Wojewoda
Zachodniopomorski

Znak: K-2.431.1.41.2025.10.IO

Szczecin, 29 stycznia 2026 r.

**WYSTĄPIENIE POKONTROLNE**

| | |
|---|---|
| **Przedmiot kontroli** | Działanie systemów teleinformatycznych używanych do realizacji zadań zleconych z zakresu administracji rządowej. |
| **Nazwa i adres organu kontrolującego** | Wojewoda Zachodniopomorski,<br>ul. Wały Chrobrego 4, 70-502 Szczecin. |
| **Nazwa i adres organu kontrolowanego** | Wójt Gminy Grzmiąca, ul. ul. 1 Maja 7, 78-450 Grzmiąca. |
| **Osoba pełniąca funkcję Wójta Gminy Grzmiąca w okresie objętym kontrolą** | Pan Patryk Makowski |
| **Okres objęty kontrolą** | od dnia 1 stycznia 2022 r. do dnia 13 października 2025 r. |
| **Kontrolerzy** | Pracownicy Wydziału Kontroli Zachodniopomorskiego Urzędu Wojewódzkiego w Szczecinie:<br>Pani Anna Dąbska – kierownik oddziału, kierownik zespołu kontrolnego,<br>Pani Iwona Olesińska – główny specjalista. |
| **Nr upoważnienia** | Nr 66/25 z dnia 2 września 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];<br>– 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** | 7 – 13 października 2025 r. |

[1] Dz. U. z 2020r., poz. 224.
[2] Dz. U. z 2025r., poz. 1703.

**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 Grzmiąca wykorzystywano system centralny (aplikacja Źródło) oraz system informatyczny wspomagający obsługę spraw obywatelskich 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. 40-41)

**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 Grzmiąca 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 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 Grzmiąca, w okresie objętym kontrolą obowiązywały następujące dokumenty z zakresu bezpieczeństwa informacji:

- *Zarządzenie nr 41/2023 Wójta Gminy Grzmiąca z dnia 11 maja 2023 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji w Urzędzie Gminy Grzmiąca.*
- *Polityka Bezpieczeństwa Informacji w Urzędzie Gminy Grzmiąca (grudzień 2021).*

Dokumentacja zawiera między innymi definicję bezpieczeństwa informacji; oświadczenie o intencjach kierownictwa; wyjaśnienie zasad i wymagań mających szczególne znaczenie dla organizacji; określenie sposobu i wskazanie osób realizujących obowiązki wynikające z rozporządzenia KRI oraz RODO[4].

Rozporządzenie KRI określa ogólne wymagania dotyczące bezpieczeństwa i interoperacyjności systemów teleinformatycznych w administracji publicznej. Jednym z tych wymagań jest zapewnienie ciągłości działania poprzez opracowanie systemu zarządzania bezpieczeństwem informacji, którego elementem jest Plan Ciągłości Działania. Dokument ten winien wskazywać w jaki sposób reagować na zagrożenia i przywracać normalne funkcjonowanie Jednostki poprzez opracowanie szczegółowych procedur, które określą czynności gwarantujące zachowanie ciągłości działania,

[4] 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), Dz. Urz. UE L2016.119, zwane dalej rozporządzeniem RODO.

wskażą osoby odpowiedzialne i potrzebne zasoby w celu zapewnienia możliwości szybkiego przywrócenia dostępności do kluczowych systemów i danych, a w rezultacie do przywrócenia pełnej działalności Podmiotu po incydencie. Zgodnie z wyjaśnieniami Wójta z dnia 8 października 2025 r. w Urzędzie *nie opracowano planów ciągłości działania.*
Dyspozycja § 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. Zgodnie z oświadczeniem Wójta z dnia 10 października 2025 r. *w Urzędzie Gminy Grzmiąca na bieżąco dokonywany jest okresowy przegląd dokumentów zgodnie z zasadami Polityki Bezpieczeństwa Informacji. Czynności te mają na celu zapewnienie aktualności, kompletności oraz zgodności dokumentacji z obowiązującymi przepisami prawa i wewnętrznymi regulacjami jednostki.*
*Z przeprowadzanych przeglądów nie sporządza się odrębnych notatek służbowych ani protokołów*. Kontrolujący wskazują aby dokumentować wyżej opisane działania, tak by realizowane czynności były w pełni potwierdzone (również działania, których efektem jest stwierdzenie braku konieczności wprowadzenia zmian w obowiązującej dokumentacji).
W wyniku analizy obowiązującej w Jednostce dokumentacji związanej z bezpieczeństwem informacji stwierdzono, że funkcjonujące w Jednostce procedury wymagają uzupełnienia o kwestie przywołane w treści powyższego dokumentu kontrolnego.

