Wojewoda
Zachodniopomorski

Znak: K-2.431.1.34.2025.8.IO

Szczecin, 21 październik 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, ul. Wały Chrobrego 4, 70-502 Szczecin.
Nazwa i adres organu kontrolowanego	Burmistrz Miasta Świdwin, Plac Konstytucji 3 Maja 1, 78-300 Świdwin.
Osoba pełniąca funkcję Burmistrza Miasta Świdwin w okresie objętym kontrolą	Pan Piotr Feliński
Okres objęty kontrolą	od dnia 1 stycznia 2022 r. do dnia 4 lipca 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 53/25 z dnia 2 czerwca 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	30 czerwca – 4 lipca 2025 r.

[1] Dz. U. z 2020r., poz. 224.
[2] Dz. U. z 2025r., poz. 1158.

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 Miasta Świdwin 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. 42-43, 105-115)

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 Miasta Świdwin 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 Miasta Świdwin, w okresie objętym kontrolą obowiązywały następujące dokumenty z zakresu bezpieczeństwa informacji:

- *Zarządzenie Nr WO/137/20 Burmistrza Miasta Świdwin z dnia 20 października 2020 r. w sprawie dokumentacji przetwarzania informacji w Urzędzie Miasta Świdwin.*
- *Zarządzenie Nr WO/90/25 Burmistrza Miasta Świdwin z dnia 28 kwietnia 2025 r. w sprawie dokumentacji przetwarzania informacji w Urzędzie Miasta Świdwin.*
- *Polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym systemów informatycznych służącym do przetwarzania danych osobowych w Urzędzie Miasta Świdwin*. Data dokumentu: 2025 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 danych osobowych oraz zakres stosowania wprowadzonych regulacji. Funkcjonująca w Urzędzie dokumentacja odnosi się głównie do zagadnień związanych z ochroną danych osobowych a odwołanie w samej nazwie dokumentu (zarówno w polityce jak i instrukcji do ochrony danych osobowych - *Polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym systemów informatycznych służącym do przetwarzania danych*

osobowych w Urzędzie Miasta Świdwin), sugeruje zawężenie problemu bezpieczeństwa informacji do zagadnień związanych z tego typu danymi, podczas gdy ochronie winny podlegać wszystkie przetwarzane przez Urząd informacje. Stwierdzono również, że istnieje konieczność uzupełnienia wewnętrznych regulacji o kwestie przywołane
w treści powyższego dokumentu kontrolnego.
Dyspozycja § 19 ust. 2 pkt 1 rozporządzenia KRI wskazuje na obowiązek zapewnienia *aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia* (zmian organizacyjnych Jednostki, unormowań prawnych i warunków technicznych), co przekłada się na konieczność monitorowania i przeglądu systemu zarządzania bezpieczeństwem informacji. W okresie objętym kontrolą dokumentacja dotycząca bezpieczeństwa informacji nie była poddawana przeglądowi i aktualizacji, wobec czego należy stwierdzić, że nie zrealizowano § 19 ust. 2 pkt 1 rozporządzenia KRI*.*

(dowód: akta kontroli str. 66-69, 154-296)

2.2 Analiza zagrożeń związanych z przetwarzaniem informacji.

Podstawa prawna: § 19 ust. 2 pkt 3 rozporządzenia KRI: *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy.*

Ustalenia kontroli

Analiza ryzyka, obejmująca wszystkie aktywa Jednostki oraz odpowiednie i pogłębione szacowanie zidentyfikowanych ryzyk jest jednym z najistotniejszych elementów zarządzania bezpieczeństwem informacji, pozwalającym na zastosowanie odpowiednich mechanizmów przeciwdziałania w sytuacji materializacji ryzyk.
Kontrolującym przedstawiono następujące dokumenty dotyczące okresu objętego weryfikacją:

- Ankieta szacowania ryzyka dla Urzędu Miasta Świdwin z dostępności, integralności i poufności. Data dokumentu 6 czerwca 2022 r.
- Ankieta szacowania ryzyka dla Urzędu Miasta Świdwin z dostępności, integralności i poufności. Data dokumentu 28 kwietnia 2025 r.

