WOJEWODA
ZACHODNIOPOMORSKI

Szczecin, dnia 7 lutego 2023 r.

Znak: K-2.431.1.33.2022.7.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 Pełczyc, ul. Rynek Bursztynowy 2, 73-260 Pełczyce.
Osoba pełniąca funkcję Burmistrza Pełczyc w okresie objętym kontrolą / okresie prowadzenia kontroli	Pan Mirosław Józef Kluk
Okres objęty kontrolą	od dnia 1 stycznia 2019 r. do dnia 7 października 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 49/22 z dnia 30 września 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	3-7 października 2022 r.
Rodzaj i tryb kontroli	kontrola planowa, tryb zwykły
Osoba udzielająca wyjaśnień w trakcie kontroli	Pan Maciej Krzyśko - Informatyk

[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 Pełczycach wykorzystywano jeden system centralny (aplikacja Źródło) oraz system informatyczny wspomagający obsługę spraw obywatelskich w zakresie ewidencji ludności - (XXX.). System XXX posiada homologację Departamentu Rozwoju Informatyki i Systemu Rejestrów Państwowych MSWiA. 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. 40-41)	
1.2 Formaty danych udostępniane przez systemy teleinformatyczne	
Podstawa prawna	**§ 17 ust. 1 rozporządzenia KRI:** *Kodowanie znaków w dokumentach wysyłanych z systemów teleinformatycznych podmiotów realizujących zadania publiczne lub odbieranych przez takie systemy, także w odniesieniu do informacji wymienianej przez te systemy z innymi systemami na drodze teletransmisji, o ile wymiana ta ma charakter wymiany znaków, odbywa się według standardu Unicode UTF-8 określonego przez normę ISO/IEC 10646 wraz ze zmianami lub normę ją zastępującą.* **§ 18 ust. 1 rozporządzenia KRI:** *Systemy teleinformatyczne podmiotów realizujących zadania publiczne udostępniają zasoby informacyjne co najmniej w jednym z formatów danych określonych w załączniku nr 2 do rozporządzenia.* **§ 18 ust. 2 rozporządzenia KRI:** *Jeżeli z przepisów szczegółowych albo opublikowanych w repozytorium interoperacyjności schematów XML lub innych wzorów nie wynika inaczej, podmioty realizujące zadania publiczne umożliwiają przyjmowanie dokumentów elektronicznych*

[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".

	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 Pełczycach 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, Windows-1250. (dowód: akta kontroli str. 305)	
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 Pełczycach w zakresie bezpieczeństwa informacji, w okresie objętym kontrolą obowiązywały następujące dokumenty: – *Zarządzenie Nr 54.2018 Burmistrza Pełczyc z dnia 3 sierpnia 2018 r. w sprawie wprowadzenia Regulaminu Ochrony Danych Osobowych, rejestru udostępnień danych osobowych oraz rejestru naruszeń danych osobowych* (okres funkcjonowania regulacji: 3 sierpnia 2018 r.- 29 grudnia 2020 r.).	

Ustalono, że w ciągu okresu obowiązywania dokumentacja nie była aktualizowana, co skutkowało brakiem wdrożenia wymogów obowiązującego od dnia 12 kwietnia 2012r. rozporządzenia KRI. Procedury nie zawierały elementów określonych w rozporządzeniu KRI i ograniczały się do zagadnień związanych z ochroną danych osobowych, czym nie wypełniały dyspozycji ww. rozporządzenia, nie tworząc zarazem skutecznego systemu zarządzania bezpieczeństwem informacji[4].

- *Zarządzenie Nr 88.2020 Burmistrza Pełczyc z dnia 29 grudnia 2020 r. w sprawie Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miejskim w Pełczycach,*
- *Zarządzenie Nr 87.2020 Burmistrza Pełczyc z dnia 29 grudnia 2020 r. w sprawie wprowadzenia Instrukcji Bezpieczeństwa Danych Osobowych, Zarządzania Systemem Informatycznym oraz Postepowania w sytuacji naruszenia systemu ochrony danych osobowych w Urzędzie Miejskim w Pełczycach* (oba dokumenty funkcjonują od 29 grudnia 2020 r.).

