WOJEWODA
ZACHODNIOPOMORSKI

Szczecin, dnia 6 grudnia 2022 r.

Znak: K-2.431.1.39.2022.6.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	Burmistrz Tuczna, ul. Wolności 6, 78-640 Tuczno.
Osoba pełniąca funkcję Burmistrza Tuczna w okresie objętym kontrolą / okresie prowadzenia kontroli	Pan Krzysztof Hara- do 18 października 2020 r. Pan Piotr Stanisław Pierzyński - od 3 listopada 2020 r. do 4 lipca 2021 r. Pan Krzysztof Mikołajczyk od 5 lipca 2021 r.
Okres objęty kontrolą	od dnia 1 stycznia 2019 r. do dnia 16 sierpnia 2022 r.
Kontrolujący	Pracownicy Wydziału Kontroli Zachodniopomorskiego Urzędu Wojewódzkiego w Szczecinie: Pani Anna Dąbska – kierownik oddziału, *kierownik zespołu kontrolnego,* Pani Iwona Olesińska – inspektor wojewódzki.
Nr upoważnienia	Nr 59/22 z dnia 8 sierpnia 2022 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	9-16 sierpnia 2022 r.
Rodzaj i tryb kontroli	kontrola planowa, tryb zwykły
Osoba udzielająca wyjaśnień w trakcie kontroli	Pan Maciej Kubisz- Informatyk urzędu

[1] Dz. U. z 2020r., poz. 224.
[2] Dz. U. z 2021r., poz. 2070.

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 Tucznie wykorzystywano jeden system centralny (aplikacja Źródło) oraz systemy informatyczne wspomagające obsługę spraw obywatelskich: Rejestr Mieszkańców - XXX oraz Rejestr Wyborców – XXX. System centralny (aplikacja Źródło), dostępny przez stronę WWW podlegał kontroli w zakresie formalnego posiadania uprawnień przez pracowników Urzędu. System do realizacji zadań zleconych z zakresu administracji rządowej współpracuje z systemem zewnętrznym oraz spełnia minimalne wymogi interoperacyjności w zakresie współpracy z innymi systemami, określone w § 5 ust. 3 pkt 3 rozporządzenia KRI. (dowód: akta kontroli str. 38-39)	
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*

[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".

	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 Tucznie 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. 30)	
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 Tucznie, w zakresie bezpieczeństwa informacji, w okresie objętym	

kontrolą obowiązywało *Zarządzenie Nr 52/2018 Burmistrza Tuczna z dnia 25 maja 2018 r. w sprawie wprowadzenia Polityki Ochrony Danych Osobowych i Instrukcji Zarządzania Systemami Informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Miejskim w Tucznie*.

Wdrożone w Jednostce regulacje nie obejmują wszystkich informacji jakie są przetwarzane w Urzędzie a odnoszą się głównie do danych osobowych. Odwołanie w samej nazwie dokumentu, zarówno w polityce jak i instrukcji do ochrony danych osobowych (*Polityka Bezpieczeństwa w Zakresie Ochrony Danych Osobowych i Instrukcja Zarządzania Systemami Informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Miejskim w Tucznie)* sugeruje zawężenie problemu bezpieczeństwa informacji do zagadnień związanych z ochroną danych osobowych.

Obowiązująca dokumentacja, nie zawiera wszystkich elementów, które decydują o skuteczności i poprawności zarządzania bezpieczeństwem informacji. Przedłożona dokumentacja nie obejmuje m. in.:

- regulacji w zakresie przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy,
- sposobu postępowania z ryzykiem z uwzględnieniem wyników szacowania ryzyka,
- opisu procesu ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji,
- zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji.

Ponadto należy zauważyć, że w *Polityce Bezpieczeństwa w Zakresie Ochrony Danych Osobowych,* w § 2 pkt 5 określono pojęcie administratora, którym (co wynika z treści tego dokumentu) ma być *Dyrektor Szkoły Podstawowej (...) w Tucznie, który samodzielnie lub wspólnie z innymi podmiotami określa cele i sposoby przetwarzania danych*. Tak definiowanemu administratorowi powierzono szeroki zakres odpowiedzialności i przypisano szereg obowiązków.

