Wojewoda
Zachodniopomorski

Znak: K-2.431.1.31.2024.7.IO

Szczecin, dnia 12 listopada 2024 r.

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 Chociwla, ul. Armii Krajowej 52, 73-120 Chociwel.
Osoba pełniąca funkcję Burmistrza Chociwla w okresie objętym kontrolą	Pan Stanisław Szymczak
Okres objęty kontrolą	od dnia 1 stycznia 2021 r. do dnia 26 lipca 2024 r.
Kontrolerzy	Pracownicy Wydziału Kontroli Zachodniopomorskiego Urzędu Wojewódzkiego w Szczecinie: Pani Anna Dąbska – kierownik oddziału, kierownik zespołu kontrolnego, Pani Iwona Olesińska – główny specjalista.
Nr upoważnienia	Nr 48/24 z dnia 14 czerwca 2024 r.
Podstawy prawne do przeprowadzenia kontroli	– art. 6 ust. 4 pkt 3 w związku z art. 2 ust. 1 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej[1]; – art. 25 ust. 1 pkt 3 lit. a, w związku z ust. 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[2].
Kryteria prowadzenia kontroli	legalność, rzetelność
Rodzaj kontroli i tryb kontroli	kontrola planowa, tryb zwykły
Termin kontroli	18-24 czerwca 2024 r.

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

Osoba udzielająca wyjaśnień w trakcie kontroli	xxxxxxxxxxxx – stanowisko ds. obronnych, obrony cywilnej, zarządzania kryzysowego, informatyzacji i pozyskiwania środków unijnych[3].

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[4]: *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 Chociwlu wykorzystywano system centralny (aplikacja Źródło) oraz systemy informatyczne wspomagające obsługę spraw obywatelskich w zakresie ewidencji mieszkańców oraz rejestru zamieszkania cudzoziemców XXX.
System informatyczny wspomagający realizację zadań zleconych z zakresu administracji rządowej, spełniał minimalne wymogi interoperacyjności w zakresie współpracy z innymi aplikacjami Urzędu, jak i innych jednostek administracji publicznej, określone w § 5 ust. 3 pkt 3 rozporządzenia KRI.
System centralny podlegał kontroli jedynie w zakresie formalnego posiadania uprawnień przez pracowników Urzędu oraz zabezpieczeń związanych z dostępem do systemu.
(dowód: akta kontroli str. 34, 177-183)

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*

[3] W zakresie dotyczącym obsługi informatycznej zwany dalej Informatykiem.
[4] Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2024 poz. 773), zwane dalej „rozporządzeniem KRI".

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 Chociwlu 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.

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: § 19 ust. 1 rozporządzenia KRI: *Podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność*
i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność; **§ 19 ust. 2 pkt 1 rozporządzenia KRI:** *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie (...) aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;* **§ 19 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 § 19 ust. 1 rozporządzenia KRI. Zgodnie z tym przepisem, podmiot realizujący zadania publiczne ma obowiązek opracowania i ustanowienia, wdrożenia i eksploatowania, monitorowania i przeglądania oraz utrzymania i doskonalenia systemu bezpieczeństwa informacji zapewniającego poufność, dostępność, integralność informacji.
W Urzędzie Miejskim w Chociwlu, w okresie objętym kontrolą obowiązywały następujące dokumenty z zakresu bezpieczeństwa informacji:

- *Zarządzenie nr 15/2021 Burmistrza Chociwla z dnia 25 stycznia 2021 r. w sprawie wprowadzenia Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miejskim w Chociwlu*;
- *Regulamin pracy zdalnej,* wprowadzony *Zarządzeniem nr 85/2020 Burmistrza Chociwla z dnia 5 listopada 2020 r.*

- *Zarządzenie nr 112/2019 Burmistrza Chociwla z dnia 29 października 2019 r. w sprawie wdrożenia Polityki Bezpieczeństwa Informacji i Instrukcji Zarządzania Systemem Informatycznym w Urzędzie Miejskim w Chociwlu*.

