

**ZARZĄDZENIE nr. ....3.10.2011**  
**Wójta Gminy Chełm Śląski**  
**z dnia ....16.09.2011**

W sprawie: wyznaczenia Administratora systemów oraz Inspektora Bezpieczeństwa Sieci Teleinformatycznej w Urzędzie Gminy Chełm Śląski.

Na podstawie art. 52 ust. 1 Ustawy z dnia 5 sierpnia 2010r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz.1228), Rozporządzenia Prezesa Rady Ministrów z dnia 25 lutego 1999r. w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych (Dz. U. Nr 18 poz. 162) oraz szczegółowych zaleceń Urzędu Ochrony Państwa – Biura Bezpieczeństwa Łączności i Informatyki dotyczących bezpieczeństwa teleinformatycznego z 2006r.

**Zarządzam:**

§ 1

1. Wyznaczam Pana Czesław Jochemczyk odpowiedzialnego za Funkcjonowanie Systemu Teleinformatycznego oraz za przestrzeganie zasad i wymagań bezpieczeństwa Systemu Teleinformatycznego zwanym dalej – Administratorem Systemów.
2. Zakres obowiązków i uprawnień Administratora Systemów określa załącznik Nr 1 do niniejszego zarządzenia.

§ 2

1. Wyznaczam Pana Henryk Misterek na Inspektora Bezpieczeństwa Systemu Teleinformatycznego odpowiedzialnego za bieżącą kontrolę zgodności funkcjonowania Systemu Teleinformatycznego ze szczególnymi wymaganiami bezpieczeństwa .
2. Zakres obowiązków i uprawnień Inspektora Systemu Teleinformatycznego określa załącznik Nr 2 do niniejszego zarządzenia.

§ 3

Administrator Systemów i Inspektor Bezpieczeństwa Sieci Teleinformatycznej, pozostają nadal na dotychczasowych stanowiskach..

§ 4

Zobowiązuję Kierowników Referatów, pracowników stanowisk samodzielnych, do ścisłej współpracy z Administratorem Systemów i Inspektorem Bezpieczeństwa Systemu Teleinformatycznego w zakresie bezpiecznej eksploatacji systemu teleinformatycznego do przetwarzania informacji niejawnych.

§ 5

Nadzór nad wykonaniem zarządzenia powierzam Pełnomocnikowi ds. Ochrony Informacji Niejawnych.

§ 6

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJTCZYNY  
Chem. S. Jagoda  
  
mgr inż. Stanisław Jagoda



Administrator Systemu TI - odpowiedzialny za bezpieczeństwo teleinformatyczne, zarządzanie uprawnieniami Użytkowników oraz konserwację sprzętu i oprogramowania. Do jego obowiązków należą:

