WOJEWODA OPOLSKI

Opole, dnia 4 sierpnia 2025 r.
PN.I.431.4.2.2025.NL

Pan
Krzysztof Marek Ficoń
Wójt Gminy Bierawa
Urząd Gminy Bierawa
ul. Wojska Polskiego 12
47-240 Bierawa

WYSTĄPIENIE POKONTROLNE

I. Dane identyfikacyjne kontroli

1. Nazwa i adres jednostki kontrolowanej: Urząd Gminy Bierawa, ul. Wojska Polskiego 12, 47-240 Bierawa[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 2024 r. poz. 1557 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 2020 r. poz.224)[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

[1] UG Bierawa
[2] Dalej: ustawa o informatyzacji działalności podmiotów
[3] Dalej: ustawa o kontroli

(z uwzględnieniem okresu wcześniejszego i późniejszego w zakresie niezbędnym do realizacji celu kontroli);

4. Rodzaj kontroli: problemowa;
5. Tryb kontroli: zwykły;
6. Termin kontroli: 9 maja 2025 r. – 23 maja 2025 r., kontrola prowadzona była w trybie hybrydowym, tj. dnia 9 maja 2025 r. – rozpoczęcie czynności kontrolnych w UG Bierawa oraz oględziny serwerowni na miejscu w jednostce. Pozostałe dni (10 – 23 maja 2025 r.) 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: Pan **Krzysztof Marek Ficoń** – Wójt Gminy Bierawa, od dnia 6 maja 2024 r.[4]
9. Kontrolę wpisano do książki kontroli prowadzonej w jednostce kontrolowanej, pod poz. nr 3/2025.

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. 9 maja 2025 r. w Urzędzie Gminy Bierawa ocenia się negatywnie.

W trakcie kontroli zostały stwierdzone nieprawidłowości i uchybienie, których ilość i znaczenie dla bezpieczeństwa informacji, uniemożliwia postawienie oceny pozytywnej.

[4] Akta kontroli - Zaświadczenie o wyborze Wójta 2024, str. 163

W kontrolowanym okresie zakres działania i zadania oraz organizację i zasady funkcjonowania UG Bierawa określał Regulamin organizacyjny Urzędu Gminy Bierawa[5] stanowiący załącznik do Zarządzenia nr 7/2017 Wójta Gminy Bierawa z dnia 14 lipca 2017 r. w sprawie regulaminu organizacyjnego Urzędu Gminy Bierawa[6].

Zgodnie z § 5 pkt 1 rozdziału III Regulaminu organizacyjnego - zasady funkcjonowania Urzędu Gminy - Burmistrz jest Kierownikiem Urzędu i zwierzchnikiem służbowym wszystkich pracowników Urzędu oraz kierowników gminnych jednostek organizacyjnych.

Osobą pełniącą funkcję Administratora Systemów Informatycznych[7] jest Pracownik na stanowisku ds. informatyki i bezpieczeństwa systemów informatycznych zajmujący samodzielne stanowisko pracy w UG Bierawa.[8]

Osobą odpowiedzialną ze strony UG Bierawa za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa jest Pracownik na samodzielnym stanowisku ds. informatycznych i bezpieczeństwa systemów informatycznych. Zgłoszenie osoby do CSIRT NASK nastąpiło dnia 15 kwietnia 2025 roku.[9] Podkreślić należy fakt, że nakładająca powyższy obowiązek ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[10], weszła w życie w dniu 28 sierpnia 2018 r.

W związku z powyższym wyznaczenie, w tak późnym terminie od dnia wejścia w życie ww. ustawy, osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, zostaje stwierdzone jako nieprawidłowość.

---

[5] Dalej: Regulamin organizacyjny, aktualizowany: zarządzeniem nr 23/2018 Wójta Gminy Bierawa z dnia 27 grudnia 2018 r. w sprawie wprowadzenia zmian w regulaminie organizacyjnym Urzędu Gminy Bierawa, zarządzaniem nr 17/2019 Wójta Gminy Bierawa z dnia 30 października 2019 r. w sprawie wprowadzenia zmian w regulaminie organizacyjnym Urzędu Gminy Bierawa, zarządzaniem nr 10/2020 Wójta Gminy Bierawa z dnia 2 lipca 2020 r. w sprawie wprowadzenia zmian w regulaminie organizacyjnym Urzędu Gminy Bierawa, zarządzeniem nr 14/2020 Wójta Gminy Bierawa z dnia 1 października 2020 r. w sprawie wprowadzenia zmian w regulaminie organizacyjnym Urzędu Gminy Bierawa, zarządzeniem nr 19/2021 Wójta Gminy Bierawa z dnia 18 października 2021 r. w sprawie wprowadzenia zmian w regulaminie organizacyjnym Urzędu Gminy Bierawa, zarządzeniem nr 11/2022 Wójta Gminy Bierawa z dnia 5 września 2022 r. w sprawie wprowadzenia zmian w regulaminie organizacyjnym Urzędu Gminy Bierawa, zarządzenie nr 8/2024 Wójta Gminy Bierawa z dnia 30 sierpnia 2024 r. w sprawie wprowadzenia zmian w regulaminie organizacyjnym Urzędu Gminy Bierawa

