Wojewoda
Zachodniopomorski

Znak: K-2.431.1.45.2025.8.IO

Szczecin, 18 grudnia 2025 r.

WYSTĄPIENIE POKONTROLNE

Przedmiot kontroli	Działanie systemów teleinformatycznych 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	Burmistrza Dębna, ul. Marszałka Józefa Piłsudskiego 5, 74 - 400 Dębno.
Osoba pełniąca funkcję Burmistrza Dębna w okresie objętym kontrolą	Pan Wojciech Czepułkowski
Okres objęty kontrolą	od dnia 1 stycznia 2022 r. do dnia 13 sierpnia 2025 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 74/25 z dnia 7 sierpnia 2025 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	7 – 13 sierpnia 2025 r.

[1] Dz. U. z 2020r., poz. 224.
[2] Dz. U. z 2025r., poz. 1703.

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 Dębnie wykorzystywano system centralny (aplikacja Źródło) oraz system informatyczny wspomagający obsługę spraw obywatelskich w zakresie ewidencji ludności 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. 44-45, 257-266)

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 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 Dębnie wymieniał dane w formatach

[3] 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".

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**

<u>Obszar kontroli Nr 2:</u> 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.*

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 Dębnie, w okresie objętym kontrolą obowiązywały następujące dokumenty z zakresu bezpieczeństwa informacji:

- *Zarządzenie nr 87/30/2025 Burmistrza Dębna z dnia 22 lipca 2025 r. zmieniające zarządzenie nr 100/27/2021 Burmistrza Dębna z dnia 14 lipca 2021 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji w Urzędzie Miejskim w Dębnie.*
- *Zarządzenie wewnętrzne nr 18/2025 Burmistrza Dębna z dnia 06 czerwca 2025 r. w sprawie wprowadzenia Procedury ochrony danych osobowych podczas wykonywania pracy zdalnej oraz pracy zdalnej wykonywanej okazjonalnie.*
- *Zarządzenie nr 76/31/2024 Burmistrza Dębna z dnia 26 listopada 2024 r. w sprawie zasad postępowania z pamięciami zewnętrznymi w Urzędzie Miejskim w Dębnie.*
- *Zarządzenie nr 56/22/2024 Burmistrza Dębna z dnia 24 września 2024 r. zmieniające zarządzenie nr 100/27/2021 Burmistrza Dębna z dnia 14 lipca 2021 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji w Urzędzie Miejskim w Dębnie.*

- *Zarządzenie nr 100/27021 Burmistrza Dębna z dnia 14 lipca 2021 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji w Urzędzie Miejskim w Dębnie*[4]*.*
- *Zarządzenia nr 105/49/2012 Burmistrza Dębna z dnia 14 grudnia 2012 r. w sprawie procedur zarządzania ryzykiem w Urzędzie Miejskim w Dębnie.*

Dyspozycja § 19 ust. 2 pkt 1 rozporządzenia KRI wskazuje na obowiązek zapewnienia *aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia,* co przekłada się na konieczność monitorowania i przeglądu systemu zarządzania bezpieczeństwem informacji. Kontrolującym przedstawiono *Notatki z przeglądu polityki bezpieczeństwa informacji* z okresu objętego sprawdzeniem (2022-2025 r.), które poświadczają przeprowadzenie weryfikacji dokumentacji dotyczącej bezpieczeństwa informacji pod kątem ważności regulacji.
W wyniku analizy obowiązującej w Jednostce dokumentacji związanej z bezpieczeństwem informacji stwierdzono, że funkcjonujące w Jednostce procedury wymagają uzupełnienia o kwestie przywołane w dalszej treści powyższego dokumentu kontrolnego. Należy zauważyć, że w przyjętych procedurach pojawia się pojęcie inspektora ochrony danych osobowych (IODO), podczas gdy obowiązujące regulacje prawne mówią o Inspektorze Ochrony Danych[5]. Powyższe wymaga wprowadzenia stosownej korekty do obowiązującej dokumentacji.

