WOJEWODA
ZACHODNIOPOMORSKI

Szczecin, dnia 24 kwietnia 2023 r.

Znak: K-2.431.1.12.2023.6.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 Cedyni, ul. Plac Wolności 1, 74-520 Cedynia.
Osoba pełniąca funkcję Burmistrza Cedyni w okresie objętym kontrolą / okresie prowadzenia kontroli	Pan Adam Zarzycki
Okres objęty kontrolą	od dnia 1 stycznia 2020 r. do dnia 28 lutego 2023 r.
Kontrolujący	Pracownicy Wydziału Kontroli Zachodniopomorskiego Urzędu Wojewódzkiego w Szczecinie: Pani Anna Dąbska – kierownik oddziału, *kierownik zespołu kontrolnego,* Pani Iwona Olesińska – starszy inspektor wojewódzki.
Nr upoważnienia	Nr 12/23 z dnia 6 lutego 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	22-28 lutego 2023 r.
Rodzaj i tryb kontroli	kontrola planowa, tryb zwykły
Osoba udzielająca wyjaśnień w trakcie kontroli	Pan Michał Nieścioruk- Informatyk

[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 Cedyni wykorzystywano jeden system centralny (aplikacja Źródło) oraz systemy informatyczne wspomagające obsługę spraw obywatelskich w zakresie ewidencji mieszkańców oraz rejestru zamieszkania cudzoziemców - program XXX - wspierający pracę z zakresu tworzenia aktów stanu cywilnego (oprogramowanie firmy XXX). Systemy informatyczne wspomagające realizację zadań zleconych z zakresu administracji rządowej Urzędu Miejskiego w Cedyni zostały zaprezentowane w czasie kontroli, 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. 57-71, 326-328)	
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*

[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".

	realizujących zadania publiczne udostępniają zasoby informacyjne co najmniej w jednym z formatów danych określonych w załączniku nr 2 do rozporządzenia. **§ 18 ust. 2 rozporządzenia KRI:** *Jeżeli z przepisów szczegółowych albo opublikowanych w repozytorium interoperacyjności schematów XML lub innych wzorów nie wynika inaczej, podmioty realizujące zadania publiczne umożliwiają przyjmowanie dokumentów elektronicznych służących do załatwiania spraw należących do zakresu ich działania w formatach danych określonych w załącznikach nr 2 i 3 do rozporządzenia*
Ustalenia kontroli System informatyczny wykorzystywany do realizacji zadań zleconych z zakresu administracji rządowej w Urzędzie Miejskim w Cedyni 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. 49)	
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 Cedyni, w okresie objętym kontrolą obowiązywały następujące dokumenty z zakresu bezpieczeństwa informacji:

- *Zarządzenie Nr 4/2020 Burmistrza Cedyni z dnia 2 stycznia 2020 r. w sprawie wprowadzenia Polityki Ochrony Danych Osobowych oraz Systemu Zarządzania Bezpieczeństwem Informacji*[4] *w Urzędzie Miejskim w Cedyni* (okres funkcjonowania regulacji - od 2 stycznia 2020 do 9 stycznia 2022 r.)
- *Zarządzenie Nr 5/2022 Burmistrza Cedyni z dnia 10 stycznia 2022 r. w sprawie wprowadzenia Polityki Ochrony Danych Osobowych oraz Systemu Zarządzania Bezpieczeństwem Informacji (Polityka Bezpieczeństwem Informacji) w Urzędzie Miejskim w Cedyni* (okres funkcjonowania regulacji - od 10 stycznia 2022 r.)

Obowiązujące Zarządzenie Burmistrza Cedyni wprowadza procedury zapewniające bezpieczeństwo informacji w Urzędzie. Na SZBI składają się następujące dokumenty:

- Polityka bezpieczeństwa informacji
- Inwentaryzacja sprzętu i oprogramowania
- Analiza ryzyka
- Zarządzanie uprawnieniami
- Plany szkoleń
- Monitorowanie dostępu do informacji
- Zasady pracy mobilnej
- Procedury kopii zapasowych
- Umowy serwisowe
- Procedury postępowania z informacjami
- Procedury aktualizacji oprogramowania
- Procedury na wypadek awarii
- Procedury ochrony oprogramowania przed błędami
- Procedury szyfrowania informacji
- Spis systemów informatycznych
- Procedury redukcji ryzyk
- Procedury w przypadku naruszeń
- Procedury kontroli systemów informatycznych
- Procedury zgłaszania incydentów
- Procedury audytowania
- Procedury gromadzenia logów.

