Z A R Z Ą D Z E N I E N R V/ 241 /2020
Wójta Gminy Krościenko Wyżne
z dnia 11 grudnia 2020 r.

w sprawie powołania w Urzędzie Gminy Krościenko Wyżne „Inspektora Bezpieczeństwa Teleinformatycznego" oraz „Administratora Systemu Teleinformatycznego"

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

§ 1. Wyznacza się Pana Bogdana Ziębę na administratora systemu teleinformatycznego ochrony informacji niejawnych odpowiedzialnego za funkcjonowanie systemu teleinformatycznego oraz za przestrzeganie zasad i wymagań bezpieczeństwa przewidzianych dla systemu teleinformatycznego.

§ 2. Wyznacza się Pana Mateusza Podkula na inspektora bezpieczeństwa teleinformatycznego ochrony informacji niejawnych odpowiedzialnego za weryfikację i bieżącą kontrolę zgodności i funkcjonowania systemu teleinformatycznego ze szczególnymi wymaganiami bezpieczeństwa oraz kontrole przestrzegania procedur bezpiecznej eksploatacji.

§ 3. Administrator systemu realizuje zadania w zakresie zapewnienia funkcjonowania oraz przestrzegania zasad bezpieczeństwa systemu teleinformatycznego, w szczególności:

1) opracowuje dokumentację bezpieczeństwa teleinformatycznego oraz propozycje jej uaktualnienia;
2) uczestniczy w procesie szacowania ryzyka;
3) wdraża procedury bezpiecznej eksploatacji systemu teleinformatycznego;
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 użytkowników posiadających wymagane uprawnienia oraz odpowiednie i ważne poświadczenia bezpieczeństwa lub upoważnienie kierownika jednostki.

§ 4. 1. Do obowiązków inspektora bezpieczeństwa w szczególności należy:
1) kontrola realizowania procedur bezpiecznej eksploatacji systemu (PBE);
2) organizowanie i prowadzenie szkoleń z zakresu bezpieczeństwa teleinformatycznego;
3) reagowanie na incydenty, wyjaśnienia ich przyczyn;
4) przeprowadzanie okresowej analizy ryzyka;
5) tworzenie planów awaryjnych;
6) organizowanie treningów symulacyjnych z różnych zagrożeń;
7) uczestnictwo w pracach zespołu ds. opracowania SWB i PBE;
8) opracowanie instrukcji (regulaminu) użytkowania programów komputerowych dla pracowników,
9) informowanie pełnomocnika ochrony o zdarzeniach związanych lub mogących mieć związek z bezpieczeństwem teleinformatycznym.

2. Inspektor bezpieczeństwa teleinformatycznego 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.

§ 5. Nadzór nad wykonaniem zarządzenia powierzam pełnomocnikowi ds. ochrony informacji niejawnych.

§ 6. Zarządzenie wchodzi w życie z dniem podpisania.