Zarządzenie Nr 19/2021
Wójta Gminy Naruszewo
z dnia 22 lutego 2021 r.

w sprawie zatwierdzenia dokumentacji bezpieczeństwa systemu teleinformatycznego i udzielenia akredytacji bezpieczeństwa teleinformatycznego dla systemu teleinformatycznego przeznaczonego do przetwarzania informacji niejawnych o klauzuli „Zastrzeżone".

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. 48 ust 9 ustawy z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych (t. j. Dz. U. z 2019 r. , poz. 742) oraz § 25 ust. 1 pkt 1 i § 26 ust.1 pkt 1 rozporządzenia Prezesa Rady Ministrów z dnia 20 lipca 2011 roku w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. z 2011 r. nr 159, poz. 948) zarządzam, co następuje:

§ 1

1. Z dniem 22 lutego 2021 roku zatwierdzam dokumentację bezpieczeństwa systemu teleinformatycznego przeznaczonego do przetwarzania informacji niejawnych o klauzuli „Zastrzeżone" i udzielam akredytacji bezpieczeństwa teleinformatycznego dla systemu teleinformatycznego ,,Autonomiczne Stanowisko Komputerowe" Urzędu Gminy w Naruszewie na okres do dnia 21 lutego 2026 r.
2. Dokumentację bezpieczeństwa systemu teleinformatycznego stanowią:
   1) Szczególne wymagania bezpieczeństwa (SWB) dla systemu teleinformatycznego ,,Autonomiczne Stanowisko Komputerowe" Urzędu Gminy w Naruszewie.
   2) Procedury bezpiecznej eksploatacji (PBE) dla systemu teleinformatycznego ,,Autonomiczne Stanowisko Komputerowe" Urzędu Gminy w Naruszewie.
3. Dokumentacja bezpieczeństwa systemu teleinformatycznego stanowi informacje niejawne oznaczone klauzulą ,,Zastrzeżone" i podlega ochronie na zasadach określonych w ustawie o ochronie informacji niejawnych.

§ 2

1. Wyznaczam Pana Romana Kozłowskiego do pełnienia funkcji inspektora bezpieczeństwa teleinformatycznego, odpowiedzialnego za weryfikację i bieżącą kontrolę zgodności funkcjonowania systemu teleinformatycznego służącego do przetwarzania informacji niejawnych o klauzuli „Zastrzeżone" ze szczególnymi wymaganiami bezpieczeństwa oraz przestrzegania procedur bezpiecznej eksploatacji.
2. Wyznaczam Pana Marka Lewandowskiego do pełnienia funkcji administratora systemu, odpowiedzialnego za funkcjonowanie systemu teleinformatycznego służącego do przetwarzania informacji niejawnych o klauzuli „Zastrzeżone" oraz za przestrzeganie zasad i wymagań bezpieczeństwa przewidzianych dla tego systemu.
3. Wyżej wymienione osoby funkcyjne oraz Pełnomocnik ds. ochrony informacji niejawnych stanowią skład zespołu do spraw zarządzania bezpieczeństwem systemu teleinformatycznego, odpowiedzialnego za kreowanie polityki bezpieczeństwa systemu teleinformatycznego oraz za planowanie, wdrażanie i eksploatację systemu.
4. Szczegółowe obowiązki osób funkcyjnych wymienionych w pkt 1 i 2 zawiera załącznik do niniejszego zarządzenia.

§ 3

1. Autonomiczne Stanowisko Komputerowe przeznaczone do przetwarzania informacji niejawnych o klauzuli ,,Zastrzeżone" zlokalizowane jest w pomieszczeniu nr 6.

2. Wytwarzanie dokumentów niejawnych oznaczonych klauzulą „Zastrzeżone" odbywa się tylko i wyłącznie na wydzielonym Autonomicznym Stanowisku Komputerowym.

§ 4

1. Użytkownicy Autonomicznego Stanowiska Komputerowego zobowiązani są do posiadania aktualnego poświadczenia bezpieczeństwa bądź upoważnienia nadanego przez Wójta Gminy uprawniającego do dostępu do informacji niejawnych oznaczonych klauzulą „Zastrzeżone".
2. Użytkownicy Autonomicznego Stanowiska Komputerowego uzyskują formalne uprawnienia dostępu do systemu teleinformatycznego na podstawie formularza ,,Karty użytkownika systemu teleinformatycznego". Zakres uprawnień określa przełożony użytkownika.
3. Pełnomocnik ds. ochrony informacji niejawnych potwierdza w ,,Karcie użytkownika...." fakt posiadania przez użytkownika, określonych przepisami prawa, wymagań do nadania uprawnień do dostępu do systemu teleinformatycznego, a administrator systemu stwierdza założenie konta użytkownika.

