Wojewoda Zachodniopomorski

Znak: K-2.431.1.15.2025.9.IO

Szczecin, 24 czerwca 2025 r.

WYSTĄPIENIE POKONTROLNE

Przedmiot kontroli	Działanie systemów teleinformatycznych oraz rejestrów publicznych używanych do realizacji zadań zleconych z zakresu administracji rządowej.
Nazwa i adres organu kontrolującego	Wojewoda Zachodniopomorski, ul. Wały Chrobrego 4, 70-502 Szczecin.
Nazwa i adres organu kontrolowanego	Wójt Gminy Banie, ul. Skośna 6, 74-110 Banie.
Osoba pełniąca funkcję Wójta Gminy Banie w okresie objętym kontrolą	Pan Arkadiusz Augustyniak
Okres objęty kontrolą	od dnia 1 stycznia 2022 r. do dnia 28 marca 2025 r.
Kontrolerzy	Pracownicy Wydziału Kontroli Zachodniopomorskiego Urzędu Wojewódzkiego w Szczecinie: Pani Anna Dąbska – kierownik oddziału, kierownik zespołu kontrolnego, Pani Iwona Olesińska – główny specjalista.
Nr upoważnienia	Nr 17/25 z dnia 17 marca 2025 r.
Podstawy prawne do przeprowadzenia kontroli	– art. 6 ust. 4 pkt 3 w związku z art. 2 ust. 1 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej[1]; – 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[2].
Kryteria prowadzenia kontroli	legalność, rzetelność
Rodzaj kontroli i tryb kontroli	kontrola planowa, tryb zwykły
Termin kontroli	24 – 28 marca 2025 r.

[1] Dz. U. z 2020r., poz. 224.
[2] Dz. U. z 2023r., poz. 57.

Obszar kontroli Nr 1: Wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami/rejestrami informatycznymi i wspomaganie świadczenia usług drogą elektroniczną.

1.1 Współpraca systemów teleinformatycznych z innymi systemami.
Podstawa prawna: § 5 ust. 3 pkt 3 rozporządzenia KRI[3]: *Interoperacyjność na poziomie semantycznym osiągana jest przez: stosowanie w rejestrach prowadzonych przez podmioty publiczne odwołań do rejestrów zawierających dane referencyjne w zakresie niezbędnym do realizacji zadań;* **§ 16 ust. 1 rozporządzenia KRI:** *Systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne wyposaża się w składniki sprzętowe lub oprogramowanie umożliwiające wymianę danych z innymi systemami teleinformatycznymi za pomocą protokołów komunikacyjnych i szyfrujących określonych w obowiązujących przepisach, normach, standardach lub rekomendacjach ustanowionych przez krajową jednostkę normalizacyjną lub jednostkę normalizacyjną Unii Europejskiej.*
Ustalenia kontroli
Na podstawie przedstawionej dokumentacji ustalono, że do realizacji zadań zleconych z zakresu administracji rządowej w Urzędzie Gminy Banie wykorzystywano system centralny (aplikacja Źródło) oraz system informatyczny wspomagający obsługę spraw obywatelskich w zakresie ewidencji ludności XXX.
System informatyczny wspomagający realizację zadań zleconych z zakresu administracji rządowej spełniał minimalne wymogi interoperacyjności w zakresie współpracy z innymi aplikacjami Urzędu, jak i innych jednostek administracji publicznej, określone w § 5 ust. 3 pkt 3 rozporządzenia KRI. System centralny podlegał kontroli jedynie w zakresie formalnego posiadania uprawnień przez pracowników Urzędu oraz zabezpieczeń związanych z dostępem do systemu.
(dowód: akta kontroli str. 38)

1.2 Formaty danych udostępniane przez systemy teleinformatyczne.
Podstawa prawna: § 17 ust. 1 rozporządzenia KRI: *Kodowanie znaków w dokumentach wysyłanych z systemów teleinformatycznych podmiotów realizujących zadania publiczne lub odbieranych przez takie systemy, także w odniesieniu do informacji wymienianej przez te systemy z innymi systemami na drodze teletransmisji, o ile wymiana ta ma charakter wymiany znaków, odbywa się według standardu Unicode UTF-8 określonego przez normę ISO/IEC 10646 wraz ze zmianami lub normę ją zastępującą;* **§ 18 ust. 1 rozporządzenia KRI:** *Systemy teleinformatyczne podmiotów realizujących zadania publiczne udostępniają zasoby informacyjne co najmniej w jednym z formatów danych określonych w załączniku nr 2 do rozporządzenia;* **§ 18 ust. 2 rozporządzenia KRI:** *Jeżeli z przepisów szczegółowych albo opublikowanych w repozytorium interoperacyjności schematów XML lub innych wzorów nie wynika inaczej, podmioty realizujące zadania publiczne umożliwiają przyjmowanie dokumentów elektronicznych służących do załatwiania spraw należących do zakresu ich działania w formatach danych określonych w załącznikach nr 2 i 3 do rozporządzenia.*
Ustalenia kontroli
System informatyczny wykorzystywany do realizacji zadań zleconych z zakresu administracji rządowej w Urzędzie Gminy Banie wymieniał dane w formatach

[3] Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2024 poz. 773), zwane dalej „rozporządzeniem KRI".

określonych w § 18 ust. 1 rozporządzenia KRI o udostępnianiu zasobów informacyjnych w co najmniej w jednym z formatów wymienionych w załączniku nr 2 do rozporządzenia.

