Opolski Urząd Wojewódzki
Wydział Prawny i Nadzoru
45-082 Opole, ul. Piastowska 14
Skrytka pocztowa 3

Opole, 16 kwietnia 2026 r.

PN.I.431.4.2.2026.AOG

Pani
Iwona Sobania
Burmistrz Byczyny
Urząd Miejski w Byczynie
ul. Rynek 1
46-220 Byczyna

WYSTĄPIENIE POKONTROLNE

I. Dane identyfikacyjne kontroli

1. Nazwa i adres jednostki kontrolowanej: Urząd Miejski w Byczynie, ul. Rynek 1, 46-220 Byczyna[1];
2. Podstawa prawna podjęcia kontroli:
   a) Art. 25 ust. 1 pkt 3 lit. a i ust. 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz.U. z 2025 r. poz. 1703 ze zm.)[2],
   b) Art. 6 ust. 4 pkt 3 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (t.j. Dz.U z 2026 r. poz. 158)[3];
3. Zakres kontroli:
   a) Przedmiot kontroli: Działanie systemów teleinformatycznych i rejestrów publicznych używanych do realizacji zadań zleconych z zakresu administracji rządowej,
   b) Okres objęty kontrolą: od 1 stycznia 2025 r. do dnia rozpoczęcia kontroli (z uwzględnieniem okresu wcześniejszego i późniejszego w zakresie niezbędnym do realizacji celu kontroli);

[1] UM w Byczynie
[2] Dalej: ustawa o informatyzacji działalności podmiotów
[3] Dalej: ustawa o kontroli

4. Rodzaj kontroli: problemowa;
5. Tryb kontroli: zwykły;
6. Termin kontroli: 20 lutego 2026 r. – 6 marca 2026 r., kontrola prowadzona była w trybie hybrydowym, tj. dnia 20 lutego 2026 r. – rozpoczęcie czynności kontrolnych w UM w Byczynie oraz oględziny serwerowni na miejscu w jednostce. W pozostałe dni kontrola prowadzona była zdalnie;
7. Skład zespołu kontrolnego:
   a) Natalia Lenart – Inspektor Wojewódzki w Oddziale Organizacji, Kontroli i Skarg w Wydziale Prawnym i Nadzoru w Opolskim Urzędzie Wojewódzkim – kierownik zespołu kontrolnego,
   b) Agnieszka Orlińska-Gocka - Inspektor Wojewódzki w Oddziale Organizacji, Kontroli i Skarg w Wydziale Prawnym i Nadzoru w Opolskim Urzędzie Wojewódzkim – członek zespołu kontrolnego,
   c) Kamil Dziechciński - Starszy Specjalista w Oddziale Informatyki i Rozwoju w Biurze Obsługi Urzędu w Opolskim Urzędzie Wojewódzkim – członek zespołu kontrolnego;
8. Kierownik jednostki kontrolowanej: Pani Iwona Sobania – Burmistrz Byczyny, od dnia 2 maja 2024 r.[4]
9. Kontrolę wpisano do książki kontroli prowadzonej w jednostce kontrolowanej, pod poz. nr 1/2026.

II. Ocena skontrolowanej działalności, ze wskazaniem ustaleń, na których została oparta

Działanie systemów teleinformatycznych i rejestrów publicznych używanych do realizacji zadań zleconych z zakresu administracji rządowej, w okresie od 1 stycznia 2025 r. do dnia rozpoczęcia kontroli (z uwzględnieniem okresu wcześniejszego i późniejszego w zakresie niezbędnym do realizacji celu kontroli), tj. 20 lutego 2026 r. w Urzędzie Miejskim w Byczynie ocenia się pozytywnie z nieprawidłowościami.

W trakcie kontroli zostały stwierdzone nieprawidłowości oraz uchybienia, mające znaczenie dla bezpieczeństwa informacji[5], które opisano poniżej.

[4] Akta kontroli - Dokumentacja kontrolna 1: 4a.Powołanie

[5] Dalej: BI

W kontrolowanym okresie zakres działania i zadania oraz organizację i zasady funkcjonowania UM w Byczynie określał Regulamin organizacyjny Urzędu Miejskiego w Byczynie[6] stanowiący załącznik nr 1 do Zarządzenia nr 187/2019 Burmistrza Byczyny z dnia 30 października 2019 r. w sprawie nadania Regulaminu Organizacyjnego Urzędu Miejskiego w Byczynie[7].

Zgodnie z § 4 pkt 1 – Pracą Urzędu kieruje Burmistrz przy pomocy Zastępcy Burmistrza, Sekretarza i Skarbnika.

Osobą pełniącą funkcję Administratora Systemów Informatycznych[8] jest Informatyk.[9]

Osobami odpowiedzialnymi za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa są: Pracownik zatrudniony na stanowisku Pomoc administracyjna oraz Informatyk. Zgłoszenie osób do CSIRT NASK nastąpiło dnia 8 października 2020 roku.[10]

W UM w Byczynie do realizacji zadań zleconych z zakresu administracji rządowej wykorzystywanych jest 6 systemów teleinformatycznych[11], w tym:

- 2 o zasięgu krajowym;
- 4 o zasięgu lokalnym (w tym jeden archiwalny).

