

**Zarządzenie Nr 1/2015  
Wójta Gminy Grzegorzew  
z dnia 11 maja 2015 roku**

***w sprawie zmiany Regulaminu Organizacyjnego Urzędu Gminy w Grzegorzewie***

Na podstawie art. 33 ust. 2 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U z 2013r. poz. 594, ze zm.) zarządzam co następuje:

W Regulaminie Organizacyjnym Urzędu Gminy w Grzegorzewie przyjętym Zarządzeniem Wójta Gminy Grzegorzew Nr 29/04 z dnia 9 września 2004r, zwanego dalej regulaminem wprowadza się następujące zmiany:

§ 1.

1. Zmienia się w całości brzmienie pkt 17 w § 37 Rozdziału VI, który otrzymuje następujące brzmienie: „Prowadzenie kancelarii niejawnego Urzędu”.
2. Zmienia się w całości brzmienie § 8 w Rozdziale III, który otrzymuje następujące brzmienie:  
„ 1. W Urzędzie funkcjonuje Pion Ochrony Informacji Niejawnych (OIN), który tworzą:
  - a) Pełnomocnik ds. Ochrony Informacji Niejawnych
  - b) Pracownik do spraw prowadzenia kancelarii niejawnego
  - c) Inspektor Bezpieczeństwa Teleinformatycznego
  - d) Administrator Systemu Teleinformatycznego
3. Zmienia się w całości brzmienie rozdziału VI § 39, który otrzymuje następującą treść:

Zadania Pionu Ochrony Informacji Niejawnych (OIN) określa się następująco:

**a) Do zadań Pełnomocnika ds. Ochrony Informacji Niejawnych w szczególności należy:**

- 1) Kierowanie Pionem Ochrony Informacji Niejawnych.
- 2) Zapewnienie ochrony informacji niejawnych, w tym ochrony fizycznej.
- 3) Kontrola ochrony informacji niejawnych oraz przestrzeganie przepisów o ochronie informacji niejawnych.
- 4) Zapewnienie ochrony systemu i sieci teleinformatycznych, w których są wytwarzane, przechowywane lub przekazywane informacje niejawne.
- 5) Opracowywanie planu ochrony informacji niejawnych w jednostce organizacyjnej i nadzorowanie jego realizacji.
- 6) Szkolenie pracowników w zakresie ochrony informacji niejawnych.

- 7) Okresowa kontrola ewidencji, materiałów i obiegu dokumentów.
- 8) Prowadzenie postępowań sprawdzających zwykłych oraz przechowywanie akt tych postępowań.
- 9) Prowadzenie stanowisk i prac zleconych oraz osób dopuszczonych do pracy na stanowiskach, z którymi wiąże się dostęp do informacji niejawnych.

**b) Do zadań pracownika do spraw prowadzenia kancelarii niejawnej należy:**

- 1) Prowadzenie kancelarii niejawnej.
- 2) Współpraca z pełnomocnikiem do spraw ochrony informacji niejawnych w zakresie szkolenia, kontroli i ochrony informacji niejawnych.
- 3) Nadzór nad wprowadzaniem zaleceń odpowiednich służb dotyczących bezpieczeństwa teleinformatycznego.
- 4) Przygotowywanie i odbieranie przesyłek poczty specjalnej.
- 5) Przechowywanie i zabezpieczanie dokumentów niejawnych.
- 6) Przekazywanie korespondencji niejawnej upoważnionym pracownikom Urzędu.
- 7) Nadzór nad opracowywaniem i przechowywaniem materiałów zastrzeżonych przez upoważnionych pracowników Urzędu.
- 8) Egzekwowanie zwrotu dokumentów zawierających informacje niejawne.
- 9) Kontrola przestrzegania właściwego oznaczania i rejestrowania dokumentów w kancelarii niejawnej.
- 10) Prowadzenie bieżącej kontroli postępowania z dokumentami zawierającymi informacje niejawne, które zostały udostępnione pracownikom.
- 11) Sprawdzanie poprawności zabezpieczania materiałów niejawnych, zamykanie i plombowanie pomieszczeń kancelarii po zakończeniu pracy.
- 12) Archiwizacja dokumentów niejawnych.

**c) Do zadań Inspektora Bezpieczeństwa Teleinformatycznego należy:**

1. Kontrola przestrzegania realizacji procedur bezpiecznej eksploatacji;
2. Organizowanie i prowadzenie szkoleń.
3. Monitorowanie zmian dotyczących mechanizmów zabezpieczeń itp.
4. Reagowanie na sygnały o incydentach w zakresie bezpieczeństwa, wyjaśnienie ich przyczyn.
5. Okresowe przeglądanie i dokumentowanie logów systemowych.
6. Przeprowadzanie okresowej analizy zagrożeń.
7. Tworzenie planów awaryjnych i organizowanie treningów w ich realizacji.
8. Opracowanie i wdrożenie dokumentów Szczególnych Wymagań Bezpieczeństwa i Procedur Bezpiecznej Eksploatacji.
9. Informowanie pełnomocnika ochrony o wszelkich zdarzeniach, związanych lub mogących mieć związek z bezpieczeństwem systemu lub sieci TI.
10. Zarządzanie materiałami (pobieranie, generowanie, ewidencjonowanie, wydawanie użytkownikom, rozliczanie).
11. Archiwizowanie dokumentów oraz niszczenie wyeksploatowanych materiałów.
12. Prowadzenie dziennika Inspektora Bezpieczeństwa Teleinformatycznego.

**d) Do zadań Administratora Systemu Teleinformatycznego należy:**

1. Przydzielanie i odbieranie kont użytkowników systemu, wraz z przydzielaniem haseł, szkolenie użytkowników.
2. Konfigurowanie urządzeń i oprogramowania.
3. Monitorowanie zmian dotyczących mechanizmów zabezpieczeń itp.
4. Przeglądanie plików zawierających informacje o wybranych zdarzeniach w systemie, tzw. logów systemowych.
5. Reagowanie na sygnały o incydentach w zakresie bezpieczeństwa i usuwanie ich skutków.
6. Prowadzenie ewidencji sprzętu, oprogramowania i nośników danych;
7. Tworzenie kopii bezpieczeństwa.
8. Udział w opracowywaniu dokumentów Szczególnych Wymagań Bezpieczeństwa i Procedur Bezpiecznej Eksploatacji.
9. Informowanie przełożonych i Inspektora Bezpieczeństwa Teleinformatycznego o wszystkich zdarzeniach związanych lub mogących mieć związek z bezpieczeństwem systemu lub sieci TI.
10. Prowadzenie dziennika administratora systemu.

§2.

Wykonanie zarządzenia powierza się Sekretarzowi Gminy.

§3.

Zarządzenie wchodzi w życie z dniem podjęcia.

WÓJT GMINY  
Bożena Dominiak