W okresie objętym badaniem, zgodnie z oświadczeniem Zastępcy Burmistrza Tuczna z dnia 11 sierpnia 2022 r. nie przeprowadzano przeglądów dokumentacji z zakresu bezpieczeństwem informacji, co bezpośrednio przełożyło się na nie wypełnienie dyrektywy § 20 ust. 2 pkt 1 rozporządzenia KRI.

Mając na względzie powyższe, należy stwierdzić, że w Urzędzie Miejskim w Tucznie nie opracowano i nie wdrożono kompleksowego systemu zarządzania bezpieczeństwem informacji zapewniającego, w sposób wyczerpujący poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność działań.

(dowód: akta kontroli str. 79-138, 182)

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

W wyniku analizy obowiązującej w Jednostce dokumentacji stwierdzono, że nie zostały opracowane i zatwierdzone regulacje wewnętrzne opisujące sposób zarządzania ryzykiem bezpieczeństwa informacji.

W okresie objętym kontrolą, zgodnie z oświadczeniem Zastępcy Burmistrza Tuczna z dnia 9 sierpnia 2022 r. w Urzędzie nie przeprowadzono analizy ryzyka utraty integralności, dostępności lub poufności informacji; czym nie zrealizowano dyspozycji, o której mowa w § 20

ust. 2 pkt 3 rozporządzenia KRI.
Analiza ryzyka, obejmująca wszystkie aktywa Jednostki oraz odpowiednie i pogłębione 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. Finalnym dokumentem procesu zarządzania ryzykiem winien być plan postępowania z ryzykiem, na który składa się wyszczególnienie ryzyk, celów stosowania zabezpieczeń oraz wskazanie zabezpieczeń.

(dowód: akta kontroli str. 60)

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:

- *Zestawienie urządzeń IT,*
- *Zestawienie oprogramowania IT.*

Przedłożone dokumenty nie obejmują wszystkich informacji wymaganych wyżej przywołanymi przepisami, takich jak: parametry procesora, ilość pamięci RAM, pojemność twardego dysku, typ monitora, podłączone urządzenia drukujące, inne współpracujące urządzenia peryferyjne. Zestawienia zawierają elementy opracowane na podstawie wytycznych ustawy o rachunkowości, co nie jest wymagane w przypadku inwentaryzacji sporządzonej zgodnie z wymogami rozporządzenia KRI (faktura vat, cena, data zakupu, oznaczenia inwentarzowe).

Mając na uwadze powyższe należy stwierdzić, że prowadzona w Urzędzie inwentaryzacja sprzętu i oprogramowania winna być uzupełniona o parametry wskazane powyżej, przez co możliwe będzie szybkie odtworzenie infrastruktury po katastrofie lub innym zdarzeniu losowym, w celu zapewnienia ciągłości działania Jednostki.

(dowód: akta kontroli str.149-175)

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.

Kontrolującym przedstawiono:

- *oświadczenie o przestrzeganiu zasad i przepisów ochrony danych osobowych i o zachowaniu tajemnicy danych osobowych,* zobowiązujące między innymi do zachowania w tajemnicy danych osobowych, do których pracownik ma lub będzie miał dostęp w związku z wykonywaniem zadań powierzonych przez pracodawcę. W dokumencie wskazano czas trwania tego zobowiązania, rozszerzając go także na okres po ustaniu stosunku pracy,
- *upoważnienia do przetwarzania danych osobowych* wystawione pracownikom realizującym zadania zlecone z zakresu administracji rządowej. Dokument upoważnienia określa jego obszar (ustalony w oparciu o zakres obowiązków) oraz okres jego ważności.

Kwestie nadawania i odbierania uprawnień do przetwarzania danych osobowych w systemach informatycznych uregulowano w § 8 *Instrukcji Zarządzania Systemami Informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Miejskim w Tucznie*. Zgodnie z regulacjami przyjętymi w Jednostce uprawnienia do pracy w systemie informatycznym nadaje Administrator Systemu Informatycznego[4] na podstawie upoważnienia wydanego przez Administratora Danych Osobowych[5]. Zgodnie z oświadczeniem Zastępcy Burmistrza Tuczna z dnia 11 sierpnia 2022 r. nadanie, modyfikacja lub cofnięcie uprawnień do pracy w systemie informatycznym poprzedza dostarczenie ASI kserokopii upoważnienia, a następuje na podstawie ustnego polecenia ADO. Dla tych czynności nie jest tworzona dodatkowa dokumentacja. Kontrolujący wskazują by wewnętrzne procedury uzupełnić o dokument, który poświadczać będzie realizowanie wymogu dokumentowania czynności nadawania i odbierania uprawnień do pracy w systemach informatycznych; ponieważ pisemny wniosek osób upoważnionych spowoduje, że proces nadawania i odbierania uprawnień będzie w pełni potwierdzony.