W 2021 r. Zarządzeniem nr 15/2021 Burmistrza Chociwla wprowadzono w Urzędzie System Zarządzania Bezpieczeństwem Informacji (SZBI) wymieniając e-numeratywnie dokumenty, które składają się na SZBI. Wśród tych dokumentów nie znalazły się obowiązujące od 2019 r. zarówno Polityka Bezpieczeństwa Informacji, jak i Instrukcja Zarządzania Systemem Informatycznym. Kontrolujący wnoszą by oba dokumenty wskazać, jako dokumenty współtworzące SZBI.
Dyrektywa § 19 ust. 2 pkt 1 rozporządzenia KRI wskazuje na konieczność zapewnienia *aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia.*
Wobec nieprzedstawienia dokumentów poświadczających dokonywanie analiz i przeglądów dokumentacji z zakresu bezpieczeństwa informacji, powyższy wymóg uznaje się za niespełniony.
W wyniku analizy aktualnie obowiązującej dokumentacji stwierdzono, że w procedurach wewnętrznych nie uregulowano kwestii związanych z testowaniem kopii zapasowych danych i systemów oraz dokumentacji tych procesów; działań związanych z regularnym przeglądaniem logów i ich analizą w celu identyfikacji działań niepożądanych; działań związanych z monitorowaniem systemów teleinformatycznych i środowiska ich pracy pod kątem wydajności i pojemności; dokonywania przeglądów obowiązujących w Jednostce procedur dotyczących bezpieczeństwa informacji. Ponadto wdrożone w Jednostce regulacje dotyczące zgłaszania incydentów bezpieczeństwa informacji odnoszą się do naruszeń danych osobowych.
(dowód: akta kontroli str. 90-120)

2.2 Analiza zagrożeń związanych z przetwarzaniem informacji.

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

Ustalenia kontroli

Analiza ryzyka, obejmująca wszystkie aktywa Jednostki oraz odpowiednie i pogłębione szacowanie zidentyfikowanych ryzyk jest jednym z najistotniejszych elementów 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.
Kontrolującym przedstawiono dokument *Analiza ryzyka*, który zgodnie z wyjaśnieniami Burmistrza Chociwla z dnia 24 czerwca 2024 r. został sporządzony w 2019 r. Z treści złożonych wyjaśnień wynika również, że *analiza (...) podlegała corocznym przeglądom i aktualizacjom (ostatnia aktualizacja grudzień 2023 r.).* Do przedłożonej informacji nie dołączono stosownych dokumentów potwierdzających podejmowanie czynności, mających na celu weryfikację aktualności zapisów. O potwierdzenie takie kontrolujący zwrócili się w piśmie znak: K-2.431.1.31.2024.3.IO, z dnia 20 czerwca 2024 r.

W zaprezentowanej analizie ryzyka, sporządzonej w 2019 r. określono zagrożenia dla wskazanych zasobów, źródła tych zagrożeń oraz prawdopodobieństwo i skutki wpływu zdarzeń na czynniki decydujące o bezpieczeństwie danych.
Stwierdzono, że wyżej przywołana analiza ryzyka obejmująca zidentyfikowane aktywa Jednostki, wypełnia w części dyspozycję, o której mowa w § 19 ust. 2 pkt 3 rozporządzenia KRI, natomiast na skutek nieprzedłożenia przez Jednostkę stosownych dokumentów, o których mowa powyżej nie można potwierdzić spełnienia wymogu okresowego przeprowadzania analiz ryzyka.
(dowód: akta kontroli str. 162-176, 208)