W wyniku analizy wyżej przywołanych zarządzeń Burmistrza dotyczących bezpieczeństwem informacji stwierdzono, że w Urzędzie Miejskim w Pełczycach opracowano i wdrożono System Zarządzania Bezpieczeństwem Informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność działań.

(dowód: akta kontroli str. 70-162, 257-303, 312-358)

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 zostały opracowane i zatwierdzone regulacje wewnętrzne opisujące sposób zarządzania ryzykiem bezpieczeństwa informacji w postaci *Procedury szacowania i postępowania z ryzykiem*, stanowiącym załącznik nr 4 do *Systemu Zarzadzania Bezpieczeństwem Informacji w Urzędzie Miejskim w Pełczycach*.

W okresie objętym kontrolą, zgodnie z oświadczeniem Burmistrza Pełczyc z dnia 5 października 2022 r. w Urzędzie przeprowadzono jedną analizę ryzyka. W dokumencie zidentyfikowano następujące zagrożenia: phishing, cybersquatting, nakłanianie do wykonania czynności, ataki na sprzęt, ataki na oprogramowanie, podsłuchiwanie transmisji (okablowanie, wifi, telefonia, internet), DOS, wirusy / trojany, backdoory, keyloggery, ransomeware, zniszczenie sprzętu, kradzież sprzętu, pożar / eksplozja, zalanie, przegrzanie, awaria zasilania, awaria sprzętu, nieuprawniona modyfikacja / usunięcie, nieuprawnione kopiowanie danych, kradzież danych w formie papierowej, kradzież danych lub nośników, utrata / kradzież danych dostępowych (hasła, klucze, certyfikaty), błąd oprogramowania, brak / błędy w wykonywaniu kopii bezpieczeństwa, udostępnienie danych osobom nieupoważnionym, nieprawidłowe / brak procedur niszczenia nośników z danymi, nieprawidłowe / brak procedur napraw w serwisach zewnętrznych, nieprzestrzeganie procedur, pomyłki administratorów i użytkowników, brak świadomości / wiedzy, brak aktualnej dokumentacji, nieprawidłowe / brak umowy o współpracy, awaria łączy telekomunikacyjnych. Dla wskazanych zagrożeń określono prawdopodobieństwo wystąpienia oraz skutki a w rezultacie poziom ryzyka utraty integralności, dostępności i poufności informacji. Z przedstawionej analizy wynika, że dla większości określonych w Jednostce zagrożeń zidentyfikowano akceptowalny poziom ryzyka. Poziom alarmowy ryzyka zdefiniowano dla wyłudzeń informacji oraz udostępnienia jej osobom nieuprawnionym,

[4] Dalej SZBI.

wynikający z błędów ludzkich. Wskazano, że w tych obszarach należy uwrażliwić pracowników na potencjalne zagrożenia. Kontrolujący wskazują by w tym celu przeprowadzać odpowiednio często szkolenia pracowników Jednostki z zakresu bezpieczeństwa informacji.
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.
Zaleca się, aby zarządzanie ryzykiem w bezpieczeństwie informacji było integralną częścią wszystkich działań związanych z tym obszarem oraz zostało zastosowane w ciągłej eksploatacji SZBI. (dowód: akta kontroli str. 222-224, 304)

