Wojewoda Zachodniopomorski

K-2.431.1.8.2025.7.IO

Szczecin, 3 czerwca 2025 r.

WYSTĄPIENIE POKONTROLNE

Przedmiot kontroli	Działanie systemów teleinformatycznych oraz rejestrów publicznych używanych do realizacji zadań zleconych z zakresu administracji rządowej.
Nazwa i adres organu kontrolującego	Wojewoda Zachodniopomorski, ul. Wały Chrobrego 4, 70-502 Szczecin.
Nazwa i adres organu kontrolowanego	Wójt Gminy Świerzno, ul. Długa 8, 72-405 Świerzno.
Osoba pełniąca funkcję Wójta Gminy Świerzno w okresie objętym kontrolą	Pan Radosław Drozdowicz
Okres objęty kontrolą	od dnia 1 stycznia 2022 r. do dnia 4 marca 2025 r.
Kontrolerzy	Pracownicy Wydziału Kontroli Zachodniopomorskiego Urzędu Wojewódzkiego w Szczecinie: Pani Anna Dąbska – kierownik oddziału, kierownik zespołu kontrolnego, Pani Iwona Olesińska – główny specjalista.
Nr upoważnienia	Nr 7/25 z dnia 25 lutego 2025 r.
Podstawy prawne do przeprowadzenia kontroli	– art. 6 ust. 4 pkt 3 w związku z art. 2 ust. 1 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej[1]; – art. 25 ust. 1 pkt 3 lit. a, w związku z ust. 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[2].
Kryteria prowadzenia kontroli	legalność, rzetelność
Rodzaj kontroli i tryb kontroli	kontrola planowa, tryb zwykły
Termin kontroli	26 lutego – 4 marca 2025 r.
Osoby udzielające wyjaśnień w trakcie kontroli	Pan XXX – Sekretarz Gminy, Pan XXX – zajmujący się obsługą informatyczną Urzędu Gminy Świerzno, na mocy umowy o świadczenie usług informatycznych[3].

[1] Dz. U. z 2020r., poz. 224.
[2] Dz. U. z 2023r., poz. 57.
[3] Zwany dalej Informatykiem.

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[4]: *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 Świerzno 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. 126-128)

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

[4] 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".

System informatyczny wykorzystywany do realizacji zadań zleconych z zakresu administracji rządowej w Urzędzie Gminy Świerzno wymieniał dane w formatach 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**

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, monitorowania i przeglądania oraz utrzymania i doskonalenia systemu bezpieczeństwa informacji zapewniającego poufność, dostępność, integralność informacji.

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

- *Zarządzenie Nr SK.0050.104.2019 Wójta Gminy Świerzno z dnia 11 września 2019 r. w sprawie wprowadzenia „Polityki bezpieczeństwa informacji" w Urzędzie Gminy Świerzno wraz z podległymi jednostkami organizacyjnymi.* Dokument obowiązuje od 11 września 2019 r.;
- *Polityka bezpieczeństwa informacji - dokument główny, Wersja dokumentu 1.01*
  z dnia 11 września 2019 roku;
- *Polityka ochrony danych osobowych - dokument główny.* Dokument obowiązuje od 21 listopada 2018 r.;
- *Instrukcja zarzadzania systemem informatycznym.* Dokument obowiązuje od 21 listopada 2018 r.;
- *Księga procedur, Wersja dokumentu 1.00 z dnia* (brak wskazania daty). Dokument obowiązuje od 21 listopada 2018 r.