2.3 Inwentaryzacja sprzętu i oprogramowania informatycznego.
Podstawa prawna: § 19 ust. 2 pkt 2 rozporządzenia KRI: *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: utrzymanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.*
Ustalenia kontroli
Zgodne z § 19 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 XXX. System umożliwia prowadzenie inwentaryzacji, generując raporty zawierające informacje dotyczące m. in. sprzętu i oprogramowania oraz rodzaju systemu operacyjnego. W związku z tym, że sieć komputerowa z jednostką wykorzystywaną do realizacji zadań z zakresu administracji rządowej jest odłączona od sieci komputerowej Urzędu inwentaryzacja dla tej jednostki operacyjnej realizowana jest w postaci zapisów w pliku, przy wykorzystaniu arkusza kalkulacyjnego Microsoft Excel.
W trakcie kontroli okazano stosowną dokumentację, potwierdzającą prowadzenie inwentaryzacji sprzętu i oprogramowania, zgodnie z wymogami rozporządzenia KRI.
(dowód: akta kontroli str. 64, 74-82)

2.4 Zarządzanie uprawnieniami do pracy w systemach informatycznych.
Podstawa prawna: § 19 ust. 2 pkt 4 rozporządzenia KRI: *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji;* **§ 19 ust. 2 pkt 5 rozporządzenia KRI:** *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4.*
Ustalenia kontroli

Przepisy § 19 ust. 2 pkt 4 i pkt 5 rozporządzenia KRI stanowią m.in, że kierownictwo podmiotu publicznego w celu zapewnienia bezpieczeństwa informacji powinno podjąć działania zapewniające, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia, adekwatne do realizowanych zadań, a także podjąć bezzwłoczne działania w przypadku zmiany zadań tych osób. Przetwarzanie informacji w systemach teleinformatycznych wymaga dostępu do danych przez uprawnione osoby, w ustalonym zakresie.
Kwestie nadawania i odbierania upoważnień do przetwarzania danych osobowych uregulowano:
- w rozdziale III *Polityki Bezpieczeństwa Informacji* (*Upoważnienia*) – wskazując administratora danych osobowych, jako osobę odpowiedzialną za nadawanie i odbieranie upoważnień;
- w rozdziale III *Instrukcji Zarządzania Systemem Informatycznym* (*Nadawanie uprawnień do przetwarzania danych osobowych*), wprowadzając wymóg zachowania formy pisemnej przy nadawaniu upoważnień.
W wewnętrznych procedurach uregulowano również kwestie nadawania uprawnień do pracy w systemie informatycznym w ten sposób, że *polecenie do utworzenia konta wraz z uprawnieniami wydaje przełożony* a za *nadanie indywidualnego identyfikatora (loginu) i hasła odpowiada (...) administrator systemu informatycznego.* Zgodnie z wyjaśnieniami Informatyka uprawnienia do pracy w systemie informatycznym nadawane są na ustne polecenie kierownictwa Urzędu. Kontrolujący wskazują by wewnętrzne procedury uzupełnić o pisemny wniosek, który poświadczać będzie realizowanie wymogu dokumentowania czynności nadawania i odbierania uprawnień do pracy w systemach informatycznych. Dokument podpisany przez upoważnione osoby sprawi, że proces nadawania i odbierania uprawnień będzie w pełni potwierdzony.
Kontrolującym przedstawiono:

- *upoważnienie 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;
- dokument zawierający między innymi oświadczenie zobowiązujące pracownika do *nie ujawniania wiadomości, z którymi zapoznał się w trakcie wykonywania czynności służbowych*. Kontrolujący wskazują, by w tym zakresie zaktualizować dokumenty, stosując przyjęte w Urzędzie wzory druków – załącznik numer 3 oraz załącznik numer 3a do *Zarządzenia nr 112/2019 Burmistrza Chociwla z dnia 29 października 2019 r. w sprawie wdrożenia Polityki Bezpieczeństwa Informacji i Instrukcji Zarządzania Systemem Informatycznym w Urzędzie Miejskim w Chociwlu*.

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. 63-64, 183-198)

2.5 Szkolenia pracowników zaangażowanych w proces przetwarzania informacji.
Podstawa prawna: § 19 ust. 2 pkt 6 rozporządzenia KRI: *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie szkolenia osób zaangażowanych*
w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:

a) zagrożenia bezpieczeństwa informacji, b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna, c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich.

