Załącznik Nr 2
do Zarządzenia Nr 182/2008
Wójta Gminy Chojnice
z dnia 31.12.2008 r.

INSTRUKCJA ZARZĄDANIA SYSTEMEM INFORMATYCZNYM

§1

Zabezpieczenie obszaru przetwarzania danych osobowych.

1. Obszar, o którym mowa w Polityce Bezpieczeństwa, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.

2. Przebywanie osób, nieuprawnionych w obszarze, o którym mowa Polityce Bezpieczeństwa, jest dopuszczalne za zgodą Administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.

§2

Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym zwanym dalej systemem oraz wskazanie osoby odpowiedzialnej za te czynności.

1. Uprawnienia do przetwarzania danych osobowych nadawane są za zgodą Administratora danych na wniosek kierownika właściwej komórki organizacyjnej. Uprawnienia dotyczą zarówno danych osobowych gromadzonych w systemie informatycznym, jak również w tradycyjnych rejestrach papierowych.

2. Zgoda na pracę w systemie jest wymagana także dla użytkowników, którzy nie przetwarzają danych osobowych.

3. Wprowadza się rejestr osób zatrudnionych przy przetwarzaniu danych osobowych oraz osób pracujących w systemie.

4. Rejestr prowadzony jest przez Administratora Bezpieczeństwa Informacji w postaci elektronicznej lub papierowej.

5. Administratorem Bezpieczeństwa Informacji jest osoba powołana odpowiednim zarządzeniem kierownika jednostki.

6. Uprawnienia do zbiorów danych osobowych, odbierane są w przypadku ustania stosunku pracy lub na wniosek kierownika właściwej komórki organizacyjnej.

8. Użytkowników systemu tworzy oraz usuwa się na podstawie zgody Administratora Bezpieczeństwa Informacji.

9. Osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia.

§3

Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem.

1. Każdy użytkownik systemu dopuszczony do pracy przy przetwarzaniu danych osobowych powinien posiadać odrębny identyfikator.

2. Wprowadza się obowiązek uwierzytelnienia własnego identyfikatora poprzez podanie hasła.

3. Zmianę hasła należy dokonywać nie rzadziej niż co 30 dni.

4. Hasło składa się co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry znaki specjalne.

5. Początkowe hasło dostępu ustala się z Administratorem Bezpieczeństwa Informacji, a następnie samodzielnie zmienia przy użyciu odpowiednich narzędzi informatycznych.

6. Dane osobowe gromadzone są wyłącznie na serwerach. Zabrania się gromadzenia danych osobowych na innych nośnikach danych.

7. W uzasadnionych przypadkach, za zgodą Administratora Bezpieczeństwa Informacji, dane osobowe można przetwarzać poza serwerem.

8. Za zabezpieczenie danych osobowych przechowywanych w tradycyjnych rejestrach papierowych odpowiadają kierownicy właściwych komórek organizacyjnych.

§4

Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu.

1. Logowanie do systemu następuje po podaniu identyfikatora oraz hasła dostępu.

2. Użytkownik systemu jest odpowiedzialny za zabezpieczenie danych wyświetlanych przez system przed osobami nie mającymi uprawnień.

3. Zawieszenie pracy polega na opuszczeniu stanowiska pracy bez wylogowania się i jest dopuszczalne tylko w przypadku pozostania w pomieszczeniu.

4. Zabrania się opuszczania stanowiska pracy bez wcześniejszego wylogowania z systemu z zastrzeżeniem ust.3.

5. Zakończenie pracy polega na wylogowaniu się z systemu.

6. Administrator Bezpieczeństwa Informacji lub osoba przez niego upoważniona monitoruje logowanie oraz wylogowanie się użytkowników oraz nadzoruje zakres przetwarzanych przez nich zbiorów danych.

§5

Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.

1. Archiwizacja zbiorów danych osobowych znajdujących się na serwerze wykonywana jest 5 razy w tygodniu, a co najmniej raz w tygodniu zapisywana na zewnętrzne elektroniczne nośniki informacji.

2. Kopie danych, o których mowa w ust.1 wykonuje Administrator Bezpieczeństwa Informacji lub osoba przez niego upoważniona.