Stwierdzone uchybienia / nieprawidłowości w obszarze Nr 1	Nie stwierdzono uchybień oraz nieprawidłowości skutkujących naruszeniem przepisów.
Ocena obszaru kontroli	**Pozytywna**

<u>Obszar kontroli Nr 2:</u> System zarządzania bezpieczeństwem informacji w systemach teleinformatycznych.

2.1 Dokumenty z zakresu bezpieczeństwa informacji. Zaangażowanie kierownictwa podmiotu.

Podstawa prawna: § 19 ust. 1 rozporządzenia KRI: *Podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność;* **§ 19 ust. 2 pkt 1 rozporządzenia KRI:** *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie (...) aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia.*

Ustalenia kontroli

Wymagania dotyczące systemów teleinformatycznych, w których przetwarzane są rejestry publiczne w postaci teleinformatycznej określone zostały w § 19 ust. 1 rozporządzenia KRI. Zgodnie z tym przepisem, podmiot realizujący zadania publiczne ma obowiązek opracowania i ustanowienia, wdrożenia i eksploatowania, monitorowania i przeglądania oraz utrzymania i doskonalenia systemu bezpieczeństwa informacji zapewniającego poufność, dostępność, integralność informacji.

W Urzędzie Gminy Banie, w okresie objętym kontrolą obowiązywały następujące dokumenty z zakresu bezpieczeństwa informacji:

- *Zarządzenie Nr 86/2018 Wójta Gminy Banie z dnia 10 sierpnia 2018 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji w zakresie bezpieczeństwa*
  i ochrony danych osobowych podczas przetwarzania dokumentacji w postaci tradycyjnej oraz elektronicznej w Urzędzie Gminy w Baniach;
- *Zarządzenie Nr 87/2018 Wójta Gminy Banie z dnia 10 sierpnia 2018 r. w sprawie wprowadzenia Instrukcji Zarządzania Systemem Informatycznym podczas przetwarzania dokumentacji w postaci tradycyjnej oraz elektronicznej w Urzędzie Gminy w Baniach;*
- *Instrukcja Postępowania w Sytuacji Naruszeń podczas przetwarzania dokumentacji w postaci tradycyjnej i elektronicznej w Urzędzie Gminy Banie, 74-100 Banie,*
  ul. Skośnia 6. Data dokumentu 25.05.2018 r.;
- *Instrukcja Zarządzania Systemem Informatycznym podczas przetwarzania dokumentacji w postaci tradycyjnej i elektronicznej w Urzędzie Gminy Banie, 74-100 Banie, ul. Skośnia 6* [4]. Data dokumentu 25.05.2018 r.;
- *Polityka Bezpieczeństwa Informacji w zakresie bezpieczeństwa informacji i ochrony danych osobowych podczas przetwarzania dokumentacji w postaci*

[4] Dalej: Instrukcja Zarządzania Systemem Informatycznym.

tradycyjnej i elektronicznej w Urzędzie Gminy Banie , 74-100 Banie, ul. Skośnia 6.[5] Data dokumentu 25.05.2018 r.;
- *Polityka Ochrony Danych Osobowych podczas przetwarzania dokumentacji w postaci tradycyjnej i elektronicznej w Urzędzie Gminy Banie , 74-100 Banie, ul. Skośnia 6*. Data dokumentu 25.05.2018 r.

W wyniku analizy obowiązującej w Jednostce dokumentacji związanej z bezpieczeństwem informacji stwierdzono, że funkcjonujące w Jednostce procedury zawierają między innymi oświadczenie o intencjach kierownictwa potwierdzające cele i zasady bezpieczeństwa; definicje ogólnych i szczegółowych obowiązków w odniesieniu do zarządzania bezpieczeństwem informacji oraz zakres stosowania wprowadzonych regulacji. Istnieje natomiast konieczność uzupełnienia wewnętrznych rozwiązań o kwestie przywołane w treści powyższego dokumentu kontrolnego. Dyrektywa § 19 ust. 2 pkt 1 rozporządzenia KRI wskazuje na obowiązek zapewnienia *aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia,* co przekłada się na konieczność monitorowania i przeglądu systemu zarządzania bezpieczeństwem informacji. W okresie objętym kontrolą, zgodnie z wyjaśnieniami Wójta z dnia 27 marca 2025 r. dokumentacja dotycząca bezpieczeństwa informacji *nie była poddawana aktualizacji*, wobec czego należy stwierdzić, że nie zrealizowano dyspozycji § 19 ust. 2 pkt 1 rozporządzenia KRI.