Ustalenia kontroli

W okresie objętym kontrolą w Urzędzie Miejskim w Chociwlu przeprowadzono następujące szkolenia pracowników z zakresu bezpieczeństwa informacji i ochrony danych osobowych:

- Szkolenie, w trakcie którego przedstawiono Regulamin ochrony danych osobowych oraz Politykę bezpieczeństwa danych osobowych w Urzędu Miejskim w Chociwlu, które odbyło się w dniu 2 lutego 2022 r.;
- Szkolenie z zakresu RODO przeprowadzone w dniu 7 grudnia 2022 r.

Udział w szkoleniach dokumentowała lista obecności zawierająca imię i nazwisko uczestnika oraz własnoręczny podpis. Stwierdzono, że w przeprowadzonych szkoleniach wzięli udział pracownicy wskazani jako osoby realizujące zadania zlecone z zakresu administracji rządowej.

Z przedstawionej dokumentacji wynika, że zakres tematyczny szkoleń przeprowadzonych w Urzędzie nie obejmował wszystkich zagadnień wskazanych w § 19 ust. 2 pkt 6 rozporządzenia KRI, uwzględniając głównie kwestie związane z ochroną danych osobowych. Kontrolujący sugerują, aby szkolenia, których celem jest zagwarantowanie bezpieczeństwa w zakresie przetwarzania informacji miały charakter cykliczny. Ze względu na zmieniające się zagrożenia związane z dynamicznym rozwojem technologii informatycznych winny one obejmować zagadnienia wskazane w § 19 ust. 2 pkt 6 rozporządzenia KRI.

(dowód: akta kontroli str. 199-207)

2.6 Praca na odległość i mobilne przetwarzanie danych.

Podstawa prawna: § 19 ust. 2 pkt 8 rozporządzenia KRI: *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: ustanowienie podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość.*

Ustalenia kontroli

Kwestie trybu pracy przy przetwarzaniu mobilnym i pracy na odległość zostały unormowane w następujących dokumentach:

- *Polityce bezpieczeństwa informacji*, w rozdziale V pkt 5 (*Regulamin ochrony danych osobowych - Wynoszenie nośników danych poza obszar przetwarzania);*
- *Instrukcji zarządzania systemem informatycznym,* w rozdziale VII (*Regulamin używania sprzętu mobilnego poza jednostką);*
- *Regulaminie pracy zdalnej,* wprowadzonym *Zarządzeniem nr 85/2020 Burmistrza Chociwla z dnia 5 listopada 2020 r.*

W wyżej wymienionych dokumentach uregulowano między innymi kwestie wynoszenia poza obszar organizacji nośników z danymi osobowymi (w tym dokumentów wytworzonych w formie papierowej), wprowadzając wymóg uzyskania zgody przełożonego. Wdrożono obowiązek szyfrowania danych zapisanych na komputerach przenośnych oraz innych urządzeniach mobilnych.

Zgodnie z wyjaśnieniami Burmistrza z 19 czerwca 2024 r. do realizacji zadań zleconych z zakresu administracji rządowej w Urzędzie nie wykorzystywano urządzeń mobilnych.

(dowód: akta kontroli str. 63, 100, 109)

2.7 Serwis sprzętu informatycznego i oprogramowania.

Podstawa prawna: § 19 ust. 2 pkt 10 rozporządzenia KRI: *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zawieranie w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.*

Ustalenia kontroli

Obsługa informatyczna realizowana jest przez pracownika zatrudnionego w Urzędzie Miejskim w Chociwlu na stanowisku ds. obronnych, obrony cywilnej, zarządzania kryzysowego, informatyzacji i pozyskiwania środków unijnych. Wśród obowiązków pracownika z zakresu informatyki znajduje się m.in.: administrowanie lokalną siecią komputerową; wdrażanie programów i nadzorowanie eksploatacji oprogramowania użytkowanego w Urzędzie; podstawowa konserwacja sprzętu komputerowego; nadzór nad mechanizmami uwierzytelniania użytkowników systemu informatycznego; inwentaryzacja sprzętu i oprogramowania.

