WOJEWODA
ZACHODNIOPOMORSKI

Szczecin, dnia 9 listopada 2023 r.

Znak: K-2.431.1.41.2023.8.IO

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	Prezydent Miasta Stargard, ul. Hetmana Stefana Czarnieckiego 17, 73-110 Stargard.
Osoba pełniąca funkcję Prezydenta Miasta Stargard w okresie objętym kontrolą / okresie prowadzenia kontroli	Pan Rafał Zając
Okres objęty kontrolą	od dnia 1 stycznia 2020 r. do dnia 2 sierpnia 2023 r.
Kontrolujący	Pracownicy Wydziału Kontroli Zachodniopomorskiego Urzędu Wojewódzkiego w Szczecinie: Pani Anna Dąbska – kierownik oddziału, *kierownik zespołu kontrolnego,* Pani Iwona Olesińska – główny specjalista.
Nr upoważnienia	Nr 68/23 z dnia 20 lipca 2023 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
Termin kontroli	27 lipca – 2 sierpnia 2023 r.
Rodzaj i tryb kontroli	kontrola planowa, tryb zwykły
Osoby udzielające wyjaśnień w trakcie kontroli	Pan Janusz Kmita - Dyrektor Wydziału Informatyki Pan Mariusz Sikorski- Z-ca Dyrektora Wydziału Informatyki Pani Anna Rudnicka – Inspektor Ochrony Danych

[1] Dz. U. z 2020r., poz. 224.
[2] Dz. U. z 2023r., poz. 57.

Obszar kontroli Nr 1	Wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami/rejestrami informatycznymi i wspomaganie świadczenia usług drogą elektroniczną.
1.1 Współpraca systemów teleinformatycznych z innymi systemami	
Podstawa prawna	**§ 5 ust. 3 pkt 3 rozporządzenia KRI[3]:** *Interoperacyjność na poziomie semantycznym osiągana jest przez: stosowanie w rejestrach prowadzonych przez podmioty publiczne odwołań do rejestrów zawierających dane referencyjne w zakresie niezbędnym do realizacji zadań.* **§ 16 ust. 1 rozporządzenia KRI:** *Systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne wyposaża się w składniki sprzętowe lub oprogramowanie umożliwiające wymianę danych z innymi systemami teleinformatycznymi za pomocą protokołów komunikacyjnych i szyfrujących określonych w obowiązujących przepisach, normach, standardach lub rekomendacjach ustanowionych przez krajową jednostkę normalizacyjną lub jednostkę normalizacyjną Unii Europejskiej.*
Ustalenia kontroli Na podstawie przedstawionej dokumentacji ustalono, że do realizacji zadań zleconych z zakresu administracji rządowej w Urzędzie Miejskim w Stargardzie wykorzystywano jeden system centralny (aplikacja Źródło) oraz systemy informatyczne wspomagające obsługę spraw obywatelskich w zakresie ewidencji mieszkańców oraz rejestru wyborców XXX wspierający pracę z zakresu tworzenia aktów stanu cywilnego (XXX). Zaprezentowane w czasie kontroli systemy informatyczne wykorzystywane do realizacji zadań zleconych z zakresu administracji rządowej spełniały minimalne wymogi interoperacyjności w zakresie współpracy z innymi aplikacjami zarówno Urzędu, jak i innych jednostek administracji publicznej, określone w § 5 ust. 3 pkt 3 rozporządzenia KRI. System centralny (aplikacja Źródło), dostępny przez stronę WWW podlegał kontroli jedynie w zakresie formalnego posiadania uprawnień przez pracowników Urzędu Miejskiego oraz zabezpieczeń związanych z dostępem do systemu. (dowód: akta kontroli str. 40-41, 202, 205, 218-227)	
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*

[3] Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r., poz. 2247), zwane dalej „rozporządzeniem KRI".