(dowód: akta kontroli str. 83-131, 163-171, 209-210)

2.2 Analiza zagrożeń związanych z przetwarzaniem informacji.
Podstawa prawna: § 19 ust. 2 pkt 3 rozporządzenia KRI: *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy.*
Ustalenia kontroli
Analiza ryzyka, obejmująca wszystkie aktywa Jednostki oraz odpowiednie i pogłębione szacowanie zidentyfikowanych ryzyk jest jednym z najistotniejszych elementów zarządzania bezpieczeństwem informacji, pozwalającym na zastosowanie odpowiednich mechanizmów przeciwdziałania w sytuacji materializacji ryzyk. Kontrolującym przedstawiono dokument *Analiza i szacowanie ryzyka w bezpieczeństwie informacji w Urzędzie Gminy Banie, 74-100 Banie, ul. Skośnia 6*. Dokument sporządzono 25 maja 2018 r. W okresie objętym kontrolą w Jednostce nie wykonano analizy ryzyka.
Mając na względzie powyższe, należy stwierdzić, że w Urzędzie Gminy Banie nie realizowano dyspozycji, o której mowa w § 19 ust. 2 pkt 3 rozporządzenia KRI. Procedura szacowania ryzyka powinna być przeprowadzana okresowo, ponadto obligatoryjnie w przypadku pojawienia się nowych zagrożeń, co wynika z faktu, że rodzaj i poziom zastosowanych zabezpieczeń jest względny i jest zależny od istotności informacji podlegających ochronie.

(dowód: akta kontroli str. 132-147, 209, 211)

2.3 Inwentaryzacja sprzętu i oprogramowania informatycznego.
Podstawa prawna: § 19 ust. 2 pkt 2 rozporządzenia KRI: *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: utrzymanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.*

[5] Dalej: Polityka Bezpieczeństwa Informacji.

Ustalenia kontroli

Inwentaryzacja sprzętu informatycznego powinna zawierać informację o jego rodzaju i konfiguracji, przez co możliwe będzie jego odtworzenie po katastrofie lub innym zdarzeniu losowym.

Kontrolującym przedstawiono zestawienie sprzętu i oprogramowania wykorzystywanego w Urzędzie, zawierające informacje dotyczące rodzaju użytkowanego sprzętu i jego charakterystyki; zainstalowanego oprogramowania; rodzaju systemu operacyjnego oraz współpracujących urządzeń peryferyjnych.

W udostępnionym zestawieniu zidentyfikowano sprzęty wykorzystywane przy realizacji zadań zleconych z zakresu administracji rządowej.

(dowód: akta kontroli str.172-175)

2.4 Zarządzanie uprawnieniami do pracy w systemach informatycznych.

Podstawa prawna: § 19 ust. 2 pkt 4 rozporządzenia KRI: *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji;*

§ 19 ust. 2 pkt 5 rozporządzenia KRI: *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4.*

Ustalenia kontroli

Przepisy § 19 ust. 2 pkt 4 i pkt 5 rozporządzenia KRI stanowią m.in, że kierownictwo podmiotu publicznego w celu zapewnienia bezpieczeństwa informacji powinno podjąć działania zapewniające, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia, adekwatne do realizowanych zadań, a także podjąć bezzwłoczne działania w przypadku zmiany zadań tych osób. Przetwarzanie informacji w systemach teleinformatycznych wymaga by dostęp do danych realizowany był przez uprawnione osoby, w ściśle ustalonym zakresie.

Kwestie nadawania i odbierania uprawnień do pracy w systemie informatycznym uregulowano w punkcie 5 *Instrukcji Zarzadzania Systemem Informatycznym (Procedury nadawania uprawnień*). Zgodnie z zapisami procedury *do przetwarzania danych osobowych (...) wymagane jest upoważnienie. Upoważnienie nadaje ADO[6] na podstawie wniosku o nadanie uprawnień do systemów.*

Kontrolującym przedstawiono:

- *Upoważnienie do przetwarzania danych osobowych* wystawione pracownikowi realizującemu zadania zlecone z zakresu administracji rządowej. Upoważnienie określa jego obszar, wynikający z zadań realizowanych na zajmowanym stanowisku oraz okres jego ważności;
- *Oświadczenie pracownika o zachowaniu poufności i przestrzeganiu zasad przetwarzanych danych osobowych oraz informacji stanowiących tajemnicę firmową,* w którym zawarto między innymi zobowiązanie pracownika do zachowaniu w tajemnicy przetwarzanych danych, wskazując okres obowiązywania zobowiązania zarówno w trakcie zatrudnienia, jak również po ustaniu stosunku pracy;
- *Wnioski o dostęp do systemu Rejestrów Państwowych (SRP)- użytkownicy aplikacji Źródło*. Wnioski dotyczyły usunięcia kont trzech pracowników Urzędu, w związku z ustaniem stosunków pracy. W jednym przypadku zakończona

[6] ADO- Administrator Danych Osobowych.

została kadencja wójta (21 listopada 2018 r.), a z dwoma pracownikami rozwiązano stosunek pracy (25 września 2020 r.). Dokumenty wypełniono 15 stycznia 2024 r. W przypadku podjętych działań stwierdzono nieprawidłowość, polegającą na niezachowaniu wymogu bezzwłocznego odbierania uprawnień w systemach informatycznych (od ustania stosunku pracy do złożenia wniosków upłynęło od 39 do 61 miesięcy).
Mimo, że czas zakończenia współpracy z pracownikami wykracza poza okres objęty kontrolą, to z uwagi na wagę stwierdzonych błędów kontrolujący postanowili wskazać tę nieprawidłowość w celu uniknięcia przedmiotowych naruszeń w przyszłości.

Kontrolującym nie przedstawiono wniosku o nadanie uprawnień do systemów, o którym mowa w pkt 5 *Instrukcji Zarzadzania Systemem Informatycznym.*
W procedurze nie wskazano wprost, kto i w jakiej formie przekazuje ADO wniosek o nadanie uprawnień do systemów. Zgodnie z wyjaśnieniami Wójta z 27 marca 2025 r. uprawnienia do pracy w systemach informatycznych nadawane są na ustne polecenie Wójta Gminy. Dla czynności, o których mowa powyżej nie jest tworzona dokumentacja. Kontrolujący wskazują, by zgodnie z wewnętrznymi procedurami (po ich doprecyzowaniu) stosować dokument, który poświadczać będzie realizowanie wymogu dokumentowania czynności nadawania i odbierania uprawnień do pracy w systemach informatycznych; pisemny wniosek osób upoważnionych spowoduje, że proces nadawania i odbierania uprawnień będzie w pełni potwierdzony.

(dowód: akta kontroli str. 74-82, 126, 195-206, 210)

2.5 Szkolenia pracowników zaangażowanych w proces przetwarzania informacji.
Podstawa prawna: § 19 ust. 2 pkt 6 rozporządzenia KRI: *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak: a) zagrożenia bezpieczeństwa informacji, b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna, c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich.*
Ustalenia kontroli
W okresie objętym kontrolą w Urzędzie Gminy Banie przeprowadzono trzy szkolenia pracowników z zakresu bezpieczeństwa informacji (w dniu 21 października 2022 r., 18 września 2023 r., 23 września 2024 r.). Udział w szkoleniach dokumentowała lista obecności zawierająca imię i nazwisko uczestnika oraz własnoręczny podpis. Stwierdzono, że w szkoleniu wzięli udział pracownicy wskazani jako osoby realizujące zadania zlecone z zakresu administracji rządowej.
Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie szkolenia osób zaangażowanych w proces przetwarzania informacji. Istotne jest by szkolenia, których celem jest zagwarantowanie bezpieczeństwa w zakresie przetwarzania informacji, ze względu na zmieniające się zagrożenia związane z dynamicznym rozwojem technologii informatycznych miały charakter cykliczny.
Z analizy okazanych dokumentów oraz przedstawionych wyjaśnień wynika, że zakres tematyczny szkoleń przeprowadzonych w Urzędzie obejmował zagadnienia wskazane w § 19 ust. 2 pkt 6 rozporządzenia KRI.

(dowód: akta kontroli str. 176-181)

2.6 Praca na odległość i mobilne przetwarzanie danych.

Podstawa prawna: § 19 ust. 2 pkt 8 rozporządzenia KRI: *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: ustanowienie podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość.*

Ustalenia kontroli

Zasady wykorzystywania w pracy urządzeń mobilnych zostały uregulowane w pkt 8 *Instrukcji Zarzadzania Systemem Informatycznym (Procedury korzystania ze sprzętu przenośnego).*

Procedura przyjęta w Jednostce określa między innymi kwestie wynoszenia poza obszar organizacji sprzętu mobilnego ograniczając tą możliwość tylko do przypadków uzasadnionych wykonywanymi obowiązkami; wdrożono obowiązek szyfrowania danych zapisanych na komputerach przenośnych oraz innych urządzeniach mobilnych a także wymóg zabezpieczenia ich hasłem. W procedurach nie uregulowano kwestii pracy na odległość.

