

Zarządzenie Nr 76C/2020
WÓJTA GMINY STRZELCE
z 7 września 2020 r.

w sprawie powołania systemu teleinformatycznego służącego do przetwarzania informacji niejawnych o klauzuli „zastrzeżone” oraz określenie składu oraz zadań wypełnianych przez Zespół ds. zarządzania bezpieczeństwem teleinformatycznego systemu przetwarzania informacji niejawnych w Urzędzie Gminy Strzelce

Na podstawie art. 33 ust. 1, 3 ustawy z dnia 8 marca 1990 roku o samorządzie gminnym (tj. Dz. U. z 2020 r. poz. 713 z późn. zm.), art. 48, 49, 52 ust. 1 ustawy z 5 sierpnia 2010 r. o ochronie informacji niejawnych (tj. Dz. U. z 2019 r., poz. 742 z późn. zm.) oraz Rozporządzenia Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. Nr 159, poz. 948 z późn. zm.), zarządza się co następuje:

§ 1. W Urzędzie Gminy Strzelce wprowadza się do eksploatacji system teleinformatyczny służący do przetwarzania informacji niejawnych o klauzuli „zastrzeżone”.

§ 2. 1. System teleinformatyczny, w którym przetwarza się informacje niejawne, podlega akredytacji bezpieczeństwa teleinformatycznego.

2. Podstawą uzyskania akredytacji jest opracowanie dokumentacji bezpieczeństwa teleinformatycznego, zgodnie z odpowiednimi zaleceniami Agencji Bezpieczeństwa Wewnętrznego.

3. Akredytacji systemu dokonuje Wójt przez zatwierdzenia dokumentacji bezpieczeństwa systemu, w tym Szczegółowych Wymagań Bezpieczeństwa oraz Procedury Bezpiecznej Eksploatacji.

4. Akredytacji udziela się na okres 5 lat.

§ 3. W Urzędzie Gminy Strzelce tworzy się system teleinformatyczny przeznaczony do przetwarzania informacji niejawnych w postaci elektronicznej o klauzuli „zastrzeżone” zwany dalej Systemem.

§ 4. System składał się będzie z:

- jednej stacji roboczej, typu przenośnego, odpowiednio skonfigurowanej i zabezpieczonej, brak dostępu do sieci internetowej bez możliwości wymiany danych z innymi systemami;
- drukarki.

§ 5. Powołuję zespół ds. zarządzania bezpieczeństwem teleinformatycznego systemu przetwarzania informacji niejawnych w Urzędzie Gminy Strzelce, zwany dalej Zespołem ds. zarządzania bezpieczeństwem niejawnego systemu teleinformatycznego.

§ 6. W skład Zespołu wchodzi:

- Wioleta Maćczak – Pełnomocnik ds. Ochrony Informacji Niejawnych,
- Marcin Lewandowski – Administrator Sytemu,
- Klaudia Pietrzak – Inspektor Bezpieczeństwa Teleinformatycznego.

§ 7. 1. Pełnomocnik ds. Ochrony Informacji Niejawnych odpowiedzialny jest za:

- zapewnienie ochrony informacji niejawnych, w tym stosowanie środków bezpieczeństwa fizycznego;
- zapewnienie ochrony systemów teleinformatycznych, w których są przetwarzane informacje niejawne;
- zarządzanie ryzykiem bezpieczeństwa informacji niejawnych, w szczególności szacowanie ryzyka;

2. Pełnomocnik ds. ochrony informacji niejawnych opracowuje i uaktualnia (wymagające akceptacji kierownika jednostki organizacyjnej) następujące dokumenty:

- plan ochrony informacji niejawnych w jednostce organizacyjnej, w tym w razie wprowadzenia stanu nadzwyczajnego;
- dokumentację określającą poziom zagrożeń związanych z nieuprawnionym dostępem do informacji niejawnych lub ich utratą;
- instrukcję dotyczącą sposobu i trybu przetwarzania informacji niejawnych o klauzuli „zastrzeżone” w podległych komórkach organizacyjnych oraz zakres i warunki stosowania środków bezpieczeństwa fizycznego w celu ich ochrony.