W wyniku analizy obowiązującej w Jednostce dokumentacji związanej z bezpieczeństwem informacji stwierdzono, że funkcjonujące w Jednostce procedury zawierają między innymi oświadczenie o intencjach kierownictwa potwierdzające cele i

zasady bezpieczeństwa; definicje ogólnych i szczegółowych obowiązków w odniesieniu do zarządzania bezpieczeństwem informacji oraz zakres stosowania wprowadzonych regulacji.
Dyrektywa § 19 ust. 2 pkt 1 rozporządzenia KRI wskazuje na konieczność zapewnienia *aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia* co przekłada się na konieczność monitorowania i przeglądu systemu zarządzania bezpieczeństwem informacji. Regulacje wewnętrzne Jednostki w tym zakresie (*Polityka bezpieczeństwa informacji,* rozdział 15 *Przeglądy Polityki bezpieczeństwa informacji i audyty systemu)* zawierają wymóg *poddawania planowemu (*bądź pozaplanowemu) *sprawdzeniu* Politykę bezpieczeństwa informacji *przynajmniej raz na rok, pod kątem zgodności z obowiązującymi przepisami prawa, w formie zadania audytowego.*
W okresie objętym kontrolą, zgodnie z wyjaśnieniami Wójta z dnia 3 marca 2025 r. w 2022 r. został przeprowadzony *przegląd w formie zadania audytowego (...).*
Kontrolującym nie przedstawiono dokumentacji potwierdzającej realizację przeglądów w kolejnych latach podlegających badaniu, wobec czego należy stwierdzić, że nie zrealizowano w pełni dyspozycji § 19 ust. 2 pkt 1 rozporządzenia KRI w powiązaniu z zapisami rozdziału 15 pkt 1 i 2 obowiązującej w Jednostce *Polityki bezpieczeństwa informacji.*

(dowód: akta kontroli str. 66-67, 131-251, 300-301)

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.
Procedura szacowania ryzyka powinna być przeprowadzana okresowo, jednak zawsze 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.
Kontrolującym przedstawiono następujące dokumenty dotyczące okresu objętego weryfikacją:

- *Analizę ryzyka utraty atrybutu poufności, integralności i dostępności danych osobowych przetwarzanych w Urzędzie Gminy w Świerznie, Świerzno czerwiec 2024;*
- *Analizę ryzyka utraty atrybutu poufności, integralności i dostępności danych osobowych przetwarzanych w Urzędzie Gminy w Świerznie. Świerzno, sierpień 2023;*
- *Analizę ryzyka utraty atrybutu poufności, integralności i dostępności danych osobowych przetwarzanych w Urzędzie Gminy w Świerznie. Świerzno, sierpień 2022.*

Kontrolującym nie przedstawiono planu postępowania z ryzykiem, o który zwrócili się pismem znak: K-2.431.1.8.2025.2.IO z 26 lutego 2025 r. W odpowiedzi na powyższe Wójt pismem z dnia 3 marca 2025 r. wskazał, że *sposób postępowania z ryzykiem określa Polityka Bezpieczeństwa Informacji (...).* W *Polityce bezpieczeństwa informacji*

w rozdziale 7 (*Zarządzanie ryzykiem*) wyjaśniono pojęcie zarządzania ryzykiem, przedstawiono etapy przeprowadzania analizy ryzyka oraz częstotliwość jej wykonywania, wskazano osobę odpowiedzialną za jej sporządzenie, natomiast nie określono sposobu postępowania ze zidentyfikowanym ryzykiem.

Należy wskazać, że w załączniku nr 8 do obowiązującej w Jednostce *Polityki ochrony danych osobowych,* w którym zawarto metodykę przeprowadzania analizy ryzyka wskazano wprost, że *końcowym etapem jest opracowanie planów mających na celu obniżenie ryzyk szczątkowych w odniesieniu do poszczególnych zagrożeń do poziomu ryzyka akceptowalnego. Powyższe działanie dotyczy sytuacji, w której mimo istniejących zabezpieczeń ryzyko szczątkowe przekracza wartością poziom ryzyka akceptowalnego.*

(dowód: akta kontroli str. 143-144, 216-221, 252-257. 300-301)

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 karty ewidencyjne sprzętu komputerowego. Karty zawierają informacje dotyczące rodzaju sprzętu; nazwy i jego charakterystyki; zainstalowanego oprogramowania; rodzaju systemu operacyjnego oraz współpracujących urządzeń peryferyjnych.