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.
Inwentaryzacja zasobów informatycznych w Urzędzie jest realizowana w wersji elektronicznej przy wykorzystaniu programu komputerowego generującego raporty zawierające informacje dotyczące m. in. sprzętu i oprogramowania oraz rodzaju systemu operacyjnego, co wypełnia wymogi rozporządzenia KRI dotyczące utrzymania aktualności inwentaryzacji sprzętu i oprogramowania. (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.
Kwestie nadawania i odbierania uprawnień do przetwarzania danych osobowych w systemach informatycznych uregulowano w *Instrukcji zarządzania systemem informatycznym,* stanowiącym

załącznik nr 2 do *Zarządzenia 87.2020 Burmistrza Pełczyc z dnia 29 grudnia 2020 r.* Zgodnie z regulacjami przyjętymi w Jednostce uprawnienia do pracy w systemie informatycznym nadaje Administrator Systemu Informatycznego[5] lub inny upoważniony przez Administratora Danych Osobowych pracownik, na podstawie pisemnego wniosku administratora danych.
Kontrolującym przedstawiono:

- *upoważnienia do przetwarzania danych osobowych* wystawione pracownikom realizującym zadania zlecone z zakresu administracji rządowej. Upoważnienie określa jego obszar, wynikający z zadań realizowanych na zajmowanym stanowisku oraz okres jego ważności. W dokumencie zawarto oświadczenie pracownika o przestrzeganiu zasad i przepisów ochrony danych osobowych oraz o zachowaniu w tajemnicy przetwarzanych danych. Nie wskazano natomiast czasu trwania tego zobowiązania. Kontrolujący sugerują, by zrewidować powyższy dokument pod kątem wskazania okresu obowiązywania zobowiązania i rozszerzyć go na okres po ustaniu stosunku pracy.
- *wnioski o dostęp do aktywów Urzędu* (nadanie uprawnień) - dokument wskazuje aktywa (programy i systemy informatyczne), do których pracownik uzyskuje dostęp. W wyniku analizy przedstawionych wniosków ustalono, że w dokumentach pracowników realizujących zadania zlecone z zakresu administracji rządowej brak było wskazania nadania uprawnień do systemu XXX, wykorzystywanego do realizacji tych zadań. Zgodnie z oświadczeniem Burmistrza Pełczyc z dnia 7 października 2022 r. dokumentacja w wyżej opisanym zakresie zostanie uzupełniona.

W trakcie prowadzenia czynności kontrolnych ustalono, że użytkownicy programu wykorzystywanego do obsługi spraw obywatelskich w zakresie ewidencji ludności - XXX posługiwali się jednym identyfikatorem i kluczem sprzętowym dostępu do programu, 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. Po stwierdzeniu faktu wykorzystywania jednego identyfikatora przez kilku pracowników (zgodnie z wyjaśnieniami Informatyka) poszczególnym użytkownikom zostały nadane (zgodnie z wymogami rozporządzenia KRI), indywidualne identyfikatory do pracy w systemie oraz indywidualnie przypisane klucze sprzętowe.
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. 151-152, 211-221, 308-310)

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 przeprowadzono szkolenie pracowników Jednostki z zakresu bezpieczeństwa informacji. Udział w szkoleniu dokumentowała lista obecności

[5] Administrator Systemu Informatycznego dalej ASI.

zawierająca imię i nazwisko uczestnika oraz własnoręczny podpis. Stwierdzono, że w szkoleniu uczestniczyli pracownicy zaangażowani w proces przetwarzania informacji w systemach teleinformatycznych oraz rejestrach publicznych używanych do realizacji zadań zleconych z zakresu administracji rządowej. Zakres tematyczny szkolenia obejmował zagadnienia wskazane w § 20 ust. 2 pkt 6 rozporządzenia KRI.
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.

(dowód: akta kontroli str. 225-226)