[6] Akta kontroli - Regulamin organizacyjny UG 2017 + zmiany, str. 164-230

[7] Dalej: ASI

[8] Akta kontroli - Zakres czynności informatyka + upoważnienie, str. 231-235, Akta kontroli - Powołanie na Administratora Systemów Informatycznych, str. 249-250

[9] Akta kontroli - Zgłoszenie do NASK UG Bierawa, str. 251-252, Akta kontroli - Zarządzenie nr 13/2025, str. 381

[10] (t.j. Dz.U. z 2024 r. poz. 1077 ze zm.), dalej: ustawa o krajowym systemie cyberbezpieczeństwa

W UG Bierawa do realizacji zadań zleconych z zakresu administracji rządowej wykorzystywane są 3 systemy teleinformatyczne[11], w tym:

1. 2 o zasięgu krajowym, stanowiące rejestry publiczne;
2. 1 o zasięgu lokalnym.

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[12] UG Bierawa została udostępniona Elektroniczna Skrzynka Podawcza[13]: /792mxfq6mg/SkrytkaESP, znajdująca się na Elektronicznej Platformie Usług Administracji Publicznej[14], pozwalająca na wysyłanie i odbieranie pism w formie dokumentów elektronicznych. Dodatkowo na BIP został udostępniony adres do doręczeń elektronicznych, tj. AE:PL-72201-44359-AVVHG-17, który UG Bierawa posiada zgodnie z art. 8 ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (t.j. Dz.U. z 2024 r. poz. 1045 ze zm.).

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[15]: Zarządzanie bezpieczeństwem informacji[16] 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

[11] Akta kontroli - Zestawienie systemów teleinformatycznych, str. 18-19
[12] Dalej: BIP
[13] Dalej: ESP
[14] Dalej: ePUAP
[15] Dz.U. z 2024 r. poz. 773, dalej: Rozporządzenie KRI
[16] Dalej: BI

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 trakcie kontroli od Wójta Gminy Bierawa wynika, że w UG Bierawa podstawowym sposobem dokumentowania przebiegu załatwiania i rozstrzygania spraw jest tradycyjny (tj. papierowy) system wykonywania czynności kancelaryjnych[17].

Zgodnie z zapisami § 54 ust. 2 Regulaminu organizacyjnego zasady i tryb wykonywania czynności kancelaryjnych określa instrukcja kancelaryjna.[18]

3. 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 rozporządzenia 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 rozporządzenia 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[19], 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.

[17] Akta kontroli - Odpowiedź na pismo nr PN.I.431.4.2.2025, str. 292-294
[18] Akta kontroli - Regulamin organizacyjny UG 2017 + zmiany, str. 164-230
[19] Dalej: SZBI

Podstawowym elementem SZBI jest Polityka Bezpieczeństwa Informacji[20], 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.

W trakcie kontroli ustalono, że w UG Bierawa nie został opracowany i ustanowiony, wdrożony i eksploatowany, monitorowany i przeglądany oraz utrzymywany i doskonalony SZBI.

Z dokumentacji przekazanej kontrolerom wynika, że zostało wprowadzone Zarządzenie nr 16/2021 Wójta Gminy Bierawa z dnia 18 października 2021 r. w sprawie wdrożenia dokumentacji dotyczącej ochrony danych w Urzędzie Gminy Bierawa, polityki bezpieczeństwa informacji i instrukcji zarządzania systemem informatycznym[21].