(dowód: akta kontroli str. 76-104)

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 9 *Polityki bezpieczeństwa informacji (Zarzadzanie uprawnieniami związanymi z dostępem do informacji)*,
- rozdziale 8 *Polityki ochrony danych osobowych (Osoba upoważniona do przetwarzania danych osobowych),*
- rozdziale 2 *Instrukcji zarzadzania systemem informatycznym (Uprawnienia dostępu do systemów informatycznych, nadawanie i odbieranie),*
- punkcie 2 *Księgi procedur, Wersja dokumentu 1.00 z dnia* [brak wskazania daty] *(Procedura nadawania i odbierania uprawnień).*

Zgodnie z zapisami procedur dostęp do przetwarzania danych osobowych w Jednostce pracownicy otrzymują na podstawie upoważnienia wydanego przez ADO[5]. Zakres upoważnienia wynika wprost z zakresu czynności pracownika. Natomiast uprawnienia do pracy w systemie informatycznym nadaje ASI[6] na podstawie wydanego upoważnienia do przetwarzania danych osobowych.
Kontrolującym przedstawiono:

- *Upoważnienie do przetwarzania danych osobowych* wystawione pracownikowi realizującemu zadania zlecone z zakresu administracji rządowej. Upoważnienie określa jego obszar, wynikający z zadań realizowanych na zajmowanym stanowisku oraz okres jego ważności,
- *Oświadczenie o zachowaniu w tajemnicy przetwarzania danych osobowych*, w którym wskazano okres obowiązywania zobowiązania - czas zatrudnienia w Jednostce, jak również czas po ustaniu stosunku pracy.

(dowód: akta kontroli str. 126-128, 145-146, 160-162, 198, 239-243, 296-297)

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
Kontrolującym przedstawiono zaświadczenie potwierdzające przeprowadzenie w Urzędzie 3 listopada 2023 r. szkolenia z zakresu regulacji prawnych, dotyczących ochrony danych osobowych i kwestii bezpiecznego przetwarzania tych danych.
Z treści przedłożonego dokumentu nie wynika jednak, którzy pracownicy uczestniczyli w szkoleniu, wobec czego nie ma możliwości potwierdzenia, że wzięli w nim udział pracownicy wskazani jako osoby realizujące zadania zlecone z zakresu administracji rządowej.
Z pisma Wójta Gminy z dnia 3 marca 2025 r., w zakresie szkoleń (odpowiadających wymogom § 19 ust. 2 pkt 6 rozporządzenia KRI) przeprowadzonych w Urzędzie wynika, że w Jednostce *szkolenia z zakresu cyberbezpieczeństwa (...) były przeprowadzane w formie indywidualnej na poszczególnych stanowiskach pracy przez Administratora Systemu Informatycznego (...). Szkolenia nie były dokumentowane (...).*
Szkolenia z zakresu cyberbezpieczeństwa nie wyczerpują zakresu delegacji § 19 ust. 2 pkt 6 rozporządzenia KRI, który wskazuje również na inne zagrożenia bezpieczeństwa informacji, nie zawężając problemu jedynie do zagadnień wskazanych w piśmie Wójta.

[5] ADO- Administrator Danych Osobowych.
[6] ASI- Administrator Systemu Informatycznego.

Ponadto kontrolujący wskazują by udział w szkoleniach dokumentowała lista obecności zawierająca co najmniej imię i nazwisko uczestnika, datę czynności oraz zakres tematyczny szkoleń. Tego typu dokument sprawi, że realizacja wymogu *zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji* będzie
w pełni potwierdzony.
Z analizy okazanych dokumentów oraz przedstawionych wyjaśnień nie wynika, że zakres tematyczny szkoleń przeprowadzonych w Urzędzie obejmował wszystkie zagadnienia wskazane w § 19 ust. 2 pkt 6 rozporządzenia KRI.
Odwołując się do wewnętrznych regulacji, w zakresie częstotliwości realizacji szkoleń (*Polityka bezpieczeństwa informacji* -rozdział 12 Szkolenia i upowszechnianie wiedzy z zakresu bezpieczeństwa przetwarzania informacji), który stanowi, że szkolenia okresowe są *realizowane cykliczne, co najmniej raz w roku prowadzone przez ASI w zakresie bezpiecznego wykorzystania infrastruktury informatycznej przy przetwarzaniu informacji oraz IOD w zakresie obowiązujących przepisów regulujących obszar przetwarzania informacji* należy zauważyć, iż działania Jednostki nie realizują w tym zakresie dyspozycji własnych unormowań.
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.