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 poruszone w *Instrukcji zarządzania systemem teleinformatycznym,* stanowiącym załącznik nr 9 do dokumentu *Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miejskim w Pełczycach Polityka Bezpieczeństwa Informacji*. Zgodnie z dyspozycją punktu 3.4 wyżej wzmiankowanej instrukcji wynoszenie poza obszar organizacji niezabezpieczonych nośników z danymi osobowymi bez zgody Administratora Danych jest zabronione a nośniki przed opuszczeniem Jednostki muszą być zaszyfrowane. W punkcie 3.5 zawarto wymóg zabezpieczenia hasłem lub zaszyfrowania informacji przekazywanych przy użyciu poczty elektronicznej. Ponadto w *Instrukcji zarządzania systemem informatycznym,* stanowiącym załącznik nr 2 do *Zarządzenia 87.2020 Burmistrza Pełczyc z dnia 29 grudnia 2020 r.* uregulowano kwestie dodatkowych zabezpieczeń hasłem plików zawierających dane osobowe i wskazano osobę odpowiedzialną za ochronę danych zawartych na komputerach przenośnych. Zgodnie z powyższą procedurą przesyłanie drogą elektroniczną informacji zawierających dane osobowe może odbywać się tylko w formie zaszyfrowanej, a sam proces wysyłania tego typu danych uzależniono od uzyskaniu zgody ADO.
Zgodnie z wyjaśnieniami Burmistrza Pełczyc z 5 października 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. 116, 149-150, 305)

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 Urzędu realizowana jest na podstawie umowy o świadczenie usług informatycznych, zawartej z firmą XXX[6], w ramach której wykonywane są następujące zadania: administrowanie siecią informatyczną; nadzór nad poprawnością działania sprzętu komputerowego; instalacja i konfiguracja oprogramowania oraz sprzętu komputerowego i sieciowego; przegląd, konserwacja i naprawa sprzętu; aktualizacja oprogramowania; pełnienie funkcji administratora systemów informatycznych; wykonywanie kopii danych. W powyższej

[6] Umowa nr RIP.215.127.2019 z dnia 16 października 2019 r.

umowie uregulowano kwestię czasu reakcji na zgłoszenie związane z awarią systemu informatycznego. Z firmą XXX 16 października 2019 r. zawarto *Umowę powierzenia przetwarzania danych osobowych.*

W celu wykonywania zadań z zakresu administracji rządowej XXX zawarto umowę[7] na sprawowanie opieki autorskiej nad systemami XXX. Jej przedmiotem jest udostępnienie nowych wersji oprogramowania; usuwanie wad, błędów, awarii i usterek w działaniu oprogramowania oraz udzielanie wsparcia w zakresie jego eksploatacji. Dokument stanowi, że powyższe usługi będą świadczone z zachowaniem postanowień umowy powierzenia przetwarzania danych osobowych,[8] zawartej z jednostką autorską oprogramowania (XXX). W przedmiotowym dokumencie 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.

(dowód: akta kontroli str. 227-238)

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 postępowania w sytuacji naruszenia systemu ochrony danych osobowych* stanowiącej załącznik Nr 3 do *Zarządzenia Nr 87.2020 Burmistrza Pełczyc z dnia 29 grudnia 2020 r.*, w § 15 i 16 określono sposób postępowania w przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych oraz zabezpieczeń systemu informatycznego. W *Instrukcji zarządzania systemem teleinformatycznym*, będącej załącznikiem nr 9 do *Systemu Zarzadzania Bezpieczeństwem Informacji w Urzędzie Miejskim w Pełczycach - Incydenty i zdarzenia w bezpieczeństwie informacji* umieszczono informację wskazującą drogi kontaktu (e- mail, numer telefonu) przy zgłaszaniu stwierdzenia lub podejrzenia zaistnienia incydentu.

Kontrolujący sugerują stworzenie jednolitego tekstu procedury normującej kwestie zgłaszania incydentów naruszenia bezpieczeństwa informacji, co pozwoli na szybsze, bardziej intuicyjne odnalezienie stosownych informacji a przede wszystkim kompleksowe zastosowanie odpowiednich zapisów.

Z oświadczenia Burmistrza Pełczyc z dnia 5 października 2022 r. wynika, że w Jednostce nie odnotowano incydentów naruszenia bezpieczeństwa informacji, wobec czego prowadzony w Urzędzie Rejestr naruszeń bezpieczeństwa informacji nie zawiera wpisów.