Z dokumentacji kontrolnej nie wynika, aby ww. zarządzenie było monitorowane, poddawane przeglądom ani doskonalone. W związku z powyższym zwrócono się o złożenie wyjaśnień, z których wynika, że „Zarządzenie nr 16/2021 Wójta Gminy Bierawa z dnia 18.10.2021 r. jest weryfikowane i aktualizowane poprzez bieżącą aktualizację jego załączników – formularzy 1 do 20, przykładowo w momencie zmiany pracowników, nadawania lub cofania upoważnień dla pracowników, aktualizacji zbiorów danych osobowych. (…) Ostatnia aktualizacja załączników dokonana była w dniu 12.05.2025 r. w związku z zatrudnieniem nowego pracownika.”[22] Pomimo złożonych wyjaśnień, zespół kontrolny nie otrzymał dokumentacji potwierdzającej przeprowadzenie wskazanych czynności.

[20] Dalej: PBI

[21] Akta kontroli - Zarządzenie nr 16/2021 w sprawie wdrożenia dokumentacji ochrony danych, str. 20-43, Akta kontroli - Formularze (załączniki do zarządzenia nr 16/2021), str. 301-316, Akta kontroli - Formularze (załączniki do zarządzenia nr 16/2021), str. 317-324, Dalej: zarządzenie w sprawie wdrożenia dokumentacji dotyczącej ochrony danych, polityki bezpieczeństwa informacji i instrukcji zarządzania systemem informatycznym

[22] Akta kontroli - Odpowiedź na pismo nr PN.I.431.4.2.2025, str. 292-294

W związku z powyższym przedmiotowe wyjaśnienia nie zostały przyjęte przez zespół kontrolny.

Dodatkowo kontrolerom została przekazana lista pracowników, którzy zapoznali się z ww. zarządzeniem[23]. W dokumentacji kontrolnej znajdują się również oświadczenia o zaznajomieniu się z przepisami dotyczącymi ochrony danych osobowych, stanowiące załącznik nr 6 do zarządzenia w sprawie wdrożenia dokumentacji dotyczącej ochrony danych, polityki bezpieczeństwa informacji i instrukcji zarządzania systemem informatycznym.[24]

W zakresie dokumentacji z zakresu bezpieczeństwa informacji, zespół kontrolny stwierdził dwie nieprawidłowości. Pierwszą z nich jest brak opracowania, ustanowienia, wdrożenia i eksploatowania, monitorowania i przeglądania oraz utrzymania i doskonalenia SZBI. Natomiast druga to brak przeprowadzania przeglądów zarządzenia w sprawie wdrożenia dokumentacji dotyczącej ochrony danych, polityki bezpieczeństwa informacji i instrukcji zarządzania systemem informatycznym wraz z jego załącznikami.

4. 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 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

[23] Akta kontroli - Potwierdzenie zapoznania się z zarządzeniem nr 16/2021, str. 342-343
[24] Akta kontroli - Oświadczenia pracowników o ochronie danych osobowych, str. 333-339

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

Z dokumentacji przedstawionej kontrolerom wynika, że ostatnia analiza ryzyka została przeprowadzona w 2021 r.[25] W związku z powyższym zwrócono się do Wójta Gminy Bierawa o złożenie wyjaśnień w przedmiotowym zakresie. Wynika z nich, że: „Analiza ryzyka, która planowana była do wykonania w IV kwartale 2024 r. nie została przeprowadzona, z uwagi na fakt wystąpienia powodzi na terenie gminy i nawarstwienie spraw związanych z usuwaniem jej skutków (…)”[26]. Powyższe wyjaśnienia zostały przyjęte przez zespół kontrolny. Jednakże z zakresów czynności zarówno Inspektora Ochrony Danych[27], jak i ASI widnieją zapisy o przeprowadzaniu co najmniej raz w roku analizy ryzyka[28]. Co prawda nie istnieje podstawa prawna określająca częstotliwość dokonywania analizy ryzyka, jednak zalecane jest przeprowadzanie jej co najmniej raz w roku oraz dodatkowo w przypadku wystąpienia naruszenia ochrony danych osobowych. W związku z powyższym brak przeprowadzania analiz ryzyka co roku, a także ostatnie jej przeprowadzanie w roku 2021, zostaje stwierdzone jako nieprawidłowość.

5. Inwentaryzacja sprzętu i oprogramowania informatycznego

Podstawa prawna:

- § 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.

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, tj. szczegółowe dane o urządzeniach technicznych, oprogramowaniu i środkach komunikacji, ich rodzaju, parametrach, aktualnej konfiguracji i relacjach między elementami konfiguracji oraz użytkowniku. Stworzona baza ma na celu podejmowanie właściwych decyzji i działań w zakresie zmian w środowisku teleinformatycznym.