1. Elektroniczna skrzynka podawcza

Podstawa prawna:

- Art. 16 ust. 1a ustawy o informatyzacji działalności podmiotów: Podmiot publiczny udostępnia elektroniczną skrzynkę podawczą, spełniającą standardy określone i opublikowane na ePUAP przez ministra właściwego do spraw informatyzacji, oraz zapewnia jej obsługę.

Na stronie głównej Biuletynu Informacji Publicznej UM w Byczynie została udostępniona Elektroniczna Skrzynka Podawcza: /urzadbyczyna/skrytka, znajdująca się na Elektronicznej Platformie Usług Administracji Publicznej, pozwalająca na wysyłanie i odbieranie pism w formie dokumentów elektronicznych. Dodatkowo na BIP został udostępniony adres do doręczeń

[6] Dalej: Regulamin organizacyjny
[7] Akta kontroli - Dokumentacja kontrolna 1: 4b.Załącznik do zarządzenia nr 187-2019 (Regulamin Organizacyjny), Akta kontroli - Dokumentacja kontrolna 2: 4. Regulamin organizacyjny
[8] Dalej: ASI
[9] Osoba zatrudniona na umowę zlecenie, Akta kontroli - Dokumentacja kontrolna 2: 6.6 Umowa ASI 2024-2025, 6.7 Umowa ASI 2025-2026
[10] Akta kontroli - Dokumentacja kontrolna 1: 4e.Zgłoszenie CSIRT NASK
[11] Akta kontroli - Dokumentacja kontrolna 1: 1.Załącznik nr 1 - Zestawienie systemów teleinformatycznych

elektronicznych, tj. AE:PL-48129-31179-JHGEE-32, który UM w Byczynie posiada zgodnie z art. 8 ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (t.j. Dz.U. z 2026 r. poz. 3).

2. Obieg dokumentów elektronicznych w urzędzie

Podstawa prawna:

- § 19 ust. 2 pkt 9 Rozporządzenia 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[12]: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie.

Wykorzystanie systemu elektronicznego w zakresie zarządzania dokumentami elektronicznymi poprawia przepływ dokumentów w Urzędzie oraz usprawnia przeprowadzenie archiwizacji, co wpływa na przyspieszenie załatwianych spraw oraz wzrost poziomu BI. Zastosowanie systemu teleinformatycznego wspomagającego elektroniczny obieg dokumentów pozwala na realizację interfejsów z innymi systemami podmiotu publicznego w celu przekazywania dokumentów pomiędzy tymi systemami w postaci elektronicznej.

Z informacji uzyskanych w analizie przedkontrolnej wynika, że w UM w Byczynie podstawowym sposobem dokumentowania przebiegu załatwiania i rozstrzygania spraw jest tradycyjny (tj. papierowy) system wykonywania czynności kancelaryjnych[13].

3. Dokumenty z zakresu bezpieczeństwa informacji; zaangażowanie kierownictwa podmiotu.

Podstawa prawna:

- § 19 ust. 1 rozporządzenie 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

[12] Dz.U. z 2024 r. poz. 773, dalej: Rozporządzenie KRI
[13] Akta kontroli - Dokumentacja kontrolna 1: 2.Załącznik nr 2 – Ankieta dotycząca działania systemów teleinformatycznych

takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność;

- § 19 ust. 2 rozporządzenie KRI: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie działań związanych z bezpieczeństwem informacji;
- § 19 ust. 2 pkt 1 rozporządzenie KRI: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia.

Zgodnie z zapisami rozporządzenia KRI, podmiot publiczny realizujący zadania publiczne powinien opracować dokumentację Systemu Zarządzania Bezpieczeństwem Informacji[14], w tym regulacje wewnętrzne oraz zapewnienie ich aktualizacji zgodnie ze zmieniającym się otoczeniem. Kompleksowa dokumentacja SZBI jest warunkiem niezbędnym do skutecznego zarządzania bezpieczeństwem informacji w Urzędzie.

Podstawowym elementem SZBI jest Polityka Bezpieczeństwa Informacji[15], która zgodnie z § 2 pkt 15 rozporządzenia KRI stanowi zestaw efektywnych, udokumentowanych zasad i procedur bezpieczeństwa wraz z ich planem wdrożenia i egzekwowania. PBI zazwyczaj zawiera wyrażoną przez kierownictwo deklarację stosowania, opisuje organizację i ustala osoby odpowiedzialne oraz ich zakresy odpowiedzialności, wprowadza klasyfikacje informacji, sposób postępowania z poszczególnymi rodzajami informacji. Dodatkowo może określać aktywa oraz ich właścicieli, oraz sposób szacowania ryzyka i postępowania z ryzykiem.

