Kontrole z zakresu działania systemów teleinformatycznych używanych do realizacji zadań zleconych z zakresu administracji rządowej –2022 r.

Podstawa prawna do przeprowadzenia kontroli:
art. 25 ust. 1 pkt 3 lit. a w związku z ust. 3 ustawy z dnia 17 lutego 2005 r.
o informatyzacji działalności podmiotów realizujących zadania publiczne[1].

Przedmiot kontroli:
Działanie systemów teleinformatycznych używanych do realizacji zadań zleconych z zakresu administracji rządowej;

Łączna liczba przeprowadzonych kontroli: **6**

Jednostki kontrolowane: Urząd Gminy Rąbino, Urząd Miejski w Moryniu, Urząd Gminy i Miasta Ińsko, Urząd Miejski w Pełczycach, Urząd Miasta i Gminy w Tucznie, Urząd Miejski w Maszewie.

Liczba kontroli, w których stwierdzono nieprawidłowości: 6

Zakres stwierdzonych nieprawidłowości:
- Nieprzeglądanie i nieaktualizowanie obowiązującej w Urzędzie dokumentacji dotyczącej bezpieczeństwa informacji;
- Nieprzeprowadzenie audytu wewnętrznego z zakresu bezpieczeństwa informacji;
- Nieprzeprowadzenie okresowo analizy ryzyka utraty integralności, dostępności lub poufności informacji;
- W umowie regulującej kwestię serwisu programu podlegającego kontroli brak zapisów określających maksymalny czas skutecznej naprawy oprogramowania;
- Nieprzeprowadzanie szkoleń pracowników dotyczących bezpieczeństwa informacji;
- Dokumentacja regulująca kwestie bezpieczeństwa informacji nie zawiera wszystkich elementów wymaganych przepisami rozporządzenia KRI;
- Inwentaryzacja sprzętu i oprogramowania nie zawiera wszystkich wymaganych informacji,
- Zakres tematyczny szkoleń przeprowadzonych w Urzędzie nie obejmował wszystkich zagadnień wskazanych w § 20 ust. 2 pkt 6 rozporządzenia KRI;
- Zawężenie incydentów naruszenia bezpieczeństwa informacji do naruszeń danych osobowych;
- Wykorzystywanie jednego identyfikatora do programu podlegającego kontroli przez kilku użytkowników;
- Nieodnotowywanie w dziennikach systemów działań użytkowników z uprawnieniami administracyjnymi;
- Nieprzeprowadzanie testowych odtworzeń kopii zapasowych na potrzeby weryfikacji poprawności i stanu wykonywania;
- Niedokonywanie przeglądów oraz analizy logów systemu podlegającego kontroli w celu identyfikacji działań niepożądanych;
- Brak umowy powierzenia przetwarzania danych osobowych;

[1] Dz. U. z 2021 r., poz. 2070,

- W umowie regulującej kwestię serwisu programu podlegającego kontroli brak zapisów określających maksymalny czas skutecznej naprawy oprogramowania;
- Nieaktualizowanie oprogramowania antywirusowego;
- Niewłaściwe ustawienie monitora umożliwiające odczyt wyświetlanych danych przez osoby postronne;
- Niesporządzanie dokumentacji dotyczącej testowania kopii zapasowych danych i systemów na potrzeby weryfikacji poprawności i stanu ich wykonywania;
- Pomieszczenie serwerowni nie jest wyposażone we wszystkie wymagane zabezpieczenia chroniące przed nieuprawnionym dostępem, uszkodzeniem lub zniszczeniem infrastruktury IT.