Zgodnie z wyjaśnieniami Wójta z dnia 23 marca 2025 r. do realizacji zadań zleconych z zakresu administracji rządowej w Urzędzie nie wykorzystywano urządzeń mobilnych i nie realizowano pracy na odległość.

(dowód: akta kontroli str. 127-128, 210-211)

2.7 Serwis sprzętu informatycznego i oprogramowania.

Podstawa prawna: § 19 ust. 2 pkt 10 rozporządzenia KRI: *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zawieranie w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.*

Ustalenia kontroli

Obsługa informatyczna Urzędu realizowana jest na podstawie *Umowy na świadczenie usług informatycznych*, XXX.[7] Obsługa informatyczna wg. zapisów umowy obejmuje między innymi następujące czynności: administrowanie siecią teleinformatyczną (utrzymanie i bieżąca obsługa), zarządzanie uprawnieniami użytkowników, zarządzanie oprogramowaniem antywirusowym, administrowanie dostępem do internetu i poczty elektronicznej, serwis oraz ewidencja sprzętu i oprogramowania, wykonywanie kopii bezpieczeństwa, administrowanie bazami danych. W umowie uregulowano kwestię czasu reakcji na zgłoszenie awarii. Z Firmą zawarto ponadto *Umowę o zachowaniu poufności*.[8]

W celu realizacji zadań z zakresu administracji rządowej XXX, zawarto umowę o asystę techniczną oprogramowania komputerowego XXX, obejmującą swym zakresem między innymi: aktualizację i modyfikację, diagnozowanie i usuwanie błędów oprogramowania oraz wsparcie techniczne[9]. W umowie wprowadzono zapisy dotyczące poziomu dostępności oferowanych usług oraz sposobu dostarczania ich na zadeklarowanym poziomie, określono maksymalny czas skutecznej naprawy oprogramowania, zdefiniowano grupy błędów i maksymalny czas ich usunięcia.

Z firmą zawarto również *Umowę powierzenia przetwarzania danych osobowych*

Postanowienia umów przekładają się na realizację dyspozycji § 19 ust. 2 pkt 10 rozporządzenia KRI w zakresie zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.

(dowód: akta kontroli str. 184-194)

[7] Umowa zawarta w dniu 18 kwietnia 2023 r.
[8] Umowa zawarta w dniu 15 marca 2023 r.
[9] Umowa nr EA-005-2025 z dnia 7 stycznia 2025 r.

2.8 Procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji.
Podstawa prawna: § 19 ust. 2 pkt 13 rozporządzenia KRI: *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: bezzwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.*
Ustalenia kontroli
Kwestie postępowania w przypadku stwierdzenia zaistnienia incydentu związanego z bezpieczeństwem informacji ujęto w *Instrukcji Postępowania w Sytuacji Naruszeń podczas przetwarzania dokumentacji w postaci tradycyjnej i elektronicznej w Urzędzie Gminy Banie , 74-100 Banie, ul. Skośnia 6.* W procedurze uregulowano sposób postępowania w przypadku stwierdzenia zaistnienia incydentu związanego z bezpieczeństwem informacji, określając zasady postępowania w przypadku takiego naruszenia. Wskazano katalog zdarzeń, które mogą sygnalizować wystąpienie naruszenia. Przypisano odpowiednie zadania ADO[10] oraz ASI[11] w przypadku powzięcia informacji o naruszeniu bezpieczeństwa informacji.
Kontrolujący wskazują by wewnętrzne procedury uzupełnić o zasady i sposób postępowania w przypadku naruszenia ochrony danych osobowych, zgodnie z wymogami rozporządzenia RODO[12].
W Urzędzie prowadzony jest *Rejestr incydentów bezpieczeństwa oraz działań korygujących i zapobiegawczych*, który nie zawiera wpisów. Zgodnie z wyjaśnieniami Wójta z 27 marca 2025r. w okresie objętym kontrolą nie wystąpiły incydenty naruszenia bezpieczeństwa informacji.

(dowód: akta kontroli str. 182, 163-171)

2.9 Audyt wewnętrzny z zakresu bezpieczeństwa informacji.
Podstawa prawna: § 19 ust. 2 pkt 14 rozporządzenia KRI: *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.*
Ustalenia kontroli
W myśl § 19 ust. 2 pkt 14 rozporządzenia KRI, zarządzanie bezpieczeństwem informacji realizowane jest m.in. poprzez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie działania polegającego na okresowym audycie wewnętrznym w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.
Kontrolującym przedstawiono następujące dokumenty dotyczące okresu objętego weryfikacją:

- *Audyt bezpieczeństwa informacji w ramach realizacji projektu„ Cyberbezpieczny samorząd".* Data przeprowadzenia audytu 3-13 grudnia 2024 r.
- *Audyt wewnętrzny z zakresu zarządzania bezpieczeństwa informacji zgodnie z Krajowymi Ramami Interoperacyjności*. Data przeprowadzenia audytu 3-13 grudnia 2024 r.