[25] Akta kontroli - Analiza ryzyka 2021, str. 44-46, Akta kontroli - Mapa ryzyka, str. 47
[26] Akta kontroli - Odpowiedź na pismo nr PN.I.431.4.2.2025, str. 292-294
[27] Akta kontroli - Powołanie inspektora ochrony danych, str. 246-248, Akta kontroli - Zakres czynności inspektora ochrony danych, str. 236-245, Dalej: IOD
[28] Akta kontroli - Powołanie na Administratora Systemów Informatycznych, str. 249-250

W UG Bierawa sporządzany jest wykaz oprogramowań używanych przez pracowników do wykonywania zadań zleconych z zakresu administracji rządowej. Ostatni taki dokument sporządzony został w 2024 r.[29] Dodatkowo z dokumentacji przekazanej kontrolerom wynika, że wykaz sprzętu tworzony jest na podstawie oprogramowania antywirusowego, firewalla oraz dodatkowego darmowego oprogramowania[30].

6. 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: 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 UG Bierawa realizujący zadania zlecone z zakresu administracji rządowej posiadają upoważnienia do przetwarzania informacji wraz z odpowiednimi uprawnieniami w systemach[31].

W okresie objętym kontrolą miał miejsce przypadek nadania i cofania uprawnień dostępu do systemu SRP, co zostało potwierdzone stosowną dokumentacją[32].

---

[29] Akta kontroli - Wykaz oprogramowania, str. 353-354
[30] Akta kontroli - Wykaz sprzętu, str. 356-368
[31] Akta kontroli - A.M. Zakres obowiązków + upoważnienia, str. 253-259, Akta kontroli - M.M. zakres obowiązków + upoważnienia, str. 260-264, Akta kontroli - Upoważnienie do CEIDG - BZ, str. 265, Akta kontroli - Upoważnienie do CEIDG - BG, str. 266, Akta kontroli - Upoważnienie dot. wprowadzania danych do SRPP akcyza, str. 267
[32] Akta kontroli - Wniosek o nadanie uprawnień, str. 386-387, Akta kontroli - Wniosek o usunięcie uprawnień, str. 388-389, Akta kontroli - Odpowiedź na pismo nr PN.I.431.4.2.2025, str. 385

7. 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.

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 bezpieczeństwa informacji oraz zabezpieczenia przed takimi incydentami, szkolenia osób zaangażowanych w proces przetwarzania informacji powinny być przeprowadzane cyklicznie.

W okresie objętym kontrolą odbyły się dwa szkolenia wewnętrzne przeprowadzone przez ASI. Pierwsze z nich w przedmiocie „Cyberbezpieczeństwo w pracy urzędu", natomiast drugie w zakresie „Bezpieczeństwo pracy w systemach teleinformatycznych i bezpieczeństwo danych"[33].

W § 6 PBI zarządzenia w sprawie wdrożenia dokumentacji dotyczącej ochrony danych, polityki bezpieczeństwa informacji i instrukcji zarządzania systemem informatycznym dot. szkoleń pracowników zawarta jest informacja o przeprowadzaniu na polecenie Administratora, osobiście lub przy wykorzystaniu podmiotu zewnętrznego okresowych szkoleń pracowników w zakresie przepisów prawa oraz uregulowań wewnętrznych przez IOD.

Pomimo realizowania regularnych szkoleń w zakresie cyberbezpieczeństwa i bezpieczeństwa danych, nieprzeprowadzanie ich przez IOD, który zgodnie z zapisami PBI winien organizować szkolenia z ochrony danych osobowych co najmniej raz w roku, zespół kontrolny stwierdza to jako uchybienie.

8. Praca na odległość i mobilne przetwarzanie danych

Podstawa prawna:

[33] Akta kontroli - Listy obecności i zakresy tematyczne szkoleń, str. 325-331

- § 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.

W UG Bierawa zostały ustanowione podstawowe zasady gwarantujące bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość określone w Regulaminie Pracy Zdalnej stanowiącym załącznik do Zarządzenia nr 3/2025 Wójta Gminy Bierawa z dnia 3.01.2025 r. w sprawie wprowadzenia regulaminu pracy zdalnej dla pracowników Urzędu Gminy Bierawa[34]. Z dokumentacji wynika, że pracownicy UG Bierawa zapoznali się z Regulaminem Pracy Zdalnej oraz zobowiązali się do przestrzegania ustaleń w nim zawartych[35].

