Wojewoda
Zachodniopomorski

Znak: K-2.431.1.9.2026.7.IO

Szczecin, 23 kwietnia 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, ul. Wały Chrobrego 4, 70-502 Szczecin.
Nazwa i adres organu kontrolowanego	Wójt Gminy Przybiernów, ul. Cisowa 3, 72-110 Przybiernów.
Osoba pełniąca funkcję Wójta Gminy Przybiernów w okresie objętym kontrolą	Pan Bogdan Jarosław Czaplicki
Okres objęty kontrolą	od dnia 1 stycznia 2023 r. do dnia 27 lutego 2026 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 8/26 z dnia 12 lutego 2026 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	22 – 27 lutego 2026 r.

[1] Dz. U. z 2026 r., poz. 158.
[2] Dz. U. z 2025 r., 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 w Przybiernowie 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. 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 w Przybiernowie wymieniał dane

[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".

w formatach 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**

Obszar kontroli Nr 2: 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 systemu bezpieczeństwa informacji zapewniającego poufność, dostępność, integralność informacji. W Urzędzie Gminy w Przybiernowie, w okresie objętym kontrolą obowiązywało *Zarządzenie nr 115/19 Wójta Gminy Przybiernów z dnia 31 grudnia 2019 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji*.

Dyspozycja § 19 ust. 1 rozporządzenia KRI wskazuje również na obowiązek *przeglądu systemu zarządzania bezpieczeństwem informacji a* ust. 2 pkt 1 na konieczność zapewnienia *aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia,* co przekłada się na konieczność okresowego przeglądu i uaktualnienia dokumentacji regulującej bezpieczeństwo informacji. Kontrolującym przedstawiono zapisy *Planu postępowania z ryzykiem*, wśród których znajdują się informacje o przeprowadzonym przeglądzie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), ze wskazaniem konieczności zmiany zapisów SZBI. Konieczność zmian w Systemie Zarządzania Bezpieczeństwem Informacji wskazano w dokumentach dotyczących kolejnych lat 2023, 2024, 2025. Sam zapis w dokumentacji wskazujący potrzebę zmian, bez ich faktycznego wdrożenia, świadczy o tym, że proces monitorowania i przeglądu jest nieskuteczny. Przegląd ma prowadzić bowiem do działań naprawczych, a nie tylko do faktu odnotowania jego przeprowadzenia.

W *Planie postępowania z ryzykiem* wskazano konieczność zmian, co oznacza, że Jednostka uznała dotychczasowe regulacje za nieadekwatne do obecnego stanu (technologicznego, prawnego lub organizacyjnego). W ślad za tymi ustaleniami należało dokonać zmian w obszarach zidentyfikowanych jako te, które wymagają korekty.

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, wskażą osoby odpowiedzialne i potrzebne zasoby w celu zapewnienia możliwości szybkiego przywrócenia dostępności do kluczowych systemów i danych Podmiotu po zaistnieniu potencjalnego incydentu. Zgodnie z wyjaśnieniami Wójta z dnia 23 lutego 2026 r. w Urzędzie nie opracowano planu ciągłości działania. 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. 76, 78-80, 115-175)

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:

- *Analizę ryzyka bezpieczeństwa informacji dla Urzędu Gminy w Przybiernowie.* Data utworzenia 17.03.2025 r.;
- *Analizę ryzyka bezpieczeństwa informacji dla Urzędu Gminy w Przybiernowie.* Data utworzenia 19.03.2024 r.;
- *Analizę ryzyka bezpieczeństwa informacji*. Data utworzenia 21.03.2023 r.

Zaprezentowane analizy ryzyka obejmują aktywa Jednostki. W dokumentach określono zagrożenia dla wskazanych zasobów, prawdopodobieństwo i skutki wpływu zdarzeń na czynniki decydujące o bezpieczeństwie informacji. Dokumenty zawierają również plany postępowania z ryzykiem.

(dowód: akta kontroli str. 78-80, 201-205)

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 spis sprzętu komputerowego i oprogramowania oraz urządzeń peryferyjnych użytkowanych w Jednostce. W dokumentach wykazano sprzęt wykorzystywany przy realizacji zadań zleconych z zakresu administracji rządowej.