Zgodnie z wyjaśnieniami Wójta z 27 marca 2025 r. audyt wewnętrzny z zakresu bezpieczeństwa informacji w latach 2022-2023 nie został przeprowadzony.

[10] Administrator Danych Osobowych
[11] Administrator Systemów Informatycznych
[12] Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r., w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

Mając na względzie powyższe, należy stwierdzić, że w Urzędzie Gminy Banie w 2022 i 2023 roku nie wypełniono obowiązku, o którym mowa w § 19 ust. 2 pkt 14 rozporządzenia KRI.

(dowód: akta kontroli str. 150-171, 211)

2.10 Kopie zapasowe.

Podstawa prawna: § 19 ust. 2 pkt 12 lit. b, e rozporządzenia KRI: *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: minimalizowanie ryzyka utraty informacji w wyniku awarii, zapewnieniu bezpieczeństwa plików systemowych.*

Ustalenia kontroli

Zgodnie z wymogami określonymi w § 19 ust. 2 pkt 12 lit. b i e rozporządzenia KRI, zarządzanie bezpieczeństwem informacji realizowane jest w szczególności poprzez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie m.in. odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na minimalizowaniu ryzyka utraty informacji w wyniku awarii i zapewnieniu bezpieczeństwa plików systemowych.

Kwestie wykonywania kopii bezpieczeństwa opisano w pkt 10 (*Procedury tworzenia i sposobu przechowywania kopii zapasowych*) *Instrukcji Zarządzania Systemem Informatycznym.* W procedurze nie uregulowano zasad tworzenia kopii zapasowych (w tym interwałów czasowych ich tworzenia), nie uregulowano zasad testowania kopii zapasowych, nie wskazano osoby odpowiedzialnej za realizację tych zadań.

Zgodnie z oświadczeniem Wójta z dnia 27 marca 2025 r. w Urzędzie nie są wykonywane kopie bezpieczeństwa oprogramowania XXX i nie przeprowadza się testowania kopii zapasowych.

Mając na względzie powyższe, należy stwierdzić, że w Urzędzie Gminy Banie nie zrealizowano dyspozycji, o której mowa w § 19 ust. 2 pkt 12 lit. b, e rozporządzenia KRI.

(dowód: akta kontroli str. 128-129, 207)

2.11 Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych.

Podstawa prawna: § 15 ust. 1 rozporządzenia KRI: *Systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne projektuje się, wdraża oraz eksploatuje*
z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności przenoszalności i pielęgnowalności, przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk.

Ustalenia kontroli

W celu realizacji zadań z zakresu administracji rządowej XXX, zawarto umowę o asystę techniczną, obejmującą swym zakresem między innymi aktualizację i modyfikację, diagnozowanie i usuwanie błędów oraz wsparcie techniczne oprogramowania komputerowego XXX.

(dowód: akta kontroli str. 184-188)

2.12 Zabezpieczenia techniczno – organizacyjne dostępu do informacji.

Podstawa prawna: § 19 ust. 2 rozporządzenia KRI: *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez:* **pkt 7:** *zapewnienie ochrony przetwarzania informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez: a) monitorowanie dostępu do informacji; b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,*
c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie

systemów operacyjnych, usług sieciowych i aplikacji; pkt 9: *zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie;* pkt 11: *ustalenie zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych.*

Ustalenia kontroli

W celu ustanowienia zabezpieczeń uniemożliwiających osobom nieuprawnionym modyfikację, usunięcie lub zniszczenie informacji każdemu pracownikowi nadano identyfikator i hasło wejścia do systemów zainstalowanych na komputerach oraz do programów, z których korzystają.

W przypadku systemu „Źródło" dostęp jest możliwy wyłącznie z użyciem karty, na której zapisany jest certyfikat umożliwiający zalogowanie się do centralnego systemu.

Pracownicy złożyli oświadczenia o zachowaniu w tajemnicy danych osobowych, do których będą mieli dostęp w trakcie wykonywania obowiązków służbowych.