System SZBI winien być na bieżąco monitorowany i poddawany przeglądom, celem udoskonalenia go. Czynności te powinny znaleźć odzwierciedlenie w dokumentacji systemu.

Obecnie w UM w Byczynie stosowana jest Polityka Ochrony Danych Osobowych i Bezpieczeństwa Informacji[16] wprowadzona Zarządzeniem nr 155/2021 Burmistrza Byczyny z dnia 18 listopada 2021 r. w sprawie ustanowienia Systemu Zarządzania Bezpieczeństwem Informacji oraz wprowadzenia Polityki Ochrony Danych Osobowych i Bezpieczeństwa Informacji

[14] Dalej: SZBI
[15] Dalej: PBI
[16] Dalej: PODOiBI

w Urzędzie Miejskim w Byczynie[17]. Zgodnie z Protokołem przeglądu PODOiBI sporządzonym w 2025 r. oraz złożonymi wyjaśnieniami, UM w Byczynie bierze udział w projekcie „Cyberbezpieczna Gmina Byczyna" w ramach którego zostanie, m. in. zaktualizowana dokumentacja SZBI i PODOiBI, przeprowadzony audyt KRI, przeprowadzone szkolenia oraz przeprowadzone testy penetracyjne oraz socjotechniczne[18].

Pracownicy UM w Byczynie zapoznali się z Polityką Ochrony Danych Osobowych i Bezpieczeństwa Informacji[19].

W UM w Byczynie nie został wyznaczony Pełnomocnik ds. bezpieczeństwa informacji, co zespół kontrolny kwalifikuje jako nieprawidłowość. Z przesłanych wyjaśnień wynika, że po aktualizacji dokumentacji SZBI i PBI zostanie powołany Zespół ds. bezpieczeństwa informacji[20]. Zespół kontrolny przyjął złożone wyjaśnienia.

4. Analiza zagrożeń związanych z przetwarzaniem informacji

Podstawa prawna:

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

Wymogiem skuteczności SZBI jest przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji. Kluczowa rola analizy ryzyka wynika z faktu, że rodzaj i poziom zastosowanych zabezpieczeń jest względny oraz zależny od ważności aktywów informatycznych danego podmiotu. Proces szacowania ryzyka powinien być przeprowadzony i udokumentowany w celu wykazania, że ryzyko zostało oszacowane i wprowadzono odpowiednie środki obrony. Szacowanie ryzyka pozwala na aktywne zarządzanie BI, w tym przeciwdziałanie zagrożeniom, ograniczenie skutków zmaterializowanych ryzyk oraz racjonalne zarządzenie środkami finansowymi poprzez stosowanie zabezpieczeń adekwatnych do oszacowanego poziomu ryzyka. Jednocześnie

[17] Akta kontroli - Dokumentacja kontrolna 1: 3a.Zarządzenie PODOIBI 18.11.2021, 3a.Zarządzenie podpisane PODOIBI
[18] Akta kontroli - Dokumentacja kontrolna 2: 1.1 Ogłoszenie o zamówieniu, 1.4 Informacja o wyborze oferty najkorzystniejszej, 27. Protokół przeglądu Polityki Danych Osobowych, Akta kontroli - Pismo przewodnie nr OR.1710.1.2026.MC
[19] Akta kontroli - Dokumentacja kontrolna 2: 2. Zapoznanie się z PODOIBI
[20] Akta kontroli - Pismo przewodnie nr OR.1710.1.2026.MC

należy zaznaczyć, że prawidłowość przeprowadzenia analizy ryzyka polega na jego regularnym i ciągłym monitorowaniu.

W 2025 r., zatrudniony przez UM w Byczynie IOD, przeprowadził analizę ryzyka utraty integralności, dostępności i poufności informacji[21].

5. Inwentaryzacja sprzętu i oprogramowania informatycznego

Podstawa prawna:

- § 19 ust. 2 pkt 2 rozporządzenie KRI: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: utrzymywanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.

Zarządzenie infrastrukturą informatyczną wymaga utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację. W przedmiotowym spisie winny być wykazane wszystkie zidentyfikowane aktywa informatyczne wraz z najistotniejszymi informacjami o nich. Stworzona baza ma na celu podejmowanie właściwych decyzji i działań w zakresie zmian w środowisku teleinformatycznym.

W UM w Byczynie prowadzone są zestawienia sprzętu komputerowego, informatycznego oraz oprogramowań informatycznych, które zapewniają utrzymanie aktualności użytkowanego sprzętu i oprogramowania. Przedmiotowa inwentaryzacja odbywa się w systemie GLPI [22].

