Załącznik Nr 8
do Zarządzenia Nr 253/18
Starosty Świeckiego
z dnia 29 czerwca 2018 r.
w sprawie Polityki Rachunkowości
Starostwa Powiatowego w Świeciu

Instrukcja określająca
sposób zarządzania systemami informatycznymi
w Wydziale Finansowym Starostwa Powiatowego w Świeciu

Zarządzanie systemami haseł.

§ 1.1 Każdy użytkownik systemu informatycznego ma przydzielony jednorazowo niepowtarzalny identyfikator oraz okresowo zmieniane hasło dostępu (przynajmniej raz na miesiąc).

2. Dostęp do zasobów systemów odbywać się może tylko w oparciu o system haseł przydzielanych indywidualnie dla użytkowników systemu.

3. Osobą odpowiedzialną za sposób przydziału haseł dla użytkowników oraz częstotliwość ich zmiany jest główny księgowy i skarbnik w porozumieniu z informatykiem Starostwa Powiatowego w Świeciu.

4. Użytkownik nie może udostępniać swego hasła innym osobom.

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

Zasady rejestrowania i wyrejestrowywania użytkowników.

§ 2. 1. Osobą odpowiedzialną za rejestrowanie i wyrejestrowywanie użytkowników w jednostce jest główny księgowy i skarbnik w porozumieniu z informatykiem Starostwa Powiatowego w Świeciu.

2. 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.

3. Informatyk na wniosek głównego księgowego lub skarbnika rejestruje oraz wyrejestrowuje użytkowników w systemie komputerowym, używanym w Wydziale Finansowym.

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.

Procedury rozpoczęcia i zakończenia pracy.

§ 3. 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 postępować zgodnie z „Instrukcją postępowania w sytuacji naruszenia zasad ochrony systemów informatycznych zawartych w „Polityce Bezpieczeństwa Systemów informatycznych".

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

Obsługa kopii bezpieczeństwa, nośników informacji oraz wydruków.

§ 4. 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 (np. 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, zawierające dane przed ich przekazaniem innemu podmiotowi, winny być pozbawione zawartości. Naprawa wymienionych urządzeń zawierających dane, jeżeli nie można danych usunąć, winna być wykonywana pod nadzorem osoby upoważnionej (informatyka).
4. Za wykonanie na serwerze, przynajmniej raz dziennie kopii wszystkich danych zawartych w systemie finansowym Finanse, Wyposażenie, Kadry, Płace, Przelewy, Zlecone, Kasa, Magazyn odpowiedzialny jest informatyk. Tak tworzone kopie, ze względu na częstotliwość ich tworzenia, spełniają podwójną rolę: kopii bezpieczeństwa oraz kopii archiwalnych.

Ochrona danych przed ich utratą z systemów informatycznych.

§ 5. 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 zabezpieczenie okien i drzwi wejściowych (urządzenie alarmowe).
3. Instalacja oprogramowania może odbywać się tylko przez informatyka Starostwa Powiatowego w Świeciu.
4. W celu ochrony przed wirusami komputerowymi, używanie nośników danych (np. dyski optyczne, itp.) spoza jednostki jest dopuszczalne dopiero po uprzednim sprawdzeniu ich przez administratora i upewnieniu się, że nośniki te nie są „zarażone" wirusem.
5. W przypadku stwierdzenia obecności wirusów komputerowych w systemie należy postępować zgodnie z „Instrukcją postępowania w sytuacji naruszenia zasad ochrony systemów informatycznych".

Przeglądy i konserwacja systemów i zbiorów danych.

§ 6. 1. Przeglądów i konserwacji systemów przetwarzania danych dokonuje informatyk Starostwa Powiatowego w Świeciu.

2. Ocenie podlegają stan techniczny urządzeń (komputery, serwery, UPS-y, itp.), stan okablowania budynku w sieć logiczną, spójność baz danych, stan rejestrów systemów serwera lokalnej sieci komputerowej.

Postępowanie w sytuacjach naruszenia zasad ochrony systemów informatycznych.

§ 7. 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) o 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 informatyka;
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:
   a) usunięcie uchybień (np. wymiana niesprawnego zasilacza awaryjnego, usunięcie wirusów komputerowych z systemu, itp.);
   b) zastosowanie dodatkowych środków zabezpieczających zgromadzone dane;
   c) wstrzymanie przetwarzania danych do czasu usunięcia awarii systemu informatycznego.

STAROSTA

Franciszek Koszowski

.....

Starosta