiego z dnia 12 sierpnia 2008 r. w sprawie ustalania dokumentacji przyjętych zasad polityki rachunkowości dla Starostwa Powiatowego w Rybniku Załącznik Nr 6 otrzymuje brzmienie jak Załącznik Nr 1 do niniejszego Zarządzenia.

§ 2

Wykonanie zarządzenia powierza się Skarbnikowi.

§ 3

Zarządzenie wchodzi w życie z dniem podpisania.

STAROSTA

mgr Damian Mrowiec



Załącznik Nr 1
do Zarządzenia Nr..... 3/10.....
Starosty Powiatu Rybnickiego
z dnia 08 lutego 2010r.....

Instrukcja określająca sposób zarządzania systemami informatycznymi w Wydziale Finansowo-Budżetowym Starostwa Powiatowego w Rybniku

§ 1

Zarządzanie systemami haseł

1. Dostęp do zasobów systemów odbywać się może tylko w oparciu o system haseł przydzielanych indywidualnie dla pracowników oraz użytkowników systemu.
2. Użytkownicy mają obowiązek zmieniać swoje hasło nie rzadziej niż co 30 dni.
3. Użytkownik nie może udostępniać swego hasła innym osobom
4. W przypadku utraty hasła lub istnienia podejrzenia naruszenia systemu haseł przez osoby nieuprawnione, dotychczasowy zestaw haseł musi być niezwłocznie unieważniony i zastąpiony nowym.
5. Każdy użytkownik systemu informacyjnego ma przydzielony jednorazowo niepowtarzalny identyfikator oraz okresowo zmieniane hasło dostępu.

§ 2

Zasady rejestrowania i wyrejestrowywania użytkowników

1. Podstawą do zarejestrowania użytkownika do danego systemu przetwarzania danych jest zakres czynności pracownika, w którym musi być jawnie wskazane, że dana osoba ma za zadanie pracować przy przetwarzaniu danych danego systemu w podanym zakresie. Natomiast podstawą do wyrejestrowania użytkownika z danego systemu przetwarzania danych jest nowy zakres czynności pracownika lub jego zwolnienie.
2. Identyfikatory osób, które utraciły uprawnienia dostępu do danych, należy wyrejestrować z systemu, unieważniając przekazane hasła. Identyfikator po wyrejestrowaniu użytkownika nie jest przydzielany innej osobie.
3. Osoby dopuszczone do przetwarzania danych zobowiązane są do zachowania tajemnicy (dostępu do danych i ich merytorycznej treści). Obowiązek ten istnieje również po ustaniu zatrudnienia.

§ 3

Procedury rozpoczęcia i zakończenia pracy

1. Użytkownicy przed przystąpieniem do pracy przy przetwarzaniu danych powinni zwrócić uwagę, czy nie istnieją przesłanki do tego, że zostało naruszone bezpieczeństwo systemu informatycznego. Jeżeli istnieje takie podejrzenie, należy postępować zgodnie z §7 niniejszej instrukcji.

2. Dostęp do konkretnych zasobów danych jest możliwy dopiero po podaniu właściwego identyfikatora i hasła dostępu.
3. Hasło użytkownika należy podawać do systemu w sposób dyskretny (nie literować, nie czytać na głos, wpisywać osobiście, nie pozwalać na bezpośrednią obecność drugiej osoby podczas wpisywania hasła, itp.).
4. Użytkownik ma obowiązek zamykania systemu (programu komputerowego) po zakończeniu pracy. Stanowisko komputerowe z uruchomionym systemem (programem) nie może pozostawać bez kontroli pracującego na nim użytkownika.

§ 4

Obsługa kopii bezpieczeństwa, nośników informacji oraz wydruków

1. Wydruki z systemów informatycznych oraz inne nośniki informacji muszą być zabezpieczone w sposób uniemożliwiający do nich dostęp przez osoby nieupoważnione w każdym momencie przetwarzania, a po upływie czasu ich przydatności są niszczone lub archiwizowane w zależności od kategorii archiwalnej.
2. Wydruki, maszynowe nośniki informacji (dyskietki, dyski optyczne, itp.) oraz inne dokumenty, zawierające dane przeznaczone do likwidacji, muszą być pozbawione zapisów lub w przypadku gdy jest to możliwe, muszą być trwale uszkodzone w sposób uniemożliwiający odczytanie z nich informacji.
3. Urządzenia, dyski i inne informatyczne nośniki danych (np. dyskietki) zawierające dane przed ich przekazaniem innemu podmiotowi, winny być pozbawione zawartości.