	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 Miejskim w Stargardzie 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. Kodowanie znaków w dokumentach wysyłanych z systemów teleinformatycznych Jednostki odbywa się w formacie Unicode UTF-8. (dowód: akta kontroli str. 252)	
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	**§ 20 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 działań związanych z bezpieczeństwem informacji.* **§ 20 ust. 2 pkt 1 rozporządzenia KRI:** *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia.* **§ 20 ust. 3 rozporządzenia KRI:** *Wymagania określone w ust. 1 i 2 uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą.*
Ustalenia kontroli Wymagania dotyczące systemów teleinformatycznych, w których przetwarzane są rejestry publiczne w postaci teleinformatycznej określone zostały w § 20 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 Miejskim w Stargardzie, w okresie objętym kontrolą obowiązywały następujące dokumenty z zakresu bezpieczeństwa informacji:

- *Zarządzenie Nr 286/2020 Prezydenta Miasta Stargard z dnia 28 października 2020 r. w sprawie wprowadzenia polityki bezpieczeństwa informacji w Urzędzie Miejskim w Stargardzie,*
- *Zarządzenie Nr 285/2020 Prezydenta Miasta Stargard z dnia 28 października 2020 r. w sprawie wprowadzenia polityki ochrony danych Urzędu Miejskiego w Stargardzie,*
- *Regulamin pracy zdalnej pracowników zatrudnionych w Urzędzie Miejskim w Stargardzie,* wprowadzony *Zarządzeniem Nr 115/2023 Prezydenta Miasta Stargard z dnia 4 maja 2023 r.,*
- *Zarządzenie Nr 179/2018 Prezydenta Miasta Stargard z dnia 20 czerwca 2018 r. w sprawie wprowadzenia dokumentacji w zakresie ochrony danych w Urzędzie Miejskim w Stargardzie.*

W wyniku analizy procedur związanych z bezpieczeństwem informacji stwierdzono, że określono sposób i wskazano osoby realizujące obowiązki wynikające z rozporządzenia KRI, a funkcjonująca w Urzędzie dokumentacja spełnia wymogi określone w § 20 ust. 2 pkt 1 rozporządzenia KRI w zakresie bezpieczeństwa informacji. Stwierdzono również, że obowiązujące regulacje zostały zaktualizowane pod kątem dostosowania zapisów do obowiązujących od dnia 25 maja 2018 r. przepisów 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)[4].
Mając na względzie powyższe, należy stwierdzić, że w Urzędzie Miejskim w Stargardzie wdrożono system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji.

(dowód: akta kontroli str. 83-179)

2.2 Analiza zagrożeń związanych z przetwarzaniem informacji

Podstawa prawna	**§ 20 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
Kontrolującym przedstawiono *Analizę ryzyka utraty integralności, poufności i dostępności informacji w Urzędzie Miejskim w Stargardzie,* zrealizowaną w 2020 r., *stanowiącą załącznik nr 5 do Polityki Bezpieczeństwa Informacji.*
Zaprezentowana analiza ryzyka obejmuje aktywa Jednostki, ponadto w dokumencie określono zagrożenia dla wskazanych zasobów, źródła tych zagrożeń oraz siłę wpływu zdarzeń na czynniki decydujące o bezpieczeństwie informacji. Zgodnie z wyjaśnieniami Dyrektora Wydziału Informatyki z 27 lipca 2023 r. dokument powyższy jest aktualny, a w przypadku *pojawienia się nowych potencjalnych źródeł zagrożenia* zostanie zaktualizowany.
Analiza ryzyka, obejmująca wszystkie aktywa Jednostki oraz odpowiednie i pogłębione

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

szacowanie zidentyfikowanych ryzyk jest jednym z najistotniejszych elementów zarzadzania 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.

(dowód: akta kontroli str. 65, 263-268)

2.3 Inwentaryzacja sprzętu i oprogramowania informatycznego

Podstawa prawna	**§ 20 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

Zgodne z § 20 ust. 2 pkt 2 rozporządzenia KRI zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez utrzymywanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację. Ponadto, zgodnie z pkt 8.1.1 normy PN-ISO/IEC 27002:2014, wszystkie aktywa informatyczne powinny być zidentyfikowane oraz powinien być sporządzany i aktualizowany ich spis. Inwentaryzacja m.in. sprzętu informatycznego powinna także zawierać informację o jego rodzaju i konfiguracji, przez co możliwe będzie jego odtworzenie po katastrofie lub innym zdarzeniu losowym.

Kontrolującym przedstawiono inwentaryzację urządzeń wykorzystywanych do realizacji zadań zleconych z zakresu administracji rządowej zawierającą informacje dotyczące sprzętu i oprogramowania oraz użytkowanych urządzeń peryferyjnych.