(dowód: akta kontroli str. 149, 298-299, 301)

2.6 Praca na odległość i mobilne przetwarzanie danych.

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

Ustalenia kontroli

Zasady prowadzenia pracy prowadzonej na odległość i wykorzystywania urządzeń mobilnych zostały uregulowane w:

- rozdziale 10 (*Przetwarzanie mobilne informacji oraz w trakcie pracy na odległość) Polityki bezpieczeństwa informacji;*
- załączniku nr 4 (*Regulamin użytkowania komputerów przenośnych*) do *Instrukcji zarządzania systemem informatycznym;*
- rozdziale 3 (*Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu informatycznego służącego do przetwarzania danych osobowych*) *Instrukcji zarządzania systemem informatycznym;*
- rozdziale 11 (*Pozostałe zasady bezpiecznego przetwarzania danych osobowych*) *Polityki ochrony danych osobowych- dokument główny*.

W wyżej wymienionych dokumentach uregulowano między innymi kwestie wynoszenia poza obszar Urzędu nośników z danymi osobowymi wprowadzając wymóg uzyskania zgody Administratora Danych Osobowych. Wdrożono obowiązek szyfrowania danych zapisanych na komputerach przenośnych oraz innych urządzeniach mobilnych a także wymóg zabezpieczenia ich hasłem.
Procedury przyjęte w Jednostce określają zasady bezpiecznej pracy przy przetwarzaniu mobilnym i w przypadku świadczenia pracy na odległość, zgodnie z § 19 ust. 2 pkt 8 rozporządzenia KRI.

Zgodnie z wyjaśnieniami Wójta z dnia 3 marca 2025 r. do realizacji zadań zleconych z zakresu administracji rządowej w Urzędzie nie wykorzystywano urządzeń mobilnych i nie realizowano pracy na odległość.

(dowód: akta kontroli str. 146-147, 162-164, 182, 203-204, 300-301)

2.7 Serwis sprzętu informatycznego i oprogramowania.

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

Ustalenia kontroli

Obsługa informatyczna Urzędu realizowana jest na podstawie umowy na świadczenie usług dotyczących obsługi informatycznej XXX.[7]

Obsługa informatyczna wg zapisów umowy obejmuje między innymi następujące czynności: pełnienie funkcji administratora systemu informatycznego, administrowanie siecią komputerową i sprzętem komputerowym, wykonywanie kopii zapasowych, instalację i konfigurację oprogramowania, prowadzenie ewidencji urządzeń i programów komputerowych, świadczenie pomocy technicznej związanej z obsługą sprzętu. W umowie uregulowano kwestię czasu reakcji na zgłoszenie konieczności realizacji zadań wynikających z jej zapisów. Z firmą zawarto również *Umowę powierzenia danych osobowych do dalszego przetwarzania*, co przekłada się na realizację dyspozycji § 19 ust. 2 pkt 10 rozporządzenia KRI w zakresie zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.

W celu realizacji zadań z zakresu administracji rządowej XXX zawarto umowę serwisową, której przedmiotem jest nadzór serwisowy XXX.[8]

W umowie wskazano zadania jakie wykonawca zobowiązuje się zrealizować w ramach nadzoru serwisowego:

- stworzenie nowych wersji oprogramowania,
- udzielanie bezpłatnych porad i konsultacji telefonicznych, internetowych (...), za pomocą poczty oraz (...) szkolenia (...) w zakresie korzystania z oprogramowania (...),
- wykonywanie dodatkowej obsługi serwisowej systemów objętych umową (...).

