

**ZARZĄDZENIE NR 64/2021
BURMISTRZA MIASTA I GMINY FROMBORK**

z dnia 14 września 2021 r.

**w sprawie powołania w Urzędzie Miasta i Gminy Frombork
„Administradora systemu teleinformatycznego ochrony informacji niejawnych” oraz
„Inspektora bezpieczeństwa teleinformatycznego ochrony informacji niejawnych”**

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

§ 1. Wyznaczam Pana Damiana Krasieńskiego na Administratora Systemu Teleinformatycznego Ochrony Informacji Niejawnych odpowiedzialnego za funkcjonowanie systemu teleinformatycznego oraz za przestrzeganie zasad i wymagań bezpieczeństwa przewidzianych dla systemu teleinformatycznego, zwanego dalej „administratorem systemu”.

§ 2. Wyznaczam Pana Mirosława Witczak na Inspektora Bezpieczeństwa Teleinformatycznego Ochrony Informacji Niejawnych odpowiedzialnego za weryfikację i bieżącą kontrolę zgodności i funkcjonowania systemu teleinformatycznego ze szczególnymi wymaganiami bezpieczeństwa oraz kontrolę przestrzegania procedur bezpiecznej eksploatacji, zwanego dalej „inspektorem bezpieczeństwa”.

§ 3. Administrator systemu bierze udział w tworzeniu dokumentacji bezpieczeństwa oraz w procesie zarządzania ryzykiem w systemie teleinformatycznym, w szczególności:

- 1) opracowuje dokumentację bezpieczeństwa teleinformatycznego oraz propozycje jej uaktualniania;
- 2) uczestniczy w procesie szacowania ryzyka;
- 3) wdraża szczegółowe wymagania bezpieczeństwa oraz procedury bezpiecznej eksploatacji systemu teleinformatycznego (SWB, PBE);
- 4) współuczestniczy w szkoleniu użytkowników systemu teleinformatycznego z zakresu procedur bezpiecznej eksploatacji;
- 5) utrzymuje zgodność konfiguracji i parametrów systemu teleinformatycznego z dokumentacją bezpieczeństwa systemu;
- 6) systematycznie kontroluje funkcjonowanie mechanizmów zabezpieczeń oraz poprawność działania systemu teleinformatycznego;
- 7) informuje pełnomocnika ochrony o stwierdzonych naruszeniach bezpieczeństwa systemu teleinformatycznego;
- 8) zgłasza pełnomocnikowi ochrony potrzeby w zakresie serwisowania systemu,
- 9) analizuje i archiwizuje rejestr zdarzeń w systemie;
- 10) prowadzi na bieżąco wykaz osób mających dostęp do systemu teleinformatycznego oraz przydziela użytkownikom konta, zgodnie z uprawnieniami nadanymi przez kierownika jednostki organizacyjnej;
- 11) zapewnia dostęp do systemu teleinformatycznego wyłącznie użytkownikom posiadających wymagane uprawnienia oraz odpowiednie i ważne poświadczenia bezpieczeństwa lub upoważnienie kierownika jednostki.

§ 4. Inspektor bezpieczeństwa bierze udział w procesie zarządzania ryzykiem w szczególności kontroluje:

- 1) przestrzeganie zasad ochrony informacji niejawnych w systemie lub sieci teleinformatycznej,

2) stan zabezpieczeń fizycznych, elektromagnetycznych i elektronicznych pomieszczeń lub obszarów, w których usytuowane są systemy lub sieci teleinformatyczne,

3) aktualność wykazów osób mających dostęp do systemu lub sieci teleinformatycznej, przydzielanie kont użytkownikom, zakres nadanych im uprawnień oraz prawidłowość zabezpieczeń zastosowanych w systemie lub sieci;

4) znajomość i przestrzeganie przez użytkowników procedur bezpiecznej eksploatacji systemu lub sieci teleinformatycznej,

5) przestrzeganie zasad i wymagań w zakresie oznaczania, ewidencjonowania, przechowywania i przekazywania wytworzonych dokumentów niejawnych oraz ich terminowe rozliczanie,

6) zgodność konfiguracji systemu lub sieci teleinformatycznej z dokumentacją bezpieczeństwa teleinformatycznego.

2. Do obowiązków inspektora bezpieczeństwa w szczególności należy:

1) kontrola realizowania procedur bezpiecznej eksploatacji systemu,

2) organizowanie i prowadzenie szkoleń z zakresu bezpieczeństwa teleinformatycznego,

3) przeprowadzanie okresowej analizy ryzyka,

4) tworzenie planów awaryjnych,

5) organizowanie treningów symulacyjnych z różnych zagrożeń.

6) opracowanie instrukcji (regulaminu) użytkowania programów komputerowych dla pracowników,

7) informowanie Pełnomocnika ochrony o zdarzeniach związanych lub mogących mieć związek z bezpieczeństwem teleinformatycznym.

§ 5. Uruchamia się system teleinformatyczny (TI) „Zalew”.

§ 6. Nadzór nad wykonaniem zarządzenia powierzam Pełnomocnikowi ds. ochrony informacji niejawnych.

§ 7. Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ

Zbigniew Pietkiewicz