Mając na uwadze powyższe stwierdzono, że w Urzędzie jest prowadzona inwentaryzacja sprzętu i oprogramowania, zgodnie z wymogami rozporządzenia KRI.

(dowód: akta kontroli str. 259-262)

2.4 Zarządzanie uprawnieniami do pracy w systemach informatycznych

Podstawa prawna	**§ 20 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.* **§ 20 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 § 20 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 dostępu do danych przez uprawnione osoby, w ustalonym zakresie.

Kwestie nadawania i odbierania uprawnień do pracy w systemie informatycznym uregulowano w rozdziale 7 *Instrukcji Zarządzania Systemami Informatycznymi w Urzędzie Miejskim w Stargardzie – Procedury nadawania, zmiany, rejestracji i cofania uprawnień.* Zgodnie z regulacjami przyjętymi w Jednostce uprawnienia w zakresie dostępu do systemu informatycznego nadaje administrator systemu informatycznego, na podstawie pisemnego wniosku kierownika komórki organizacyjnej *o nadanie pracownikowi uprawnień do pracy w systemach informatycznych Urzędu Miejskiego.*
Kontrolującym przedstawiono:

- *upoważnienia do przetwarzania danych osobowych* wystawione pracownikom Jednostki. Upoważnienie określa jego obszar, wynikający z zadań realizowanych na zajmowanym stanowisku;
- *oświadczenia pracowników,* w których zawarto między innymi zobowiązanie pracownika o zachowaniu w tajemnicy przetwarzanych danych. W dokumencie nie wskazano czasu trwania tego zobowiązania. Kontrolujący wskazują, by zaktualizować powyższy dokument, wprowadzając zapisy pod kątem wskazania okresu obowiązywania zobowiązania, rozszerzając go na okres po ustaniu stosunku pracy;
- *Dokumenty Uprawnień Jednostkowych w systemie informatycznym* - formularze potwierdzające nadanie uprawnień do pracy w systemach informatycznych pracownikom realizującym zadania zlecone z zakresu administracji rządowej.

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. 84-85, 200-205, 253-258)

2.5 Szkolenia pracowników zaangażowanych w proces przetwarzania informacji

Podstawa prawna	**§ 20 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 Miejskim w Stargardzie przeprowadzano szkolenia pracowników z zakresu bezpieczeństwa informacji i ochrony danych osobowych w kontekście obowiązujących aktów prawnych – rozporządzenia KRI oraz RODO. Ponadto IOD (w formie wiadomości e-mail) cyklicznie informował pracowników o aktualnych zagrożeniach dotyczących bezpieczeństwa informacji.
Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie szkolenia osób zaangażowanych w proces przetwarzania informacji. Szkolenia, których celem jest zagwarantowanie bezpieczeństwa w zakresie przetwarzania informacji winny mieć charakter cykliczny, ze względu na zmieniające się zagrożenia związane z dynamicznym rozwojem technologii informatycznych.
Z przedstawionej dokumentacji oraz wyjaśnień IOD wynika, że zakres tematyczny szkoleń przeprowadzonych w Urzędzie obejmował zagadnienia wskazane w § 20 ust. 2 pkt 6 rozporządzenia KRI.

(dowód: akta kontroli str. 66, 228-251)

2.6 Praca na odległość i mobilne przetwarzanie danych

Podstawa prawna	**§ 20 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 uregulowane w następujących procedurach wewnętrznych Urzędu:

- załączniku nr 4 do *Polityki Bezpieczeństwa Informacji - Podstawowe założenia oraz zasady zabezpieczenia sprzętu i informacji służących podczas wykonywania pracy zdalnej w tym pracy na odległość;*
- rozdziale 10 *Instrukcji Zarządzania Systemami Informatycznymi w Urzędzie Miejskim w Stargardzie - Przetwarzanie danych przy wykorzystaniu urządzeń przenośnych;*
- *Regulaminie pracy zdalnej pracowników zatrudnionych w Urzędzie Miejskim w Stargardzie*, wprowadzonym *Zarządzeniem Nr 115/2023 Prezydenta Miasta Stargard z dnia 4 maja 2023 r.*

Zgodnie z wyjaśnieniami Z-ca Dyrektora Wydziału Informatyki z dnia 27 lipca 2023 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. 63, 100-101, 109-111)

2.7 Serwis sprzętu informatycznego i oprogramowania

Podstawa prawna	**§ 20 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 Jednostki realizowana jest przez pracowników zatrudnionych w Wydziale Informatyki Urzędu Miejskiego w Stargardzie.