(dowód: akta kontroli str. 104-112, 164-241)

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 zarządzania bezpieczeństwem informacji, pozwalającym na zastosowanie odpowiednich mechanizmów przeciwdziałania w sytuacji materializacji ryzyk.
Kontrolującym przedstawiono dokument *Zbiorczy rejestr ryzyk i metod przeciwdziałania ryzyku w Urzędzie Miejskim w Dębnie,* sporządzony 14 lutego 2025 r. W zaprezentowanej analizie wskazano zidentyfikowane ryzyka oraz określone w skali punktowej: wpływ na Jednostkę, prawdopodobieństwo materializacji ryzyka oraz istotność ryzyka. W treści dokumentu nie zawarto przyjętej metodologii, zastosowanej do interpretacji wdrożonej skali punktowej. W celu dokonania oceny skali zagrożeń, a w ślad za tym podjęcia adekwatnych do tej oceny odpowiednich działań należy odwołać się do *Zarządzenia nr 105/49/2012 Burmistrza Dębna z dnia 14 grudnia 2012 r. w sprawie procedur zarządzania ryzykiem w Urzędzie Miejskim w Dębnie.*
Kontrolujący sugerują by metodykę sporządzania analiz ryzyka ująć w *Polityce Bezpieczeństwa Informacji*, uzupełniając np. § 16 (*Prowadzenie okresowych analiz ryzyka w zakresie bezpieczeństwa informacji),* co umożliwi interpretację wyników

[4] Dalej: Polityka Bezpieczeństwa Informacji.
[5] Art. 37 ust. 1 rozporządzenia RODO: Administrator i podmiot przetwarzający wyznaczają inspektora ochrony danych (...). Rozporządzenie RODO - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r., w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

sporządzanych analiz ryzyka w oparciu o najnowsze regulacje, bez konieczności odwoływania się do dokumentu z 2012 roku.

(dowód: akta kontroli str. 104-112, 182, 124-142)

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

Inwentaryzacja sprzętu informatycznego powinna zawierać informację o jego rodzaju i konfiguracji, przez co możliwe będzie jego odtworzenie po katastrofie lub innym zdarzeniu losowym. Kontrolującym przedstawiono *Metryki komputerów używanych w Urzędzie Miejskim w Dębnie*, które zawierają między innymi informacje dotyczące rodzaju użytkowanego sprzętu (i jego charakterystykę); zainstalowanego oprogramowania; rodzaju systemu operacyjnego. W dokumentach wykazano sprzęt wykorzystywany przy realizacji zadań zleconych z zakresu administracji rządowej.

(dowód: akta kontroli str. 306-310)

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 by dostęp do danych realizowany był przez uprawnione osoby, w ściśle ustalonym zakresie.

Kwestie nadawania i odbierania uprawnień do pracy w systemie informatycznym uregulowano w:

- dokumencie *Procedura nadawania i cofania uprawnień do przetwarzania danych osobowych oraz metody i środki uwierzytelnienia w systemie informatycznym,* stanowiącym załącznik nr 19 do *Polityki Bezpieczeństwa Informacji;*
- § 5 *Polityki Bezpieczeństwa Informacji (Obowiązki osób przetwarzających dane osobowe).*

Zgodnie z zapisami procedury ASI[6] przyznaje uprawnienia na podstawie pisemnego zlecenia bezpośredniego przełożonego pracownika. Dla czynności, o których mowa

[6] Administrator Systemu Informatycznego.

powyżej tworzona jest dokumentacja, co powoduje, że proces nadawania i odbierania uprawnień jest w pełni potwierdzony.
Kontrolującym przedstawiono następujące dokumenty:

- *Upoważnienie do przetwarzania danych osobowych* wystawione pracownikom realizującym zadania zlecone z zakresu administracji rządowej. W treści dokumentu zawarto *Oświadczenie osoby upoważnionej* zobowiązujące do zachowania poufności danych pozyskanych w trakcie zatrudnienia, wskazując okres obowiązywania zobowiązania zarówno w trakcie zatrudnienia, jak również po ustaniu stosunku pracy;
- *Zobowiązanie pracownika do zachowania tajemnicy służbowej;*
- *Oświadczenie o wyrażeniu zgody na przetwarzanie danych osobowych* pracowników*;*
- *Wnioski o dostęp do Systemu Rejestrów Państwowych (SRP)- użytkownicy aplikacji Źródło*. Wnioski dotyczyły przyznania użytkownikom dostępu do systemu oraz wnioski dotyczące usunięcia użytkowników;
- *Zlecenia nadania /cofania/modyfikacji uprawnień* pracownikom realizującym zadania zlecone z zakresu administracji rządowej.

W trakcie kontroli dokonano sprawdzenia odbierania uprawnień dostępu do systemów informatycznych pracownikom, z którymi ustał lub rozwiązano stosunek pracy. Stwierdzono nieprawidłowości polegające na niezachowaniu wymogu bezzwłocznego odebrania uprawnień w systemach informatycznych. W przypadku pracownika W. K. konto zablokowano po 4 miesiącach a w przypadku pracownika T.K. konto zablokowano po 14 miesiącach od momentu rozwiązania stosunku pracy.