(dowód: akta kontroli str. 117, 160-167, 307)

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

[7] Umowa z dnia 6 grudnia 2021 r.

[8] Umowa powierzenia przetwarzania danych osobowych z dnia 29.11.2018 r.

bezpieczeństwa, różnych aspektach jego utrzymania oraz wskazuje obszary wymagające podjęcia działań korygujących.
Zgodnie z wyjaśnieniami Burmistrza Pełczyc z 5 października 2022 r. audyt wewnętrzny z zakresu bezpieczeństwa informacji w 2019 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. 162-210)

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, zgodnie z wyjaśnieniami Informatyka wykonywane są codziennie na dwa serwery NAS usytuowane w różnych lokalizacjach. Ponadto jeden raz w tygodniu wykonuje się kopie bezpieczeństwa na dysk zewnętrzny, przechowywany poza siedzibą Urzędu.
Z oświadczenia Informatyka wynika również, że próbne testowane w celu sprawdzenia poprawności wykonania kopii bezpieczeństwa wykonywane jest jeden raz w kwartale, przy czym nie sporządza się dokumentacji potwierdzającej przeprowadzenie testów.
W *Procedurze wykonania i odzyskania kopii zapasowej*, będącej załącznikiem nr 10 do *Polityki Bezpieczeństwa Informacji* wskazano osoby odpowiedzialne za sporządzanie kopii zapasowych oraz wskazano częstotliwość ich tworzenia. Ponadto określono zasady i częstotliwości testowania kopii zapasowych danych i systemów na potrzeby weryfikacji poprawności i stanu ich wykonywania. W § 24 *Instrukcji Zarządzania Systemem Informatycznym*, będącej załącznikiem nr 2 do Zarządzenia Nr 87.2020 Burmistrza Pełczyc z dnia 29 grudnia 2020 r. określono tryb dokumentacji tych działań. ASI prowadzi Dziennik ewidencji kopii bezpieczeństwa systemów informatycznych, w którym rejestruje fakt sporządzenia, sprawdzania, niszczenia kopii bezpieczeństwa jak również odtwarzania danych z tych kopii. Kontrolujący wskazują żeby zgodnie z wewnętrznymi uregulowaniami Jednostki prowadzić Dziennik ewidencji kopii bezpieczeństwa systemów informatycznych, tak by realizowane działania były w pełni potwierdzone.
W dokumentacji wewnętrznej Urzędu (Polityce oraz Instrukcji) funkcjonują sprzeczne zapisy dotyczące kopii zapasowych w zakresie dostępu do kopii, osób odpowiedzialnych za ich wykonanie oraz sposobu tworzenia; wobec czego należy powyższe regulacje uściślić i doprecyzować.

(dowód: akta kontroli str. 118-121, 154, 308)

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 XXX zawarto umowę na sprawowanie opieki autorskiej nad systemami XXX. Jej przedmiotem jest udostępnienie nowych wersji oprogramowania; usuwanie wad, błędów, awarii i usterek w działaniu oprogramowania oraz udzielanie wsparcia w zakresie jego eksploatacji.

(dowód: akta kontroli str. 231)

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 programu „Źródło" dostęp następuje przy użyciu 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 przeprowadzonych w toku czynności kontrolnych ustalono, że:

- użytkownik systemu Windows, realizujący zadania zlecone z zakresu administracji rządowej posiadał uprawnienia administratora, co umożliwiało instalowanie oprogramowania niewiadomego pochodzenia lub zmianę ustawień systemu operacyjnego, a także ingerencję w rejestry zdarzeń;
- ustawienie monitora stanowiska obsługi Systemów Rejestrów Państwowych umożliwiał odczyt wyświetlanych danych przez osoby trzecie;
- stanowisko komputerowe przeznaczone do realizacji zadań zleconych z zakresu administracji rządowej nie posiadało skonfigurowanego wygaszacza ekranu. Zgodnie z wyjaśnieniami Informatyka powrót do systemu operacyjnego wymaga użycia klucza sprzętowego, a brak klucza powoduje zablokowanie komputera.