(dowód: akta kontroli str. 109, 111-213)

### 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 następujące dokumenty:

- *Szacowanie ryzyka dla bezpieczeństwa danych osobowych, 2023-05-31*.
- *Szacowanie ryzyka dla bezpieczeństwa danych osobowych, 2025-01-15*.

Zgodnie z § 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 (...),* wobec czego elementy systemu zarządzania bezpieczeństwem informacji (w tym analiza ryzyka) powinny obejmować bezpieczeństwo wszystkich informacji w organizacji i nie ograniczać się wyłącznie do danych osobowych, na co wskazuje wprost tytuł oraz treść przedstawionych dokumentów. Kontrolujący wskazują by analizy ryzyka nie zawężać do zagadnień związanych z bezpieczeństwem danych osobowych, lecz realizować ją pod kątem ryzyka utraty integralności, dostępności, poufności wszystkich przetwarzanych w Jednostce informacji. W zaprezentowanych analizach wskazano zidentyfikowane ryzyka oraz określone w skali punktowej: skutki wpływu zdarzeń, prawdopodobieństwo materializacji ryzyka oraz istotność ryzyka. W treści dokumentu

zawarto wytyczne dotyczące interpretacji zastosowanej skali punktowej. Dla zidentyfikowanych podatności opracowano plan postępowania z ryzykiem.
(dowód: akta kontroli str. 214-314)

**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.*
**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.
Inwentaryzacja realizowana jest w Urzędzie w wersji elektronicznej, przy wykorzystaniu oprogramowania XXX. System umożliwia generowanie raportów zawierających informacje dotyczące m. in. sprzętu i oprogramowania oraz rodzaju systemu operacyjnego. Kontrolującym przedstawiono metryki komputerów i urządzeń peryferyjnych użytkowanych w Jednostce.
W dokumentach wykazano sprzęt wykorzystywany przy realizacji zadań zleconych z zakresu administracji rządowej.
Mając na uwadze powyższe stwierdzono, że w Urzędzie jest prowadzona inwentaryzacja sprzętu i oprogramowania, zgodnie z wymogami rozporządzenia KRI.
(dowód: akta kontroli str. 379-380)

**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 rozdziale XIX (§ 66-68) *Polityki Bezpieczeństwa Informacji*. Zgodnie z zapisami procedury ASI[5] przyznaje i odbiera uprawnienia na podstawie pisemnego wniosku. Dla czynności, o których mowa powyżej tworzona jest dokumentacja, co powoduje, że proces nadawania i odbierania uprawnień jest w pełni potwierdzony.
Kontrolującym przedstawiono następujące dokumenty:

[5] Administrator Systemu Informatycznego.

- *Wniosek o nadanie/odebranie uprawnień i upoważnień* pracownikom realizującym zadania zlecone z zakresu administracji rządowej*;*
- *Upoważnienie do przetwarzania danych osobowych* - upoważnienie określa jego obszar (wynikający z zadań realizowanych na zajmowanym stanowisku); wskazuje zbiory, do których pracownik uzyskuje dostęp (w celu przetwarzania danych) oraz okres jego ważności*;*
- *Oświadczenie o zapoznaniu się z Polityką Bezpieczeństwa Informacji (PBI);*
- *Deklarację o zachowaniu poufności* - zobowiązujące pracownika do zachowania w poufności danych pozyskanych w trakcie zatrudnienia, 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 przyznania użytkownikom dostępu do systemu
  oraz usunięcia użytkowników.

W trakcie kontroli dokonano sprawdzenia odbierania uprawnień dostępu do systemów informatycznych pracownikom, z którymi ustał lub rozwiązano stosunek pracy. Nie stwierdzono nieprawidłowości w tym zakresie.

(dowód: akta kontroli str. 73-74, 90-91, 159-161, 359-370)

**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 Grzmiąca przeprowadzono następujące szkolenia pracowników z zakresu bezpieczeństwa informacji i ochrony danych osobowych:

- Szkolenie z zakresu ochrony danych osobowych, które odbyło się w dniu 23 czerwca 2025 r.;
- Szkolenie z zakresu ochrony danych osobowych, które przeprowadzono 22 listopada 2024 r.;
- Szkolenie z zakresu ochrony danych osobowych, które przeprowadzono 11 maja 2023 r.;
- Szkolenie z zakresu ochrony danych osobowych oraz cyberbezpieczeństwa, które odbyło się w dniu 1 grudnia 2022 r.

Udział w szkoleniach dokumentowała lista obecności zawierająca imię i nazwisko uczestnika, zajmowane stanowisko oraz własnoręczny podpis.