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. 144-154)

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, zgodnie z wymogami rozporządzenia KRI powinna zawierać informację o rodzaju i konfiguracji urządzeń, przez co możliwe będzie odtworzenie zasobów po katastrofie lub innym zdarzeniu losowym.
Inwentaryzacja realizowana jest w Urzędzie, w wersji elektronicznej przy wykorzystaniu oprogramowania XXX. System umożliwia generowanie raportów zawierających informacje dotyczące m. in. sprzętu i oprogramowania oraz rodzaju

systemu operacyjnego. W związku z tym, że sieć komputerowa z jednostkami wykorzystywanymi do realizacji zadań zleconych z zakresu administracji rządowej jest odłączona od sieci komputerowej Urzędu inwentaryzacja dla tej jednostki operacyjnej realizowana jest w postaci zapisów w odrębnym pliku.
W trakcie kontroli okazano stosowną dokumentację, potwierdzającą prowadzenie inwentaryzacji sprzętu i oprogramowania, zgodnie z wymogami rozporządzenia KRI.

(dowód: akta kontroli str.70-71, 73-77)

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 2, pkt 7 (Zabezpieczenie danych osobowych) *Instrukcji Zarządzania Systemem Informatycznym.* Zgodnie z zapisami procedury, w celu uzyskania dostępu do zasobów sieci Urzędu, należy zwrócić się do Informatyka z odpowiednim wnioskiem. Wniosek przygotowuje bezpośredni przełożony pracownika. Administrator systemu wydaje potwierdzenie nadania uprawnień do systemów (według odpowiedniego wzoru) z podaniem nazwy systemu, loginu i rodzaju uprawnień. *W przypadku zwolnienia pracownika lub zmiany charakteru jego pracy Administrator systemu na pisemny wniosek przełożonego pracownika zmienia uprawnienia dostępu do systemu lub całkowicie zamyka dostęp do systemu.*
Dla czynności, o których mowa powyżej jest tworzona dokumentacja, wobec czego realizowany jest wymóg dokumentowania czynności nadawania i odbierania uprawnień do pracy w systemach informatycznych; pisemny wniosek osób upoważnionych powoduje, że proces nadawania i odbierania uprawnień jest w pełni potwierdzony.
Kontrolującym przedstawiono:

- *Wniosek przełożonego o nadanie uprawnień dla użytkownika w systemie informatycznym*- dokument realizuje wymóg poświadczenia czynności nadawania i odbierania uprawnień do pracy w systemach informatycznych;
- *Oświadczenie* pracownika o zachowaniu poufności i przestrzeganiu zasad przetwarzanych danych osobowych oraz informacji stanowiących tajemnicę Jednostki, 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;
- *Upoważnienie do przetwarzania danych osobowych*. Upoważnienie określa jego obszar wynikający z zadań realizowanych na zajmowanym stanowisku;
- *Wniosek o dostęp do systemu Rejestrów Państwowych (SRP)- użytkownicy aplikacji Źródło*. Wnioski dotyczyły nadania dostępu dla nowych użytkowników oraz usunięcia konta jednego z pracowników Urzędu.

W okresie objętym kontrolą z jednym pracownikiem rozwiązano stosunek pracy. Kontrolującym przedstawiono dokumenty poświadczające wypełnienie wymogu bezzwłocznego odbierania uprawnień w systemach informatycznych.

(dowód: akta kontroli str. 77-115, 201-203)

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

Z analizy przedłożonej dokumentacji oraz złożonych wyjaśnień wynika, że w okresie objętym kontrolą pracownikom Urzędu zaproponowano udział w szkoleniu on-line z zakresu cyberbezpieczeństwa (22 maja 2025 r.- szkolenie dla kadry zarządzającej, 21 i 30 maja 2025 r. dla pozostałych pracowników). Zakres tematyczny szkoleń obejmował zagadnienia wskazane w § 19 ust. 2 pkt 6 rozporządzenia KRI. Kontrolującym nie przedstawiono dokumentów potwierdzających udział pracowników w wyżej opisanych szkoleniach, wobec czego nie można stwierdzić czy w szkoleniu wzięli udział pracownicy wskazani jako osoby realizujące zadania zlecone z zakresu administracji rządowej.

Szkolenia, których celem jest zagwarantowanie bezpieczeństwa w zakresie przetwarzania informacji, ze względu na zmieniające się zagrożenia związane z dynamicznym rozwojem technologii informatycznych winny mieć charakter cykliczny i obejmować wszystkie zagadnienia wskazane w § 19 ust. 2 pkt 6 rozporządzenia KRI.