§ 5

Ochrona danych przed ich utratą z systemów informatycznych

1. Urządzenia i systemy informatyczne zasilane energią elektryczną powinny być zabezpieczone przed utratą danych, spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej poprzez zastosowanie zasilaczy awaryjnych UPS).
2. Instalacja oprogramowania może odbywać się tylko przez administratora lub pod jego nadzorem.
3. W celu ochrony przed wirusami komputerowymi, używanie nośników danych (np. dyskietki, dyski optyczne, itp.) spoza jednostki jest dopuszczalne dopiero po uprzednim sprawdzeniu ich przez administratora i upewnieniu się, że nośniki te nie zawierają wirusa.
4. W przypadku stwierdzenia obecności wirusów komputerowych w systemie należy postępować zgodnie z § 7 niniejszej instrukcji.

§ 6

Przeglądy i konserwacja systemów i zbiorów danych

1. Przeglądów i konserwacji systemów przetwarzania danych dokonuje administrator co najmniej raz w miesiącu.
2. Ocenie podlegają stan techniczny urządzeń (komputery, serwery, UPS-y, itp.), stan okablowania budynku w sieć logiczną, spójność baz danych, stan zabezpieczeń fizycznych (zamki, kraty), stan rejestrów systemów serwera lokalnej sieci komputerowej.

§ 7

Postępowanie w sytuacjach naruszenia zasad ochrony systemów informatycznych

1. Możliwe sytuacje świadczące o naruszeniu zasad ochrony danych przetwarzanych w systemie informatycznym.

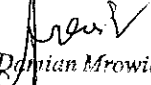
Każde domniemanie, przesłanka, fakt wskazujący na naruszenie zasad ochrony danych, a zwłaszcza stan różny od ustalonego w systemie informatycznym, w tym:

- 1) stan urządzeń (np. brak zasilania, problemy z uruchomieniem),
 - 2) stan systemu zabezpieczeń obiektu,
 - 3) stan aktywnych urządzeń sieciowych i pozostałej infrastruktury informatycznej,
 - 4) zawartość zbioru danych (np. brak lub nadmiar danych),
 - 5) ujawnione metody pracy,
 - 6) sposób działania programu (np. komunikaty informujące o błędach, brak dostępu do funkcji programu, nieprawidłowości w wykonywanych operacjach),
 - 7) przebywanie osób nieuprawnionych w obszarze przetwarzania danych,
 - 8) inne zdarzenia mogące mieć wpływ na naruszenie systemu informatycznego (np. obecność wirusów komputerowych)
- stanowi dla osoby uprawnionej do przetwarzania danych, podstawę do natychmiastowego działania.

2. Sposób postępowania.

- 1) każdej sytuacji odbiegającej od normy, a w szczególności o przesłankach naruszenia zasad ochrony danych w systemie informatycznym, opisanych w pkt. 1, należy:
 - natychmiast informować administratora lub osobę przez niego upoważnioną,
 - niezwłocznie taką sytuację zarejestrować w dzienniku pracy właściwym dla stanowisk, na którym to zdarzenie miało miejsce.
- 2) Osoba stwierdzająca naruszenie przepisów lub stan mogący mieć wpływ na bezpieczeństwo, zobowiązana jest do możliwie pełnego udokumentowania zdarzenia, celem precyzyjnego określenia przyczyn i ewentualnych skutków naruszenia obowiązujących zasad.
- 3) Stwierdzone przez administratora naruszenie zasad ochrony danych osobowych wymaga powiadomienia kierownika jednostki oraz natychmiastowej reakcji poprzez:
 - usunięcie uchybień (np. wymiana niesprawnego zasilacza awaryjnego, usunięcie wirusów komputerowych z systemu, itp.),
 - zastosowanie dodatkowych środków zabezpieczających zgromadzone dane,
 - wstrzymanie przetwarzania danych do czasu usunięcia awarii systemu informatycznego.

STAROSTA


mgr Damian Mrowiec