Stwierdzono, że w szkoleniu przeprowadzonym 23 czerwca 2025 r. nie wzięli udziału pracownicy wskazani jako osoby realizujące zadania zlecone z zakresu administracji rządowej.

Z przedstawionej dokumentacji oraz złożonych wyjaśnień wynika, że zakres tematyczny szkoleń przeprowadzonych w Urzędzie obejmował zagadnienia wskazane w § 19 ust. 2 pkt 6 rozporządzenia KRI.

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 i realizowane były przy udziale wszystkich pracowników Urzędu.

(dowód: akta kontroli str. 108, 371-374)

### 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**

Kwestie trybu pracy przy przetwarzaniu mobilnym i pracy na odległość zostały unormowane w:

- rozdziale XIV *Polityki Bezpieczeństwa Informacji* (*Urządzenia mobilne*),
- rozdziale XV *Polityki Bezpieczeństwa Informacji* (*Praca zdalna*).

W dokumencie uregulowano między innymi kwestie wynoszenia poza obszar organizacji nośników z danymi osobowymi, wprowadzono minimalne wymagania sprzętowe dotyczące urządzeń wykorzystywanych do pracy zdalnej w zakresie zabezpieczeń i kryptografii. Wdrożono również obowiązek szyfrowania danych zapisanych na komputerach przenośnych oraz innych urządzeniach mobilnych.
Zgodnie z wyjaśnieniami Wójta z dnia 8 października 2025 r. w Urzędzie nie wykorzystywano urządzeń mobilnych oraz nie realizowano zadań zleconych z zakresu administracji rządowej w formie pracy zdalnej.

(dowód: akta kontroli str. 74, 149-152)

### 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 realizowana jest przez pracownika zatrudnionego w Urzędzie Gminy Grzmiąca na stanowisku informatyka. Wśród obowiązków pracownika znajduje się m.in.: administrowanie siecią teleinformatyczną, zarządzanie uprawnieniami użytkowników w systemach informatycznych, przechowywanie i archiwizowanie zasobów elektronicznych.
W celu realizacji zadań z zakresu administracji rządowej XXX zawarto umowę, której przedmiotem jest prowadzenie nadzoru i serwisu oprogramowania użytkowanego systemu XXX. Stwierdzono, że w powyższej umowie (wraz z obowiązującymi aneksami) nie wprowadzono zapisów określających maksymalny czas skutecznej naprawy oprogramowania. Z XXX zawarto umowę dotyczącą powierzenia przetwarzania danych osobowych[6].

(dowód: akta kontroli str. 75-78, 375-378)

### 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**

[6] Umowa nr 9728 z dnia 6.12.2016 r.

*W Polityce Bezpieczeństwa Informacji,* w rozdziale IV (*Zgłaszanie* n*aruszenia ochrony danych osobowych)* określono zasady i sposób postępowania w przypadku wystąpienia incydentów związanych z naruszeniem ochrony danych osobowych. W procedurze wskazano katalog zdarzeń, które mogą sygnalizować wystąpienie naruszenia oraz przypisano odpowiednie zadania ADO[7] oraz IOD[8] w przypadku powzięcia informacji o naruszeniu danych osobowych. W rozdziale XXIII § 89 (*Reagowanie na naruszenia zasad PBI i niewłaściwe funkcjonowanie systemu*) określono zasady i sposób postępowania w przypadku wystąpienia incydentów związanych z funkcjonowaniem systemu teleinformatycznego.
W trakcie kontroli kontrolującym przedstawiono dokument *Rejestr incydentów, rok 2024,* który zawiera dwa wpisy dotyczące zdarzeń zakwalifikowanych, jako incydenty z zakresu bezpieczeństwa. Z *Protokołów obsługi incydentu* wynika, że w jednym przypadku wystąpiła konieczność zgłoszenia tego przypadku organowi nadzorczemu.
(dowód: akta kontroli str.128-129, 172, 381)

### 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 wewnętrzny z zakresu zarządzania bezpieczeństwem informacji zgodnie z Krajowymi Ramami Interoperacyjności, data przeprowadzenia: 8 listopada 2024 roku;
- Audyt wewnętrzny z zakresu zarządzania bezpieczeństwem informacji zgodnie z Krajowymi Ramami Interoperacyjności, data przeprowadzenia: 15 listopad 2023 roku;
- Raport z audytu „Praktyczna realizacja założeń Polityki Bezpieczeństwa Informacji w Urzędzie Gminy Grzmiąca", listopad 2022.