W wyniku oględzin stanowiska komputerowego wykorzystywanego do realizacji zadań zleconych z zakresu administracji rządowej, przeprowadzonych w toku czynności kontrolnych ustalono, że:

- dostęp do systemu operacyjnego na urządzeniu możliwy był jedynie po wprowadzeniu nazwy użytkownika i hasła,
- komputer miał zainstalowane oprogramowanie antywirusowe oraz skonfigurowany wygaszacz ekranu,
- złożoność hasła była zgodna z wymogami rozporządzenia w sprawie dokumentacji i warunków technicznych,
- ustawienie monitora stanowiska obsługi systemów informatycznych wykorzystywanych do realizacji zadań zleconych z zakresu administracji rządowej uniemożliwiało odczyt wyświetlanych danych przez osoby postronne,
- użytkownikom systemów wykorzystywanych do realizacji zadań zleconych z zakresu administracji rządowej nie nadano uprawnień administratora, uniemożliwiając w ten sposób instalowanie oprogramowania niewiadomego pochodzenia lub zmianę ustawień systemu operacyjnego a także ingerencję w rejestry zdarzeń.

(dowód: akta kontroli str. 148-149)

2.13 Zabezpieczenia techniczno – organizacyjne systemów informatycznych.

Podstawa prawna: § 19 ust. 2 pkt 12 rozporządzenia KRI: *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie (...) odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na: a) dbałości o aktualizację oprogramowania; b) minimalizowaniu ryzyka utraty informacji w wyniku awarii; c) ochronie przed błędami, nieuprawnioną modyfikacją; d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa; e) zapewnieniu bezpieczeństwa plików systemowych; f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych; g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa; h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;* § 19 ust. 4 rozporządzenia KRI: *Niezależnie od zapewnienia działań, o których mowa w ust. 2, w przypadkach uzasadnionych analizą ryzyka w systemach teleinformatycznych podmiotów realizujących zadania publiczne należy ustanowić dodatkowe zabezpieczenia.*

Ustalenia kontroli

- Urząd dysponuje zasilaczami awaryjnymi UPS.

- Na komputerze podlegającym badaniu zainstalowano oprogramowanie antywirusowe.
- Serwerownię wyposażono w klimatyzację i czujkę dymu, natomiast drzwi wejściowe do pomieszczenia nie dysponują należytymi zabezpieczeniami.
- Wejścia do serwerowni podlegają ewidencjonowaniu.
- W procedurach wewnętrznych Jednostki określono zasady:
  - przesyłania danych poza obszar przetwarzania,
  - wykonywania przeglądów i konserwacji elektronicznych nośników informacji.

(dowód: akta kontroli str. 148-149, 207-208)

2.14 Rozliczalność działań w systemach teleinformatycznych.

Podstawa prawna: § 20 ust. 2 rozporządzenia KRI: *W dziennikach systemów odnotowuje się obligatoryjnie działania użytkowników lub obiektów systemowych polegające na dostępie do: 1) systemu z uprawnieniami administracyjnymi; 2) konfiguracji systemu, w tym konfiguracji zabezpieczeń; 3) przetwarzanych w systemach danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa;* **§ 20 ust. 3 rozporządzenia KRI:** *Poza informacjami wymienionymi w ust. 2 mogą być odnotowywane działania użytkowników lub obiektów systemowych, a także inne zdarzenia związane*
z eksploatacją systemu w postaci: 1) działań użytkowników nieposiadających uprawnień administracyjnych, 2) zdarzeń systemowych nieposiadających krytycznego znaczenia dla funkcjonowania systemu, 3) zdarzeń i parametrów środowiska, w którym eksploatowany jest system teleinformatyczny – w zakresie wynikającym z analizy ryzyka; **§ 20 ust. 4 rozporządzenia KRI:** *informacje w dziennikach systemów przechowywane są od dnia ich zapisu, przez okres wskazany w przepisach odrębnych, a w przypadku braku przepisów odrębnych przez dwa lata.*

Ustalenia kontroli

Przetwarzanie informacji w systemach teleinformatycznych wymaga dostępu do danych przez uprawnione osoby i obiekty systemowe (procesy) w ustalonym zakresie. Zapewnienie rozliczalności operacji polega na gromadzeniu informacji o tym, kto, kiedy i jakie czynności wykonał w systemie teleinformatycznym. Obligatoryjnie podlegają dokumentowaniu w postaci zapisów w dziennikach systemów (logi) wszelkie działania dostępu do systemu teleinformatycznego z uprawnieniami administracyjnymi, w zakresie konfiguracji systemu i jego zabezpieczeń a także działania, gdy przetwarzanie danych podlega prawnej ochronie (np. zgodnie z ustawą o ochronie danych osobowych).

Zgodnie z wyjaśnieniami Wójta z dnia 27 marca 2025 r. logi programu XXX nie są przechowywane przez okres 2 lat. Zapis § 20 ust. 4 rozporządzenia KRI zobowiązuje do przechowywania *w dziennikach systemów działań użytkowników lub obiektów systemowych* przez okres 2 lat, wobec czego w tym zakresie nie wypełniono dyspozycji § 20 ust. 4 wyżej opisanego rozporządzenia.

