ZARZĄDZENIE NR 98/2014
BURMISTRZA MIASTA-GMINY STRYKÓW

z dnia 3 września 2014 r.

w sprawie wprowadzenia instrukcji określającej sposób zarządzania systemami informatycznymi w Urzędzie Miasta - Gminy Stryków

Na podstawie art. 30 ust. 2 pkt 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. 2013 r., poz. 594 z późn. zm.[1)]) i art. 10 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. 2013 r., poz. 330 z późn. zm.[2)]) zarządza się, co następuje:

§ 1. Wprowadzam do użytku wewnętrznego instrukcję określającą sposób zarządzania systemami informatycznymi określoną w załączniku do niniejszego zarządzenia.

§ 2. Nadzór nad wykonaniem zarządzenia powierzam Sekretarzowi Miasta - Gminy Stryków.

§ 3. Zarządzenie wchodzi w życie z dniem podpisania.

[1)] Zm. poz. 645 i 1318 oraz z 2014 r. poz. 379 i 1072
[2)] Zm. poz. 613.

Załącznik do Zarządzenia Nr 98/2014

Burmistrza Miasta-Gminy Stryków

z dnia 3 września 2014 r.

INSTRUKCJA OKREŚLAJĄCA SPOSÓB ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI W URZĘDZIE MIASTA - GMINY STRYKÓW

§ 1. Zarządzenie systemami haseł

1.Osobą odpowiedzialną za sposób przydziału haseł dla użytkowników oprogramowania komputerowego, o którym mowa w niniejszym zarządzeniu, oraz częstotliwość ich zmiany jest pracownik zatrudniony na stanowisku informatyka działający w tym zakresie w porozumieniu z głównym księgowym jednostki.

2. Każdy użytkownik systemu informatycznego ma przydzielony jednorazowo niepowtarzalny identyfikator oraz okresowo zmieniane hasło dostępu.

3. Dostęp do zasobów obsługiwanych przez systemy informatyczne może odbywać się tylko na podstawie systemu haseł przydzielonych indywidualnie każdemu z pracowników oraz użytkowników systemu informatycznego.

4. Zapewnione jest generowanie haseł w cyklu miesięcznym; użytkownicy systemów informatycznych mają obowiązek zmieniać swoje hasło nie rzadziej niż co 30 dni.

5. Użytkownik nie może udostępniać swego hasła innym osobom.

6. Przekazywanie haseł odbywa się w sposób poufny i nie może ono być zapisywane w miejscu pozwalającym na dostęp osób nieupoważnionych.

7. W przypadku utraty hasła lub istnienia podejrzenia naruszenia systemu haseł przez osoby nieuprawnione dotychczasowy zestaw haseł musi być niezwłocznie unieważniony i zastąpiony nowym.

§ 2. Zasady rejestrowania i wyrejestrowania użytkowników

1. Osobą odpowiedzialną za rejestrowanie i wyrejestrowanie użytkowników systemów informatycznych w Urzędzie Miasta - Gminy Stryków jest pracownik zatrudniony na stanowisku informatyka.

2. Podstawą do zarejestrowania użytkownika w danym systemie informatycznym służącym przetwarzaniu danych jest zakres czynności pracownika, natomiast podstawą do wyrejestrowania użytkownika z danego systemu przetwarzania danych jest nowy zakres czynności pracownika lub ustanie zatrudnienia.

3. Administrator rejestruje oraz wyrejestrowuje użytkowników z danego systemu informatycznego, prowadzi ewidencję osób zatrudnionych przy przetwarzaniu danych, archiwizując identyfikator, imię i nazwisko użytkownika.

4. Identyfikatory osób, które utraciły uprawnienia dostępu do danych, należy wyrejestrować z systemu, unieważniając przekazane hasła; identyfikator po wyrejestrowaniu użytkownika nie jest przydzielany innej osobie.

5. 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 dane zostały naruszone; jeżeli istnieje takie podejrzenie, należy zastosować się do instrukcji postępowania w sytuacji naruszenia zasada ochrony systemów informatycznych, o której mowa w § 8.

2. Dostęp do zasobów obsługiwanych przez systemy informatyczne możliwy jest dopiero po podaniu właściwego identyfikatora i hasła dostępu lub programu.

3. Hasło dostępu użytkownika do systemu informatycznego należy podawać 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 informatycznego po zakończeniu pracy; stanowisko komputerowe z uruchomionym systemem informatycznym nie może pozostawać bez kontroli pracującego na nim użytkownika.

5. Pomieszczenia, w których znajdują się urządzenia służące do przetwarzania danych oraz wydruki lub inne nośniki zawierające dane, pod nieobecność personelu muszą być zamknięte.