W wyniku analizy aktualnej dokumentacji związanej z bezpieczeństwem informacji stwierdzono, że funkcjonujące w Jednostce procedury spełniają wymogi określone w § 20 ust. 2 pkt 1 rozporządzenia KRI w zakresie bezpieczeństwa informacji. SZBI zawiera miedzy innymi

[4] System Zarządzania Bezpieczeństwem Informacji-dalej SZBI.

definicję bezpieczeństwa informacji, oświadczenie o intencjach kierownictwa; wyjaśnienie zasad, norm i wymagań zgodności mających szczególne znaczenie dla organizacji; definicje ogólnych i szczególnych obowiązków w odniesieniu do zarządzania bezpieczeństwem informacji. Dyrektywa § 20 ust. 2 pkt 1 rozporządzenia KRI wskazuje na konieczność *zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia.* Stwierdzono, że obowiązująca w Jednostce dokumentacja była poddana przeglądowi i weryfikacji pod kątem jej aktualizacji.

Mając na względzie powyższe, należy stwierdzić, że w Urzędzie Miejskim w Cedyni 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. 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

W Jednostce zostały opracowane oraz zatwierdzone regulacje wewnętrzne opisujące sposób zarządzania ryzykiem w bezpieczeństwie informacji, w postaci procedury *Analiza ryzyka w bezpieczeństwie informacji.*

Kontrolującym przedstawiono następujące dokumenty potwierdzające przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, dotyczące okresu objętego kontrolą:

- Analiza zagrożeń i ryzyka 2022
- Analiza zagrożeń i ryzyka 2021
- Analiza zagrożeń i ryzyka 2020
- Analiza ryzyka związana z zapewnieniem bezpiecznej pracy zdalnej dla urzędników podczas pandemii COVID-19.

Zaprezentowane analizy ryzyka obejmują wszystkie aktywa Jednostki, a szacowanie zidentyfikowanych ryzyk pozwala na zastosowanie odpowiednich mechanizmów przeciwdziałania w sytuacji materializacji ryzyk. W dokumencie określono zagrożenia dla wskazanych zasobów, źródła tych zagrożeń oraz siłę wpływu zdarzeń na czynniki decydujące o bezpieczeństwie informacji. Dla zdefiniowanych zagrożeń przedstawiono sugerowane działania korygujące, w celu przeciwdziałania bądź też zmniejszenia prawdopodobieństwa 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. Procedura szacowania ryzyka przeprowadzana jest w Jednostce corocznie. Ponadto stwierdzono, że procedura taka została przeprowadzana w Urzędzie w momencie pojawienia się nowego zagrożenia (COVID-19).

Mając na względzie powyższe, należy stwierdzić, że w Urzędzie Miejskim w Cedyni w badanym okresie realizowano w pełni dyspozycję, o której mowa w § 20 ust. 2 pkt 3 rozporządzenia KRI.

(dowód: akta kontroli str. 179-201)

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 oprogramowania do inwentaryzacji XXX oraz oprogramowania antywirusowego XXX. Oba systemy umożliwiają prowadzenia inwentaryzacji generując raporty zawierające informacje dotyczące m. in. sprzętu i oprogramowania oraz rodzaju systemu operacyjnego. W związku z tym, że sieć komputerowa z jednostkami wykorzystywanymi do realizacji zadań z zakresu administracji rządowej jest odłączona od sieci komputerowej Urzędu Miejskiego inwentaryzacja w tej grupie jednostek operacyjnych realizowana jest w postaci zapisów w pliku, przy wykorzystaniu arkusza kalkulacyjnego Microsoft Excel.

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

(dowód: akta kontroli str. 335-345)

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 *Polityce Bezpieczeństwa Informacji*. Zgodnie z regulacjami przyjętymi w Jednostce

uprawnienia w zakresie dostępu do systemu informatycznego nadaje administrator systemu informatycznego, na podstawie pisemnego wniosku administratora danych osobowych o nadanie uprawnień dla użytkownika w systemie informatycznym.
Kontrolującym przedstawiono:

- *upoważnienia do przetwarzania danych osobowych* wystawione pracownikom Jednostki. Upoważnienie określa jego obszar, wynikający z zadań realizowanych na zajmowanym stanowisku oraz okres jego ważności,
- *oświadczenia o poufności*, w których zawarto miedzy innymi oświadczenie pracownika o zachowaniu w tajemnicy przetwarzanych danych, wskazując okres obowiązywania zobowiązania również na okres po ustaniu stosunku pracy,
- *wnioski o nadania/odebranie upoważnienia do przetwarzania danych*,
- *wniosek o nadanie uprawnień dla użytkownika w systemie informatycznym.*