6. Zarządzanie uprawnieniami do pracy w systemach informatycznych

Podstawa prawna:

- § 19 ust. 2 pkt 4 rozporządzenie 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;

[21] Akta kontroli - Dokumentacja kontrolna 1: 3b.ANALIZA RYZYKA

[22] Akta kontroli - Dokumentacja kontrolna 2: 5.1 Inwentaryzacja sprzętu 1, 5.2 Inwentaryzacja sprzętu 2, 5.3 Inwentaryzacja sprzętu drukarki, 5.4 Inwentaryzacja sprzętu monitory, 5.5 Wybrane oprogramowanie, 5.6 Wybrane oprogramowanie komputerowe, Akta kontroli - Pismo przewodnie nr OR.1710.1.2026.MC

- § 19 ust. 2 pkt 5 rozporządzenie KRI: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: bezzwłoczną zmianę uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4.

Kluczowym elementem polityki BI jest zarządzanie dostępem do systemów teleinformatycznych przetwarzających informacje. Zarządzenie dostępem ma zapewnić, 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, a w przypadku zmiany zadań lub zakończenia stosunku pracy następuje zmiana lub odebranie uprawnień.

Pracownicy UM w Byczynie realizujący zadania zlecone z zakresu administracji rządowej posiadają upoważnienia do przetwarzania informacji wraz z odpowiednimi uprawnieniami w systemach, które zgodne są z ich zakresami czynności[23].

W okresie objętym kontrolą były przypadki nadania/zmiany/cofania uprawnień dostępu do systemów. Proces ten odbywa się poprzez złożenie wniosku w systemie GLPI, a następnie nadanie, zmianę lub odebranie uprawnień przez ASI (Informatyka) [24].

Z przesłanej dokumentacji wynika, że 6 sierpnia 2025 r. został przesłany wniosek o odebranie uprawnień w systemach pracownikowi, który zakończył pracę w UM w Byczynie. Faktyczne ich odebranie nastąpiło 19 lutego 2026 r., co oznacza brak natychmiastowego odebrania uprawnień w systemach. Działanie to, zespół kontrolny stwierdza jako nieprawidłowość.

7. Szkolenia pracowników zaangażowanych w proces przetwarzania informacji

Podstawa prawna:

- § 19 ust. 2 pkt 6 rozporządzenie 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,

[23] Akta kontroli - Dokumentacja kontrolna 2: 6.1. Zakres obowiązków FN, 6.2. Zakres obowiązków OB, 6.3 Zakres obowiązków OR, 6.4. Zakres obowiązków OR, 7.1 Upoważnienie CEDIG, 7.2 Upoważnienie, 7.3 Upoważnienia OB, 8.1 Uprawnienia sigid akcyza, 8.2 Uprawnienia pb ewid, 8.3 Uprawnienia Źródło, Akta kontroli - Uprawnienia system CEIDG

[24] Akta kontroli - Dokumentacja kontrolna 2: 9.1 Nadawanie uprawnień, 9.2 Przykład odebranie uprawnień, Akta kontroli - Pismo przewodnie nr OR.1710.1.2026.MC

w tym odpowiedzialność prawna, c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich.

Szkolenia podnoszące świadomość zagrożeń i konsekwencji zaistnienia incydentów związanych z BI winny obejmować wszystkie osoby uczestniczące w procesie przetwarzania informacji. Z uwagi na stale zmieniające się zagrożenia BI oraz zabezpieczenia przed takimi incydentami, szkolenia osób zaangażowanych w proces przetwarzania informacji powinny być przeprowadzane cyklicznie.

W 2025 r. w UM w Byczynie zostało przeprowadzone dla wszystkich pracowników szkolenie z zakresu RODO. Dodatkowo pracownicy uczestniczyli w szkoleniach zewnętrznych organizowanych przez Fundację Partycypacji Społecznej z zakresu „E-Bezpieczeństwo", a także Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy (NASK-PIB) w zakresie „Działania prewencyjno-edukacyjne z zakresu cyberbezpieczeństwa w latach 2025-2026 – podnoszenie odporności Rzeczypospolitej Polskiej na zagrożenia w przestrzeni cyfrowej"[25].

Zgodnie z zapisami § 2 pkt 3 Procedury bezpieczeństwa fizycznego i bezpieczeństwa informacji szkolenia z zakresu ochrony danych osobowych i bezpieczeństwa są realizowane przynajmniej raz w roku kalendarzowym. W związku z powyższym, brak przeprowadzenia szkolenia z zakresu bezpieczeństwa przez ASI, zespół kontrolny stwierdza jako uchybienie.

8. Praca na odległość i mobilne przetwarzanie danych

Podstawa prawna:

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

W UM w Byczynie nie zostały ustanowione podstawowe zasady gwarantujące bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość, co zespół

[25] Akta kontroli - Dokumentacja kontrolna 2: 10. Szkolenie RODO, 11.1 Certyfikaty szkolenie wewnętrzne, 11.2 Szkolenie podział na grupy i zakres tematyczny, 12.1 Szkolenia z cyberbezpieczeństwa NASK PIB, 12.2 Harmonogram szkoleń uczestników, 12.3 Harmonogram szkoleń, 12.4 Harmonogram szkoleń, 12.5 UM Byczyna Zaświadczenia, 12.6 UM Byczyna Zaświadczenia, 12.7 UM w Byczynie Zaświadczenia, 12.8 UM w Byczynie Zaświadczenia, Akta kontroli - Pismo przewodnie nr OR.1710.1.2026.MC

kontrolny stwierdza jako nieprawidłowość. Z wyjaśnień Burmistrza Byczyny wynika, że w ramach aktualizacji SZBI zostaną opracowane zasady gwarantujące bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość[26]. Złożone wyjaśnienia zostały przyjęte.

