Załącznik Nr 7
do Zarządzenia Nr 131/2016
Burmistrza Lipian z 30.12.2016r.

INSTRUKCJA OKREŚLAJĄCA SPOSÓB ZARZĄDZANIA SYTEMAMI INFORMATYCZNYMI – OPIS SYSTEMU OCHRONY DANYCH I ICH ZBIORÓW

§ 1. Zarządzanie systemami haseł.

1. Osobą odpowiedzialną za sposób przydziału haseł dla użytkowników oraz częstotliwość ich zmiany jest informatyk – konserwator systemów informatycznych oraz z tytułu nadzoru sekretarz oraz skarbnik.
2. Każdy użytkownik systemu informacyjnego ma przydzielony jednorazowo niepowtarzalny identyfikator oraz okresowo zmieniane hasło dostępu.
3. Dostęp do zasobów systemów odbywać się może tylko w oparciu o system haseł przydzielanych indywidualnie dla pracowników oraz użytkowników systemu.
4. Zapewnione jest generowanie haseł w cyklu miesięcznym. Użytkownicy 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 dla 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 wyrejestrowywania użytkowników.

1. Osobą odpowiedzialną za rejestrowanie i wyrejestrowywanie użytkowników w jednostce jest informatyk – konserwator systemu.
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. Administrator rejestruje oraz wyrejestrowuje użytkowników, 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.
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 na dwa zamki.

§ 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, cyfrowe nośniki informacji (pendrive, 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. pendrive) 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.
4. Administrator wykonuje dwa razy w tygodniu kopię wszystkich danych , prowadzi rejestr tych kopii oraz, po uprzednim zaplombowaniu, przekazuje je w formie depozytu do sejfu jednostki. Kopie te mają kategorię archiwalną „A". Tak tworzone dyski, ze względu na częstotliwość ich tworzenia, spełniają podwójną rolę: kopii bezpieczeństwa oraz kopii archiwalnych.

§ 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 zabezpieczenie okien i drzwi wejściowych.
3. Pomieszczenia komputerowe powinny być zabezpieczone przed pożarem.
4. Instalacja oprogramowania może odbywać się tylko przez administratora lub pod jego nadzorem.
5. W celu ochrony przed wirusami komputerowymi, używanie nośników danych (np. pendrive, dyski optyczne, itp.) spoza jednostki jest dopuszczalne dopiero po uprzednim sprawdzeniu ich przez administratora i upewnieniu się, że nośniki te nie są „zarażone" wirusem.

§ 6. Sposób komunikacji w zakresie sieci komputerowej.

1. Przesyłanie danych na nośnikach zewnętrznych (np. pendrive, wydruki) na zewnątrz jednostki może odbywać się tylko w formie przesyłki poleconej.

§ 7. Przeglądy i konserwacja systemów i zbiorów danych.

1. Przeglądów i konserwacji systemów przetwarzania danych dokonuje administrator bezpieczeństwa informacji 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.

§ 8. 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) 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 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.