Wojewoda
Zachodniopomorski

Znak: K-2.431.1.20.2025.10.IO

Szczecin, 28 sierpnia 2025 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 Dolice, ul. Ogrodowa 16, 73-115 Dolice. |
| **Osoba pełniąca funkcję Wójta Gminy Dolice w okresie objętym kontrolą** | Pan Paweł Nowakowski |
| **Okres objęty kontrolą** | od dnia 1 stycznia 2022 r. do dnia 2 czerwca 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 26/25 z dnia 15 kwietnia 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** | 27 maja -2 czerwca 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 Dolice 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. 52-56, 88-91, 213-215)

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

- *Zarządzenie Nr 182/20 Wójta Gminy Dolice z dnia 2 października 2020 r. w sprawie wprowadzenia Regulaminu monitoringu wizyjnego.*
- *Zarządzenie Nr 187/20 Wójta Gminy Dolice z dnia 9 października 2020 r. w sprawie ustalenia Instrukcji pobierania, zdawania i przechowywania kluczy od pomieszczeń służbowych w Urzędzie Gminy Dolice.*
- *Zarządzenie Nr 8/2022 Wójta Gminy Dolice z dnia 25.01.2022 r. w sprawie wyłączenia pracowników urzędu Gminy Dolice z wykonywania zadań w ramach pracy zdalnej.*
- *Zarządzenie Nr 17/2022 Wójta Gminy Dolice z dnia 1 marca 2022 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji oraz Instrukcji Zarządzania Systemami Informatycznymi[4] wraz z wykazem zabezpieczeń regulacji ochrony danych osobowych w Urzędzie Gminy Dolice.*

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. W okresie objętym kontrolą, zgodnie z

[4] Instrukcja Zarządzania Systemami Informatycznymi wraz z wykazem zabezpieczeń regulacji ochrony danych osobowych dalej: Instrukcja Zarządzania Systemami Informatycznymi.

wyjaśnieniami Wójta z dnia 27 maja 2025 r. dokumentacja dotycząca bezpieczeństwa informacji nie była *przedmiotem aktualizacji*, wobec czego należy stwierdzić, że nie zrealizowano dyspozycji § 19 ust. 2 pkt 1 rozporządzenia KRI.
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. 99, 104-150)

**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 ryzyka*, który zgodnie z wyjaśnieniami Wójta z dnia 27 maja 2025 r. został sporządzony w 2018 r. Z treści złożonych wyjaśnień wynika również, że analiza podlegała aktualizacjom, przy czym ostatnia przeprowadzona została w 2021 r. W zaprezentowanej analizie ryzyka, określono zagrożenia dla wskazanych zasobów, źródła tych zagrożeń oraz prawdopodobieństwo i skutki wpływu zdarzeń na czynniki decydujące o bezpieczeństwie danych.
Stwierdzono, że wyżej przywołana analiza ryzyka obejmująca zidentyfikowane aktywa Jednostki, wypełnia w części dyspozycję, o której mowa w § 19 ust. 2 pkt 3 rozporządzenia KRI, nie spełnienia natomiast wymogu dotyczącego okresowości jej przeprowadzania. 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. 101, 179-187)

**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.
Kontrolującym przedstawiono dokument *Inwentaryzacja sprzętu, audyt zainstalowanego oprogramowania*, który zawiera informacje dotyczące rodzaju użytkowanego sprzętu i jego charakterystyki; zainstalowanego oprogramowania; rodzaju systemu operacyjnego oraz współpracujących urządzeń peryferyjnych.

W udostępnionym zestawieniu zidentyfikowano sprzęt wykorzystywany przy realizacji zadań zleconych z zakresu administracji rządowej.

(dowód: akta kontroli str. 205-208)

**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 IV *Instrukcji Zarzadzania Systemami Informatycznymi (Nadawanie uprawnień do przetwarzania danych osobowych*). Zgodnie z zapisami procedury *bezpośredni przełożony (…) wydaje na piśmie polecenie administratorowi*[5] *o nadaniu, zmianie odebraniu lub ograniczeniu uprawnień do zasobów i aplikacji.*
Zgodnie z wyjaśnieniami Wójta z 30 maja 2025 r. uprawnienia do pracy w systemie informatycznym (służącym do realizacji zadań zleconych z zakresu administracji rządowej) nadawane są na podstawie ustnego wniosku bezpośredniego przełożonego pracownika, skierowanego do Wójta Gminy i proces realizowany jest w ten sam sposób przez informatyka (ustne polecenie). Dla czynności, o których mowa powyżej nie jest tworzona dokumentacja. Kontrolujący wskazują, by zgodnie z wewnętrznymi procedurami 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.
Kontrolującym przedstawiono:

- *Upoważnienie do przetwarzania danych osobowych* wystawione pracownikom realizującym zadania zlecone z zakresu administracji rządowej. Upoważnienie określa zakres przetwarzania, wskazując określone enumeratywnie zbiory papierowe jak i systemy informatyczne.
- *Oświadczenie pracowników 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;

[5] informatyk

- *Wnioski o dostęp do Systemu Rejestrów Państwowych (SRP)- użytkownicy aplikacji Źródło*. Wnioski dotyczyły przyznania użytkownikom dostępu do systemu.