W trakcie prowadzenia czynności sprawdzających ustalono, że użytkownicy programu wykorzystywanego do obsługi spraw obywatelskich (Rejestr Mieszkańców XXX) posługiwali się jednym identyfikatorem i hasłem dostępu, co narusza wewnętrzne regulacje Jednostki oraz zapisy § 10 i § 21 rozporządzenia KRI. Każdy użytkownik winien bowiem posiadać unikalny identyfikator dostępności do systemu, a wykorzystywanie identyfikatora przez 2 i więcej osób jest niedopuszczalne. Ponadto zapewnienie rozliczalności operacji polega na gromadzeniu informacji o tym, kto, kiedy i jakie działania wykonał w systemie teleinformatycznym, szczególnie gdy przetwarzanie danych podlega prawnej ochronie.

W toku kontroli, po stwierdzeniu faktu wykorzystywania jednego identyfikatora przez kilku pracowników Informatyk urzędu nadał, zgodnie z wymogami rozporządzenia KRI, poszczególnym użytkownikom indywidualne identyfikatory do pracy w systemie.

[4] Administrator Systemu Informatycznego dalej ASI.

[5] Administratora Danych Osobowych dalej ADO.

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. 62,68-78, 102-103, 176-180, 185-186, 188)

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, zgodnie z oświadczeniem Zastępcy Burmistrza Tuczna z dnia 9 sierpnia 2022 r. *pracownicy zaangażowani w proces przetwarzania informacji w systemach teleinformatycznych oraz rejestrach publicznych używanych do realizacji zadań zleconych z zakresu administracji rządowej nie uczestniczyli w szkoleniach z zakresu bezpieczeństwa informacji*. Ponadto stwierdzono, że w Urzędzie nie wprowadzono wewnętrznych regulacji normujących przeprowadzanie szkoleń użytkowników zaangażowanych w procesie przetwarzania informacji w systemach teleinformatycznych. Jedyne odwołanie do procesu szkolenia znajduje się w § 7 *Polityki bezpieczeństwa w zakresie ochrony danych osobowych* i odnosi się do zadań Inspektora ochrony danych, w postaci przeprowadzania wstępnego szkolenia z zakresu ochrony danych osobowych i zapoznania pracowników z obowiązującą w Jednostce dokumentacją, związaną z bezpieczeństwem 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.

Wobec powyższych ustaleń należy stwierdzić, że w Jednostce nie zrealizowano dyspozycji § 20 ust. 2 pkt 6 rozporządzenia KRI.

(dowód: akta kontroli str. 63, 83)

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 unormowane w § 6 *Instrukcji Zarządzania Systemami Informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Miejskim w Tucznie*. Zgodnie z dyspozycją § 6 pkt 1 wyżej wzmiankowanej instrukcji *przetwarzanie danych poza obszarem przetwarzania na komputerach przenośnych wymaga zgody indywidualnej ADO*. W dokumencie zawarto zapisy o odpowiedzialności użytkownika komputera przenośnego za bezpieczeństwo danych.

Kontrolujący sugerują, aby dopracować procedurę w zakresie bezpiecznej pracy przy przetwarzaniu mobilnym i pracy na odległość oraz przy wykorzystaniu komputerów przenośnych

zgodnie z § 20 ust. 2 pkt 8 rozporządzenia KRI z uwzględnieniem niezbędnych zabezpieczeń np. szyfrowania twardych dysków, połączeń szyfrowanych itp.
Zgodnie z oświadczeniem zastępcy Burmistrza Tuczna z 11 sierpnia 2022 r. do realizacji zadań zleconych z zakresu administracji rządowej w Jednostce nie wykorzystywano urządzeń mobilnych i nie realizowano pracy na odległość.