Z zapisów zawartych w dokumentach wynika, że audyt wewnętrzny przeprowadzony w Jednostce, w 2024 oraz 2023 roku został zrealizowany przez zespół, w skład którego wszedł pracownik zatrudniony w Urzędzie na stanowisku Informatyka, wykonujący zadania Administratora Systemów Informatycznych.
Administrator Systemu Informatycznego odpowiedzialny jest za funkcjonowanie systemu informatycznego, za przestrzeganie zasad i wymagań bezpieczeństwa przewidzianych dla systemu informatycznego oraz weryfikację i bieżącą kontrolę zgodności funkcjonowania z wymaganiami bezpieczeństwa, wobec czego nie powinna mieć miejsca sytuacja by osoba odpowiadająca za bieżące funkcjonowanie bezpieczeństwa danych w systemach informatycznych weryfikowała swoje własne kompetencje i działania, pod kątem zgodności z wymogami rozporządzenia KRI.

[7] Administrator Danych Osobowych
[8] Inspektor Ochrony Danych

Z wyjaśnień Wójta z 10 października 2025 r. wynika, że audyty wewnętrzne z zakresu zarządzania bezpieczeństwem informacji, *zostały przeprowadzone i opracowane przez podmiot zewnętrzny (...). Natomiast pracownik Urzędu (...) był jedynie odpowiedzialny za udzielnie niezbędnych informacji oraz wskazanie systemów informatycznych funkcjonujących w jednostce i nie uczestniczył w dokonywaniu czynności kontrolnych w tym zakresie.* Kontrolujący przyjmują wyjaśnienia złożone w tym zakresie.

(dowód: akta kontroli str. 110, 315-370)

**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.

Zasady wykonywania, przechowywania oraz testowego odtworzenia kopii bezpieczeństwa uregulowano w rozdziale XIII (*Zapasowe kopie informacji*) oraz rozdziale XVIII (*Zarządzanie kopiami nośników i danych) Polityki Bezpieczeństwa Informacji.*

Zgodnie z wyjaśnieniami Informatyka z dnia 9 października 2025 r.:

- kopie baz danych oraz oprogramowania wykorzystywanego do realizacji zadań zleconych z zakresu administracji rządowej są wykonywane w cyklach tygodniowych i zapisywane na dysku zewnętrznym oraz przechowywane poza miejscem wytworzenia;
- kopie systemów pracujących w sieci oraz maszyn wirtualnych wykonywane są codziennie, i podlegają szyfrowaniu;
- kopie oprogramowania podlegającego kontroli XXX sprawdzane są pod kątem poprawności ich wykonania lecz nie jest tworzona dokumentacja potwierdzająca przeprowadzanie testów.

Kontrolujący wskazują by dokumentować czynności związane z próbnym testowaniem kopii zapasowych programu XXX na potrzeby weryfikacji poprawności i stanu ich wykonywania, tak by realizowane działania były w pełni potwierdzone.

(dowód: akta kontroli str. 79-84, 148, 157)

**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, której przedmiotem jest prowadzenie nadzoru i serwisu oprogramowania użytkowanego systemu XXX.

(dowód: akta kontroli str. 377-378)

**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 stanowisk komputerowych wykorzystywanych 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,
- złożoność hasła była zgodna z wymogami rozporządzenia w sprawie dokumentacji i warunków technicznych,
- ustawienie monitorów stanowisk obsługi systemów informatycznych wykorzystywanych do realizacji zadań zleconych z zakresu administracji rządowej uniemożliwiało odczyt wyświetlanych danych przez osoby postronne,
- komputery miały zainstalowane oprogramowanie antywirusowe oraz skonfigurowany wygaszacz ekranu,
- 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. 97-105)

**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**

- Urządzenia informatyczne Jednostki są podłączone do zasilaczy awaryjnych UPS.
- Na komputerach podlegających badaniu zainstalowano oprogramowanie antywirusowe.
- W Jednostce zastosowano zintegrowane rozwiązania do zarządzania bezpieczeństwem w sieci.
- XXX.
- W procedurach wewnętrznych Jednostki określono:
  - zasady wykonywania konserwacji i naprawy sprzętu;
  - zasady wycofywania sprzętu i niszczenia nośników informacji;
  - zasady szyfrowania informacji i sposoby stosowania kryptografii;
  - reguły przesyłania danych poza obszar przetwarzania;
  - procedury korzystania z Internetu i poczty elektronicznej.
- W procedurach wewnętrznych brak uregulowań dotyczących zasad dostępu do serwerowni oraz kwestii pobierania, zdawania i przechowywania kluczy do pomieszczeń służbowych w Urzędzie.