Stwierdzono, że w powyższej umowie wprowadzono zapis określający maksymalny czas skutecznej naprawy oprogramowania, czym wypełniono dyspozycję § 19 ust. 2 pkt 10 rozporządzenia KRI, zawierając zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji. W powyższej umowie uregulowano kwestie powierzenia przetwarzania danych osobowych.

(dowód: akta kontroli str. 105-120)

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 11 *Reagowanie na incydent* określono sposób postępowania w przypadku stwierdzenia zaistnienia incydentu związanego

[7] Umowa nr KA.215.3.2025 z dnia 2.01.2025 r.
[8] Umowa serwisowa nr US219/2025 z dnia 18.12.2024 r.

z bezpieczeństwem informacji, wskazując zasady postępowania w przypadku takiego naruszenia. *Procedura reakcji na ujawnione naruszenie* ujęta w *Księdze procedur, Wersja dokumentu 1.00 z dnia* [brak wskazania daty] określa zasady i sposób postępowania
w przypadku naruszenia ochrony danych osobowych, w oparciu o wymogi rozporządzenia RODO[9]. Powyższe dokumenty przypisują odpowiednie zadania IOD[10] oraz ASI w przypadku powzięcia informacji o naruszeniu bezpieczeństwa informacji. Kontrolującym przedstawiono *Rejestr Incydentów Bezpieczeństwa* za lata objęte kontrolą, które nie zawierają wpisów. Zgodnie z wyjaśnieniami Wójta z 7 marca 2025r. w okresie objętym kontrolą nie wystąpiły incydenty naruszenia bezpieczeństwa informacji.

(dowód: akta kontroli str. 125, 147-148, 243-245, 302)

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 z realizacji zadania audytowego o charakterze zapewniającym pn.: Ocena funkcjonującego Systemu Zarządzania Bezpieczeństwem Informacji pod kątem jego zgodności z wymogami Krajowych Ram Interoperacyjności wraz z cyberdiagnozą na potrzeby Programu Cyfrowa Gmina. Data dokumentu 2 sierpnia 2022 r.
- Sprawozdanie z realizacji zadania audytowego o charakterze zapewniającym pn.: Ocena funkcjonującego Systemu Zarządzania Bezpieczeństwem Informacji pod kątem jego zgodności z wymogami Krajowych Ram Interoperacyjności. Data dokumentu 2 listopada 2023 r.

W świetle rozbieżnych wyjaśnień Wójta w kwestii realizacji audytu wewnętrznego w 2024 r. :

- pismo z dnia 3 marca 2025 r.*: Audyt został przeprowadzony w roku 2023. W roku 2024 odstąpiono od jego realizacji (...);*
- pismo z dnia 6 marca 2025 r.: *realizacja zadania audytowego za 2024 r. w trakcie,*

kontrolujący stwierdzają, że w okresie przeprowadzania czynności sprawdzających nie otrzymali dokumentu potwierdzającego przeprowadzenie audytu wewnętrznego z zakresu bezpieczeństwa informacji w Jednostce w 2024 r., wobec czego uznają, iż

[9] 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).
[10] IOD- Inspektor Ochrony Danych.

w Urzędzie Gminy Świerzno w 2024 roku nie wypełniono obowiązku, o którym mowa w § 19 ust. 2 pkt 14 rozporządzenia KRI.

(dowód: akta kontroli str. 257-295, 300-303)

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 kopii bezpieczeństwa uregulowano w rozdziale 4 (Za*sady tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania) Instrukcji zarzadzania systemem informatycznym.*

Zgodnie z oświadczeniem Informatyka z dnia 27 lutego 2025 r. w Urzędzie tworzone są codziennie kopie przyrostowe, natomiast raz w tygodniu pełne kopie baz danych. Kopie zapasowe przechowywane są lokalnie oraz zamiejscowo (poza miejscem wytworzenia). W Urzędzie, zgodnie z oświadczeniem Informatyka realizowane jest próbne testowane kopii zapasowych na potrzeby weryfikacji poprawności i stanu ich wykonywania, przy czym nie sporządza się dokumentacji potwierdzającej przeprowadzenie testów. 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. 68-72, 164-166)

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 serwisową, której przedmiotem jest nadzór serwisowy XXX.