(dowód: akta kontroli str. 176, 214-215, 242-266)

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 Dębnie przeprowadzono następujące szkolenia pracowników z zakresu bezpieczeństwa informacji i ochrony danych osobowych:

- Szkolenie z zakresu ochrony danych osobowych oraz cyberbezpieczeństwa, które odbyło się w dniu 25 lutego 2025 r.;
- Szkolenie z zakresu przetwarzania danych osobowych, przeprowadzone w dniu 17 października 2024 r.
- Udział w szkoleniach dokumentowała lista obecności zawierająca imię i nazwisko uczestnika oraz własnoręczny podpis.

Stwierdzono, że w szkoleniu przeprowadzonym 25 lutego 2025 r. wzięli udział wszyscy pracownicy wskazani jako osoby realizujące zadania zlecone z zakresu administracji rządowej. Z przedstawionej dokumentacji oraz złożonych wyjaśnień wynika, że zakres tematyczny szkoleń przeprowadzonych w Urzędzie obejmował zagadnienia wskazane w § 19 ust. 2 pkt 6 rozporządzenia KRI.
Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie szkolenia osób zaangażowanych w proces przetwarzania informacji. Istotne jest by szkolenia, których celem jest zagwarantowanie bezpieczeństwa

w zakresie przetwarzania informacji, ze względu na zmieniające się zagrożenia związane z dynamicznym rozwojem technologii informatycznych miały charakter cykliczny i realizowane były przy udziale wszystkich pracowników Urzędu.

(dowód: akta kontroli str. 267-275)

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:

- *Zarządzeniu wewnętrznym nr 18/2025 Burmistrza Dębna z dnia 06 czerwca 2025r. w sprawie wprowadzenia Procedury ochrony danych osobowych podczas wykonywania pracy zdalnej oraz pracy zdalnej wykonywanej okazjonalnie;*
- *Zarządzeniu nr 76/31/2024 Burmistrza Dębna z dnia 26 listopada 2024 r. w sprawie zasad postępowania z pamięciami zewnętrznymi w Urzędzie Miejskim w Dębnie;*
- *Procedurze bezpiecznej eksploatacji sprzętu i oprogramowania*, stanowiącej załącznik nr 16 do *Polityki Bezpieczeństwa Informacji* (punkt 27 i 29).

W wyżej wymienionych dokumentach uregulowano między innymi kwestie wynoszenia poza obszar organizacji nośników z danymi osobowymi, wprowadzono minimalne wymagania sprzętowe dotyczące urządzeń wykorzystywanych do pracy zdalnej w zakresie zabezpieczeń i kryptografii oraz wymagania dotyczące pracy z dokumentami w formie papierowej. Wdrożono obowiązek szyfrowania danych zapisanych na komputerach przenośnych oraz innych urządzeniach mobilnych. Zgodnie z wyjaśnieniami Burmistrza z dnia 8 sierpnia 2025 r. w Urzędzie nie realizowano zadań zleconych z zakresu administracji rządowej w formie pracy zdalnej.

(dowód: akta kontroli str. 82, 204-206, 232-241)

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 pracowników zatrudnionych w Urzędzie Miejskim w Dębnie na stanowiskach starszych informatyków. Wśród obowiązków pracowników znajduje się m.in.: nadzór nad prawidłowym działaniem systemów informatycznych, administrowanie systemami i serwerami, instalacja i konfiguracja oprogramowania i sprzętu komputerowego, nadzór nad bezpieczeństwem danych w systemach informatycznych, zarządzanie uprawnieniami użytkowników, wykonywanie kopii bezpieczeństwa oraz archiwizowanie zasobów elektronicznych.

W zakresie nadzoru i administrowania infrastrukturą serwerową zawarto umowę[7] XXX. W umowie uregulowano kwestię czasu reakcji na zgłoszenie konieczności realizacji zadań wynikających z jej zapisów. Z podmiotem zawarto *Umowę powierzenia przetwarzania danych osobowych*[8].
W celu realizacji zadań zleconych z zakresu administracji rządowej XXX zawarto *umowę o opiekę autorską* programów XXX, obejmującą aktualizacje systemu i bieżące konsultacje związane z jego eksploatacją.[9] Stwierdzono, że w powyższej umowie wprowadzono zapisy określające maksymalny czas skutecznej naprawy oprogramowania (zdefiniowano grupy błędów i maksymalny czas ich usunięcia) czym wypełniono dyspozycję § 19 ust. 2 pkt 10 rozporządzenia KRI, zawierając zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji. Z firmą zawarto również *Umowę powierzenia przetwarzania danych osobowych*[10].

