Kontrole z zakresu działania systemów teleinformatycznych używanych do realizacji zadań zleconych z zakresu administracji rządowej –2023 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] ;
- art. 28 ust. 1 pkt 1 ustawy z dnia 23 stycznia 2009 r. o wojewodzie i administracji rządowej w województwie.[2]

Przedmiot kontroli:
- **Działanie systemów teleinformatycznych używanych do realizacji zadań zleconych z zakresu administracji rządowej;**
- **Bezpieczeństwo teleinformatyczne w administracji rządowej i ochrona danych osobowych.**

Łączna liczba przeprowadzonych kontroli: **7**

Jednostki kontrolowane: Urząd Miejski w Cedyni, Urząd Gminy Wierzchowo, Urząd Gminy Krzęcin, Urząd Gminy Stargard, Urząd Miasta Świnoujście, Urząd Gminy Warnice, Wojewódzki Inspektorat Nadzoru Budowlanego w Szczecinie.

Liczba kontroli, w których stwierdzono nieprawidłowości: 7

Zakres stwierdzonych nieprawidłowości:
- Nieprzeglądanie i nieaktualizowanie obowiązującej w Urzędzie dokumentacji dotyczącej bezpieczeństwa informacji;
- Nieprzeprowadzenie audytu wewnętrznego z zakresu bezpieczeństwa informacji;
- Dokumentacja regulująca kwestie bezpieczeństwa informacji nie zawiera wszystkich elementów wymaganych przepisami rozporządzenia KRI;
- 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;
- Zawężenie analizy ryzyka do zagadnień związanych z bezpieczeństwem danych osobowych;
- Niezachowanie wymogu bezzwłocznego odebrania uprawnień w systemach informatycznych;
- Nieodnotowywanie w dziennikach systemów działań użytkowników z uprawnieniami administracyjnymi;
- Przechowywanie kopii zapasowych w miejscu wytworzenia;
- Posiadanie przez pracownika realizującego zadania zlecone z zakresu administracji rządowej uprawnień administratora w zakresie obsługi systemu podlegającego kontroli;

[1] Dz. U. z 2023 r., poz. 57.
[2] Dz. U. z 2023r., poz. 190.

- Niewłaściwe ustawienie monitora umożliwiające odczyt wyświetlanych danych przez osoby postronne;
- Nieprzechowywanie logów programu podlegających kontroli przez okres 2 lat;
- 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.