Z uwagi na fakt, że w okresie podlegającym badaniu, nie wystąpiły przypadki cofania uprawnień nadanych pracownikom realizującym zadania zlecone z zakresu administracji rządowej, nie dokonano sprawdzenia blokowania dostępu do systemów informatycznych.

(dowód: akta kontroli str. 88-98, 99-100, 132-133, 211-220)

**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 Dolice przeprowadzono szkolenie pracowników z zakresu cyberbezpieczeństwa. Szkolenie zorganizowano w dniach 27, 28, 29 marca 2023 r. z podziałem pracowników na trzy grupy wykładowe.
Udział w szkoleniu 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. Z analizy okazanych dokumentów oraz przedstawionych wyjaśnień wynika, że zakres tematyczny szkolenia przeprowadzonego 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.
Z dokumentu opracowanego w Jednostce - *Analiza ryzyka* wynika, że dla zidentyfikowanych zagrożeń (np. infekcja złośliwym oprogramowaniem, nieuprawnione kopiowanie danych, brak świadomości/wiedzy, sabotaż wewnętrzny, kradzież dokumentów przez osoby upoważnione, atak hakerski, nieprzestrzeganie procedur, pomyłki) przy ocenie ryzyka ich materializacji na poziomie, który nakazuje podjęcie działań w celu redukcji do poziomu akceptowalnego, wskazano działanie w postaci *szkolenia pracowników.* Należy rozważyć, czy w związku z powyższym przeprowadzenie, na przestrzeni kilku lat tylko jednego szkolenia pracowników jest wystarczające i skutecznie realizuje cele założone w analizie ryzyka.

(dowód: akta kontroli str. 100, 200-204)

**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 następujących dokumentach:

- *Polityce bezpieczeństwa informacji*, w rozdziale VI pkt 5 (*Regulamin ochrony danych osobowych - Wynoszenie nośników danych poza obszar przetwarzania);*
- *Instrukcji zarządzania systemem informatycznym,* w rozdziale VII (*Zabezpieczenie systemu informatycznego);*

W wyżej wymienionych dokumentach uregulowano między innymi kwestie wynoszenia poza obszar organizacji nośników z danymi osobowymi (w tym dokumentów wytworzonych w formie papierowej), wprowadzając wymóg uzyskania zgody przełożonego. Wdrożono obowiązek szyfrowania danych zapisanych na komputerach przenośnych oraz innych urządzeniach mobilnych.
Zgodnie z wyjaśnieniami Wójta z dnia 27 maja 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. 100, 113-114, 134-135)

## 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 Dolice na stanowisku informatyka Urzędu Gminy. Wśród obowiązków pracownika znajduje się m.in.: administrowanie systemami, sieciami informatycznymi oraz archiwizowanie zasobów elektronicznych; wdrażanie nowych systemów informatycznych; pełnienie roli lokalnego administratora systemu w SRP[6]; nadzór nad zabezpieczeniem sprzętu i pomieszczeń w celu zabezpieczenia danych.
W celu realizacji zadań z zakresu administracji rządowej XXX, zawarto umowę o asystę techniczną oprogramowania komputerowego XXX, obejmującą swym zakresem między innymi: aktualizację, modyfikację, diagnozowanie i usuwanie błędów oprogramowania oraz wsparcie techniczne[7]. 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*[8]*.* 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. 188-199)

## 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.*

[6] SRP- System Rejestrów Państwowych.
[7] Umowa nr EA-058-2025 z dnia 2 stycznia 2025 r.
[8] Umowa nr EP-058-2025 z dnia 2 stycznia 2025 r.

**Ustalenia kontroli**

W *Polityce bezpieczeństwa informacji*, w rozdziale V (*Incydenty)* oraz w rozdziale VI, pkt 8 (*Regulamin ochrony danych osobowych, Incydenty związane z naruszeniem bezpieczeństwa informacji)* określono zasady i sposób postępowania w przypadku zaistnienia incydentu związanego z bezpieczeństwem informacji. Wskazano katalog zdarzeń, które mogą sygnalizować wystąpienie naruszenia i przypisano odpowiednie zadania ADO[9] oraz ASI[10].