(dowód: akta kontroli str.101-102, 181)

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 pracownika zatrudnionego w Urzędzie Miejskim w Tucznie, na stanowisku Informatyka urzędu. W zakresie obowiązków pracownika znajduje się m.in.: administrowanie siecią teleinformatyczną, wykonywanie obowiązków Administratora Systemów Informatycznych, instalacja i aktualizacja oprogramowania, ewidencjonowanie sprzętu i oprogramowania, zarządzanie bezpieczeństwem danych i systemów.
W celu realizacji zadań z zakresu administracji rządowej zawarto Umowę XXX, której przedmiotem jest prowadzenie nadzoru i serwisu oprogramowania użytkowanych systemów XXX.[6] Stwierdzono, że w powyższej umowie nie wprowadzono zapisów określających maksymalny czas skutecznej naprawy oprogramowania, powyższym nie wypełniono dyspozycji § 20 ust. 2 pkt 10 rozporządzenia KRI, zawierającego zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji.
W załączniku do wyżej opisanej umowy określono zasady powierzenia przetwarzania danych osobowych.

(dowód: akta kontroli str. 64-65, 132-138)

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

Ustalenia kontroli

W *Instrukcji Zarządzania Systemami Informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Miejskim w Tucznie,* w § 15 i 16 przedstawiono katalog przypadków zakwalifikowanych jako naruszenie lub podejrzenie naruszenia zabezpieczeń systemu informatycznego oraz określono sposób postępowania w przypadku stwierdzenia naruszenia bezpieczeństwa tego systemu.
Z oświadczenia zastępcy Burmistrza Tuczna z dnia 9 sierpnia 2022 r. wynika, że w Jednostce nie odnotowano incydentów naruszenia bezpieczeństwa informacji, wobec czego prowadzony w Urzędzie *Rejestr naruszeń bezpieczeństwa systemu informatycznego* (…) nie zawiera wpisów.

(dowód: akta kontroli str.61, 66-67, 107-108)

[6] Umowa nr 13865 z dnia 14.12.2021 r.

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.

Zgodnie z oświadczeniem zastępcy Burmistrza Tuczna z dnia 9 sierpnia 2022 r. *w latach 2019, 2020, 2021 w Urzędzie Miejskim w Tucznie nie przeprowadzono audytów wewnętrznych w zakresie bezpieczeństwa informacji*. Nieprzeprowadzanie kompleksowego audytu wewnętrznego w zakresie bezpieczeństwa informacji może wpływać na ocenę skuteczności przyjętych w Jednostce rozwiązań w zakresie bezpieczeństwa informacji.

Mając na względzie powyższe, należy stwierdzić, że w Urzędzie Miejskim w Tucznie nie wypełniono obowiązku, o którym mowa w § 20 ust. 2 pkt 14 rozporządzenia KRI,

(dowód: akta kontroli str. 59)

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 przez 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.

Kopie zapasowe oprogramowania wykorzystywanego do realizacji zadań zleconych z zakresu administracji rządowej, zgodnie z wyjaśnieniami Informatyka urzędu wykonywane są w dni robocze po uruchomieniu systemu operacyjnego, z wykorzystaniem oprogramowania zainstalowanego na komputerze. Kopia zapasowa baz danych wykonywana jest również każdorazowo przed instalacją aktualizacji programu. Na koniec tygodnia kopie zapasowe przenoszone są do serwera. Z wyjaśnień Informatyka urzędu wynika, ze przed skopiowaniem wykonane archiwa są testowane w celu sprawdzenia poprawności ich wykonania. W Jednostce nie sporządza się dokumentacji potwierdzającej przeprowadzenie testów.