§6

Sposób, miejsce i okres przechowywania elektronicznych nośników informacji.

1. Dane o których mowa w § 5 ust.1 zapisywane są na nośniki optyczne lub dyski zewnętrzne.

2. Nośniki z danymi przechowywane są w kasie pancernej, w pomieszczeniu z okratowaniem, do której wyłączny dostęp ma Administrator Bezpieczeństwa Informacji lub osoba przez niego upoważniona.

3. Kopie danych, o których mowa w § 5 ust.1 usuwa się niezwłocznie po ustaniu ich użyteczności.

4. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:

- likwidacji — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
- przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia

się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
- naprawy — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez Administratora danych.

§7

Sposób zabezpieczenia systemu przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego.

1. System obejmuje się ochroną antywirusową polegającą na skanowaniu serwerów oraz stacji roboczych programem antywirusowym.

2. Skanowanie serwerów wykonywane jest, co najmniej raz w tygodniu przez Administratora Bezpieczeństwa Informacji lub osobę przez niego upoważnioną.

3. Skanowanie stacji roboczych wykonują ich użytkownicy.

4. Użytkownicy systemu mają również obowiązek skanowania każdego zewnętrznego elektronicznego nośnika informacji, a także plików danych pobieranych z zasobów sieci Internet oraz otrzymanych w poczcie elektronicznej.

5. Pocztę elektroniczną przychodzącą na serwer pocztowy skanuje się bezpośrednio w trakcie jej odbierania, za co odpowiedzialny jest Administrator Bezpieczeństwa Informacji lub osoba przez niego upoważniona.

6. W celu zabezpieczenia systemu przed ingerencją z zewnątrz, stosuje się urządzenia sprzętowe zabezpieczające dostęp do sieci internet (firewall).

7. Przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej serwery są chronione zasilaczami awaryjnymi - UPS.

8. Administrator Bezpieczeństwa Informacji lub osoba przez niego upoważniona monitoruje stan systemu, ruch użytkowników w sieci oraz próby ingerencji z zewnątrz w system.

§8

Informacje o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy o ochronie danych osobowych, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia.

1. Tworzy się centralną ewidencję udostępniania danych prowadzoną w formie elektronicznej lub papierowej, która w szczególności powinna zawierać co najmniej następujące pola: nazwa odbiorcy, data udostępnienia, zakres udostępnienia.

2. Ewidencję prowadzi Administrator Bezpieczeństwa Informacji.

3. Kierownicy komórek organizacyjnych są zobowiązani do zgłaszania faktu udostępniania danych Administratorowi Bezpieczeństwa Informacji, który dokonuje odpowiednich zapisów w ewidencji, o której mowa w ust.2

§9

Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

1. Przeglądy i konserwacje systemu oraz nośników informacji służących do przetwarzania danych mogą być wykonywane jedynie przez osoby posiadające upoważnienie wydane przez Administratora danych.

2. Czynności określone w ust.1 mogą być wykonywane w obecności osoby upoważnionej do przetwarzania danych osobowych.

3. Tworzy się ewidencję osób upoważnionych do wykonywania prac, o których mowa w ust.1.

4. Tworzy się ewidencję przeglądów i konserwacji, która w szczególności powinna posiadać, co najmniej następujące pola: nazwa systemu, opis procedury, zakres przeglądu, nazwisko osoby uprawnionej do wykonywania przeglądu, data wykonania przeglądu.

5. Ewidencje, o których mowa w ust. 3 i 4 prowadzi w formie elektronicznej lub papierowej Administrator Bezpieczeństwa Informacji.

§10

1. Za kontakty oraz prowadzenie korespondencji z Generalnym Inspektorem Ochrony Danych Osobowych odpowiedzialny jest Administratora Bezpieczeństwa Informacji.

2. Administrator Bezpieczeństwa Informacji nadzoruje przestrzeganie zasad ochrony danych osobowych zgromadzonych w systemie oraz w tradycyjnych rejestrach papierowych, określonych w Polityce Bezpieczeństwa Informacji oraz niniejszej instrukcji.

3. Do zadań Administratora Bezpieczeństwa Informacji należy również bieżąca aktualizacja niniejszej instrukcji.