(dowód: akta kontroli str. 105-108)

2.12 Zabezpieczenia techniczno – organizacyjne dostępu do informacji.

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

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

Ustalenia kontroli

W celu ustanowienia zabezpieczeń uniemożliwiających osobom nieuprawnionym modyfikację, usunięcie lub zniszczenie informacji każdemu pracownikowi nadano identyfikator i hasło wejścia do systemów zainstalowanych na komputerach oraz do programów, z których korzystają.
W przypadku systemu „Źródło" dostęp jest możliwy wyłącznie z użyciem karty, na której zapisany jest certyfikat umożliwiający zalogowanie się do centralnego systemu.
Pracownicy złożyli oświadczenia o zachowaniu w tajemnicy danych osobowych, do których będą mieli dostęp w trakcie wykonywania obowiązków służbowych.
W wyniku oględzin stanowiska komputerowego wykorzystywanego do realizacji zadań zleconych z zakresu administracji rządowej, przeprowadzonych w toku czynności kontrolnych ustalono, że:
- dostęp do systemu operacyjnego na urządzeniu możliwy był jedynie po wprowadzeniu nazwy użytkownika i hasła,
- komputer miał zainstalowane oprogramowanie antywirusowe oraz skonfigurowany wygaszacz ekranu,
- złożoność hasła była zgodna z wymogami rozporządzenia w sprawie dokumentacji i warunków technicznych,
- ustawienie monitora stanowiska obsługi systemów informatycznych wykorzystywanych do realizacji zadań zleconych z zakresu administracji rządowej uniemożliwiało odczyt wyświetlanych danych przez osoby postronne,
- użytkownikom systemów wykorzystywanych do realizacji zadań zleconych z zakresu administracji rządowej nie nadano uprawnień administratora, uniemożliwiając w ten sposób instalowanie oprogramowania niewiadomego pochodzenia lub zmianę ustawień systemu operacyjnego a także ingerencję w rejestry zdarzeń.

(dowód: akta kontroli str. 121-124, 129-130)

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

- Sieć informatyczną Urzędu zabezpieczono przy wykorzystaniu zapory sieciowej firewall.
- Na komputerze podlegającym badaniu zainstalowano oprogramowanie antywirusowe.
- Urząd wykorzystuje systemy monitorowania sieci w celu oceny stanu połączeń i aktywności urządzeń, prób nieautoryzowanego dostępu, występowania podejrzanego ruchu sieciowego, działania blokad oraz skuteczności zabezpieczeń.
- Dostęp do serwerowni ograniczony do osób wskazanych przez ADO, przy czym brak sformalizowanych uregulowań w tym zakresie. Drzwi wejściowe do pomieszczenia bez zabezpieczeń i wzmocnień. Serwerownię wyposażono w klimatyzację i gaśnicę. W pomieszczeniu brak czujki dymu.
- W procedurach wewnętrznych Jednostki określono zasady:
  - przekazania i likwidacji elektronicznych nośników informacji,
  - konserwacji urządzeń stanowiących system informatyczny,
  - naprawy sprzętu przez podmioty zewnętrzne.

(dowód: akta kontroli str. 73-75, 129-130)

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).