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

W procedurach wewnętrznych Urzędu nie uregulowano zasad wykorzystywania w pracy urządzeń mobilnych, nie uregulowano również kwestii pracy na odległość; co jest istotne zwłaszcza w świetle wyjaśnień Informatyka, że do realizacji zadań zleconych z zakresu administracji rządowej w Urzędzie wykorzystuje się urządzenia mobilne.

Brak regulacji w tym obszarze nie wypełnia dyspozycji § 19 ust. 2 pkt 8 rozporządzenia KRI.

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 przez pracownika zatrudnionego w Jednostce na stanowisku Informatyka. Wśród obowiązków pracownika znajduje się m.in.: nadzór techniczny nad infrastrukturą sieci komputerowej w Urzędzie, bieżąca konserwacja i naprawa sprzętu, prowadzenie dokumentacji sprzętu komputerowego, prowadzenie działań w celu ochrony zbiorów danych, opracowanie i nadzór nad realizacją instrukcji zabezpieczenia systemów informatycznych, prowadzenie szkoleń pracowników w zakresie obsługi sprzętu komputerowego oraz zabezpieczeń systemu informatycznego przed dostępem osób nieupoważnionych.

W celu realizacji zadań z zakresu administracji rządowej XXX zawarto umowę, której przedmiotem jest prowadzenie nadzoru i serwisu oprogramowania użytkowanego systemu XXX. Stwierdzono, że w powyższej umowie (wraz z obowiązującymi aneksami) nie wprowadzono zapisów określających maksymalny czas skutecznej naprawy oprogramowania. W umowie stwierdzono brak uregulowania kwestii powierzenia przetwarzania danych osobowych. Kontrolującym przedstawiono *Umowę powierzenia przetwarzania danych osobowych* zawartą XXX, w związku z wykonaniem zadania polegającego na *zakupie i wdrożeniu elektronicznego systemu obiegu dokumentów* XXX. Umowa powyższa obowiązywała do 31 grudnia 2020 r.

Brak zapisów określających maksymalny czas skutecznej naprawy oprogramowania oraz brak regulacji kwestii powierzenia przetwarzania danych osobowych wskazują na niewypełnienie dyspozycji § 19 ust. 2 pkt 10 rozporządzenia KRI.

(dowód: akta kontroli str. 116-128)

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 i instrukcji zarządzania systemem informatycznym systemów informatycznych służącym do przetwarzania danych osobowych w Urzędzie Miasta Świdwin określono zasady i sposób postępowania w przypadku wystąpienia incydentów związanych z naruszeniem ochrony danych osobowych (rozdział III Polityki bezpieczeństwa – Incydenty; rozdział 4 Instrukcji zarządzania systemem informatycznym - Postępowanie w przypadku naruszenia ochrony danych osobowych oraz rozdział 1 Opis zdarzeń naruszających ochronę danych osobowych).

W procedurze wskazano katalog zdarzeń, które mogą sygnalizować wystąpienie naruszenia. Przypisano ponadto odpowiednie zadania ADO[4] oraz IOD[5] w przypadku powzięcia informacji o naruszeniu danych osobowych.

Zgodnie z § 19 ust. 2 pkt 13 rozporządzenia KRI *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: bezzwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji (...),* wobec czego elementy systemu zarządzania bezpieczeństwem informacji powinny obejmować bezpieczeństwo informacji w całej organizacji i nie ograniczać się wyłącznie do ochrony danych osobowych. Kontrolujący wskazują by procedury regulujące kwestie incydentów nie ograniczały się jedynie do

[4] Administrator Danych Osobowych
[5] Inspektor Ochrony Danych

naruszeń ochrony danych osobowych a obejmowały mogące potencjalnie wystąpić naruszenia bezpieczeństwa wszystkich przetwarzanych informacji.
Kontrolującym przedstawiono *Rejestr incydentów Urząd Miasta Świdwin*, który nie zawiera wpisów. Zgodnie z wyjaśnieniami Informatyka w Jednostce nie wystąpiły przypadki incydentów w obszarze ochrony informacji.