W *Instrukcji Zarządzania Systemami Informatycznymi (...)* wskazano osoby odpowiedzialne za sporządzanie kopii zapasowych oraz wskazano częstotliwość ich tworzenia. Nie określono natomiast zasad i częstotliwości (użycie w procedurze określenia okresowo nie wyznacza precyzyjnie interwału czasowego) testowania kopii zapasowych danych i systemów na potrzeby weryfikacji poprawności i stanu ich wykonywania, nie określono również sposobu dokumentacji tych działań. Z wyjaśnień Informatyka urzędu wynika, że wprowadzono praktykę testowania

kopii zapasowych jeden raz w tygodniu, co nie znajduje odzwierciedlenia w obowiązującej procedurze.
Kontrolujący wskazują by w wewnętrznych procedurach doprecyzować zapisy dotyczące częstotliwości testowania kopii zapasowych (np. zgodne z dotychczasową praktyką) oraz określić sposób dokumentowania tych czynności, tak by realizowane działania były w pełni potwierdzone.
(dowód: akta kontroli str. 104, 183)

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 zawarto Umowę XXX, której przedmiotem jest prowadzenie nadzoru i serwisu oprogramowania użytkowanych systemów XXX.
(dowód: akta kontroli str. 132-137)

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. Dostęp do danych upoważniony użytkownik uzyskuje po wpisaniu hasła. Pracownicy złożyli oświadczenia o zachowaniu w tajemnicy danych osobowych, do których będą mieli dostęp w trakcie wykonywania obowiązków służbowych, jak również po ustaniu zatrudnienia w Urzędzie.
W wyniku oględzin 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, które posiadało aktualne definicje ochrony,
- na wszystkich jednostkach skonfigurowano wygaszacz ekranu (powrót do systemu operacyjnego wymagał podania loginu i hasła użytkownika),
- złożoność hasła była zgodna z wymogami rozporządzenia w sprawie dokumentacji i warunków technicznych,
- 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 wyposażono w klimatyzację, co wpływa na możliwość utrzymania odpowiedniego poziomu temperatury powietrza, zamontowano również czujkę dymu. Wejście do serwerowni dysponuje należytymi zabezpieczeniami w postaci drzwi antywłamaniowych z zamkiem elektronicznym otwieranym z użyciem kodu. Dostęp osób nieupoważnionych do serwerowni jest ograniczony.

(dowód: akta kontroli str. 69-78, 188-189)

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

W celu minimalizowania ryzyka utraty informacji w Urzędzie Miejskim w Tucznie zastosowano środki ochrony fizycznej w postaci systemu alarmowego, obejmującego wszystkie pomieszczenia oraz monitoring wizyjny pokoi, w których przechowywane są dokumenty zawierające wrażliwe dane osobowe. W *Polityce Bezpieczeństwa w zakresie Ochrony Danych Osobowych* szczegółowo określono zasady nadzoru nad kluczami do pomieszczeń Jednostki.

W celu zabezpieczenia sprzętu przed zanikiem zasilania Jednostkę wyposażono w zasilacze zapasowe UPS. Sieci i systemy zabezpieczono przy wykorzystaniu zapory sieciowej -firewall.

W procedurach wewnętrznych Jednostki określono zasady przechowywania i niszczenia elektronicznych nośników informacji oraz zasady naprawy urządzeń komputerowych zawierających dane osobowe.

(dowód: akta kontroli str. 84-85, 106)

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). Systemy objęte kontrolą zawierają logi, w których są odnotowanie działania użytkowników zgodnie z § 21 rozporządzenia KRI. Logi systemów przechowywane są przez okres 2 lat, co jest zgodne z § 21 ust. 4 rozporządzenia KRI. Zgodnie z wyjaśnieniami Informatyka urzędu w Jednostce prowadzone są działania związane z przeglądaniem logów, jednak nie jest sporządzana dokumentacja tego procesu. Kontrolujący wskazują aby dokumentować działania związane z przeglądaniem logów systemowych, tak by realizowane czynności były w pełni potwierdzone (dowód: akta kontroli str. 184, 187)	

Stwierdzone nieprawidłowości w obszarze nr 2:

1. Obowiązująca w Urzędzie dokumentacja regulująca kwestie bezpieczeństwa informacji, nie zawiera wszystkich elementów wymaganych przepisami rozporządzenia KRI.
2. Nieprzeglądanie obowiązującej w Urzędzie dokumentacji dotyczącej bezpieczeństwa informacji, do czego zobowiązują zapisy § 20 ust. 1 i 2 rozporządzenia KRI.
3. Nieprzeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, zgodnie z § 20 ust. 2 pkt 3 rozporządzenia KRI.
4. Inwentaryzacja sprzętu i oprogramowania nie zawiera wszystkich informacji, zgodnie z dyspozycją § 20 ust. 2 pkt 2 rozporządzenia KRI.
5. Wykorzystywanie jednego identyfikatora do programu XXX przez kilku użytkowników, czym naruszono wewnętrzne regulacje Jednostki oraz zapisy § 10 i § 21 rozporządzenia KRI.
6. Nieprzeprowadzenie szkoleń pracowników z zakresu bezpieczeństwa informacji, do czego zobowiązują zapisy § 20 ust. 2 pkt 6 rozporządzenia KRI.
7. W umowie XXX, regulującej kwestię serwisu oprogramowania programu wykorzystywanego do realizacji zadań zleconych z zakresu z zakresu administracji rządowej brak zapisów określających maksymalny czas skutecznej naprawy oprogramowania, czym nie wypełniono dyspozycji § 20 ust. 2 pkt 10 rozporządzenia KRI.

Ocena obszaru kontroli	**negatywna**
Wpis do książki kontroli	Nr 9
Wnioski dotyczące uzyskanych efektów zrealizowanego zadania	W Urzędzie Miejskim w Tucznie funkcjonują procedury regulujące kwestie bezpieczeństwa informacji, niemniej jednak wymagają one podjęcia działań korygujących i usprawniających. Istotną kwestią z punktu widzenia bezpieczeństwa informacji jest ciągłe podnoszenie świadomości pracowników dotyczące istnienia potencjalnych zagrożeń oraz wiedza w jaki sposób unikać, zminimalizować ale także postępować w przypadku materializacji ryzyk związanych z naruszeniem bezpieczeństwa informacji a w szczególności naruszenia ochrony danych osobowych; dlatego też szkolenia, których celem jest zagwarantowanie bezpieczeństwa w zakresie przetwarzania informacji winny być w Urzędzie przeprowadzane i mieć charakter cykliczny. Nieprawidłowości polegające na nieprzeprowadzaniu corocznych audytów wewnętrznych z zakresu bezpieczeństwa informacji mogą 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. Jednym z elementów SZBI, znacząco wpływającym na skuteczność zarządzania bezpieczeństwem informacji jest okresowo przeprowadzana analiza ryzyka utraty integralności, dostępności lub poufności informacji (nie była realizowana w Jednostce) w celu jego monitorowania i zapobiegania lub minimalizacji jego materializacji. Odpowiednio przygotowany proces szacowania ryzyka winien

	odnosić się i obejmować wszystkie posiadane i przetwarzane informacje, z uwzględnieniem specyfiki realizowanych przez Jednostkę zadań. Kluczowa rola analizy ryzyka wynika z faktu, że rodzaj i poziom zastosowanych zabezpieczeń jest względny i jest zależny od istotności informacji podlegających ochronie. Brak zapisów w umowach serwisowych określających maksymalny czas skutecznej naprawy oprogramowania wykorzystywanego do realizacji zadań zleconych z zakresu administracji rządowej potencjalnie zagraża ciągłości działania Urzędu.
Zalecenia	• uzupełnić dokumentację regulującą kwestie bezpieczeństwa informacji, zgodnie z wymogami rozporządzenia KRI, • przeglądać dokumentację regulującą kwestie bezpieczeństwa informacji, do czego zobowiązuje § 20 ust. 1 i 2 rozporządzenia KRI, • przeprowadzać okresowo analizy ryzyka utraty integralności, dostępności lub poufności informacji, zgodnie z § 20 ust. 2 pkt 3 rozporządzenia KRI, • uzupełnić inwentaryzację sprzętu i oprogramowania, zgodnie z dyspozycją § 20 ust. 2 pkt 2 rozporządzenia KRI, • nadawać każdemu użytkownikowi unikalny identyfikator dostępu do systemu, zgodnie z wewnętrznymi regulacjami Jednostki oraz zapisami § 10 rozporządzenia KRI, • przeprowadzać szkolenia pracowników, których celem jest zagwarantowanie bezpieczeństwa w zakresie przetwarzania informacji, zgodnie z zapisami § 20 ust. 2 pkt 6 rozporządzenia KRI, • w umowie regulującej kwestie serwisu oprogramowania programu wykorzystywanego do realizacji zadań zleconych z zakresu administracji rządowej wprowadzić zapisy określające maksymalny czas skutecznej naprawy oprogramowania, zgodnie z dyspozycją § 20 ust. 2 pkt 10 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