W okresie objętym kontrolą miały miejsce przypadki przechodzenia na okazjonalną pracę zdalną zgodnie z 67[33] Kodeksu Pracy, co zostało potwierdzone stosowną dokumentacją[27].

9. Serwis sprzętu informatycznego i oprogramowania

Podstawa prawna:

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

W przypadku systemów informatycznych niezbędnym jest objęcie ich (w zakresie oprogramowania użytkowego i systemowego, sprzętu oraz rozwiązań telekomunikacyjnych) stosownymi umowami serwisowymi, zapewniającymi zarówno szybkie uruchomienie pracy systemu w przypadku awarii, jak i bezpieczeństwo dla informacji uzyskanych przez wykonawców w związku z ich realizacją.

W UM w Byczynie wykorzystywane są cztery systemy teleinformatyczne (w tym jeden konfiguracyjny oraz jeden archiwalny) przeznaczone do realizacji zadań zaleconych z zakresu administracji rządowej zakupione u zewnętrznego dostawcy.

W związku z powyższym, na aktualnie użytkowane systemy zostały podpisane dwie umowy licencyjne. Jedna z nich z firmą Technika IT Sp. z o.o., i druga z Zakładem Systemów Informatycznych SIGID Sp. z o.o. W przypadku obu umów zostały zawarte umowy powierzenia przetwarzania danych osobowych[28].

Dodatkowo UM w Byczynie zawarł umowę z Informatykiem, w której nie zostały zawarte zapisy dot. czasu wykonania usługi oraz kar umownych za niewykonanie lub opóźnione wykonanie zadania[29]. Brak takich zapisów stwarza ryzyko niezapewnienia ciągłości działania systemów.

[26] Akta kontroli - Pismo przewodnie nr OR.1710.1.2026.MC

[27] Akta kontroli - Uzupełnienie pisma nr OR.1710.1.2026.MC, Akta kontroli - dot. pkt 14 Wnioski praca zdalna okazjonalna, Akta kontroli - Uzupełnienie pisma nr OR.1710.1.2026.MC

[28] Akta kontroli - Dokumentacja kontrolna 1: 4.Byczyna asysta techniczna EWID, 4.Byczyna asysta techniczna PPDO, Akta kontroli - Dokumentacja kontrolna 2: 16. Umowa SIGID, Akta kontroli - Pismo przewodnie nr OR.1710.1.2026.MC

[29] Akta kontroli - Dokumentacja kontrolna 1: 6.6 Umowa ASI 2024-2025, 6.7 Umowa ASI 2025-2026

Biorąc powyższe pod uwagę, brak zapisów dot. czasu wykonania usługi oraz kar umownych za niewykonanie lub opóźnione wykonanie zadania, zespół kontrolny stwierdza jako nieprawidłowość.

10. Procedury zgłaszania incydentów naruszania BI

Podstawa prawna:

- § 19 ust. 2 pkt 13 rozporządzenie 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.

W SZBI opracowanym przez UM w Byczynie znajduje się Instrukcja postępowania w przypadku naruszenia ochrony danych osobowych oraz bezpieczeństwa informacji w Urzędzie Miejskim w Byczynie. Przedmiotowy dokument skupia się przede wszystkim na działaniach podejmowanych podczas wykrycia naruszenia ochrony danych osobowych. Z zapisów §16 ust. 8 pkt 3 wynika, że załącznikami do ww. dokumentu są: Rejestr incydentów bezpieczeństwa informacji oraz Protokół stwierdzenia wystąpienia incydentów bezpieczeństwa informacji, które nie znajdują się w przesłanej dokumentacji. Brak szczegółowego opisu reagowania na wystąpienie incydentu bezpieczeństwa informacji oraz wskazanych załączników, zespół kontrolny stwierdza jako uchybienie.

Dodatkowo analiza przedkontrolna wykazała, że w okresie objętym kontrolą nie miały miejsca przypadki wystąpienia incydentów naruszenia bezpieczeństwa informacji, jednakże z przesłanej dokumentacji wynika, że na stronie cert.pl zostały zgłoszone 3 incydenty bezpieczeństwa teleinformatycznego[30]. W związku z powyższym zespół kontrolny zwrócił się o złożenie wyjaśnień w tej kwestii. Wynika z nich, że we wszystkich 3 przypadkach nie doszło do wycieku danych osobowych ani zainfekowania urządzeń w systemie teleinformatycznym. Ponadto w wyjaśnieniach została opisana dokładna ścieżka zgłoszenia incydentów[31]. Zespół kontrolny przyjmuje powyższe wyjaśnienia, jednakże zaleca aby w UM w Byczynie sporządzono instrukcję postępowania w przypadku naruszenia, określającą w bardziej szczegółowy sposób, drogę zgłaszania incydentów naruszenia bezpieczeństwa informacji, np. zgubienie kluczy do pomieszczenia.