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. 151-161)

2.8 Procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji.

Podstawa prawna: § 19 ust. 2 pkt 13 rozporządzenia KRI: *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: bezzwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.*

Ustalenia kontroli

W *Polityce bezpieczeństwa informacji*, w rozdziale IV (*Incydenty)* oraz w rozdziale V, pkt 8 (*Regulamin ochrony danych osobowych, Incydenty związane z ochroną danych osobowych*) określono zasady i sposób postępowania w przypadku wystąpienia incydentów związanych z naruszeniem ochrony danych osobowych.

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

Kontrolujący wskazują by procedura zgłaszania naruszeń nie ograniczała się jedynie do naruszeń ochrony danych osobowych a obejmowała mogące potencjalnie wystąpić naruszenia bezpieczeństwa wszystkich przetwarzanych informacji.

[5] Umowa nr EA-035-2024 z dnia 12 stycznia 2024 r.

[6] Umowa nr EP-035-2024 z dnia 12 stycznia 2024 r.

Kontrolującym przedstawiono *Rejestr naruszeń ochrony danych osobowych oraz incydentów naruszeń bezpieczeństwa informacji*, w którym odnotowano dwa zdarzenia. Kontrolujący przyjęli wyjaśnienia, że we wskazanych przypadkach nie nastąpiła konieczność zgłoszenia tego faktu organowi nadzorczemu.
(dowód: akta kontroli str. 63, 97, 101-102)

2.9 Audyt wewnętrzny z zakresu bezpieczeństwa informacji.

Podstawa prawna: § 19 ust. 2 pkt 14 rozporządzenia KRI: *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.*

Ustalenia kontroli

W myśl § 19 ust. 2 pkt 14 rozporządzenia KRI, zarządzanie bezpieczeństwem informacji realizowane jest m.in. poprzez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie działania polegającego na okresowym audycie wewnętrznym w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.
Kontrolującym przedstawiono następujące dokumenty dotyczące okresu objętego weryfikacją:

- *Sprawozdanie roczne 2023. Audyt w zakresie znajomości i przestrzegania regulaminu ochrony danych osobowych przyjętego w jednostce.*
- *Sprawozdanie roczne 2022. Audyt w zakresie ochrony danych osobowych, prowadzenie strony www oraz BIP.*
- *Sprawozdanie z wykonanego audytu w zakresie ochrony danych osobowych w procesie rekrutacji oraz w okresie zatrudnienia pracowników.* Chociwel 30.11.2021 r*.*

Zagadnienia poddane ocenie w przedstawionych kontrolującym dokumentach, potwierdzających wykonanie w Jednostce audytów wewnętrznych dotyczyły głównie kwestii ochrony danych osobowych.
(dowód: akta kontroli str.121-150)

2.10 Kopie zapasowe.

Podstawa prawna: § 19 ust. 2 pkt 12 lit. b, e rozporządzenia KRI: *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: minimalizowanie ryzyka utraty informacji w wyniku awarii, zapewnieniu bezpieczeństwa plików systemowych.*

Ustalenia kontroli

Zgodnie z wymogami określonymi w § 19 ust. 2 pkt 12 lit. b) i e) rozporządzenia KRI, zarządzanie bezpieczeństwem informacji realizowane jest w szczególności poprzez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie m.in. odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na minimalizowaniu ryzyka utraty informacji w wyniku awarii i zapewnieniu bezpieczeństwa plików systemowych.
Zasady wykonywania kopii bezpieczeństwa uregulowano w *Instrukcji Zarządzania Systemem Informatycznym*, w rozdziale IV (*Tworzenie kopii zapasowych).* W procedurze wskazano, że *kopie zapasowe sporządza się cyklicznie (…)*. Pojęcie cyklicznie nie określa ściśle interwału czasowego, w którym należy wykonać kopie zapasowe danych i systemów, co uniemożliwia weryfikację terminowości realizacji tak określonej czynności. W regulacjach wewnętrznych nie określono zasad testowania kopii zapasowych danych i systemów na