(dowód: akta kontroli str. 129-130, 169-181, 198-199, 205-207)

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 zadania audytowego nr 2/2022 „Polityka bezpieczeństwa informacji w Urzędzie Miasta Świdwin". Świdwin 2022.
- Sprawozdanie z przeprowadzenia zadania audytowego „Funkcjonowanie stron podmiotowych BIP Urzędu Miasta i wybranych jednostek organizacyjnych". Świdwin 2023.
- Notatka z czynności doradczych. Zakres przedmiotowy: Audyt bezpieczeństwa informacji. Ocena w zakresie realizacji obowiązku wykonywania testów kopii zapasowych. Data sporządzenia dokumentu 17.12.2024 r.

Analiza uwag i rekomendacji audytowych wydanych w wyniku audytu polityki bezpieczeństwa informacji przeprowadzonego w 2022 r. wykazała brak realizacji tych rekomendacji w zakresie aktualizacji i uzupełnienia dokumentacji dotyczącej bezpieczeństwa informacji, szczególnie w świetle wprowadzenia w 2025 r. *Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym systemów informatycznych służącym do przetwarzania danych osobowych w Urzędzie Miasta Świdwin.*
Rekomendacje i uwagi wynikające z audytu są kluczową wartością dodaną audytu, bowiem służą one usprawnieniu procesów i wzmocnieniu kontroli wewnętrznej w organizacji, a nie tylko identyfikacji braków i problemów. Efektywne wdrożenie rekomendacji prowadzi do realnej poprawy działania Jednostki, a brak ich realizacji sprawia, że audyt staje się nieefektywny.

(dowód: akta kontroli str. 297-349)

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 8, w pkt II i III *Instrukcji zarządzania systemem informatycznym.* W procedurze uregulowano zasady sporządzania, przechowywania, zabezpieczania i wykorzystywania kopii zapasowych, oraz weryfikacji poprawności ich wykonania.
Zgodnie z wyjaśnieniami Informatyka kopie bezpieczeństwa wykonywane są codziennie i dotyczą całych serwerów XXX a przechowywane są na macierzy dyskowej. Kopie baz danych wykonywane są codziennie (ostatnia kopia), a na koniec miesiąca bazy zgrywane są na płytę DVD i umieszczane poza miejscem wytworzenia.
Kontrolującym przedstawiono *Protokoły z przeprowadzonych testów kopii zapasowych* Testy kopii przeprowadzono 3 czerwca i 6 grudnia 2024 r.
Mając na względzie powyższe, należy stwierdzić, że w Urzędzie Miasta Świdwin zrealizowano dyspozycję, o której mowa w § 19 ust. 2 pkt 12 lit. b, e rozporządzenia KRI.

(dowód: akta kontroli str. 131-132, 209-210, 352)

2.11 Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych.
Podstawa prawna: § 15 ust. 1 rozporządzenia KRI: *Systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne projektuje się, wdraża oraz eksploatuje*
z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności przenoszalności i pielęgnowalności, przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk.
Ustalenia kontroli
W celu realizacji zadań z zakresu administracji rządowej XXX zawarto umowę, której przedmiotem jest prowadzenie nadzoru i serwisu oprogramowania użytkowanego systemu XXX.

(dowód: akta kontroli str. 117-128)

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,
- komputery miały zainstalowane oprogramowanie antywirusowe oraz skonfigurowane wygaszacze ekranu,
- złożoność haseł 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,
- 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. 100-101, 136-143)

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

- Serwery Urzędu zabezpieczone są zasilaczami awaryjnymi.
- Na komputerach podlegających badaniu zainstalowano oprogramowanie antywirusowe.
- W celu zabezpieczenia przed nieautoryzowanym dostępem do danych Urzędu zastosowano wielofunkcyjną zaporę sieciową.
- Serwerownię wyposażono w klimatyzację, gaśnicę. Brak czujki dymu.
- Drzwi wejściowe do pomieszczenia serwerowni nie dysponują należytymi zabezpieczeniami.
- Wejścia do serwerowni nie podlegają ewidencjonowaniu.
- W procedurach wewnętrznych Jednostki określono zasady:
  - niszczenia wydruków i zapisów na nośnikach zawierających dane osobowe,
  - przekazywania nośników danych poza obręb Jednostki.