[30] Akta kontroli - Dokumentacja kontrolna 1: 2.Załącznik nr 2 – Ankieta dotycząca działania systemów teleinformatycznych, 17.1 Incydenty glpi, 17.2 Incydenty eport
[31] Akta kontroli - Wyjaśnienia pismo nr OR.1710.1.2026.MC

11. Audyt wewnętrzny z zakresu bezpieczeństwa informacji

Podstawa prawna:

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

Audyt bezpieczeństwa informacji jest działaniem mającym na celu zidentyfikowanie zagrożeń, które mogą powodować utratę poufności, integralności lub dostępności informacji. Celem przeprowadzenia audytu wewnętrznego bezpieczeństwa informacji jest ocena zakresu zgodności SZBI jednostki z kryteriami audytu.

W 2025 r. w UM w Byczynie nie został przeprowadzony audyt z zakresu bezpieczeństwa informacji[32], co jest niezgodne z § 19 ust. 2 pkt 14 rozporządzenia KRI. W związku z powyższym, zespół kontrolny stwierdził nieprawidłowość.

12. Kopie zapasowe

Podstawa prawna:

- § 19 ust. 2 pkt 12 lit. b rozporządzenie KRI: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na minimalizowaniu ryzyka utraty informacji w wyniku awarii.

Jednym z kluczowych sposobów zapobiegania utraty informacji w wyniku awarii jest wykonywanie kopii zapasowych. Takie działanie jest elementem planu ciągłości działania. Celem tworzenia kopii zapasowych jest możliwość odzyskania danych i przywrócenia do pracy użytkowej systemu teleinformatycznego wraz z informacjami przechowywanymi przez ten system, np. w bazie danych. Wymóg ten można osiągnąć poprzez przeprowadzanie regularnych kopii zapasowych całego środowiska pracy danego systemu teleinformatycznego, tj. systemu operacyjnego, jego konfiguracji (w tym konfiguracji zabezpieczeń), systemu informatycznego i informacji w nim przechowywanych.

W celu zapewnienia bezpieczeństwa informacji oraz systemów teleinformatycznych, w których informacje te są przetwarzane, w SZBI opracowanym w UM w Byczynie znajdują się zapisy dot. tworzenia kopii

[32] Akta kontroli - Pismo przewodnie nr OR.1710.1.2026.MC

zapasowych. Analiza powyższych zapisów wskazuje, że procedury dotyczące kopii zapasowych są zbyt ogólne, co zespół kontrolny ocenia jako uchybienie.

W wyjaśnieniach został opisany proces wykonywania kopii zapasowych[33], jednakże kontrolujący rekomendują, aby w celu zwiększenia bezpieczeństwa informacji oraz zminimalizowaniu ryzyka utraty przetwarzanych informacji w wyniku awarii, w UM w Byczynie zostały opracowane i wdrożone szczegółowe procedury uwzględniające, m.in:

- wykonywanie kopii zapasowych zgodnie z ustalonym harmonogramem;
- przywracanie danych z kopii wraz z opisaniem procedur weryfikacji;
- poprawności wykonania i przywracania kopii;
- wykonywanie kopii zapasowych poza system informatyczny przechowywanie kopii zapasowych poza siedzą urzędu.

13. Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych

Podstawa prawna:

- § 15 ust. 1 rozporządzenie 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.

W UM w Byczynie do realizacji zadań z zakresu administracji rządowej wykorzystywane są wspomagające systemy teleinformatyczne, które dzielą się na systemy centralne oraz lokalne (zakupione u dostawcy zewnętrznego).
Na obsługę zakupionych systemów informatycznych zawarte zostały stosowne umowy licencyjne, gwarantujące rozwój i dostosowanie do obowiązujących przepisów prawa. Przedmiotowe systemy teleinformatyczne zostały zaprojektowane, wdrożone i eksploatowane z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności, przenoszalności i pielęgnowalności.

14. Zabezpieczenia techniczno-organizacyjne dostępu do informacji

Podstawa prawna:

- § 19 ust. 2 rozporządzenie KRI: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez:

[33] Akta kontroli - Pismo przewodnie nr OR.1710.1.2026.MC

pkt 7 - zapewnienie ochrony przetwarzanych 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, modyfikacje, usunięcie lub zniszczenie;
pkt 11 - ustalenie zasad postępowania z informacjami, zapewniającymi minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych.

W celu uzyskania odpowiedniego poziomu BI przy jednoczesnym zapewnieniu właściwego do nich dostępu przez uprawnionych użytkowników stosowany jest szereg zabezpieczeń informatycznych. Celem takich zabezpieczeń jest uzyskanie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, a także np. kradzieżą środków przetwarzania informacji.