Kontrolującym przedstawiono dokument *Rejestr naruszeń ochrony danych osobowych oraz incydentów bezpieczeństwa danych*, w którym opisano jedno, konkretne zdarzenie wraz z przedstawieniem oceny naruszenia oraz podjętych działań. W wyniku ewaluacji zdarzenia, przeprowadzonej przez administratora danych stwierdzono, że nie wystąpiła konieczność zgłoszenia tego przypadku organowi nadzorczemu.

Kontrolujący wskazują, by rejestr naruszeń był prowadzony w formie ewidencji czyli wykazu (listy, spisu) i odnosił się nie do jednostkowych zdarzeń, a porządkował wszystkie zdarzenia, które mogą wystąpić w Jednostce.

(dowód: akta kontroli str. 111-112, 209-210)

**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:

- *Sprawozdanie roczne 2022. Audyt w zakresie ochrony danych osobowych, prowadzenie strony www oraz BIP.*
- *Sprawozdanie roczne 2023. Audyt w zakresie znajomości i przestrzegania regulaminu ochrony danych osobowych przyjętego w Jednostce.*
- *Sprawozdanie roczne 2024. Audyt w zakresie spełnienia obowiązków wynikających z rozporządzenia ws. ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych - RODO.*

Zagadnienia poddane ocenie, w przypadku audytów przeprowadzonych w latach 2022-2024, dotyczyły głównie kwestii ochrony danych osobowych. W ocenie kontrolujących skupienie się w ciągu kolejnych trzech lat na zagadnieniach opisanych powyżej może skutkować niepełnym rozpoznaniem problemów i potrzeb w zakresie innych obszarów bezpieczeństwa informacji. Audyt wewnętrzny stanowi bowiem istotne źródło informacji dla kierownictwa Jednostki o realnym stanie bezpieczeństwa, różnych aspektach jego utrzymania oraz wskazuje obszary wymagające podjęcia działań korygujących.

(dowód: akta kontroli str. 151-178)

[9] Administrator Danych Osobowych
[10] Administrator Systemów Informatycznych

**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 rozdziale V (*Tworzenie kopii zapasowych*) *Instrukcji Zarządzania Systemami Informatycznymi.* W dokumencie nie uregulowano zasad tworzenia kopii zapasowych w przypadku programów, które nie podlegają procedurze tworzenia w sposób zautomatyzowany, *w oparciu o skrypt lub specjalne oprogramowanie.* Nie uregulowano również zasad testowania kopii zapasowych oraz nie wskazano osoby odpowiedzialnej za realizację tworzenia i testowego odtworzenia tych kopii.
Zgodnie z wyjaśnieniami Wójta z dnia 4 czerwca 2025 r. kopie zapasowe oprogramowania XXX wykonywane są raz w tygodniu, przez podłączenie dysku twardego USB i zgraniu bazy danych. Przechowywane są poza miejscem ich wytworzenia. Ponadto z wyjaśnień wynika, że *nie przeprowadzano testowych odtwarzań kopii zapasowych.*

(dowód: akta kontroli str. 133-134, 221-222 )

**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. 190-199)

**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 monitora stanowiska obsługi systemów informatycznych wykorzystywanych do realizacji zadań zleconych z zakresu administracji rządowej uniemożliwiało odczyt wyświetlanych danych przez osoby postronne,
- jeden z komputerów miał zainstalowane oprogramowanie antywirusowe oraz skonfigurowany wygaszacz ekranu, natomiast w przypadku drugiej jednostki stwierdzono brak zainstalowanego oprogramowania antywirusowego.

(dowód: akta kontroli str. 102-103, 222-225)

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.
- W Jednostce zastosowano zintegrowane rozwiązania do zarządzania bezpieczeństwem w sieci.

- Na jednym z dwóch komputerów podlegających badaniu nie zainstalowano oprogramowania antywirusowego.
- Serwerownię wyposażono w klimatyzację, czujkę ruchu i dymu oraz gaśnicę. Drzwi wejściowe do pomieszczenia nie dysponują natomiast należytymi zabezpieczeniami.
- W procedurach wewnętrznych Jednostki określono zasady:
  - przesyłania danych poza obszar przetwarzania,
  - wykonywania przeglądów i konserwacji elektronicznych nośników informacji,
  - naprawy sprzętu wykonywanej przez podmioty zewnętrzne,
  - niszczenia elektronicznych i papierowych nośników danych,
  - pobierania, zdawania i przechowywania kluczy od pomieszczeń służbowych w Urzędzie.
- W pomieszczeniu serwerowni umieszczone zostały urządzenia serwerowe należące do odrębnej organizacyjnie jednostki. Zgodnie z wyjaśnieniami Informatyka dostęp do serwerowni posiadają jedynie osoby upoważnione przez Wójta Gminy i będące pracownikami Urzędu, natomiast dostęp innych osób – przedstawicieli właściciela umieszczonych w pomieszczeniu urządzeń odbywa się tylko w obecności upoważnionych pracowników Urzędu. Kontrolującym nie przedstawiono dziennika dokumentującego fakty wejścia do pomieszczenia serwerowni. Kontrolujący wskazują, że (szczególnie wobec wyżej opisanego stanu) konieczne jest uregulowanie tej sytuacji w procedurach wewnętrznych (np. poprzez uzupełnienie *Instrukcji pobierania, zdawania i przechowywania kluczy od pomieszczeń służbowych w Urzędzie Gminy Dolice)* pod kątem wskazania osób uprawnionych do wejścia do stref wydzielonych.