(dowód: akta kontroli str. 74, 93-96, 105-106)

**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).

Logi programu XXX są przechowywane przez okres 2 lat. Z przedstawionych dokumentów wynika, że logi odnotowujące działania administratora zawierają tylko informacje o udanym zalogowaniu oraz wylogowaniu z systemu, natomiast nie wskazują innych aktywności, w tym dotyczących nadania oraz odebrania uprawnień użytkownikom.
Działania związane z zapewnieniem rozliczalności użytkowników, szczególnie posiadających uprawnienia do administrowania systemami oraz zmianami konfiguracji systemów operacyjnych i ich zabezpieczeń, zwłaszcza podczas przetwarzania danych podlegających prawnej ochronie wymagają bieżącego dostępu do logów zawierających informacje o tym kto, kiedy i jakiego rodzaju operacje przeprowadzał wykorzystując dostęp do użytkowanego programu. Kontrolujący wskazują by wystąpić do producenta oprogramowania o zaimplementowanie do programu funkcjonalności pozwalającej na śledzenie zmian dotyczących uprawnień (nadawania
i ich modyfikacji) oraz innych rodzajów działań administratora i użytkowników, co pozwoli usprawnić bieżące zarządzanie uprawnieniami w systemie jak i czynności sprawdzające związane z przeglądaniem logów (np. pod kątem czy operacje wykonywane w systemie informatycznym są zgodne z kompetencjami użytkownika).
Zgodnie z wyjaśnieniami Informatyka w Jednostce prowadzone są 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 prowadzić wyżej opisane działania oraz dokumentować je (np. w postaci dziennika administratora), tak by realizowane czynności były w pełni potwierdzone.

(dowód: akta kontroli str. 85-93)

| | |
|---|---|
| **Wpis do książki kontroli** | 3/2025 |
| **Stwierdzone nieprawidłowości w obszarze Nr 2** | • Dokumentacja regulująca kwestie bezpieczeństwa informacji nie zawiera wszystkich elementów wymaganych przepisami rozporządzenia KRI.<br>• Zawężenie analizy ryzyka do zagadnień związanych z bezpieczeństwem danych osobowych, co nie realizuje w pełni dyspozycji § 19 ust. 2 pkt 3 rozporządzenia KRI.<br>• Nieopracowanie Planu Ciągłości Działania, do czego zobowiązują zapisy § 19 ust. 1 rozporządzenia KRI.<br>• W umowie XXX, której przedmiotem jest sprawowanie opieki autorskiej nad systemami wykorzystywanymi do realizacji zadań zleconych z zakresu administracji rządowej brak zapisów określających maksymalny czas skutecznej naprawy oprogramowania, co nie wypełnia dyspozycji § 19 ust. 2 pkt 10 rozporządzenia KRI.<br>• Nieodnotowywanie w dziennikach systemów wszystkich rodzajów aktywności użytkowników z uprawnieniami administracyjnymi, co jest niezgodne z dyspozycją § 20 ust. 2 rozporządzenia KRI. |

| | |
|---|---|
| | • Pomieszczenie serwerowni nie wypełnia dyspozycji § 19 ust. 2 pkt 12 oraz ust. 4 rozporządzenia KRI. |
| Ocena obszaru kontroli | Pozytywna z nieprawidłowościami |
| Zalecenia | • Uzupełnić dokumentację regulującą kwestie bezpieczeństwa informacji o elementy wymagane przepisami rozporządzenia KRI, wskazane w treści wystąpienia pokontrolnego.<br>• Uzupełnić analizę ryzyka o zagadnienia dotyczące ryzyka utraty integralności, dostępności, poufności wszystkich przetwarzanych w Jednostce informacji, zgodne z dyspozycją § 19 ust. 2 pkt 3 rozporządzenia KRI.<br>• Opracować Plan Ciągłości Działania, do czego zobowiązują zapisy § 19 ust. 1 rozporządzenia KRI.<br>• W umowie XXX, której przedmiotem jest sprawowanie opieki autorskiej nad systemami wykorzystywanymi do realizacji zadań zleconych z zakresu administracji rządowej wprowadzić zapisy określające maksymalny czas skutecznej naprawy oprogramowania, zgodnie z dyspozycją § 19 ust. 2 pkt 10 rozporządzenia KRI.<br>• Odnotowywać w dziennikach systemów wszystkie rodzaje aktywności użytkowników z uprawnieniami administracyjnymi, zgodne z dyspozycją § 20 ust. 2 rozporządzenia KRI.<br>• 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<br>Wojewody Zachodniopomorskiego<br>Bartosz Brożyński<br>I Wicewojewoda Zachodniopomorski<br>*/podpisano kwalifikowanym podpisem elektronicznym/* |