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. 126, 167, 321-334)

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 (9 stycznia 2020 r.) w Urzędzie Miejskim w Cedyni przeprowadzono szkolenie pracowników z zakresu bezpieczeństwa i ochrony danych osobowych. Udział w szkoleniu dokumentowała lista obecności zawierająca imię i nazwisko uczestnika, stanowisko służbowe oraz własnoręczny podpis. Stwierdzono, że pracownicy zaangażowani w proces przetwarzania informacji w systemach teleinformatycznych używanych do realizacji zadań zleconych z zakresu administracji rządowej uczestniczyli w wyżej opisanym szkoleniu.
Ponadto pracownicy Urzędu, zostali zobligowani do zapoznania się (w formie samodzielnej pracy) z informacjami dotyczącymi bezpieczeństwa informacji i ochrony danych osobowych publikowanymi na wewnętrznej stronie internetowej w Urzędzie Miejskim w Cedyni. Na stronie umieszczono między innymi materiały CERT o hasłach dostępu do systemów; najważniejsze zasady ochrony informacji; informację dotyczącą RODO; wskazówki odnośnie sposobów tworzenia własnych kopii zapasowych. Kontrolującym przestawiono oświadczenia pracowników z dnia 1 lutego 2023 r. o zapoznaniu się z wyżej opisanym materiałem szkoleniowym.
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 wynika, że zakres tematyczny szkoleń przeprowadzonych w Urzędzie obejmował zagadnienia wskazane w § 20 ust. 2 pkt 6 rozporządzenia KRI.

(dowód: akta kontroli str. 361-363)

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 procedurach Jednostki wprowadzonych *Zarządzeniem Nr 5/2022 Burmistrza Cedyni z dnia 10 stycznia 2022 r. w sprawie wprowadzenia Polityki Ochrony Danych Osobowych oraz Systemu Zarządzania Bezpieczeństwem Informacji (Polityka Bezpieczeństwem Informacji) w Urzędzie Miejskim w Cedyni.* Komputery przenośne użytkowane w Jednostce zostały zabezpieczone programem do szyfrowania XXX. W Urzędzie opracowano i wdrożono również *Instrukcję szyfrowania i hasłowania danych osobowych przeznaczonych do wysyłki komunikacją elektroniczną.*

Zgodnie z wyjaśnieniami Burmistrza Cedyni z dnia 24 lutego 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. 77-78, 170)

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 realizowana jest przez pracownika zatrudnionego w Urzędzie Miejskim w Cedyni na stanowisku Informatyka. W zakresie obowiązków pracownika znajduje się m.in.: administrowanie siecią informatyczną; nadzór nad rozwojem i eksploatacją oprogramowania; administrowanie siecią komputerową; instalacja i aktualizacja nowego oprogramowania; wykonywanie kopii zapasowych i zabezpieczenie zbiorów.

W celu realizacji zadań z zakresu administracji rządowej z firmą XXX, zawarto umowę o asystę techniczną oprogramowania komputerowego XXX, obejmującą swym zakresem między innymi: aktualizację i modyfikację oprogramowania, diagnozowanie i usuwanie błędów oraz wsparcie techniczne[5]. W umowie 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 *Umowę 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. 346-360)

[5] Umowa nr EA-034-2023 z dnia 28 grudnia 2022 r.

[6] Umowa nr EP-034-2023 z dnia 28 grudnia 2022 r.

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 z incydentami* i *Procedurze zgłaszania naruszenia ochrony danych osobowych organowi nadzorczemu,* stanowiącymi załącznik nr 9 do *Polityki Ochrony Danych Osobowych* określono sposób postępowania w przypadku stwierdzenia naruszenia danych osobowych, wskazując jednocześnie katalog zdarzeń, które mogą wskazywać na wystąpienie incydentu naruszenia tych danych. *Procedura postępowania w sytuacji naruszenia ochrony bezpieczeństwa informacji* (element *Polityki bezpieczeństwa informacji),* porusza kwestie naruszeń danych osobowych, wskazując na podstawie jakich przesłanek można stwierdzić *naruszenie systemu danych osobowych* i jakie czynności należy podjąć w wypadku stwierdzenia *naruszenia ochrony danych osobowych.* Ponadto przedstawia zadania przypisane IOD[7] oraz przełożonemu pracownika w przypadku powzięcia informacji o *naruszeniu bezpieczeństwa danych osobowych.*

Zgodnie z § 20 ust. 2 pkt 13 rozporządzenia KRI *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: bezzwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji (...),* wobec czego elementy systemu zarządzania bezpieczeństwem informacji powinny obejmować bezpieczeństwo informacji w całej organizacji i nie ograniczać się do ochrony danych osobowych.