potrzeby weryfikacji poprawności i stanu ich wykonywania. Istnieje jedynie zapis, że *tworzone kopie zapasowe należy regularnie testować*. Nie wskazano również sposobu dokumentacji tych działań.
Kopie zapasowe baz danych, zgodnie z oświadczeniem Informatyka z dnia 19 czerwca 2024r. wykonywane są raz w tygodniu i przechowuje się je na zewnętrznym nośniku poza miejscem wytworzenia. W Urzędzie nie jest realizowane próbne testowanie kopii zapasowych na potrzeby weryfikacji poprawności i stanu ich wykonywania.
(dowód: akta kontroli str. 64, 107-108)

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 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[7].
(dowód: akta kontroli str. 151-158)

2.12 Zabezpieczenia techniczno – organizacyjne dostępu do informacji.
Podstawa prawna: § 19 ust. 2 rozporządzenia KRI: *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez:* **pkt 7:** *zapewnienie ochrony przetwarzania informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:*
a) monitorowanie dostępu do informacji; b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji, c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji; **pkt 9:** *zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie;* **pkt 11:** *ustalenie zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych.*
Ustalenia kontroli
W celu ustanowienia zabezpieczeń uniemożliwiających osobom nieuprawnionym modyfikację, usunięcie lub zniszczenie informacji każdemu pracownikowi nadano identyfikator i hasło wejścia do systemów zainstalowanych na komputerach oraz do programów, z których korzystają.
W przypadku systemu „Źródło" dostęp jest możliwy wyłącznie z użyciem karty, na której zapisany jest certyfikat umożliwiający zalogowanie się do centralnego systemu.
W wyniku oględzin stanowiska komputerowego wykorzystywanego do realizacji zadań zleconych z zakresu administracji rządowej, przeprowadzonych w toku czynności kontrolnych ustalono, że:

[7] Umowa nr EA-035-2024 z dnia 12 stycznia 2024 r.

- dostęp do systemu operacyjnego na urządzeniu możliwy był jedynie po wprowadzeniu nazwy użytkownika i hasła,
- komputer miał zainstalowane oprogramowanie antywirusowe oraz skonfigurowany 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 uniemożliwiało odczyt wyświetlanych danych przez osoby postronne,
- użytkownikom systemów wykorzystywanych do realizacji zadań zleconych z zakresu administracji rządowej nie nadano uprawnień administratora, uniemożliwiając w ten sposób instalowanie oprogramowania niewiadomego pochodzenia lub zmianę ustawień systemu operacyjnego a także ingerencję w rejestry zdarzeń.
(dowód: akta kontroli str. 65-69, 88-89)

2.13 Zabezpieczenia techniczno – organizacyjne systemów informatycznych.

Podstawa prawna: § 19 ust. 2 pkt 12 rozporządzenia KRI: *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie (...) odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na: a) dbałości o aktualizację oprogramowania; b) minimalizowaniu ryzyka utraty informacji w wyniku awarii;*
c) ochronie przed błędami, nieuprawnioną modyfikacją; d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa;
e) zapewnieniu bezpieczeństwa plików systemowych; f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych; g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa; h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa; **§ 19 ust. 4 rozporządzenia KRI:** *Niezależnie od zapewnienia działań, o których mowa w ust. 2,*
w przypadkach uzasadnionych analizą ryzyka w systemach teleinformatycznych podmiotów realizujących zadania publiczne należy ustanowić dodatkowe zabezpieczenia.