(dowód: akta kontroli str. 109-112)

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 uprawnień do pracy w systemie informatycznym uregulowano w rozdziale V, pkt 2 *Polityki Bezpieczeństwa Informacji* (Regulamin ochrony danych osobowych. Uprawnienia.). Zgodnie z zapisem procedury *polecenie do utworzenia konta wraz z uprawnieniami wydaje przełożony. Czynności te wykonuje osoba wyznaczona, tj. informatyk (ASI)*. Zgodnie z wyjaśnieniami Wójta z 23 lutego 2026 r. uprawnienia do pracy w systemie informatycznym (służącym do realizacji zadań zleconych z zakresu administracji rządowej) nadawane są na podstawie ustnego polecenia Sekretarza lub Wójta.
Kontrolujący wskazują by w wewnętrznych procedurach uregulować kwestie nadawania i odbierania uprawnień do pracy w systemach informatycznych.
W odniesieniu do czynności opisanych powyżej, zastosować dokument potwierdzający wypełnienie wymogu ich egzemplifikacji - pisemny wniosek osób upoważnionych spowoduje, że proces nadawania i odbierania uprawnień będzie w pełni potwierdzony.
W trakcie czynności sprawdzających przedstawiono:

- *Upoważnienie do przetwarzania danych osobowych* wystawione pracownikom realizującym zadania zlecone z zakresu administracji rządowej. Upoważnienie określa cele i zakres przetwarzania.
- *Oświadczenie pracownika,* 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.

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. 76, 122, 209-215)

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 w Przybiernowie przeprowadzono następujące szkolenia pracowników z zakresu bezpieczeństwa informacji i ochrony danych osobowych:

- Szkolenie „*RODO dla Pracowników Urzędu Gminy. Ochrona danych osobowych i bezpieczeństwo informacji w administracji publicznej"*, które zrealizowano w listopadzie 2025 r.;
- Szkolenie *„Sztuczna inteligencja i e-Doręczenia w administracji – bezpieczna cyfryzacja urzędu".* Szkolenie realizowane w terminach: *27.10.2025, 31.10.2025, 12.11.2025, 17.11.2025 r.*

Udział w szkoleniach potwierdzają certyfikaty wydane osobom w nich uczestniczącym. Ponadto pracownicy Urzędu, zostali zobligowani do zapoznania się (w formie samodzielnej pracy) z informacjami dotyczącymi zasad ochrony danych osobowych, przygotowanych w formie *poradnika dla pracowników*. Kontrolującym przestawiono oświadczenia pracowników z lutego 2024 r. o zapoznaniu się z wyżej opisanym materiałem szkoleniowym.

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.

(dowód: akta kontroli str. 76, 206-208)

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 dokumentach:

- *Polityce bezpieczeństwa informacji*, w rozdziale V pkt 5 (*Regulamin ochrony danych osobowych - Wynoszenie nośników danych poza obszar przetwarzania);*
- *Instrukcji zarządzania systemem informatycznym,* w rozdziale VII (*Regulamin używania sprzętu mobilnego poza jednostką*).

W wyżej wymienionych procedurach 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 23 lutego 2026 r. do realizacji zadań zleconych z zakresu administracji rządowej nie wykorzystywano w Jednostce urządzeń mobilnych oraz nie realizowano pracy na odległość.

(dowód: akta kontroli str. 123-124, 172)

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 o świadczenie usług w ramach działalności gospodarczej* XXX.[4] Obsługa informatyczna wg. zapisów umowy obejmuje między innymi następujące czynności: administrowanie i konserwację sieci komputerowej; usuwanie awarii sieci i urządzeń komputerowych; instalację i aktualizowanie oprogramowania; archiwizację danych. W umowie uregulowano kwestię czasu reakcji na zgłoszenie awarii. Z Firmą zawarto ponadto *Umowę powierzenia przetwarzania danych osobowych*.[5]
W celu realizacji zadań z zakresu administracji rządowej z firmą XXX, zawarto umowę o asystę techniczną oprogramowania komputerowego XXX obejmującą swym zakresem między innymi: aktualizację i modyfikację, diagnozowanie i usuwanie błędów oraz wykonywanie czynności serwisowych i konserwacyjnych oprogramowania.[6] 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.*[7] 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. 81-84, 222-249)

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
W *Polityce bezpieczeństwa informacji*, w rozdziale IV (*Incydenty)* oraz w rozdziale V, pkt 8 (*Regulamin ochrony danych osobowych, Incydenty związane z ochroną danych osobowych)* określono zasady i sposób postępowania w przypadku zaistnienia incydentu związanego z naruszeniem ochrony danych osobowych. Wskazano katalog zdarzeń, które mogą sygnalizować wystąpienie naruszenia i przypisano odpowiednie zadania ADO[8] oraz IOD[9]. § 19 ust. 2 pkt 13 rozporządzenia KRI wskazuje, że *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: bezzwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji (...),* wobec czego elementy systemu zarządzania bezpieczeństwem informacji powinny obejmować bezpieczeństwo wszystkich informacji przetwarzanych w Jednostce i nie ograniczać się do ochrony danych osobowych. Zaleca się uzupełnienie regulacji wewnętrznych o kwestie wskazane powyżej.
Kontrolującym przedstawiono dokument *Rejestr naruszeń ochrony danych osobowych oraz incydentów bezpieczeństwa danych*, w którym opisano jedno (konkretne)