Ponadto zgodnie z wyjaśnieniami Wójta w Jednostce prowadzone są *sporadyczne* działania związane z przeglądaniem logów systemu informatycznego, w celu stwierdzenia i ewentualnej identyfikacji działań niepożądanych, lecz nie jest sporządzana dokumentacja tych czynności. Kontrolujący wskazują aby dokumentować działania związane z przeglądaniem logów systemowych (np. w postaci dziennika administratora), tak by realizowane czynności były w pełni potwierdzone, a w procedurach wewnętrznych uregulować zasady realizacji tych procesów.

(dowód: akta kontroli str. 207-208)

Wpis do książki kontroli	2
Stwierdzone nieprawidłowości w obszarze Nr 2	• Nieprzeglądanie obowiązującej w Urzędzie dokumentacji dotyczącej bezpieczeństwa informacji, do czego zobowiązują zapisy § 19 ust. 2 pkt 1 rozporządzenia KRI. • Dokumentacja regulująca kwestie bezpieczeństwa informacji nie zawiera wszystkich elementów wymaganych przepisami rozporządzenia KRI. • Nieprzeprowadzenie okresowo analizy ryzyka utraty integralności, dostępności lub poufności informacji, do czego zobowiązuje zapis § 19 ust. 2 pkt 3 rozporządzenia KRI. • Niezachowanie wymogu bezzwłocznego odebrania uprawnień w systemach informatycznych, co wynika z zapisów § 19 ust. 2 pkt 5 rozporządzenia KRI. • Nieprzeprowadzenie w 2022 i 2023 roku audytu wewnętrznego w zakresie bezpieczeństwa informacji, zgodnie z wymogami § 19 ust. 2 pkt 14 rozporządzenia KRI. • Niewykonywane kopii bezpieczeństwa oprogramowania XXX, do czego zobowiązują zapisy § 19 ust. 2 pkt 12 lit. b, e rozporządzenia KRI. • Nieprzechowywanie logów systemu XXX przez okres 2 lat, co jest sprzeczne z dyspozycją § 20 ust. 4 rozporządzenia KRI. • Pomieszczenie serwerowni nie dysponuje zabezpieczeniami, zgodnie z dyspozycją § 19 ust. 2 pkt 12 oraz ust. 4 rozporządzenia KRI.
Ocena obszaru kontroli	**Pozytywna z nieprawidłowościami**
Zalecenia	• Wykonywać analizy i przeglądy dokumentacji z zakresu bezpieczeństwa informacji, zgodnie z dyrektywą § 19 ust. 2 pkt 1 rozporządzenia KRI. • Uzupełnić dokumentację regulującą kwestie bezpieczeństwa informacji o elementy wymagane przepisami rozporządzenia KRI, wskazane w treści wystąpienia pokontrolnego. • Przeprowadzać okresowo analizy ryzyka utraty integralności, dostępności lub poufności informacji, do czego zobowiązuje zapis § 19 ust. 2 pkt 3 rozporządzenia KRI. • Przestrzegać wymogu bezzwłocznego odbierania uprawnień w systemach

	informatycznych w przypadku ustania okoliczności ich nadania, zgodnie z dyspozycją § 19 ust. 2 pkt 5 rozporządzenia KRI. • Przeprowadzać audyty wewnętrzne z zakresu bezpieczeństwa informacji, do czego zobowiązują zapisy § 19 ust. 2 pkt 14 rozporządzenia KRI. • Wykonywać kopie bezpieczeństwa oprogramowania XXX, do czego zobowiązują zapisy § 19 ust. 2 pkt 12 lit. b, e rozporządzenia KRI. • Przechowywać logi systemu XXX przez okres 2 lat, zgodnie z dyspozycją § 20 ust. 4 rozporządzenia KRI. • W pomieszczeniu serwerowni zapewnić warunki gwarantujące utrzymanie odpowiedniego poziomu bezpieczeństwa informacji, zgodnie z dyspozycją § 19 ust. 2 pkt 12 lit. b i e oraz ust. 4 rozporządzenia KRI.
Pouczenia	Zgodnie z art. 48 ustawy z dnia 15 lipca 2011 roku o kontroli w administracji rządowej (Dz.U. z 2020 r. poz. 224) od wystąpienia pokontrolnego nie przysługują środki odwoławcze, o podjętych działaniach, mających na celu realizację zaleceń pokontrolnych, proszę poinformować mnie za pośrednictwem Wydziału Kontroli Zachodniopomorskiego Urzędu Wojewódzkiego w Szczecinie w terminie 14 dni od daty otrzymania niniejszego wystąpienia.
Podpis kierownika jednostki kontrolującej	Z upoważnienia Wojewody Zachodniopomorskiego Bartosz Brożyński I Wicewojewoda Zachodniopomorski */podpisano kwalifikowanym podpisem elektronicznym/*