W UM w Byczynie zostały opracowane Procedury bezpieczeństwa fizycznego i bezpieczeństwa informacji stanowiące załącznik do PODOiBI, w których zostały określone wytyczne dot. zabezpieczeń dostępu do informacji. Opracowana dokumentacja zawiera również: Instrukcja postępowania z kluczami oraz zabezpieczenia pomieszczeń w budynku Urzędu Miejskiego w Byczynie, Rejestr pracowników/użytkowników posiadających klucze do budynku i pomieszczeń w Urzędzie Miejskim w Byczynie, Ewidencja pracowników/użytkowników posiadających klucze zapasowe od budynku i pomieszczeń w Urzędzie Miejskim w Byczynie oraz Upoważnienie do zarządzania kluczami oraz kodem cyfrowym do systemu alarmowego do budynku Urzędu Miejskiego w Byczynie wraz z Oświadczeniem pracownika[34]. W trakcie wizji lokalnej zespół potwierdził, że pracownicy po zakończonej pracy zabierają klucze do pomieszczeń Urzędu ze sobą. Pomimo sporządzenia ww. dokumentacji, zespół kontrolny rekomenduje, aby ustanowić i wdrożyć nowe, odpowiednie i proporcjonalne do wymagań Systemu Zarządzania Bezpieczeństwem Informacji UM w Byczynie zasady

[34] Akta kontroli - Dokumentacja kontrolna 2: 23. Rejestr pracowników, użytkowników posiadających klucze, 24. Ewidencja pracowników-klucze zapasowe, 25. Upoważnienia do zarządzania kluczami oraz kodem cyfrowym

postępowania z kluczami pozwalające monitorować cały proces przekazywania, przechowywania i zabezpieczenia kluczy. Dodatkowo zespół kontrolny rekomenduje, aby w analizie ryzyka zostało uwzględnione ryzyko wynikające z ww. procesu wynoszenia kluczy.

W związku z informacjami powziętymi podczas wizji lokalnej oraz zapisami zawartymi w Procedurze bezpieczeństwa fizycznego i bezpieczeństwa informacji dot. zabezpieczeń informatycznych, tj. braku blokady informatycznej nośników zewnętrznych oraz brak szyfrowania sprzętów komputerowych wynoszonych poza siedzibę budynku, zespół kontrolny stwierdza dwie nieprawidłowości[35].

15. Zabezpieczenia techniczno-organizacyjne systemów informatycznych

Podstawa prawna:

- § 19 ust. 2 pkt 12 rozporządzenie 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, utratą, 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.

Poza Zabezpieczeniami techniczno-organizacyjnymi dostępu do informacji, w PODOiBI zostały określone także zabezpieczenia dla systemów informatycznych[36].

Dodatkowo zapewniono także środki uniemożliwiające nieautoryzowany dostęp oraz zapewniające kontrolę dostępu do systemów teleinformatycznych służących

[35] Akta kontroli - Protokół oględzin
[36] Akta kontroli - Dokumentacja kontrolna 2: 26. Opis technicznych i organizacyjnych środków bezpieczeństwa

do realizacji zadań zleconych z zakresu administracji rządowej poprzez indywidualne logowanie do wybranych systemów[37].

Podczas kontroli dokonano oględzin dwóch pomieszczeń stanowiących serwerownie w UM w Byczynie. Czynność ta została przeprowadzona w obecności Informatyka oraz kierownika Referatu Organizacyjnego i Oświaty[38]. Zespół kontrolny rekomenduje, aby obie serwerownie zostały wyposażone w nowe, wzmocnione drzwi z kontrolą dostępu i rejestracją wejść i wyjść, monitoringu wewnątrz serwerowni, czujniki m.in. dymu, zawilgocenia i temperatury, ewentualny czujnik otwarcia szafy sieciowej, celem podniesienia poziomu bezpieczeństwa przetwarzanych danych.

16. Rozliczalność działań w systemach teleinformatycznych

Podstawa prawna:

- § 20 ust. 2 rozporządzenie 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 rozporządzenie 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 rozporządzenie 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.

Z dokumentacji oraz informacji uzyskanych w trakcie kontroli wynika, że UM w Byczynie odnotowuje obligatoryjne działania użytkowników

[37] Akta kontroli - Pismo przewodnie nr OR.1710.1.2026.MC
[38] Akta kontroli - Protokół oględzin

w dziennikach systemów, które są przechowywane bezterminowo, z uwagi na brak możliwości usunięcia dzienników po określonym czasie[39].