W celu realizacji zadań z zakresu administracji rządowej z firmą XXX, zawarto umowy o asystę techniczną oprogramowania komputerowego XXX, obejmującą swym zakresem między innymi: aktualizację i modyfikację oprogramowania, diagnozowanie i usuwanie błędów oraz wsparcie techniczne[5]. W umowach 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 *Umowy powierzenia przetwarzania danych osobowych*[6], co przekłada się na realizację dyspozycji § 20 ust. 2 pkt 10 rozporządzenia KRI w zakresie zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.

(dowód: akta kontroli str. 208-227)

2.8 Procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji

Podstawa prawna	**§ 20 ust. 2 pkt 13 rozporządzenia KRI:** *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: bezzwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji*

[5] Umowa nr EA-158-2023 z dnia 28 grudnia 2022 r. i UA-230-2023 z dnia 28 grudnia 2022 r.

[6] Umowa nr EP-158-2023 z dnia 28 grudnia 2022 r. i UP-230-2023 z dnia 28 grudnia 2022 r.

	w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.

Ustalenia kontroli

W *Polityce ochrony danych osobowych Urzędu Miejskiego w Stargardzie* wprowadzonej *Zarządzeniem Nr 285/2020 Prezydenta Miasta Stargard z dnia 28 października 2020 r.*, w załączniku nr 6 - *Procedura postępowania w przypadku naruszenia ochrony danych osobowych* określono zasady i sposób postępowania w przypadku naruszenia ochrony danych osobowych, zgodnie z wymogami rozporządzenia RODO. Przedstawiono katalog zdarzeń, które mogą wskazywać na wystąpienie incydentu naruszenia tych danych oraz określono czynności, które należy podjąć w wypadku stwierdzenia *naruszenia ochrony danych osobowych.*

W *Procedurze reagowania na incydenty IT związane z bezpieczeństwem informacji w Urzędzie Miejskim w Stargardzie* przedstawiono przykłady zdarzeń, które mogą wskazywać na wystąpienie naruszenie bezpieczeństwa informacji, określono sposób postępowania i zasady zgłaszania tego typu incydentów.

Kontrolującym przedstawiono *Rejestr Incydentów Bezpieczeństwa Danych,* który nie zawierał wpisów. Z wyjaśnień Dyrektora Wydziału Informatyki wynika, że w kontrolowanym okresie, w Urzędzie nie stwierdzono przypadków naruszenia bezpieczeństwa informacji.

(dowód: akta kontroli str. 104-108, 165-168, 278)

2.9 Audyt wewnętrzny z zakresu bezpieczeństwa informacji

Podstawa prawna	**§ 20 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 § 20 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 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 z audytu „Bezpieczeństwo przetwarzanych danych w systemach IT", 2020r.;
- Ocena zgodności z KRI/UoKSC, data dokumentu sierpień 2022 r.

Zgodnie z wyjaśnieniami Dyrektora Wydziału Informatyki z dnia 31 lipca 2023 r. audyt wewnętrzny z zakresu bezpieczeństwa informacji w 2021 roku nie został przeprowadzony. Audyty wewnętrzne realizowane w Jednostce, w latach 2020, 2022 obejmowały swym zakresem zagadnienia związane z bezpieczeństwem informacji, wobec czego w tym okresie spełniono wymogi określone w § 20 ust. 2 pkt 14 rozporządzenia KRI.