Ustalenia kontroli

- Sieć informatyczną Urzędu zabezpieczono przy wykorzystaniu zapory sieciowej firewall.
- Urządzenia informatyczne Jednostki są podłączone do zasilaczy awaryjnych UPS.
- Na komputerze podlegającym badaniu zainstalowano oprogramowanie antywirusowe.
- W procedurach wewnętrznych Jednostki określono zasady:

- wykonywania przeglądów i konserwacji urządzeń komputerowych,
- naprawy sprzętu wykonywanej przez podmioty zewnętrzne,
- niszczenia elektronicznych i papierowych nośników danych,
- pobierania kluczy do pomieszczeń Urzędu.

Pomieszczenie serwerowni niewydzielone (użytkowane przez pracownika wykonującego również inne - poza obsługą informatyczną zadania), sąsiadujące z lokalem, w którym usytułowany jest węzeł sanitarny. Serwerownia zabezpieczona jest drzwiami

antywłamaniowymi i wyposażona w czujkę dymu. W pomieszczeniu brak klimatyzacji i gaśnicy.
(dowód: akta kontroli str. 64, 88-89)

2.14 Rozliczalność działań w systemach teleinformatycznych.
Podstawa prawna: § 20 ust. 2 rozporządzenia KRI: *W dziennikach systemów odnotowuje się obligatoryjnie działania użytkowników lub obiektów systemowych polegające na dostępie do:*
1) systemu z uprawnieniami administracyjnymi; 2) konfiguracji systemu, w tym konfiguracji zabezpieczeń; 3) przetwarzanych w systemach danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa; **§ 20 ust. 3 rozporządzenia KRI:** *Poza informacjami wymienionymi w ust. 2 mogą być odnotowywane działania użytkowników lub obiektów systemowych, a także inne zdarzenia związane z eksploatacją systemu w postaci: 1) działań użytkowników nieposiadających uprawnień administracyjnych, 2) zdarzeń systemowych nieposiadających krytycznego znaczenia dla funkcjonowania systemu, 3) zdarzeń i parametrów środowiska, w którym eksploatowany jest system teleinformatyczny – w zakresie wynikającym*
z analizy ryzyka; **§ 20 ust. 4 rozporządzenia KRI:** *informacje w dziennikach systemów przechowywane są od dnia ich zapisu, przez okres wskazany w przepisach odrębnych, a w przypadku braku przepisów odrębnych przez dwa lata.*
Ustalenia kontroli
Przetwarzanie informacji w systemach teleinformatycznych wymaga dostępu do danych przez uprawnione osoby i obiekty systemowe (procesy) w ustalonym zakresie. Zapewnienie rozliczalności operacji polega na gromadzeniu informacji o tym, kto, kiedy i jakie czynności wykonał w systemie teleinformatycznym. Obligatoryjnie podlegają dokumentowaniu w postaci zapisów w dziennikach systemów (logi) wszelkie działania dostępu do systemu teleinformatycznego z uprawnieniami administracyjnymi, w zakresie konfiguracji systemu i jego zabezpieczeń a także działania, gdy przetwarzanie danych podlega prawnej ochronie (np. zgodnie z ustawą o ochronie danych osobowych).
System objęty kontrolą zawiera logi, w których są odnotowane działania użytkowników, zgodnie z zapisami § 20 ust. 2 i 3 rozporządzenia KRI. Logi systemu są przechowywane przez okres ponad 2 lat, wobec czego wypełniono dyspozycję § 21 ust. 4 wyżej opisanego rozporządzenia.
Zgodnie z wyjaśnieniami Informatyka w Jednostce nie są prowadzone działania związane z przeglądaniem logów systemu informatycznego wykorzystywanego do realizacji zadań zleconych z zakresu administracji rządowej, w celu stwierdzenia i ewentualnej identyfikacji działań niepożądanych.
(dowód: akta kontroli str. 70-73)

Stwierdzone nieprawidłowości w obszarze Nr 2	• Dokumentacja regulująca kwestie bezpieczeństwa informacji, obowiązująca w Urzędzie nie zawiera wszystkich elementów wymaganych przepisami rozporządzenia KRI. • Niedokonywanie analiz i przeglądów dokumentacji z zakresu bezpieczeństwa informacji, na co wskazuje dyrektywa § 19 ust. 2 pkt 1 rozporządzenia KRI.