9. 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.

W przypadku systemów informatycznych niezbędnym jest objęcie ich (w zakresie oprogramowania użytkowego i systemowego, sprzętu oraz rozwiązań telekomunikacyjnych) stosowanymi 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 UG Bierawa wykorzystywany jest jeden system teleinformatyczny przeznaczony do realizacji zadań zaleconych z zakresu administracji rządowej zakupiony u zewnętrznego dostawcy. W związku z tym została podpisana stosowana umowa licencyjna wraz z umową powierzenia przetwarzania danych osobowych, które gwarantują odpowiedni poziom bezpieczeństwa informacji[36].

10. Procedury zgłaszania incydentów naruszania BI

Podstawa prawna:

- § 19 ust. 2 pkt 13 rozporządzenia KRI: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: bezzwłoczne zgłaszanie

[34] Akta kontroli - Zarządzenie w spr. wprowadzenia regulaminu pracy zdalnej, str. 367-380
[35] Akta kontroli - Potwierdzenie zapoznania się (praca zdalna), str. 341
[36] Akta kontroli - Umowa na serwis programu podatki, str. 344-346, Akta kontroli - Umowa powierzenia przetwarzania danych, str. 347-352

incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.

W zarządzeniu w sprawie wdrożenia dokumentacji dotyczącej ochrony danych, polityki bezpieczeństwa informacji i instrukcji zarządzania systemem informatycznym nie znajdują się zapisy związane ze zgłaszaniem incydentów naruszenia bezpieczeństwa informacji.

Z zakresów tematycznych przeprowadzonych szkoleń wynika, że na ostatnim takim spotkaniu zostały omówione zagrożenia cyberbezpieczeństwa oraz sposób reagowania na nie.

Z informacji uzyskanych z UG Bierawa wynika, że w okresie objętym kontrolą nie miały miejsca przypadki wystąpienia incydentów naruszenia bezpieczeństwa informacji.

Brak zapisów dot. reagowania na incydenty w zarządzeniu w sprawie wdrożenia dokumentacji dotyczącej ochrony danych, polityki bezpieczeństwa informacji i instrukcji zarządzania systemem informatycznym, zostaje stwierdzone przez zespół kontrolny jako nieprawidłowość.

11. 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.

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.

Z dokumentacji przekazanej kontrolerom wynika, że ostatni audyt przeprowadzony przez firmę zewnętrzną odbył się w 2022 roku[37]. Dodatkowo w 2024 roku IOD zatrudniony w UG Bierawa przeprowadził audyt KRI[38].

12. Kopie zapasowe

Podstawa prawna:

[37] Akta kontroli - Audyt cyberbezpieczeństwa, str. 48-129, Akta kontroli - Formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa, str. 130, Akta kontroli - Zestawienie wykrytych podatności hostów sieci IT, str. 131-150
[38] Akta kontroli - Audyt KRI 2024, str. 151-162

- § 19 ust. 2 pkt 12 lit. b rozporządzenia 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 BI oraz systemów teleinformatycznych, w których informacje te są przetwarzane, UG Bierawa sporządził procedury tworzenia kopii awaryjnych określone w § 6 Instrukcji zarządzania systemem informatycznym Urzędu Gminy Bierawa zarządzenia w sprawie wdrożenia dokumentacji dotyczącej ochrony danych, polityki bezpieczeństwa informacji i instrukcji zarządzania systemem informatycznym.

13. 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.

W UG Bierawa 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 zakupionego systemu informatycznego zawarta została stosowna umowa licencyjna, gwarantująca 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 rozporządzenia KRI: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez:
  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.

Środki organizacyjne i techniczne ochrony danych osobowych zawarte zostały w rozdziale II - PBI - zarządzenia w sprawie wdrożenia dokumentacji dotyczącej ochrony danych, polityki bezpieczeństwa informacji i instrukcji zarządzania systemem informatycznym.

W przedmiotowym zarządzeniu zostały także opracowane zasady postępowania z kluczami do pomieszczeń oraz biurek i szaf stanowiskowych wraz z osobami odpowiedzialnymi za nie. W dokumentacji kontrolnej znajduje się wykaz pracowników UG Bierawa upoważnionych do otwierania i zamykania budynku Urzędu, a także ewidencja wydawania i zwrotów kluczy do drzwi wejściowych[39].