(dowód: akta kontroli str. 173-200, 279)

2.10 Kopie zapasowe

Podstawa prawna	**§ 20 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 § 20 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 tworzenia kopii zapasowych zbiorów danych oraz programów uregulowane zostały w rozdziale 5 *Instrukcji Zarządzania Systemami Informatycznymi w Urzędzie Miejskim w Stargardzie.* Wskazano osoby odpowiedzialne za sporządzanie kopii zapasowych oraz określono częstotliwość ich tworzenia. Ustanowiono zasady testowania kopii zapasowych danych i systemów na potrzeby weryfikacji poprawności i stanu ich wykonywania. Pełne kopie bezpieczeństwa wszystkich maszyn wirtualnych działających w sieci Urzędu wykonywane są raz w tygodniu, a w pozostałych dniach wykonywane są kopie przyrostowe. Kopie zapasowe systemów XXX, zgodnie z wyjaśnieniami Z-ca Dyrektora Wydziału Informatyki z dnia 27 lipca 2023 r. wykonywane są w odstępach siedmiodniowych i przy pomocy zaszyfrowanego pendrive'a przenoszone są i zapisywane na serwer z kopiami danych. Raz w tygodniu kopie zgrywane są na dysk zewnętrzny, który przechowywany jest w serwerowni. Kopie zapasowe przechowywane są w innej lokalizacji niż miejsce ich wytworzenia, z uwagi na ryzyko utraty informacji w przypadku zaistnienia sytuacji nadzwyczajnych. Z wyjaśnień Dyrektora Wydziału Informatyki wynika również, że realizowane jest próbne testowane w celu sprawdzenia poprawności wykonania kopii bezpieczeństwa. (dowód: akta kontroli str. 64, 89-90, 269-273)	
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 wykonywania zadań z zakresu administracji rządowej z XXX, zawarto umowy o asystę techniczną oprogramowania komputerowego XXX, obejmującą swym zakresem między innymi: aktualizację i modyfikację oprogramowania, oraz udzielanie wsparcia w zakresie jego eksploatacji. (dowód: akta kontroli str. 208-227)	
2.12 Zabezpieczenia techniczno – organizacyjne dostępu do informacji	
Podstawa prawna	**§ 20 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 realizujących zadań zleconych z zakresu administracji rządowej przy użyciu programu XXX, przeprowadzonych w toku czynności kontrolnych ustalono, że: - na każdym urządzeniu dostęp do systemu operacyjnego możliwy był jedynie po wprowadzeniu nazwy użytkownika i hasła, - komputery miały zainstalowane oprogramowanie antywirusowe, - na wszystkich jednostkach skonfigurowano wygaszacz ekranu, - złożoność hasła była zgodna z wymogami rozporządzenia w sprawie dokumentacji i warunków technicznych, - ustawienie monitora stanowiska obsługi systemów informatycznych uniemożliwia odczyt wyświetlanych danych przez osoby postronne, - żadnemu z użytkowników nie nadano uprawnień administratora uniemożliwiając w ten sposób instalowanie oprogramowania niewiadomego pochodzenia lub zmianę ustawień systemu operacyjnego a także ingerencję w rejestry zdarzeń, - pomieszczenie serwerowni zlokalizowanej w budynku, gdzie realizowane są zadania zlecone z zakresu administracji rządowej wyposażono w klimatyzację, antywłamaniowe drzwi wejściowe oraz czujnik przeciwpożarowy i czujnik dymu. (dowód: akta kontroli str. 274-277, 280-281)	
2.13 Zabezpieczenia techniczno – organizacyjne systemów informatycznych	
Podstawa prawna	**§ 20 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. **§ 20 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 Sieci i systemy Urzędu zabezpieczono przy wykorzystaniu zapory sieciowej XXX. Ponadto systemy Jednostki chronione są przy użyciu systemów wykrywania i zapobiegania włamaniom do sieci komputerowych. W procedurach wewnętrznych Jednostki określono zasady naprawy oraz wycofywania elektronicznych nośników informacji zawierających między innymi dane osobowe. (dowód: akta kontroli str. 92-94, 271)	
2.14 Rozliczalność działań w systemach teleinformatycznych.	
Podstawa prawna	**§ 21 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.* **§ 21 ust. 3 rozporządzenia KRI:** *w zakresie wynikającym z analizy ryzyka poza informacjami wymienionymi w § 21 ust. 2 rozporządzenia KRI są 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.* **§ 21 ust. 4 rozporządzenia KRI:** *informacje w dziennikach systemów przechowywane są od dnia ich zapisu, przez okres wskazany w przepisach odrębnych, a w przypadku braku przepisów odrębnych przez dwa lata.*
Ustalenia kontroli Przetwarzanie informacji w systemach teleinformatycznych wymaga dostępu do danych przez uprawnione osoby i obiekty systemowe (procesy) w ustalonym zakresie. Zapewnienie rozliczalności operacji polega na gromadzeniu informacji o tym, kto, kiedy i jakie czynności wykonał w systemie teleinformatycznym. Obligatoryjnie podlegają dokumentowaniu w postaci zapisów w dziennikach systemów (logi) wszelkie działania dostępu do systemu teleinformatycznego z uprawnieniami administracyjnymi, w zakresie konfiguracji systemu i jego zabezpieczeń a także działania, gdy przetwarzanie danych podlega prawnej ochronie (np. zgodnie z ustawą o ochronie danych osobowych). Zgodnie z wyjaśnieniami Z-ca Dyrektora Wydziału Informatyki z dnia 27 lipca 2023 r. logi systemu XXX gromadzone są *w bazie danych programu i z poziomu aplikacji do zarzadzania bazą jest możliwość uzyskania dostępu do danych* dotyczących wykonywanych czynności przez administratora i użytkowników systemu. Istotne jest ustalenie przyczyny braku możliwości przeglądania logów bezpośrednio w programie XXX, szczególnie pod kątem niezaimplementowania przez producenta oprogramowania funkcji związanej z zapisem w logach systemu faktów nadawania i odbierania uprawnień użytkownikom. 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 § 21 ust. 2 rozporządzenia KRI, stanowiącego, że *w dziennikach systemów odnotowuje się obligatoryjnie działania użytkowników (...) polegające na dostępie do (...) systemu z uprawnieniami administracyjnymi(...).*
Ponadto z wyjaśnień Z-cy Dyrektora Wydziału Informatyki wynika, że wykonywana jest analiza logów, w celu identyfikacji działań niepożądanych.

