Zarządzenie Nr ORG.120.11.2021
Wójta Gminy Baboszewo
z dnia 2 lutego 2021 r.

w sprawie utworzenia Pionu Ochrony w Urzędzie Gminy w Baboszewie.

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t. j. Dz. U. z 2020 r., poz. 713) w związku z art.15 ust.2 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t. j. Dz. U. z 2019 r., poz. 742) zarządzam, co następuje:

§ 1

1. Tworzy się w Urzędzie Gminy w Baboszewie ,,Pion Ochrony" jako wyodrębnioną komórkę organizacyjną do spraw ochrony informacji niejawnych w składzie:

1) Pełnomocnik do spraw ochrony informacji niejawnych,

2) Kierownik kancelarii materiałów niejawnych,

3) Inspektor bezpieczeństwa teleinformatycznego.

2. Pracami Pionu Ochrony kieruje pełnomocnik do spraw ochrony informacji niejawnych.

§ 2

1. Stanowiska lub funkcje, o których mowa w § 1 mogą zajmować lub pełnić osoby posiadające:

1) obywatelstwo polskie,

2) odpowiednie poświadczenie bezpieczeństwa lub upoważnienie do dostępu do informacji niejawnych o klauzuli zastrzeżone,

3) zaświadczenie o odbytym przeszkoleniu w zakresie ochrony informacji niejawnych.

2. Szczegółowy zakres zadań osób funkcyjnych wchodzących w skład Pionu Ochrony określa załącznik nr 1 do zarządzenia.

§ 3

1. Wykonanie zarządzenia powierzam Sekretarzowi Gminy.

2. Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT

mgr inż. Bogdan Janusz Pietruszewski

Załącznik do Zarządzenia Nr ORG.120.11.2021
Wójta Gminy Baboszewo
z dnia 2 lutego 2021 r.

Do zadań pełnomocnika do spraw ochrony informacji niejawnych należy:

1. Zapewnienie ochrony informacji niejawnych, w tym stosowanie środków bezpieczeństwa fizycznego.
2. Zapewnienie ochrony systemów teleinformatycznych, w których są przetwarzane informacje niejawne.
3. Zarządzanie ryzykiem bezpieczeństwa informacji niejawnych, w szczególności szacowanie ryzyka.
4. Kontrola ochrony informacji niejawnych oraz przestrzegania przepisów o ochronie tych informacji, w szczególności okresowa (co najmniej raz na trzy lata) kontrola ewidencji, materiałów i obiegu dokumentów.
5. Opracowywanie i aktualizowanie, wymagającego akceptacji Wójta Gminy, planu ochrony informacji niejawnych, w tym w razie wprowadzenia stanu nadzwyczajnego, i nadzorowanie jego realizacji.
6. Prowadzenie szkoleń w zakresie ochrony informacji niejawnych.
7. Prowadzenie zwykłych postępowań sprawdzających oraz kontrolnych postępowań sprawdzających.
8. Prowadzenie aktualnego wykazu osób zatrudnionych w Urzędzie Gminy albo wykonujących czynności zlecone, które posiadają uprawnienia do dostępu do informacji niejawnych, oraz osób, którym odmówiono wydania poświadczenia bezpieczeństwa lub je cofnięto.
9. Przekazywanie Agencji Bezpieczeństwa Wewnętrznego danych do ewidencji osób uprawnionych do dostępu do informacji niejawnych o klauzuli ,,poufne" i wyższej, a także osób, którym odmówiono wydania poświadczenia bezpieczeństwa lub wobec których podjęto decyzję o cofnięciu poświadczenia bezpieczeństwa.
10. Opracowanie, wymagającej zatwierdzenia przez Wójta Gminy, instrukcji dotyczącej sposobu i trybu przetwarzania informacji niejawnych o klauzuli ,,zastrzeżone" w podległych komórkach organizacyjnych oraz zakresu i warunków stosowania środków bezpieczeństwa fizycznego w celu ich ochrony.
11. Opracowanie, wymagającej zatwierdzenia przez Wójta Gminy, dokumentacji określającej poziom zagrożeń związanych z nieuprawnionym dostępem do informacji niejawnych lub ich utraty.
12. Nadzór nad opracowywaniem dokumentacji bezpieczeństwa teleinformatycznego.
13. Przechowywanie Akt Postępowań Sprawdzających z uwzględnieniem przepisów ustawy o narodowym zasobie archiwalnym i archiwach oraz aktów wykonawczych wydanych na jej podstawie.

Do zadań kierownika kancelarii materiałów niejawnych należy:

1. Bezpośredni nadzór nad obiegiem materiałów niejawnych.
2. Udostępnianie i wydawanie materiałów niejawnych osobom uprawnionym, zapewniającym odpowiednie warunki do ich przechowywania.
3. Egzekwowanie zwrotu materiałów niejawnych do kancelarii.
4. Kontrola przestrzegania właściwego oznaczania i rejestrowania materiałów niejawnych w kancelarii oraz w komórkach organizacyjnych Urzędu.

Do zadań inspektora bezpieczeństwa teleinformatycznego należy:

1. Uczestniczenie w procesie zarządzania ryzykiem w systemie teleinformatycznym oraz w tworzeniu dokumentacji bezpieczeństwa systemu.
2. Bieżąca kontrola zgodności funkcjonowania systemu teleinformatycznego ze szczególnymi wymaganiami bezpieczeństwa oraz przestrzegania procedur bezpiecznej eksploatacji, w ramach której sprawdza:

- poprawność realizacji zadań przez administratora systemu, w szczególności właściwe zarządzanie konfiguracją oraz uprawnieniami przydzielanymi użytkownikom,
- znajomość i przestrzeganie przez użytkowników zasad ochrony informacji niejawnych oraz procedur bezpiecznej eksploatacji w systemie teleinformatycznym, a w szczególności w zakresie wykorzystania urządzeń i narzędzi służących do ochrony informacji niejawnych w systemie,
- stan środków bezpieczeństwa fizycznego oraz stan zabezpieczeń systemu teleinformatycznego,

3. Organizacja i prowadzenie szkoleń z użytkownikami systemu.
4. Monitorowanie zmian w systemie teleinformatycznym.
5. Reagowanie na sygnały o incydentach w zakresie bezpieczeństwa oraz wyjaśnianie ich przyczyn.
6. Okresowy przegląd i dokumentowanie logów systemowych.
7. Przeprowadzanie okresowej analizy zagrożeń.
8. Analiza rejestrów zdarzeń w systemie teleinformatycznym i prawidłowości ich archiwizowania.
9. Informowanie pełnomocnika ochrony o wszelkich zdarzeniach związanych lub mogących mieć związek z bezpieczeństwem systemu teleinformatycznego.
10. Prowadzenie dziennika inspektora bezpieczeństwa teleinformatycznego.

WÓJT

mgr inż. Bogdan Janusz Pietruszewski