ZARZĄDZENIE NR 76/2019

Wójta Gminy Kotlin

z dnia 29 listopada 2019r.

w sprawie wyznaczenia Administratora Systemu Teleinformatycznego oraz Inspektora Bezpieczeństwa Teleinformatycznego Systemu Teleinformatycznego „STIUG Z-1" przeznaczonego do przetwarzania informacji niejawnych oznaczonych maksymalną klauzulą zastrzeżone w Urzędzie Gminy w Kotlinie

Na podstawie art. 52 ust. 1 ustawy z dnia 5 sierpnia 2010r. o ochronie informacji niejawnych (Dz. U. z 2019r. poz. 742) oraz § 13 i 14 Rozporządzenia Prezesa Rady Ministrów z dnia 20 lipca 2011r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. z 2011r. , Nr 159, poz. 948) zarządzam co następuje:

§ 1. Wyznaczam Pana Michała Kapałę na Administratora Systemu Teleinformatycznego odpowiedzialnego za funkcjonowanie Systemu Teleinformatycznego „STIUG Z-1" oraz za przestrzeganie zasad i wymagań bezpieczeństwa przewidzianych dla systemu teleinformatycznego

§ 2. Wyznaczam Pana Michała Urbaniaka na Inspektora Bezpieczeństwa Teleinformatycznego odpowiedzialnego za weryfikację i bieżącą kontrolę zgodności funkcjonowania Systemu Teleinformatycznego „STIUG Z-1" ze szczególnymi wymaganiami bezpieczeństwa oraz kontrolę przestrzegania procedur bezpiecznej eksploatacji.

§ 3. Administrator Systemu Teleinformatycznego, o którym mowa w § 1, odpowiedzialny jest za funkcjonowanie systemu teleinformatycznego oraz za przestrzeganie zasad i wymagań bezpieczeństwa przewidzianych dla systemu teleinformatycznego.

§ 4. Inspektor bezpieczeństwa teleinformatycznego, o którym mowa w § 2, odpowiedzialny jest za weryfikację i bieżącą kontrolę zgodności funkcjonowania systemu teleinformatycznego ze szczególnymi wymaganiami bezpieczeństwa oraz przestrzegania procedur bezpiecznej eksploatacji.

§ 5. Podstawowe zadania Administratora Systemu Teleinformatycznego „STIUG Z-1" w Urzędzie Gminy w Kotlinie zostały określone w załączniku nr 1 do niniejszego zarządzenia.

§ 6. Podstawowe zadania Inspektora Bezpieczeństwa Teleinformatycznego Systemu Teleinformatycznego „STIUG Z-1" w Urzędzie Gminy w Kotlinie zostały określone w załączniku nr 2 do niniejszego zarządzenia.

§ 7. Nadzór nad realizacją niniejszego zarządzenia powierza się Pełnomocnikowi ds. Ochrony Informacji Niejawnych.

§ 8. Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT

/-/ Mirosław Paterczyk

Załącznik nr 1 do Zarządzenia
Wójta Gminy Kotlin Nr 76/2019
z dnia 29 listopada 2019r.

ZAKRES OBOWIĄZKÓW
ADMINISTRATORA SYSTEMU TELEINFORMATYCZNEGO „STIUG Z-1”

1. Udział w procesie zarządzania ryzykiem w systemie TI oraz tworzeniu dokumentacji bezpieczeństwa systemu.
2. Utrzymaniu zgodności dokumentacji bezpieczeństwa z konfiguracją systemu TI.
3. Tworzenie i usuwanie kont użytkowników (na polecenie kierownika jednostki lub uprawnionego przez niego pracownika), wdrażanie uprawnień w systemie wynikających z przydzielonych praw dostępu, przydzielane pierwszych haseł.
4. Szkolenie użytkowników.
5. Konfigurowanie urządzeń i oprogramowania.
6. Monitorowanie zmian (np. w funkcjonowaniu mechanizmów zabezpieczeń).
7. Przeglądanie plików zawierających informacje o wybranych zdarzeniach w systemie logów systemowych.
8. Reagowanie na sygnały o incydentach w zakresie bezpieczeństwa i usuwanie ich skutków.
9. Prowadzenie ewidencji sprzętu, oprogramowania i nośników danych.
10. Tworzenie kopii bezpieczeństwa.
11. Informowanie przełożonych i inspektora BTI o wszelkich zdarzeniach związanych lub mogących mieć związek z bezpieczeństwem systemu TI.
12. Prowadzenie dziennika administratora.

Załącznik nr 2 do Zarządzenia
Wójta Gminy Kotlin Nr 76/2019
z dnia 29 listopada 2019r.

ZAKRES OBOWIĄZKÓW
INSPEKTORA BEZPIECZEŃSTWA TELEINFORMATYCZNEGO
SYSTEMU TELEINFORMATYCZNEGO „STIUG Z-1”

1. Udział w procesie zarządzania ryzykiem w systemie teleinformatycznym oraz tworzeniu dokumentacji.
2. Bieżąca kontrola zgodności funkcjonowania systemu TI ze szczególnymi wymaganiami bezpieczeństwa oraz przestrzegania procedur bezpiecznej eksploatacji, w ramach, której sprawdza:
    - poprawność realizacji zadań przez administratora, w szczególności właściwe zarządzanie konfiguracją oraz uprawnieniami przydzielanymi użytkownikom,
    - znajomość i przestrzeganie przez użytkowników zasad ochrony informacji niejawnych oraz procedur bezpiecznej eksploatacji w systemie TI, a w szczególności w zakresie wykorzystania urządzeń i narzędzi służących do ochrony informacji niejawnych w systemie,
    - stan zabezpieczeń systemu TI, w szczególności analizując rejestry zdarzeń systemu TI.
3. Organizowanie i prowadzenie szkoleń;
    - monitorowanie zmian (np. w funkcjonowaniu mechanizmów zabezpieczeń, aktualizacji oprogramowania itp.).
4. Reagowanie na sygnały o incydentach w zakresie bezpieczeństwa, wyjaśnianie ich przyczyn, okresowe przeglądanie i dokumentowanie logów systemowych.
5. Przeprowadzanie okresowej analizy zagrożeń.
6. Tworzenie planów awaryjnych i organizowanie treningów w ich realizacji.
7. Informowanie pełnomocnika ochrony o wszelkich zdarzeniach związanych lub mogących mieć związek z bezpieczeństwem systemu TI.
8. Prowadzenie dziennika inspektora BTI.