15. Zabezpieczenia techniczno-organizacyjne systemów informatycznych

Podstawa prawna:

- § 19 ust. 2 pkt 12 rozporządzenia KRI: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie odpowiedniego

[39] Akta kontroli - Ewidencja kluczy do budynku Urzędu, str. 299-300, Akta kontroli - Wykaz pracowników upoważnionych do otwierania budynku, str. 355

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 środkami ochrony danych osobowych zostały określone także zabezpieczenia dla systemów informatycznych, które opisano w rozdziale III – Instrukcja zarządzania systemem informatycznym - zarządzenia w sprawie wdrożenia dokumentacji dotyczącej ochrony danych, polityki bezpieczeństwa informacji i instrukcji zarządzania systemem informatycznym.

Dodatkowo zapewniono także środki uniemożliwiające nieautoryzowany dostęp oraz zapewniające kontrolę dostępu do systemów teleinformatycznych służących do realizacji zadań zleconych z zakresu administracji rządowej poprzez indywidualne logowanie do wybranych systemów[40].

Podczas kontroli dokonano oględzin pomieszczenia serwerowni w UG Bierawa. Czynność ta została przeprowadzona w obecności Pracownika na stanowisku ds. informatyki i bezpieczeństwa systemów informatycznych oraz IOD[41].

16. 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,

[40] Akta kontroli - Sposób logowania do systemów, str. 332
[41] Dokument „Protokół oględzin serwerowni”, str. 290.

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.

Z dokumentacji oraz informacji uzyskanych w trakcie kontroli wynika, że UG Bierawa odnotowuje obligatoryjne działania użytkowników w dziennikach systemów[42].

Dodatkowo, z wyjaśnień Wójta Gminy Bierawa wynika, że „Informacje w dziennikach systemów są przechowywane przez okres 2 lat”[43].

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

W wyniku kontroli stwierdzono następujące nieprawidłowości:

1. Wyznaczenie osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa w dniu 15 kwietnia 2025 r., pomimo wejścia w życie ustawy o krajowym systemie cyberbezpieczeństwa w dniu 28 sierpnia 2018 r.
2. Brak opracowania, ustanowienia, wdrożenia i eksploatowania, monitorowania i przeglądania oraz utrzymania i doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji, co narusza § 19 ust. 1 i 2 rozporządzenia KRI;
3. Brak przeprowadzania przeglądów zarządzenia w sprawie wdrożenia dokumentacji dotyczącej ochrony danych, polityki bezpieczeństwa informacji i instrukcji zarządzania systemem informatycznym wraz z jego załącznikami, co narusza § 19 ust. 2 pkt 1 rozporządzenia KRI;
4. Przeprowadzanie ostatniej analizy ryzyka w 2021 roku, co jest niezgodnie z zapisami zakresów czynności IOD i ASI;

[42] Akta kontroli - Dziennik logowania (program podatki), str. 295-298
[43] Akta kontroli - Odpowiedź na pismo nr PN.I.431.4.2.2025, str. 385

5. Brak zapisów dot. reagowania na incydenty w zarządzeniu w sprawie wdrożenia dokumentacji dotyczącej ochrony danych, polityki bezpieczeństwa informacji i instrukcji zarządzania systemem informatycznym.
6. Dodatkowo w wyniku kontroli zostało stwierdzone uchybienie polegające na braku przeprowadzania szkoleń z zakresu ochrony danych osobowych przez IOD, zgodnie z zapisami § 5 i § 6 rozdziału II - PBI - zarządzenia w sprawie wdrożenia dokumentacji dotyczącej ochrony danych, polityki bezpieczeństwa informacji i instrukcji zarządzania systemem informatycznym.

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

Kierownik jednostki kontrolowanej nie zgłosił zastrzeżeń do projektu wystąpienia pokontrolnego.

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

W związku z ustaleniami dokonanymi podczas kontroli zalecam:

1. Opracować, ustanowić, wdrożyć i eksploatować, monitorować i przeglądać oraz utrzymywać i doskonalić System Zarządzania Bezpieczeństwem Informacji;
2. Przeprowadzać przeglądy zarządzenia w sprawie wdrożenia dokumentacji dotyczącej ochrony danych, polityki bezpieczeństwa informacji i instrukcji zarządzania systemem informatycznym wraz z jego załącznikami;
3. Przeprowadzić analizę ryzyka;
4. Sporządzić wytyczne dot. reagowania na incydenty;
5. Przeprowadzać szkolenia z zakresu ochrony danych osobowych przez IOD.

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
radca prawny
Dyrektor
Wydział Prawny i Nadzoru