III. Zakres, przyczyny i skutki stwierdzonych nieprawidłowości oraz osoby odpowiedzialne za nieprawidłowości

W wyniku kontroli stwierdzono następujące nieprawidłowości:

1. Brak wyznaczenia Pełnomocnika ds. bezpieczeństwa informacji;
2. Brak natychmiastowego odebrania uprawnień w systemach, co narusza § 19 ust. 2 pkt 5 rozporządzenie KRI;
3. Brak ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość, co narusza § 19 ust. 2 pkt 8 rozporządzenia KRI;
4. Brak zapisów w zawartej umowie dot. czasu wykonania usługi oraz kar umownych za niewykonanie lub opóźnione wykonanie zadania, co narusza § 19 ust. 2 pkt 10 rozporządzenia KRI;
5. Brak przeprowadzenia audytu z zakresu bezpieczeństwa informacji, co narusza § 19 ust. 2 pkt 14 rozporządzenia KRI;
6. Brak blokady informatycznej nośników zewnętrznych;
7. Brak szyfrowania sprzętów komputerowych wynoszonych poza siedzibę UM w Byczynie.

Dodatkowo w wyniku kontroli zostały stwierdzone poniższe uchybienia:

1. Brak przeprowadzenia szkolenia z zakresu cyberbezpieczeństwa przez ASI, co narusza § 2 pkt 3 Procedury bezpieczeństwa fizycznego i bezpieczeństwa informacji;
2. Brak szczegółowych zapisów dot. tworzenia kopii zapasowych;
3. Brak szczegółowych zapisów dot. reagowania na wystąpienie incydentu bezpieczeństwa informacji, co narusza § 19 ust. 2 pkt 13 rozporządzenia KRI.

IV. Informacje o zastrzeżeniach zgłoszonych do projektu wystąpienia pokontrolnego i wyniku ich rozpatrzenia lub o niezgłoszeniu zastrzeżeń

[39] Akta kontroli - Dokumentacja kontrolna 2: 20.1 Log akcyza, 20.2. LOG PB EWID

W dniu 31.03.2026 r. jednostka kontrolowana wniosła zastrzeżenia do projektu wystąpienia pokontrolnego. Z uwagi na podpisanie zastrzeżeń przez Zastępcę Burmistrza Byczyny organ kontrolujący pismem z dnia 2 kwietnia 2026 r. wezwał jednostkę do przedłożenia stosownego upoważnienia w terminie 3 dni od daty otrzymania wezwania. Termin na uzupełnienie braków, po uwzględnieniu dni wolnych od pracy (zgodnie z art. 57 § 4 k.p.a.[40] w zw. z ustawą o kontroli w administracji rządowej) upłynął z dniem 7 kwietnia 2026 r. Wymagane upoważnienie wpłynęło do organu kontrolującego 8 kwietnia 2026 r., co stanowi uchybienie wyznaczonemu terminowi. W związku z powyższym, na podstawie art. 42 ust. 2 pkt 1 ustawy o kontroli w administracji rządowej, zastrzeżenia wniesione przez jednostkę kontrolowaną zostały odrzucone.

V. Zalecenia lub wnioski dotyczące usunięcia nieprawidłowości lub usprawnienia funkcjonowania jednostki kontrolowanej

W związku z ustaleniami dokonanymi podczas kontroli zalecam:

1. Wyznaczyć Pełnomocnika ds. bezpieczeństwa informacji;
2. Natychmiastowo odbierać uprawnienia w systemach;
3. Ustanowić podstawowe zasady gwarantujące bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;
4. W umowach zawrzeć zapisy dot. czasu wykonania usługi oraz kar umownych za niewykonanie lub opóźnione wykonanie zadania;
5. Przeprowadzać audyty z zakresu bezpieczeństwa informacji;
6. Zapewnić blokadę informatyczną nośników zewnętrznych;
7. Szyfrować sprzęty komputerowe wynoszone poza siedzibę UM w Byczynie.
8. Przeprowadzać szkolenia z zakresu cyberbezpieczeństwa przez ASI;
9. Stworzenie szczegółowych zapisów dot. tworzenia kopii zapasowych;
10. Stworzenie szczegółowych zapisów dot. reagowania na wystąpienie incydentu bezpieczeństwa informacji.

[40] Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (t.j. Dz.U. z 2025 r., poz. 1691)

VI. **Ocena wskazująca na niezasadność zajmowania stanowiska lub pełnienia funkcji przez osobę odpowiedzialną za stwierdzone nieprawidłowości:**
nie dotyczy.

VII. **Na podstawie art. 49 oraz art. 46 ust. 3 pkt 3 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (t.j. Dz.U. z 2020 r. poz. 224), proszę o przekazanie pisemnej informacji o sposobie wykonania zaleceń, wykorzystaniu wniosków lub przyczynach ich niewykorzystania, o podjętych działaniach lub przyczynach ich niepodjęcia, albo o innym sposobie usunięcia stwierdzonych nieprawidłowości, w terminie 90 dni od dnia otrzymania niniejszego dokumentu**.

VIII. **Zgodnie z art. 48 ustawy o kontroli, od wystąpienia pokontrolnego nie przysługują środki odwoławcze**

Z up. Wojewody Opolskiego

Joanna Sachanbińska
Dyrektor
Wydział Prawny i Nadzoru

Projekt wystąpienia pokontrolnego został wydany w postaci elektronicznej i podpisany kwalifikowanym podpisem elektronicznym.