	• Zakres tematyczny szkoleń przeprowadzonych w Urzędzie nie obejmował wszystkich zagadnień wskazanych w § 19 ust. 2 pkt 6 rozporządzenia KRI. • Zawężenie incydentów naruszenia bezpieczeństwa informacji do naruszeń danych osobowych, co nie jest zgodne z dyspozycją § 19 ust. 2 pkt 13 rozporządzenia KRI. • Nieprowadzenie działań związanych z przeglądaniem logów systemu informatycznego wykorzystywanego do realizacji zadań zleconych z zakresu administracji rządowej, w celu stwierdzenia i ewentualnej identyfikacji działań niepożądanych, zgodnie z dyspozycją § 19 ust. 2 pkt 7 rozporządzenia KRI. • Niewykonywanie próbnego testowania kopii zapasowych danych i systemów na potrzeby weryfikacji poprawności i stanu ich wykonywania, co jest niezgodne z § 19 ust. 2 pkt 12 lit. b i e rozporządzenia KRI. • Pomieszczenie serwerowni nie dysponuje należytymi zabezpieczeniami, zgodnie z wymogami § 19 ust. 2 pkt 12 oraz ust. 4 rozporządzenia KRI.
Ocena obszaru kontroli	**Pozytywna z nieprawidłowościami**
Wpis do książki kontroli	Nr 5/2024
Zalecenia	• Uzupełnić dokumentację regulującą kwestie bezpieczeństwa informacji, zgodnie z wymogami rozporządzenia KRI. • Wykonywać analizy i przeglądy dokumentacji z zakresu bezpieczeństwa informacji, zgodnie z dyrektywą § 19 ust. 2 pkt 1 rozporządzenia KRI. • Przeprowadzać szkolenia z zakresu bezpieczeństwa informacji obejmujące wszystkie zagadnienia wskazane w § 19 ust. 2 pkt 6 rozporządzenia KRI. • Uzupełnić procedurę zgłaszania incydentów naruszenia bezpieczeństwa informacji, zgodnie z dyspozycją § 19 ust. 2 pkt 13 rozporządzenia KRI. • Prowadzić działania związane z przeglądaniem logów systemu informatycznego wykorzystywanego do realizacji zadań zleconych z zakresu administracji rządowej, w celu stwierdzenia i ewentualnej identyfikacji działań niepożądanych, zgodnie z dyspozycją § 19 ust. 2 pkt 7 rozporządzenia KRI. • Wykonywać próbne testowanie kopii zapasowych danych i systemów na potrzeby weryfikacji poprawności i stanu ich wykonywania, na co wskazują zapisy § 19 ust. 2 pkt 12 lit. b i e rozporządzenia KRI. • W pomieszczeniu serwerowni zapewnić warunki gwarantujące utrzymanie odpowiedniego poziomu

	bezpieczeństwa informacji, zgodnie z dyspozycją § 19 ust. 2 pkt 12 lit. b i e oraz ust. 4 rozporządzenia KRI.
Pouczenia	– zgodnie z art. 48 ustawy z dnia 15 lipca 2011 roku o kontroli w administracji rządowej (Dz.U. z 2020 r. poz. 224) od wystąpienia pokontrolnego nie przysługują środki odwoławcze, – o podjętych działaniach, mających na celu realizację zaleceń pokontrolnych, proszę poinformować mnie za pośrednictwem Wydziału Kontroli Zachodniopomorskiego Urzędu Wojewódzkiego w Szczecinie w terminie 14 dni od daty otrzymania niniejszego wystąpienia.
Podpis kierownika jednostki kontrolującej	Z upoważnienia Wojewody Zachodniopomorskiego Bartosz Brożyński I Wicewojewoda Zachodniopomorski