Kontrolującym przedstawiono rejestr zdarzeń, w którym odnotowano zdarzenia, które w przypadku niepodjęcia odpowiednich kroków mogłyby doprowadzić do naruszenia ochrony danych osobowych lub też zagrozić bezpieczeństwu systemu informatycznego Urzędu. Z informacji uzyskanych od Informatyka w dniu 3 lutego 2023 r. oraz analizy wpisów w przedstawionym rejestrze wynika, że w kontrolowanym okresie, w Jednostce nie stwierdzono przypadków naruszenia ochrony danych osobowych, skutkujących naruszeniem praw lub wolności osób fizycznych; wobec czego nie wystąpiła konieczność zgłoszenia tego faktu organowi nadzorczemu.

(dowód: akta kontroli str. 126-127, 162-163, 172-173)

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.

[7] Inspektor Ochrony Danych

Kontrolującym przedstawiono następujące dokumenty dotyczące okresu objętego weryfikacją:

- Audyt wewnętrzny 2020,
- Audyt wewnętrzny 2021,
- Audyt z zakresu Krajowych Ram Interoperacyjności oraz Krajowego Systemu Cyberbezpieczeństwa w jednostce o nazwie Urząd Miejski w Cedyni, 2022 r.,
- Protokół poaudytowy wraz z zaleceniami z zakresu stosowania polityk ochrony danych osobowych, 2022 r.

Audyty wewnętrzne zrealizowane w Urzędzie obejmowały swym zakresem zagadnienia związane z bezpieczeństwem informacji, wobec czego w okresie objętym kontrolą spełniono wymogi określone w § 20 ust. 2 pkt 14 rozporządzenia KRI.

(dowód: akta kontroli str. 202-320)

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 procedurze *Postępowanie w zakresie wykonywania i obsługi kopii zapasowych oraz okresowego badania nośników służących do przechowywania informacji* oraz *Polityce Bezpieczeństwa Informacji* (w rozdziałach: *Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania*; *Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz wydruków).* 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.

Kopie zapasowe systemów XXX, zgodnie z wyjaśnieniami Burmistrza Cedyni z dnia 24 lutego 2023 r. wykonywane są codziennie i zapisywane na zaszyfrowany pendrive. Raz w tygodniu kopie zgrywane są na dysk zewnętrzny, który przechowywany jest w serwerowni. Kopie zapasowe systemów działających w sieci Urzędu wykonywane są codziennie, a raz w tygodniu podobnie jak kopie programu XXX zgrywane są na dysk zewnętrzny i gromadzone w serwerowni. Ponadto tygodniowa kopia zapasowa *newralgicznych systemów informatycznych przechowywana jest w biurze informatyka (…).*

Nośniki kopii zapasowych winny być przechowywane w innej lokalizacji niż miejsce ich wytworzenia, z uwagi na ryzyko utraty informacji w przypadku zaistnienia sytuacji nadzwyczajnych (w wyniku których zniszczeniu mogą ulec urządzenia i dane na nich przechowywane), co bezpośrednio może przyczynić się do braku zapewnienia ciągłości działania Jednostki i zaistnienia zakłóceń w jej funkcjonowaniu.

Z wyjaśnień Burmistrza Cedyni wynika również, że realizowane jest próbne testowane w celu sprawdzenia poprawności wykonania kopii bezpieczeństwa, przy czym nie sporządza się dokumentacji potwierdzającej przeprowadzenie testów. Zgodnie z zapewnieniem Burmistrza *raport o testowaniu odtwarzanej kopii od następnej aktualizacji SZBI wejdzie do szablonów*

dokumentów. (dowód: akta kontroli str. 77-79, 169-171, 364-381)	
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 firmą XXX zawarto umowę 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. 346-354)	
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 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 wykorzystywanych do realizacji zadań zleconych z zakresu administracji rządowej (podlegających kontroli) uniemożliwia odczyt wyświetlanych danych przez osoby postronne,
- pomieszczenie serwerowni wyposażono w klimatyzację, wzmocnione drzwi wejściowe oraz czujki przeciwwłamaniowe. W pomieszczeniu brak czujnika dymu.

W związku ze stwierdzeniem w trakcie kontroli, że pracownicy realizujący zadania zlecone z zakresu administracji rządowej posiadają uprawnienia administratora w zakresie obsługi systemu operacyjnego, przyjęto w dniu 27 lutego 2023 r. oświadczenie Informatyka o odebraniu uprawnień, co skutkuje tym, że pracownicy działają w systemie operacyjnym na prawach użytkownika.