[4] Umowa zawarta w dniu 1 czerwca 2007 r.
[5] Umowa zawarta w dniu 20 maja 2018 r.
[6] Umowa nr EA-170-2026, umowa nr UA-152-2026.
[7] Umowa nr EP-170-2026, umowa nr UP-152-2026.
[8] Administrator Danych Osobowych.
[9] Inspektor Ochrony Danych.

zdarzenie (z 2024 r.) wraz z przedstawieniem oceny naruszenia oraz podjętych działań. W wyniku analizy przypadku (przeprowadzonej przez administratora danych) incydent zaklasyfikowano do kategorii naruszenia o niskim wpływie na prawa i wolności osoby fizycznej dotkniętej zdarzeniem, wobec czego incydentu nie zgłoszono organowi nadzorczemu.
Zgodnie z oświadczeniem Wójta z 23 lutego 2026 r. w okresie objętym kontrolą, poza 2024 r. (przypadek opisany powyżej) nie wystąpiły incydenty naruszenia bezpieczeństwa informacji.
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. 76-77, 121, 125-126, 199-200)

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. 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.
Kontrolującym przedstawiono następujące dokumenty dotyczące okresu objętego weryfikacją:

- *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.*
- *Raport z inspekcji- Stan infrastruktury IT Urzędu Gminy w Przybiernowie. Data dokumentu: 02.07.2025.*
- *Sprawozdanie z przeglądu biuletynu informacji publicznej Urząd Gminy Przybiernów - przetwarzanie i publikacja danych osobowych.* Data dokumentu: 05.02.2026 r.

Audyty wewnętrzne zrealizowane w Urzędzie obejmowały zagadnienia związane z bezpieczeństwem informacji, wobec czego w okresie objętym kontrolą spełniono wymogi określone w § 19 ust. 2 pkt 14 rozporządzenia KRI.
(dowód: akta kontroli str. 85-103, 176-198)

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.
W rozdziale IV (*Tworzenie kopii zapasowych*) *Instrukcji Zarządzania Systemem Informatycznym* opisano *k*westie wykonywania kopii bezpieczeństwa w Jednostce, natomiast nie uregulowano zasad testowania kopii zapasowych oraz nie wskazano osoby odpowiedzialnej za testowe odtworzenia tych kopii.
Zgodnie z wyjaśnieniami Informatyka kopie zapasowe *systemów dziedzinowych wykonywane są codziennie, a kopie baz danych systemów pomocniczych SRP wykonywane są raz w tygodniu. Kopie wykonywane są w wersjach: online, offline i odmiejscowionej. Nieregularnie jest realizowane testowe odtwarzanie kopii zapasowych.*
W trakcie kontroli nie przedstawiono dokumentów potwierdzających przeprowadzanie testowania kopii zapasowych na potrzeby weryfikacji poprawności i stanu ich wykonywania. Kontrolujący wskazują by dokumentować te czynności, tak by realizowane działania były w pełni potwierdzone, a w wewnętrznych procedurach uregulować kwestie próbnego testowania kopii zapasowych.
(dowód: akta kontroli str. 170-171, 216)

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 z firmą 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. 228-243)

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 urządzeniach 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 realizującym zadania zlecone 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. 104-108, 113-114)

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.