(dowód: akta kontroli str. 276-304)

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 § 15 *Naruszenia zasad danych osobowych* określono zasady i sposób postępowania w przypadku wystąpienia incydentów związanych z naruszeniem ochrony danych osobowych. W procedurze przypisano odpowiednie zadania ADO[11] oraz IOD[12] w przypadku powzięcia informacji o naruszeniu 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 wszystkich informacji w organizacji i nie ograniczać się wyłącznie do ochrony danych osobowych. Kontrolujący wskazują by procedury regulujące kwestie incydentów nie ograniczały się jedynie do naruszeń ochrony danych osobowych a obejmowały mogące potencjalnie wystąpić naruszenia bezpieczeństwa wszystkich przetwarzanych informacji.
W trakcie kontroli przedstawiono dokument *Rejestr incydentów bezpieczeństwa i działań korygujących i zapobiegawczych,* prowadzony w Jednostce od 2021 r. Rejestr zawiera informacje dotyczące braku wystąpienia incydentów w latach 2021 - 2024 r. oraz jeden wpis (z 2025 r.) dokumentujący zdarzenie zakwalifikowane, jako incydent z zakresu bezpieczeństwa danych. Z *Protokołu obsługi incydentu* wynika, że nie wystąpiła konieczność zgłoszenia tego przypadku organowi nadzorczemu.

(dowód: akta kontroli str. 122-123, 181-182)

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.*

[7] Umowa nr AO.2151.21.2025 z dnia 3.02.2025 r.
[8] Umowa zawarta w dniu 3 lutego 2025 r.
[9] Umowa o opiekę autorską nr 24/0847/JU z dnia 26.11.2024 r.
[10] Umowa nr 24/1159/JU z dnia 31.12.2024 r.
[11] Administrator Danych Osobowych
[12] Inspektor Ochrony Danych

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:

- *Audyt wewnętrzny z zakresu bezpieczeństwa informacji zgodnie z Krajowymi Ramami Interoperacyjności*, data przeprowadzenia: 12 grudzień 2024 roku.
- *Audyt Wewnętrzny KRI wykonany przez ASI UM Dębno-12.2023 r.*
- Ocena wybranych aspektów bezpieczeństwa systemów informatycznych, ocena zgodności z KRI/ UoKSC, data dokumentu: lipiec 2022 r.

Audyt wewnętrzny przeprowadzony w Jednostce w 2023 roku został wykonany przez Administratora Systemu Informatycznego. Audyt z 2024 roku został zrealizowany przez zespół, w skład którego weszli pracownicy zatrudnieni na stanowisku starszych Informatyków, przy czym jeden z nich pełnił funkcję Administratora Systemu Informatycznego. Administrator Systemu Informatycznego, odpowiedzialny jest za funkcjonowanie systemu informatycznego, za przestrzeganie zasad i wymagań bezpieczeństwa przewidzianych dla systemu informatycznego oraz weryfikację i bieżącą kontrolę zgodności funkcjonowania z wymaganiami bezpieczeństwa.

W przypadku audytów wykonanych w latach 2023 i 2024 osoby odpowiadające za bieżące prowadzenie przetwarzania danych osobowych i bezpieczeństwo danych w systemach informatycznych weryfikowały swoje własne kompetencje i działania, pod kątem zgodności z wymogami rozporządzenia KRI.

Audytor wewnętrzny powinien powstrzymać się od oceny działalności operacyjnej, za którą jest odpowiedzialny, ze względu na ograniczenie obiektywizmu w ocenie tych działań. Audyt wewnętrzny stanowi bowiem istotne źródło informacji dla kierownictwa Jednostki o realnym stanie bezpieczeństwa, różnych aspektach jego utrzymania oraz wskazuje obszary wymagające podjęcia działań korygujących. W tym zakresie rozwiązaniem jest wyznaczenie audytora (lub audytorów), który będzie dokonywał analizy obszaru, za który nie odpowiada bezpośrednio w trakcie bieżącej działalności Jednostki.

(dowód: akta kontroli str. 89-101, 311-324)

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.