- zapewnienie prawidłowej i bezpiecznej eksploatacji Systemu TI (zgodność warunków faktycznych z opisanymi w Szczegółowych Wymaganiach Bezpieczeństwa);
- konfiguracja i kontrola konfiguracji urządzeń i oprogramowania wykorzystywanego w Systemie TI;
- tworzenie Użytkowników Systemu TI (przydzielanie pierwszych haseł (które powinny być przez użytkowników zmienione na ich własne po pierwszym zalogowaniu się do systemu)) i utrzymywaniu aktualnego wykazu uprawnionych użytkowników systemu TI;
- nadzorowanie Użytkowników Systemu TI;
- zapewnienie, aby cały personel posiadający dostęp do Systemu TI posiadał stosowne dopuszczenia oraz był przeszkolony w zakresie obowiązujących przepisów dotyczących zachowania bezpieczeństwa informacji podczas ich przetwarzania w Systemie TI;
- doradzania Użytkownikom Systemu w zakresie bezpieczeństwa;
- szkolenie, doradzanie i sprawowanie nadzoru nad użytkownikami Systemu TI w zakresie korzystania z Systemu TI i jego zabezpieczeń;
- uczestnictwo w ustalaniu wymagań bezpieczeństwa Systemu TI i opracowaniu dokumentacji bezpieczeństwa Systemu TI i „Procedur Bezpiecznej Eksploatacji Systemu TI”;
- wyjaśnienie i reagowanie na incydenty naruszenia bezpieczeństwa;
- monitorowanie zmian (np.: w funkcjonowaniu mechanizmów zabezpieczeń);
- przeglądanie plików zawierających informacje o wybranych zdarzeniach w Systemie TI;
- przygotowanie i utrzymanie w ciągłej aktualności wykazu osób zapoznanych z „Procedurami Bezpiecznej Eksploatacji Systemu TI”, stanowiącego formę oświadczenia, które podpisywane jest przez wszystkich Użytkowników Systemu TI;
- informowanie Pełnomocnika ds. Ochrony Informacji Niejawnych o wszelkich wykrytych lukach, naruszeniach i zagrożeniach Systemu TI;
- proponowanie zmian mających na celu poprawę stanu bezpieczeństwa Systemu TI;
- tworzenie kopii bezpieczeństwa;
- ciągła analiza ryzyka szacunkowego Systemu TI;
- utrzymanie zgodności konfiguracji Systemu TI z dokumentacją bezpieczeństwa teleinformatycznego;
- prowadzenie Dziennika Administratora Systemu TI.



Inspektor Bezpieczeństwa TI odpowiada za:

- ustalenie wymagań bezpieczeństwa dla systemu TI i opracowanie odpowiedniej dokumentacji;
- przestrzeganie zasad ochrony informacji niejawnych w Systemie TI;
- monitorowanie stanu zabezpieczeń fizycznych, elektromagnetycznych i elektronicznych pomieszczeń, w których usytuowany jest System TI;
- kontrolowanie zgodności wykorzystywania zaimplementowanych środków ochrony z zatwierdzoną dokumentacją bezpieczeństwa Systemu TI;
- monitorowanie bezpieczeństwa teleinformatycznego;
- utrzymanie w aktualności wykazów osób mających dostęp do Systemu TI, oraz weryfikowanie prawidłowości zabezpieczeń zastosowanych w Systemie TI;
- okresowe przeglądy ryzyk i analizowanie skuteczności zabezpieczeń;
- tworzenie planów awaryjnych i organizowanie treningów w ich realizacji;
- kontrola utrzymania zgodności konfiguracji Systemu TI z dokumentacją bezpieczeństwa teleinformatycznego;
- przeprowadzenie szkoleń i podnoszenie świadomości w zakresie bezpieczeństwa;
- zaznajomienie i przestrzeganie przez Użytkowników „Procedur Bezpiecznej Eksploatacji Systemu TI”;
- przestrzeganie zasad i wymagań w zakresie oznaczania, ewidencjonowania, przechowywania i przekazywania wytworzonych dokumentów niejawnych oraz ich terminowe rozliczanie;
- wyjaśnianie i reagowanie na incydenty naruszenia bezpieczeństwa;
- analizowanie rejestru zdarzeń w Systemie TI i prawidłowe dokumentowanie i archiwizowanie zdarzeń;
- informowanie Pełnomocnika ds. Ochrony Informacji Niejawnych o wszelkich zdarzeniach związanych lub mogących mieć związek z bezpieczeństwem systemu TI;
- uczestnictwo w pracach zespołu opracowującego dokumenty SWBS i PBE;
- utrzymanie bieżącego schematu obszaru (GŚB, LŚB) podlegającego nadzorowi;
- opracowywanie instrukcji dla podległych pracowników jeżeli występują ;
- zapewnienie niszczenia w regularnych odstępach czasu niejawnych odpadów, zgodnie z obowiązującymi przepisami w tym zakresie;
- prowadzenie Dziennika Inspektora Bezpieczeństwa TI.