Ponadto stwierdzono wykorzystywanie tego samego loginu i hasła przez więcej, niż 1 osobę. W trakcie trwania kontroli Informatyk poinformował o utworzeniu odrębnego loginu dostępu do programu XXX, odebraniu użytkownikowi uprawnień administratora oraz dokonaniu zmiany umiejscowienia monitora. Mając na uwadze powyższe odstępuje się od formułowania uwagi dotyczącej niewłaściwego ustawienia monitora.

Serwer znajduje się w oddzielnym pomieszczeniu, zlokalizowanym w budynku Urzędu. Pomieszczenie serwerowni nie jest wyposażone w klimatyzację, co wpływa na brak możliwości utrzymania odpowiedniego poziomu temperatury powietrza, nie zamontowano również czujki dymu. Wejście do serwerowni nie dysponuje należytymi zabezpieczeniami.

(dowód: akta kontroli str. 68-69)

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 zabezpieczenia sprzętu przed zanikiem energii Jednostkę wyposażono w zasilacze zapasowe UPS. Sieci i systemy zabezpieczono przy wykorzystaniu zapory sieciowej -firewall. Na komputerach podlegających badaniu zainstalowano oprogramowanie antywirusowe, które zawierało aktualne definicje ochrony. W procedurach wewnętrznych Jednostki określono zasady naprawy elektronicznych nośników informacji zawierających dane osobowe. (dowód: akta kontroli str. 68-69, 116-117, 310)	
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 w celu identyfikacji działań niepożądanych, tak by realizowane czynności były w pełni potwierdzone.

(dowód: akta kontroli str. 239, 310)

Stwierdzone nieprawidłowości w obszarze nr 2:

1. Wykorzystywanie jednego identyfikatora do programu XXX przez kilku użytkowników, co narusza wewnętrzne regulacje Jednostki oraz zapisy § 10 i § 21 rozporządzenia KRI.
2. W umowie XXX, regulującej kwestię serwisu oprogramowania programu wykorzystywanego do realizacji zadań zleconych z zakresu administracji rządowej brak zapisów określających maksymalny czas skutecznej naprawy oprogramowania, co nie wypełnia dyspozycji § 20 ust. 2 pkt 10 rozporządzenia KRI.
3. Nieprzeprowadzenie w 2019 roku audytu wewnętrznego w zakresie bezpieczeństwa informacji, zgodnie z wymogami § 20 ust. 2 pkt 14 rozporządzenia KRI.

Ocena obszaru kontroli	**Pozytywna z nieprawidłowościami**
Wpis do książki kontroli	Nr 4
Wnioski dotyczące uzyskanych efektów zrealizowanego zadania	W Urzędzie Miejskim w Pełczycach funkcjonują procedury regulujące kwestie bezpieczeństwa informacji, zapewniające zachowanie zasad poufności, dostępności i integralności. 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. Z tego powodu szkolenia, których celem jest zagwarantowanie bezpieczeństwa w zakresie przetwarzania informacji winny być cyklicznie przeprowadzane. Przyznanie dostępu do systemu informatycznego dwóm osobom przy wykorzystaniu tego samego identyfikatora rzutuje na kwestie rozliczalności działań w systemach teleinformatycznych, natomiast brak zapisów określających maksymalny czas skutecznej naprawy oprogramowania wykorzystywanego do realizacji zadań zleconych z zakresu administracji rządowej potencjalnie zagraża ciągłości działania Urzędu.

Zalecenia	• nadawać każdemu użytkownikowi unikalny identyfikator dostępu do systemu, zgodnie z wewnętrznymi regulacjami Jednostki oraz zapisami § 10 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, • przeprowadzać nie rzadziej niż raz na rok audyt wewnętrzny w zakresie bezpieczeństwa informacji, zgodnie z wymogami § 20 ust. 2 pkt 14 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