Wobec oświadczenia Burmistrza Dębna z dnia 8 sierpnia 2025 r. o nieobowiązywaniu *Zarządzenia nr 66/27/2005 Burmistrza Miasta i Gminy Dębno z dnia 8 czerwca 2005 r.*
w sprawie wprowadzenia instrukcji w sprawie eksploatacji systemów informatycznych

w Urzędzie Miasta i Gminy Dębno należy stwierdzić, że w dokumentacji Urzędu dotyczącej bezpieczeństwa informacji brakuje regulacji dotyczących zasad tworzenia kopii zapasowych, przechowywania oraz zasad testowego odtworzenia tych kopii. W obowiązujących unormowaniach (*Polityce Bezpieczeństwa Informacji*) przypisano te zadania ASI, bez wskazania zasad ich realizacji.
Z wyjaśnień Informatyka wynika, że kopie zapasowe baz danych oprogramowania wykorzystywanego w Jednostce (w tym podlegające badaniu) wykonywane są w każdym dniu roboczym i przechowywane przez okres trzech miesięcy. Kopie zapasowe przechowywane są w miejscu wytworzenia. W Urzędzie nie jest realizowane próbne testowanie kopii zapasowych na potrzeby weryfikacji poprawności i stanu ich wykonywania.

(dowód: akta kontroli str. 100, 145)

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 zleconych z zakresu administracji rządowej XXX zawarto *umowę o opiekę autorską* programów XXX, obejmującą aktualizacje systemu i bieżące konsultacje związane z jego eksploatacją.[13]

(dowód: akta kontroli str. 276-280)

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. Pracownicy złożyli oświadczenia o zachowaniu w tajemnicy danych osobowych, do których będą mieli dostęp w trakcie wykonywania obowiązków służbowych.

[13] Umowa o opiekę autorską nr 24/0847/JU z dnia 26.11.2024 r.

W wyniku oględzin stanowisk komputerowych wykorzystywanych do realizacji zadań zleconych z zakresu administracji rządowej, przeprowadzonych w toku czynności kontrolnych ustalono, że:
- dostęp do systemu operacyjnego na urządzeniu możliwy był jedynie po wprowadzeniu nazwy użytkownika i hasła,
- złożoność hasła była zgodna z wymogami rozporządzenia w sprawie dokumentacji i warunków technicznych,
- ustawienie monitorów stanowisk obsługi systemów informatycznych wykorzystywanych do realizacji zadań zleconych z zakresu administracji rządowej uniemożliwiało odczyt wyświetlanych danych przez osoby postronne,
- komputery miały zainstalowane oprogramowanie antywirusowe oraz skonfigurowany wygaszacz ekranu,
- 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. 154-159, 162-163)

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

- W Jednostce zastosowano zintegrowane rozwiązania do zarządzania bezpieczeństwem w sieci.
- Serwerownię wyposażono w klimatyzację, gaśnicę, okno zabezpieczono kratą a drzwi wejściowe do pomieszczenia roletą.
- W procedurach wewnętrznych Jednostki określono :
  - zasady dostępu do serwerowni (załącznik nr 22 do *Polityki Bezpieczeństwa Informacji).* W Jednostce prowadzony jest *Rejestr osób trzecich przebywających w pomieszczeniu serwerowni;*
  - zasady funkcjonowania systemu monitoringu wizyjnego (załącznik nr 14 do *Polityki Bezpieczeństwa Informacji);*
  - sposób postępowania z kluczami (załącznik nr 20 do *Polityki Bezpieczeństwa Informacji);*
  - zasady wykonywania naprawy i konserwacji sprzętu komputerowego przez podmioty zewnętrzne;
  - reguły przesyłania danych poza obszar przetwarzania;

- procedury korzystania z Internetu i poczty elektronicznej (załącznik nr 18 do *Polityki Bezpieczeństwa Informacji).*

(dowód: akta kontroli str. 143-144, 162-163, 199-202, 204-207, 212-213, 216-222)

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).

Logi programu XXX są przechowywane przez okres 2 lat, niemniej z przedstawionych dokumentów wynika, że logi zawierają tylko informacje o udanych zalogowaniach do systemu oraz wylogowaniu użytkownika.

Z wyjaśnień Informatyka z dnia 11 sierpnia 2025 r. wynika, że logi wskazujące inne aktywności, w tym dotyczące nadania oraz odbierania uprawnień użytkownikom przez administratora *mogą być dostępne po zgłoszeniu zapotrzebowania na takie dane do producenta*.