§ 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, informatyczne nośniki danych (dyski optyczne itp) oraz inne dokumenty zawierające dane przeznaczone do likwidacji muszą być pozbawione zapisów lub w sytuacji gdy jest to możliwe - muszą być trwałe uszkodzone w sposób uniemożliwiający odczytanie z nich jakichkolwiek informacji.

3. Urządzenia, dyski i inne informatyczne nośniki danych (np. dyskietki) zawierające dane, przed ich przekazaniem innemu podmiotowi, powinny być pozbawione zawartości; naprawa wymienionych urządzeń zawierających dane, jeżeli nie można danych usunąć, powinna być wykonywana pod nadzorem osoby upoważnionej.

4. Pracownik zatrudniony na stanowisku informatyka wykonuje raz na 2 tygodnie podwójną kopię wszystkich danych na dyskach optycznych, prowadzi rejestr (ewidencję) tych kopii i przechowuje je w pomieszczeniu zabezpieczonym; kopie te mają kategorie "A„ a tak tworzone kopie, ze względu na częstotliwość ich tworzenia, spełniają podwójną rolę: kopii bezpieczeństwa oraz kopii archiwalnych.

5. Pracownik zatrudniony na stanowisku informatyka przechowuje pięć ostatnich kopii zapasowych w dwóch odrębnych budynkach.

6. Kopie zapasowe wykonane na dzień 1 lipca i 31 grudnia każdego roku przechowywane są przez okres 5 lat w dwóch odrębnych budynkach.

§ 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 (zasilacze awaryjne UPS).

2. Włamanie do pomieszczeń, w których przetwarza się dane, powinno być uniemożliwione poprzez monitoring i detektor ruchu.

3. Instalacja oprogramowania może odbywać się tylko przez pracownika zatrudnionego na stanowisku informatyka.

4. W przypadku stwierdzenia obecności wirusów komputerowych w systemie należy zastosować się do instrukcji postępowania w sytuacjach naruszenia zasad ochrony systemów informatycznych, o której mowa w § 8.

§ 6. Sposób komunikacji w zakresie sieci komputerowej

1. Dopuszcza się łączenie z siecią Internetu i używanie poczty elektronicznej tylko na zestawach komputerowych.

2. Przesyłanie danych na nośnikach zewnętrznych (np. dyski optyczne, wydruki) na „zewnątrz" jednostki może odbywać się tylko w formie przesyłki poleconej; dopuszcza się również przekazywanie danych w jawnej formie za pośrednictwem Internetu, przy zachowaniu obowiązujących zasad bezpieczeństwa.

§ 7. Przeglądy i konserwacja systemów i zbiorów danych

1. Przeglądów i konserwacji systemów przetwarzania danych dokonuje administrator bezpieczeństwa informacji, co najmniej raz na 3 miesiące.

2. Ocenie podlegają: stan techniczny urządzeń (komputery, serwery, UPS-y itp.), stan okablowania budynku w sieć logiczną, spójność baz danych, stan zabezpieczeń fizycznych (m.in. zamki, kraty), stan rejestrów

systemów serwera lokalnej sieci komputerowej.

§ 8. Postępowanie w sytuacjach naruszenia zasad ochrony systemów informatycznych

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

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

a) stan urządzeń (np. brak zasilania, problemy z uruchomieniem),

b) stan systemu zabezpieczeń obiektu,

c) stan aktywnych urządzeń sieciowych i pozostałej infrastruktury informatycznej,

d) zawartość zbioru danych (np. brak lub nadmiar danych),

e) ujawnione niedopuszczalne metody pracy,

f) sposób działania programu (np. komunikaty informujące o błędach, brak dostępu do funkcji programu, nieprawidłowości w wykonywanych operacjach),

g) przebywanie osób nieuprawnionych w obszarze przetwarzania danych,

h) 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) o każdej sytuacji odbiegającej od normy, a w szczególności o przesłankach naruszenia zasad ochrony danych w systemie informatycznym, opisanych w ust. 1, należy:

a) natychmiast informować pracownika zatrudnionego na stanowisku informatyk lub osobę przez niego upoważnioną;

2) osoba stwierdzająca naruszenie przepisów lub stanu mogącego mieć wpływ na bezpieczeństwo zobowiązania jest do możliwie pełnego udokumentowania zdarzenia, w celu precyzyjnego określenia przyczyn i ewentualnych skutków naruszenia obowiązujących zasad;

3) stwierdzone przez pracownika zatrudnionego na stanowisku informatyka lub osobę przez niego upoważnioną naruszenie zasad ochrony danych osobowych wymaga powiadomienia kierownika jednostki oraz natychmiastowej reakcji poprzez:

a) usunięcie uchybień (np. wymiana niesprawnego zasilacza awaryjnego, usunięcie wirusów komputerowych z systemu),

b) zastosowanie dodatkowych środków zabezpieczających zgromadzone dane,

c) wstrzymanie przetwarzania danych do czasu usunięcia awarii systemu informatycznego.