W wewnętrznych procedurach uregulowano zasady przebywania osób w serwerowni. Wskazano enumeratywnie osoby uprawnione do przebywania w tym pomieszczeniu oraz uregulowano zasady przebywania tam innych osób.

(dowód: akta kontroli str. 81-82,134-135, 382-388)

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

Urządzenia informatyczne Jednostki podłączono do odrębnego obwodu elektrycznego, zabezpieczonego na wypadek zaniku napięcia lub awarii w sieci zasilającej centralnym UPS-em. Sieci i systemy zabezpieczono XXX. Na komputerach podlegających badaniu zainstalowano oprogramowanie antywirusowe. XXX. W Urzędzie funkcjonuje system monitorowania sieci oraz działań użytkowników.

W procedurach wewnętrznych Jednostki określono zasady naprawy oraz wycofywania elektronicznych nośników informacji zawierających dane osobowe.

(dowód: akta kontroli str. 135,170-171)

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 Informatyka logi systemu XXX gromadzone są w bazie danych XXX. 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(...).*

Zgromadzone logi przechowywane są przez okres ponad 2 lat, co jest zgodne z § 21 ust. 4 rozporządzenia KRI. Ponadto Informatyk dokonuje *na bieżąco* analizę logów, w celu identyfikacji działań niepożądanych.

(dowód: akta kontroli str. 79-80)

<table>
<tr><td colspan="2">Stwierdzone nieprawidłowości w obszarze nr 2:
1. Zawężenie incydentów naruszenia bezpieczeństwa informacji do naruszeń danych osobowych, co nie jest zgodne z dyspozycją § 20 ust. 2 pkt 13 rozporządzenia KRI.
2. Nieodnotowywanie w dziennikach systemów działań użytkowników z uprawnieniami administracyjnymi, co nie wypełnia dyspozycji § 21 ust. 2 rozporządzenia KRI.
3. Niesporządzanie dokumentacji dotyczącej testowania kopii zapasowych danych i systemów na potrzeby weryfikacji poprawności i stanu ich wykonywania oraz przechowywanie kopii zapasowych w miejscu wytwarzania danych, co jest niezgodne z § 20 ust. 2 pkt 12 lit. b i e rozporządzenia KRI.
4. Posiadanie przez pracowników realizujących zadania zlecone z zakresu administracji rządowej uprawnień administratora w zakresie obsługi systemu operacyjnego, co jest sprzeczne z dyspozycją § 20 ust. 2 pkt 9 i 4 rozporządzenia KRI. Powyższa nieprawidłowość została usunięta w trakcie kontroli.
5. W pomieszczeniu serwerowni zidentyfikowano czynnik zwiększający ryzyko związane z potencjalnymi zagrożeniami fizycznymi i środowiskowymi, co nie jest zgodne z wymogami § 20 ust. 2 pkt 12 oraz ust. 4 rozporządzenia KRI.</td></tr>
<tr><td>Ocena obszaru kontroli</td><td>Pozytywna z nieprawidłowościami</td></tr>
<tr><td>Wpis do książki kontroli</td><td>Nr 1/2023</td></tr>
<tr><td>Wnioski dotyczące uzyskanych efektów zrealizowanego zadania</td><td>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).
Działania zmierzające do zapewnienia środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych i aplikacji oraz działania związane z zapewnieniem ochrony fizycznej informacji, minimalizujące wystąpienie ryzyka ich utraty znacząco wpływają na podniesienie poziomu bezpieczeństwa teleinformatycznego Jednostki.</td></tr>
<tr><td>Zalecenia</td><td>• Uzupełnić procedury postępowania z incydentami o pozostałe obszary, w których mogą wystąpić przypadki naruszenia bezpieczeństwa przetwarzanych w Jednostce informacji, stosownie do zapisów § 20 ust. 2 pkt 13 rozporządzenia KRI,
• W dziennikach systemów odnotowywać obligatoryjnie działania użytkowników z uprawnieniami administracyjnymi, zgodnie z dyspozycją § 21 ust. 2 rozporządzenia KRI.
• Sporządzać dokumentację dotyczącą testowania kopii zapasowych danych i systemów na potrzeby weryfikacji poprawności i stanu ich wykonywania oraz przechowywać kopie zapasowe wszystkich systemów i programów poza miejscem wytwarzania danych, zgodne z § 20 ust. 2 pkt 7 i 12 lit. b i e rozporządzenia KRI.
• W pomieszczeniu serwerowni zapewnić warunki gwarantujące utrzymanie odpowiedniego poziomu bezpieczeństwa informacji.</td></tr>
</table>

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