(dowód: akta kontroli str. 102-103, 129-137, 142-150, 222, 224-225)

**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 4 czerwca 2025 r. logi programu XXX są przechowywane przez okres 2 lat.
Kontrolujący w piśmie z dnia 2 czerwca 2025 r. zwrócili się o wyjaśnienie c*zy w Jednostce są prowadzone działania związane z przeglądaniem logów i ich analizą w celu identyfikacji działań niepożądanych oraz o (...) przedstawienie stosownej dokumentacji.*
W odpowiedzi na powyższe pismem z dnia 4 czerwca 2025 r. Wójt poinformował o *braku dokumentacji potwierdzającej przeglądanie logów.* Wobec niezłożenia jednoznacznej deklaracji co do prowadzenia działań związanych z przeglądaniem logów i ich analizą w celu identyfikacji działań niepożądanych kontrolujący stwierdzają, że w Urzędzie nie są prowadzone działania związane z przeglądaniem logów i ich analizą w celu identyfikacji działań niepożądanych.
Kontrolujący wskazują aby prowadzić wyżej opisane działania oraz dokumentować je (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. 86, 221-222, 227-228)

| **Wpis do książki kontroli** | 6 |
|---|---|
| **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.<br>• Dokumentacja regulująca kwestie bezpieczeństwa informacji nie zawiera wszystkich elementów wymaganych przepisami rozporządzenia KRI.<br>• Nieprzeprowadzenie okresowo analizy ryzyka utraty integralności, dostępności lub poufności informacji, do czego zobowiązuje zapis § 19 ust. 2 pkt 3 rozporządzenia KRI.<br>• Niezachowanie wymogu formy pisemnej przy nadaniu, zmianie, odebraniu lub ograniczeniu uprawnień do pracy w systemach informatycznych, co jest niezgodne z wewnętrznymi regulacjami Urzędu.<br>• Nieprzeprowadzanie testowych odtworzeń kopii zapasowych, zgodnie z wymogami § 19 ust. 2 pkt 12 lit. b i e rozporządzenia KRI.<br>• Niezainstalowanie oprogramowania antywirusowego na jednym z dwóch stanowisk komputerowych podlegających badaniu, co jest niezgodne z zapisami § 19 ust. 2 rozporządzenia KRI oraz wewnętrznymi regulacjami Urzędu.<br>• Nieprowadzenie działań związanych z przeglądaniem logów i ich analizą w celu identyfikacji działań niepożądanych, zgodnie |

| | |
|---|---|
| | z dyspozycją § 19 ust. 2 pkt 12 rozporządzenia KRI.<br>• 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 dyspozycją § 19 ust. 2 pkt 1 rozporządzenia KRI.<br>• Uzupełnić dokumentację regulującą kwestie bezpieczeństwa informacji o elementy wymagane przepisami rozporządzenia KRI, wskazane w treści wystąpienia pokontrolnego.<br>• Przeprowadzać okresowo analizy ryzyka utraty integralności, dostępności lub poufności informacji, do czego zobowiązuje zapis § 19 ust. 2 pkt 3 rozporządzenia KRI.<br>• Zachować formę pisemną przy nadaniu, zmianie, odebraniu lub ograniczeniu uprawnień do pracy w systemach informatycznych, zgodnie z wewnętrznymi regulacjami Urzędu.<br>• Przeprowadzać testowe odtworzenia kopii zapasowych, zgodnie z wymogami § 19 ust. 2 pkt 12 lit. b i e rozporządzenia KRI.<br>• Zainstalować oprogramowanie antywirusowe na wskazanym w treści wystąpienia pokontrolnego stanowisku komputerowym, zgodne z zapisami § 19 ust. 2 rozporządzenia KRI oraz wewnętrznymi regulacjami Urzędu.<br>• Prowadzić działania związane z przeglądaniem logów i ich analizą w celu identyfikacji działań niepożądanych, zgodnie z dyspozycją § 19 ust. 2 pkt 12 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/* |