(dowód: akta kontroli str. 64)

Stwierdzone nieprawidłowości w obszarze nr 2:

- Nieprzeprowadzenie w 2021 roku audytu wewnętrznego w zakresie bezpieczeństwa informacji, zgodnie z wymogami § 20 ust. 2 pkt 14 rozporządzenia KRI.
- Nieodnotowywanie w dziennikach systemów działań użytkowników z uprawnieniami administracyjnymi, co nie wypełnia dyspozycji § 21 ust. 2 rozporządzenia KRI.

Ocena obszaru kontroli	**Pozytywna z nieprawidłowościami**
Wpis do książki kontroli	Nr 1/2023
Wnioski dotyczące uzyskanych efektów zrealizowanego zadania	Istotną kwestią z punktu widzenia bezpieczeństwa informacji jest ciągłe podnoszenie świadomości pracowników (poprzez realizację różnych formy szkoleń) istnienia potencjalnych zagrożeń oraz wiedza w jaki sposób unikać, zminimalizować ale także postępować w przypadku materializacji ryzyk związanych z naruszeniem bezpieczeństwa wszystkich przetwarzanych przez Jednostkę informacji (ze szczególnym uwzględnieniem naruszenia ochrony danych osobowych). Nieprzeprowadzenie audytu wewnętrznego z zakresu bezpieczeństwa informacji może wpłynąć negatywnie na prawidłową oceną skuteczności przyjętych w Jednostce rozwiązań w zakresie bezpieczeństwa informacji. Audyt wewnętrzny stanowi bowiem istotne źródło wiedzy kierownictwa o realnym stanie bezpieczeństwa, różnych aspektach jego utrzymania oraz wskazuje obszary wymagające podjęcia działań korygujących.
Zalecenia	• Przeprowadzać nie rzadziej niż raz na rok audyt wewnętrzny w zakresie bezpieczeństwa informacji, zgodnie z wymogami § 20 ust. 2 pkt 14 rozporządzenia KRI. • W dziennikach systemów odnotowywać obligatoryjnie działania użytkowników z uprawnieniami administracyjnymi, zgodnie z dyspozycją § 21 ust. 2 rozporządzenia KRI.
Pouczenie	– od wystąpienia pokontrolnego nie przysługują środki odwoławcze; – o podjętych działaniach, mających na celu wyeliminowanie stwierdzonych nieprawidłowości, 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 Mateusz Wagemann II Wicewojewoda Zachodniopomorski