- W Jednostce zastosowano zintegrowane rozwiązania do zarządzania bezpieczeństwem w sieci.
- Urząd dysponuje lokalnymi zasilaczami awaryjnymi.
- Na komputerach podlegających badaniu zainstalowano oprogramowanie antywirusowe.
- W procedurach wewnętrznych Jednostki określono:
  - zasady wykonywania konserwacji i naprawy sprzętu;
  - zasady wycofywania sprzętu i niszczenia nośników informacji;
  - procedury korzystania z Internetu i poczty elektronicznej;
  - kwestie pobierania, zdawania i przechowywania kluczy do pomieszczeń służbowych w Urzędzie.
- Serwerownia usytuowana w przyziemiu budynku, wyposażona w gaśnicę. Drzwi wejściowe do pomieszczenia charakteryzują się wysoką wytrzymałością mechaniczną. Okno z kratą zamontowaną od zewnątrz. Brak czujki dymu i klimatyzacji. W pomieszczeniu stwierdzono obecność tranzytowych rur wodnych, co stanowi potencjalne zagrożenie zalaniem infrastruktury IT.
  W trakcie czynności sprawdzających kontrolującym zaprezentowano docelowe pomieszczenie serwerowe, wskazując na wdrożone środki bezpieczeństwa, takie jak: dodatkowe zabezpieczenia antywłamaniowe, czujkę dymu, czujnik zalania, podesty na szafy RACK. Z uwagi na znaczny stopień zaawansowania prac adaptacyjnych prawdopodobne jest zakończenie procesu w deklarowanym przez Jednostkę terminie do końca marca 2026 roku.
  Obecne pomieszczenie serwerowni jest współdzielone z magazynem wykorzystywanym na potrzeby realizacji zadań z zakresu obrony cywilnej, wobec czego dostęp do pomieszczenia posiada poza Informatykiem inny pracownik Urzędu.
  Stwierdzono, że w Jednostce nie jest prowadzony dziennik dokumentujący fakty wejścia do pomieszczenia. Kontrolujący wskazują, że (szczególnie wobec wyżej opisanego stanu) konieczne jest uregulowanie tej sytuacji w procedurach wewnętrznych pod kątem wskazania i ewidencjonowania osób uprawnionych do wejścia do stref wydzielonych (w szczególności należy zaktualizować załącznik 1 - *Ewidencja dostępu do pomieszczeń w Urzędzie Gminy w Przybiernowie, ul. Cisowa 3, 72-110 Przybiernów)*.
  (dowód: akta kontroli str. 124-125, 171-173, 216-217)

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).

System objęty kontrolą zawiera logi, w których są odnotowane działania użytkowników, zgodnie z zapisami § 20 ust. 2 i 3 rozporządzenia KRI. Logi systemu przechowywane są przez okres ponad 2 lat, co wypełnia dyspozycję § 20 ust. 4 wyżej opisanego rozporządzenia.

Zgodnie z wyjaśnieniami Informatyka *logi* (programu*) nie są przeglądane regularnie.* Kontrolujący wskazują, aby regularnie prowadzić działania związane z przeglądaniem logów systemu informatycznego, w celu stwierdzenia i ewentualnej identyfikacji działań niepożądanych oraz dokumentować je (np. w postaci dziennika administratora), tak by realizowane czynności były w pełni potwierdzone.

(dowód: akta kontroli str. 216, 218-222)

Wpis do książki kontroli	1/2026
Stwierdzone nieprawidłowości w obszarze Nr 2	• Dokumentacja regulująca kwestie bezpieczeństwa informacji nie zawiera wszystkich elementów wymaganych przepisami rozporządzenia KRI. • Brak aktualizacji obowiązującej w Urzędzie dokumentacji dotyczącej bezpieczeństwa informacji, do czego zobowiązują zapisy § 19 ust. 2 pkt 1 rozporządzenia KRI. • Nieopracowanie Planu Ciągłości Działania, do czego zobowiązują zapisy § 19 ust. 1 rozporządzenia KRI. • Zawężenie incydentów naruszenia bezpieczeństwa informacji do naruszeń danych osobowych, co nie jest zgodne z dyspozycją § 19 ust. 2 pkt 13 rozporządzenia KRI. • Niesporządzanie dokumentacji dotyczącej testowania kopii zapasowych danych i systemów na potrzeby weryfikacji poprawności i stanu ich wykonywania oraz dokumentacji działań związanych z przeglądaniem logów systemowych, zgodnie z dyspozycją § 19 ust. 1 rozporządzenia KRI, w zakresie rozliczalności prowadzonych działań. • Aktualnie eksploatowane 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. • Opracować Plan Ciągłości Działania, do czego zobowiązują zapisy § 19 ust. 1 rozporządzenia KRI. • Aktualizować obowiązującą w Urzędzie dokumentację dotyczącą bezpieczeństwa informacji, do czego zobowiązują zapisy § 19 ust. 2 pkt 1 rozporządzenia KRI. • Uzupełnić procedury dotyczące postępowania w przypadku naruszenia ochrony danych osobowych o pozostałe obszary, w których mogą wystąpić przypadki naruszenia bezpieczeństwa przetwarzanych w Jednostce informacji, zgodne z dyspozycją § 19 ust. 2 pkt 13 rozporządzenia KRI. • Sporządzać dokumentację dotyczącą testowania kopii zapasowych danych i systemów na potrzeby weryfikacji poprawności i stanu ich wykonywania oraz dokumentacji działań związanych z przeglądaniem logów systemowych, zgodnie z dyspozycją § 19 ust. 1 rozporządzenia KRI, w zakresie rozliczalności prowadzonych działań. • 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 2026 r. poz. 158) 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/*