3. Pełnomocnik ochrony odpowiada za zapewnienie ochrony systemów teleinformatycznych funkcjonujących w jednostce organizacyjnej (z wyłączeniem organizacyjnych, technicznych, programowych i eksploatacyjnych aspektów ochrony kryptograficznej), w szczególności za:

- zapewnienie przestrzegania zasad ochrony informacji niejawnych przetwarzanych w systemach teleinformatycznych, w tym właściwego i bezpiecznego obiegu dokumentów oraz informatycznych nośników danych;
- zapewnienie bezpieczeństwa fizycznego obszarów, w których usytuowane są systemy teleinformatyczne;

- organizację i prowadzenie szkoleń użytkowników w zakresie bezpieczeństwa teleinformatycznego;
- nadzór nad konfiguracją systemów teleinformatycznych i przemieszczaniem ich elementów składowych, i inne.

§ 8. Administrator Systemu realizuje:

Zadania w zakresie odpowiedzialności za funkcjonowanie systemu teleinformatycznego oraz odpowiada za przestrzeganie zasad i wymagań bezpieczeństwa przewidzianych dla systemu teleinformatycznego, w szczególności:

- opracowuje i uaktualniania dokumentację bezpieczeństwa systemu teleinformatycznego;
- przechowuje oryginały zatwierdzonej dokumentacji bezpieczeństwa teleinformatycznego systemu teleinformatycznego;
- uczestniczy w procesie szacowania ryzyka;
- wdraża procedury bezpiecznej eksploatacji;
- szkoli użytkowników systemu teleinformatycznego z zakresu procedur bezpiecznej eksploatacji;
- utrzymuje zgodność konfiguracji i parametrów systemu teleinformatycznego z dokumentacją bezpieczeństwa systemu;
- systematycznie kontroluje funkcjonowanie mechanizmów zabezpieczeń i poprawność działania systemu teleinformatycznego;
- informuje pełnomocnika ochrony o stwierdzonych naruszeniach bezpieczeństwa systemu teleinformatycznego;
- zgłasza do pełnomocnika ochrony potrzeby w zakresie serwisowania i certyfikacji środków ochrony elektromagnetycznej;
- analizuje i archiwizuje rejestr zdarzeń w systemie teleinformatycznym;
- prowadzi wykaz osób mających dostęp do systemu teleinformatycznego;
- przydziela użytkownikom konta, zgodnie z uprawnieniami nadanymi przez kierownika jednostki (komórki) organizacyjnej;
- zapewnia dostęp do systemu teleinformatycznego wyłącznie użytkownikom posiadających wymagane uprawnienia oraz odpowiednie i ważne poświadczenia bezpieczeństwa.

§ 9. Inspektor Bezpieczeństwa Teleinformatycznego realizuje:


Zadania w zakresie weryfikacji i bieżącej kontroli zgodności funkcjonowania eksploatowanego w danej jednostce organizacyjnej systemu teleinformatycznego z jego dokumentacją bezpieczeństwa, a w szczególności kontroluje:

- przestrzeganie zasad ochrony przetwarzanych w systemie teleinformatycznym informacji niejawnych;
- poprawność realizacji zadań wykonywanych przez administratora;
- zgodność konfiguracji systemu teleinformatycznego z dokumentacją bezpieczeństwa systemu teleinformatycznego;
- stan środków bezpieczeństwa fizycznego i ochrony elektromagnetycznej;
- aktualność wykazów osób mających dostęp do systemu teleinformatycznego, prawidłowość przydzielania kont użytkownikom, zakres nadanych im uprawnień i prawidłowość zabezpieczeń zastosowanych w systemie teleinformatycznym;
- znajomość i przestrzeganie przez użytkowników procedur bezpiecznej eksploatacji systemu teleinformatycznego.

§ 10. Wykonanie zarządzenia powierza się Pełnomocnikowi ds. Ochrony Informacji Niejawnej.

§ 11. Niniejsze zarządzenie wchodzi w życie z dniem podpisania.


WOJCI
Gminy Strzelce
Tomasz Grabowski

ADWOKAT

Małgorzata Kosińska