Działania związane z zapewnieniem rozliczalności użytkowników, szczególnie posiadających uprawnienia do administrowania systemami oraz zmianami konfiguracji systemów operacyjnych i ich zabezpieczeń, zwłaszcza podczas przetwarzania danych podlegających prawnej ochronie wymagają bieżącego dostępu do logów zawierających informacje o tym kto, kiedy i jakiego rodzaju operacje przeprowadzał wykorzystując dostęp do użytkowanego programu. Kontrolujący wskazują by wystąpić do producenta oprogramowania o zaimplementowanie do programu funkcjonalności pozwalającej na śledzenie zmian dotyczących uprawnień (nadawania i ich modyfikacji) oraz innych rodzajów działań administratora oraz użytkowników, co pozwoli usprawnić bieżące zarządzanie uprawnieniami w systemie jak i czynności sprawdzające związane z przeglądaniem logów (np. pod kątem czy operacje wykonywane w systemie informatycznym są zgodne z kompetencjami użytkownika).

W Jednostce, zgodnie z wyjaśnieniami Informatyka prowadzone są *w nieregularnych odstępach czasu* działania związane z przeglądaniem logów systemu informatycznego,

w celu stwierdzenia i ewentualnej identyfikacji działań niepożądanych, lecz nie jest sporządzana dokumentacja z tych czynności. Kontrolujący wskazują aby prowadząc wyżej opisane działania dokumentować je (np. w postaci dziennika administratora), tak by realizowane czynności były w pełni potwierdzone, a w procedurach wewnętrznych uregulować zasady realizacji tych procesów.

(dowód: akta kontroli str. 145-149)

Wpis do książki kontroli	7
Stwierdzone nieprawidłowości w obszarze Nr 2	• Zrealizowanie audytów wewnętrznych z zakresu bezpieczeństwa informacji przez osoby odpowiedzialne za bieżące funkcjonowanie obszarów poddawanych analizie. • Dokumentacja regulująca kwestie bezpieczeństwa informacji nie zawiera wszystkich elementów wymaganych przepisami rozporządzenia KRI. • Zawężenie incydentów naruszenia bezpieczeństwa informacji do naruszeń danych osobowych, co nie jest zgodne z dyspozycją § 19 ust. 2 pkt 13 rozporządzenia KRI. • Przechowywanie kopii zapasowych w miejscu wytworzenia, co nie jest zgodne z dyspozycją § 19 ust. 2 pkt 12 lit. b, e rozporządzenia KRI. • Nieprzeprowadzanie testowych odtworzeń kopii zapasowych, zgodnie z wymogami § 19 ust. 2 pkt 12 lit. b i e rozporządzenia KRI. • Niezachowanie wymogu bezzwłocznego odebrania uprawnień w systemach informatycznych pracownikom, z którymi rozwiązano stosunek pracy, zgodnie z dyspozycją § 19 ust. 2 pkt 5 rozporządzenia KRI. • Nieodnotowywanie w dziennikach systemów wszystkich rodzajów aktywności użytkowników z uprawnieniami administracyjnymi, co jest niezgodne z dyspozycją § 20 ust. 2 rozporządzenia KRI.
Ocena obszaru kontroli	**Pozytywna z nieprawidłowościami**
Zalecenia	• Uzupełnić dokumentację regulującą kwestie bezpieczeństwa informacji o elementy wymagane przepisami rozporządzenia KRI, wskazane w treści wystąpienia pokontrolnego. • Powierzyć realizację audytów wewnętrznych z zakresu bezpieczeństwa informacji osobie (podmiotowi), która nie jest odpowiedzialna za bieżące funkcjonowanie obszarów poddawanych analizie. • Przestrzegać wymogu bezzwłocznego odbierania uprawnień w systemach informatycznych w przypadku ustania okoliczności ich nadania,

	zgodnie z dyspozycją § 19 ust. 2 pkt 5 rozporządzenia KRI. • Uzupełnić procedury postępowania z incydentami o pozostałe obszary, w których mogą wystąpić przypadki naruszenia bezpieczeństwa przetwarzanych w Jednostce informacji, zgodne z dyspozycją § 19 ust. 2 pkt 13 rozporządzenia KRI. • Przechowywać kopie zapasowe poza miejscem ich wytworzenia oraz przeprowadzać testowe odtworzenia kopii zapasowych, zgodne z dyspozycją § 19 ust. 2 pkt 12 lit. b, e rozporządzenia KRI. • Odnotowywać w dziennikach systemów wszystkie rodzaje aktywności użytkowników z uprawnieniami administracyjnymi, zgodne z dyspozycją § 20 ust. 2 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 */podpisano kwalifikowanym podpisem elektronicznym/*