§ 5

1. Szkolenie użytkowników z zakresu bezpieczeństwa teleinformatycznego i procedur bezpiecznej eksploatacji, w zakresie jaki ich dotyczy, przeprowadza administrator systemu lub inspektor bezpieczeństwa teleinformatycznego przed rozpoczęciem przez użytkownika pracy w systemie.
2. Szkolenie prowadzi się w pomieszczeniu systemu teleinformatycznego.

§ 6

1. Wykonanie zarządzenia powierzam Pełnomocnikowi ds. ochrony informacji niejawnych.
2. Zarządzenie wchodzi w życie z dniem podpisania.

Wójt
mgr inż. Beata Pierścińska

Załącznik do Zarządzenia Nr 19/2021 Wójta Gminy Naruszewo z dnia 22 lutego 2021 r.

I. Obowiązki Inspektora Bezpieczeństwa Teleinformatycznego:

Inspektor bezpieczeństwa teleinformatycznego, odpowiada za weryfikację i bieżącą kontrolę zgodności funkcjonowania systemu teleinformatycznego służącego do przetwarzania informacji niejawnych o klauzuli „Zastrzeżone" ze szczególnymi wymaganiami bezpieczeństwa oraz przestrzegania procedur bezpiecznej eksploatacji.

Do podstawowych zadań Inspektora Bezpieczeństwa Teleinformatycznego należy:

1. Udział 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. Organizowanie i prowadzenie szkoleń z użytkownikami systemu.
4. Monitorowanie zmian w systemie teleinformatycznym.
5. Reagowanie na sygnały o incydentach w zakresie bezpieczeństwa, wyjaśnianie ich przyczyn, okresowe przeglądanie i dokumentowanie logów systemowych.
6. Przeprowadzanie okresowej analizy zagrożeń.
7. Analizowanie rejestrów zdarzeń w systemie teleinformatycznym i prawidłowości ich archiwizowania.
8. Informowanie pełnomocnika ochrony o wszelkich zdarzeniach związanych lub mogących mieć związek z bezpieczeństwem systemu teleinformatycznego.
9. Prowadzenie dziennika inspektora bezpieczeństwa teleinformatycznego.

II. Obowiązki Administratora Systemu Teleinformatycznego:

Administrator systemu, odpowiada za funkcjonowanie systemu teleinformatycznego służącego do przetwarzania informacji niejawnych o klauzuli „Zastrzeżone" oraz za przestrzeganie zasad i wymagań bezpieczeństwa przewidzianych dla tego systemu.

Do podstawowych zadań Administratora Systemu Teleinformatycznego należy:

1. Udział w procesie zarządzania ryzykiem w systemie teleinformatycznym oraz w tworzeniu dokumentacji bezpieczeństwa systemu.
2. Utrzymanie zgodności dokumentacji bezpieczeństwa z konfiguracją systemu teleinformatycznego.
3. Tworzenie i usuwane kont użytkowników, wdrażanie uprawnień w systemie teleinformatycznym wynikających z przydzielonych praw dostępu, przydzielanie użytkownikom pierwszych haseł dostępu.
4. Szkolenie użytkowników systemu teleinformatycznego z zakresu procedur bezpiecznej eksploatacji.
5. Konfigurowanie urządzeń i oprogramowania.
6. Utrzymywanie zgodność konfiguracji i parametrów systemu teleinformatycznego z dokumentacją bezpieczeństwa systemu.
7. Monitorowanie funkcjonowania mechanizmów zabezpieczeń i poprawności działania systemu teleinformatycznego.

8. Przeglądanie plików zawierających informacje o wybranych zdarzeniach w systemie – logów systemowych.
9. Reagowanie na sygnały o incydentach w zakresie bezpieczeństwa systemu i usuwanie ich skutków.
10. Prowadzenie ewidencji sprzętu, oprogramowania i nośników danych.
11. Tworzenie kopii bezpieczeństwa.
12. Informowanie przełożonych i inspektora bezpieczeństwa teleinformatycznego o wszelkich zdarzeniach związanych lub mogących mieć związek z bezpieczeństwem systemu teleinformatycznego.
13. Prowadzenie dziennika administratora.