Kontrolującym nie przedstawiono logów XXX, w których winny być odnotowane działania użytkowników, zgodnie z zapisami § 20 ust. 2 rozporządzenia KRI. Zapewnienie rozliczalności operacji polega bowiem na gromadzeniu informacji o tym,

kto, kiedy i jakie działania wykonał w systemie teleinformatycznym, szczególnie gdy przetwarzanie danych podlega prawnej ochronie. Brak zapisów w logach systemu narusza § 20 ust. 2 rozporządzenia KRI, stanowiącego, że *w dziennikach systemów odnotowuje się obligatoryjnie działania użytkowników (...) polegające na dostępie do (...) systemu z uprawnieniami administracyjnymi(...).*
Logi systemu winny być przechowywane przez okres 2 lat, wobec czego nie wypełniono również dyspozycji § 20 ust. 4 wyżej opisanego rozporządzenia.

Wpis do książki kontroli	14
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 oraz wewnętrzne regulacje Jednostki. • Nieprzeprowadzenie w 2024 roku audytu wewnętrznego z zakresu bezpieczeństwa informacji, do czego zobowiązują zapisy § 19 ust. 2 pkt 14 rozporządzenia KRI. • Zakres tematyczny szkoleń przeprowadzonych w Urzędzie nie obejmował wszystkich zagadnień wskazanych w § 19 ust. 2 pkt 6 rozporządzenia KRI. • Niesporządzenie planu postępowania z ryzykiem, na co wskazuje § 19 ust. 2 pkt 3 rozporządzenia KRI. • Nieodnotowywanie w dziennikach systemów działań użytkowników z uprawnieniami administracyjnymi, co nie wypełnia dyspozycji § 20 ust. 2 rozporządzenia KRI. • Nieprzechowywanie logów XXX przez okres 2 lat, co jest sprzeczne z dyspozycją § 20 ust. 4 rozporządzenia KRI. • Pomieszczenie serwerowni nie dysponuje zabezpieczeniami, zgodnie z dyspozycją § 19 ust. 2 pkt 12 oraz ust. 4 rozporządzenia KRI.
Ocena obszaru kontroli	**Pozytywna z nieprawidłowościami**
Zalecenia	• Wykonywać analizy i przeglądy dokumentacji z zakresu bezpieczeństwa informacji, zgodnie z dyrektywą § 19 ust. 2 pkt 1 rozporządzenia KRI. • Przeprowadzać audyty wewnętrzne z zakresu bezpieczeństwa informacji, do czego zobowiązują zapisy § 19 ust. 2 pkt 14 rozporządzenia KRI.

	• Przeprowadzać szkolenia z zakresu bezpieczeństwa informacji obejmujące wszystkie zagadnienia wskazane w § 19 ust. 2 pkt 6 rozporządzenia KRI. • Sporządzić plan postępowania z ryzykiem, zgodnie ze wskazaniem § 19 ust. 2 pkt 3 rozporządzenia KRI. • Odnotowywać w dziennikach systemów działania użytkowników z uprawnieniami administracyjnymi, zgodnie z zapisem § 20 ust. 2 rozporządzenia KRI. • Przechowywać logi XXX przez okres 2 lat, zgodnie z dyspozycją § 20 ust. 4 rozporządzenia KRI. • W pomieszczeniu serwerowni zapewnić warunki gwarantujące utrzymanie odpowiedniego poziomu bezpieczeństwa informacji, zgodnie z dyspozycją § 19 ust. 2 pkt 12 lit. b i e oraz ust. 4 rozporządzenia KRI.
Pouczenia	Zgodnie z art. 48 ustawy z dnia 15 lipca 2011 roku o kontroli w administracji rządowej (Dz.U. z 2020 r. poz. 224) od wystąpienia pokontrolnego nie przysługują środki odwoławcze, o podjętych działaniach, mających na celu realizację zaleceń pokontrolnych, proszę poinformować mnie za pośrednictwem Wydziału Kontroli Zachodniopomorskiego Urzędu Wojewódzkiego w Szczecinie w terminie 14 dni od daty otrzymania niniejszego wystąpienia.
Podpis kierownika jednostki kontrolującej	Z upoważnienia Wojewody Zachodniopomorskiego Bartosz Brożyński I Wicewojewoda Zachodniopomorski */podpisano kwalifikowanym podpisem elektronicznym/*