Kontrole z zakresu działania systemów teleinformatycznych używanych do realizacji zadań zleconych z zakresu administracji rządowej –2025 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: **7**

Jednostki kontrolowane: Urząd Gminy Świerzno, Urząd Gminy Banie, Urząd Gminy Dolice, Urząd Miasta Świdwin, Urząd Gminy Grzmiąca, Urząd Miejski w Dębnie, Urząd Miejski w Bornem Sulinowie

Liczba kontroli, w których stwierdzono nieprawidłowości: 7

Zakres stwierdzonych nieprawidłowości:
- Nieprzeglądanie obowiązującej w Urzędzie dokumentacji dotyczącej bezpieczeństwa informacji;
- Nieprzeprowadzenie audytu wewnętrznego z zakresu bezpieczeństwa informacji;
- Zrealizowanie audytów wewnętrznych z zakresu bezpieczeństwa informacji przez osoby odpowiedzialne za bieżące funkcjonowanie obszarów poddawanych analizie;
- Nieprzeprowadzenie okresowo analizy ryzyka utraty integralności, dostępności lub poufności 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 § 19 ust. 2 pkt 6 rozporządzenia KRI;
- Niesporządzenie planu postępowania z ryzykiem;
- Przechowywanie kopii zapasowych w miejscu wytworzenia;
- Brak regulacji w obszarze dotyczącym pracy przy przetwarzaniu mobilnym i pracy na odległość;
- Niezachowanie wymogu formy pisemnej przy nadaniu, zmianie odebraniu lub ograniczeniu uprawnień do pracy w systemach informatycznych;
- W umowie regulującej kwestię serwisu programu podlegającego kontroli brak zapisów określających maksymalny czas skutecznej naprawy oprogramowania oraz brak regulacji kwestii powierzenia przetwarzania danych osobowych;
- Zawężenie incydentów naruszenia bezpieczeństwa informacji do naruszeń danych osobowych;
- Zawężenie analizy ryzyka do zagadnień związanych z bezpieczeństwem danych osobowych;
- Brak realizacji uwag i rekomendacji audytowych wydanych w wyniku audytu polityki bezpieczeństwa informacji;

[1] Dz. U. z 2025 r. poz. 1703.

- Nieodnotowywanie w dziennikach systemów działań użytkowników z uprawnieniami administracyjnymi;
- Niezachowanie wymogu bezzwłocznego odebrania uprawnień w systemach informatycznych;
- Niewykonywanie kopii bezpieczeństwa oprogramowania podlegającego kontroli;
- Nieprzechowywanie logów programu podlegających kontroli przez okres 2 lat;
- Nieprzeprowadzanie testowych odtworzeń kopii zapasowych;
- Nieprowadzenie działań związanych z przeglądaniem logów i ich analizą w celu identyfikacji działań niepożądanych;
- Niezainstalowanie oprogramowania antywirusowego na jednym ze stanowisk komputerowych objętych kontrolą;
- Pomieszczenie serwerowni nie jest wyposażone we wszystkie wymagane zabezpieczenia chroniące przed nieuprawnionym dostępem, uszkodzeniem lub zniszczeniem infrastruktury IT.