- W dokumentach wewnętrznych nie uregulowano kwestii bezpiecznego przesyłania danych poza obszar przetwarzania (np. poprzez zastosowanie szyfrowania danych) oraz nie opracowano procedury (metodyki) sporządzania planu zarządzania ciągłością działania na wypadek awarii bądź katastrofy.
(dowód: akta kontroli str. 142-143, 208, 350-352)

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 informacjami uzyskanymi od Informatyka logi programu XXX są przechowywane przez okres 2 lat. Zapis § 20 ust. 4 rozporządzenia KRI zobowiązuje do przechowywania *w dziennikach systemów działań użytkowników lub obiektów systemowych* przez okres 2 lat, wobec czego w tym zakresie wypełniono dyspozycję § 20 ust. 4 wyżej opisanego rozporządzenia. Ponadto w Jednostce co sześć miesięcy prowadzone są działania związane z przeglądaniem logów systemu informatycznego, w celu stwierdzenia i ewentualnej identyfikacji działań niepożądanych, lecz nie jest sporządzana dokumentacja tych czynności. Kontrolujący wskazują aby dokumentować działania związane z przeglądaniem logów systemowych (np. w postaci dziennika administratora), tak by realizowane czynności były w pełni potwierdzone, a w procedurach wewnętrznych uregulować zasady realizacji tych procesów.
(dowód: akta kontroli str. 133-134, 352)

Wpis do książki kontroli	2
Stwierdzone nieprawidłowości w obszarze Nr 2	• Nieprzeglądanie obowiązującej w Urzędzie dokumentacji dotyczącej bezpieczeństwa informacji, do czego zobowiązują zapisy § 19 ust. 2 pkt 1 rozporządzenia KRI.

	• Dokumentacja regulująca kwestie bezpieczeństwa informacji nie zawiera wszystkich elementów wymaganych przepisami rozporządzenia KRI. • Brak dokumentacji potwierdzającej udział pracowników w szkoleniach z zakresu bezpieczeństwa informacji. • Brak regulacji w obszarze dotyczącym pracy przy przetwarzaniu mobilnym i pracy na odległość, co nie wypełnia dyspozycji § 19 ust. 2 pkt 8 rozporządzenia KRI. • W umowie XXX regulującej kwestię serwisu programu wykorzystywanego do realizacji zadań zleconych z zakresu administracji rządowej brak zapisów określających maksymalny czas skutecznej naprawy oprogramowania oraz brak regulacji kwestii powierzenia przetwarzania danych osobowych, czym nie wypełniono dyspozycji § 19 ust. 2 pkt 10 rozporządzenia KRI. • Zawężenie incydentów naruszenia bezpieczeństwa informacji do naruszeń danych osobowych, co nie jest zgodne z dyspozycją § 19 ust. 2 pkt 13 rozporządzenia KRI. • Brak realizacji uwag i rekomendacji audytowych wydanych w wyniku audytu polityki bezpieczeństwa informacji przeprowadzonego w 2022 r. w zakresie aktualizacji i uzupełnienia dokumentacji dotyczącej bezpieczeństwa informacji. • Pomieszczenie serwerowni nie dysponuje zabezpieczeniami, wypełniającymi dyspozycję § 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. • Dokumentować udział pracowników w szkoleniach z zakresu bezpieczeństwa informacji. • W wewnętrznych procedurach uregulować kwestie pracy przy przetwarzaniu mobilnym i pracy na odległość, do czego zobowiązują zapisy § 19 ust. 2 pkt 8 rozporządzenia KRI. • W umowie XXX dotyczącej serwisu programu wykorzystywanego do realizacji zadań zleconych z zakresu administracji rządowej wprowadzić zapisy określające maksymalny

	czas skutecznej naprawy oprogramowania oraz uregulować kwestie powierzenia przetwarzania danych osobowych, zgodnie z dyspozycją § 19 ust. 2 pkt 10 rozporządzenia KRI. • Uzupełnić procedury postępowania z incydentami o pozostałe obszary, w których mogą wystąpić przypadki naruszenia bezpieczeństwa przetwarzanych w Jednostce informacji, zgodne z dyspozycją § 19 ust. 2 pkt 13 rozporządzenia KRI. • Realizować rekomendacje audytowe z przeprowadzonych audytów wewnętrznych z zakresu bezpieczeństwa informacji. • 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/*