WOJEWODA OPOLSKI

Opole, dnia 13 maja 2025 r.
PN.I.431.4.1.2025.NL

Pan
Edward Plicko
Burmistrz Białej
Urząd Miejski w Białej
ul. Rynek 10
48-210 Biała

WYSTĄPIENIE POKONTROLNE

I. Dane identyfikacyjne kontroli

1. Nazwa i adres jednostki kontrolowanej: Urząd Miejski w Białej, ul. Rynek 10, 48-210 Biała[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)[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 2024 r. do dnia rozpoczęcia kontroli

[1] UM w Białej
[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: 19 marca 2025 r. – 31 marca 2025 r., kontrola prowadzona była w trybie hybrydowym, tj. dnia 19 marca 2025 r. – rozpoczęcie czynności kontrolnych w UM w Białej oraz oględziny serwerowni na miejscu w jednostce. Pozostałe dni (20 – 31 marca 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 Edward Plicko – Burmistrz Białej, od dnia 7 maja 2024 r.[4]
9. Kontrolę wpisano do książki kontroli prowadzonej w jednostce kontrolowanej, pod poz. nr 1/2025.

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 Urzędzie Miejskim w Białej ocenia się pozytywnie z uchybieniami.

W kontrolowanym okresie zakres działania i zadania oraz organizację i zasady funkcjonowania Urzędu Miejskiego w Białej określał Regulamin organizacyjny

[4] Folder „Dokumenty do UW.zip": Folder „Dodatkowa dokumentacja": Pliki „Wybór Burmistrza – Zaświadczenie", „Wybór Burmistrza - Wyciąg z protokołu"

Urzędu Miejskiego w Białej[5] stanowiący załącznik do Zarządzenia nr OR.120.16.2020 Burmistrza Białej z dnia 27 lipca 2020 r. w sprawie nadania Regulaminu Organizacyjnego Urzędowi Miejskiemu w Białej.

Zgodnie z § 7 pkt 3 rozdziału 2 dot. postanowień ogólnych Regulaminu organizacyjnego, Burmistrz jest kierownikiem Urzędu i zwierzchnikiem służbowym wszystkich pracowników Urzędu i kierowników gminnych jednostek organizacyjnych. Dodatkowo z § 7 pkt 4 ww. Regulaminu organizacyjnego wynika, że w razie nieobecności Burmistrza, jego obowiązki pełni Zastępca Burmistrza.[6]

Osobą pełniącą funkcję Administratora Systemów Informatycznych[7] jest Pracownik na stanowisku ds. informatycznych zajmujący samodzielne stanowisko pracy w UM w Białej. Dodatkowo w celu zapewnienia ciągłości działania Urzędu, funkcję ASI w przypadkach absencji ww. osoby pełni pracownik zatrudniony na umowę zlecenie w zakresie obsługi informatycznej.[8]

Pracownikiem odpowiedzialnym ze strony UM w Białej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, na podstawie zarządzenia nr OR.120.15.2019 Burmistrza Białej z dnia 29 marca 2019 r. w sprawie wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, jest Pracownik na samodzielnym stanowisku ds. informatycznych. Zgłoszenie osób do CSIRT NASK nastąpiło dnia 23 września 2019 roku.[9]

---

[5] Dalej: Regulamin organizacyjny, aktualizowany: zarządzeniem nr OR.120.12.2021 Burmistrza Białej z dnia 29 czerwca 2021 r. w sprawie wprowadzenia zmian w Regulaminie Organizacyjnym Urzędu Miejskiego w Białej, zarządzeniem nr OR.120.26.2021 Burmistrza Białej z dnia 30 listopada 2021 r. w sprawie wprowadzenia zmian w Regulaminie Organizacyjnym Urzędu Miejskiego w Białej, zarządzeniem nr OR.120.30.2021 Burmistrza Białej z dnia 20 grudnia 2021 r. w sprawie zmiany Regulaminu Organizacyjnego Urzędu Miejskiego w Białej, zarządzeniem nr OR.120.21.2022 Burmistrza Białej z dnia 5 sierpnia 2022 r. w sprawie zmiany Regulaminu Organizacyjnego Urzędu Miejskiego w Białej, zarządzeniem nr OR.120.33.2022 Burmistrza Białej z dnia 27 grudnia 2022 r. w sprawie zmiany Regulaminu Organizacyjnego Urzędu Miejskiego w Białej, zarządzeniem nr OR.120.12.2023 Burmistrza Białej z dnia 14 kwietnia 2023 r. w sprawie zmiany Regulaminu Organizacyjnego Urzędu Miejskiego w Białej, zarządzeniem nr OR.120.15.2023 Burmistrza Białej z dnia 12 czerwca 2023 r. w sprawie zmiany Regulaminu Organizacyjnego Urzędu Miejskiego w Białej, zarządzeniem nr OR.120.19.2023 Burmistrza Białej z dnia 28 sierpnia 2023 r. w sprawie zmiany Regulaminu Organizacyjnego Urzędu Miejskiego w Białej, zarządzeniem nr OR.120.13.2024 Burmistrza Białej z dnia 9 października 2024 r. w sprawie zmiany Regulaminu Organizacyjnego Urzędu Miejskiego w Białej

[6] Folder „Dokumenty do UW.zip": Folder „Dodatkowa dokumentacja": Plik „Regulamin organizacyjny"

[7] Dalej: ASI

[8] Folder „Dokumenty do UW.zip": Folder „Dodatkowa dokumentacja": Pliki: „Starszy Informatyk - Zakres obowiązków i uprawnień", „Umowa OR.2151.1.2025 - ASI w ramach ciągłości działania"

[9] Folder „Dokumenty do UW.zip": Folder „Dodatkowa dokumentacja": Pliki: „Zarządzenie OR.120.15.2019 - Krajowy System Cyberbezpieczeństwa", „Zgłoszenie do NASK"

Z informacji przekazanych podczas kontroli wynika, że w UM w Białej do realizacji zadań zleconych z zakresu administracji rządowej wykorzystywane jest 5 systemów teleinformatycznych[10]:

1. SRP (System Rejestrów Państwowych) – to system organizacyjno-techniczny wykorzystywany do prowadzenia rejestrów publicznych, na podstawie art. 13b ust. 1 ustawy o informatyzacji działalności podmiotów. Przedmiotowy system jest połączeniem najważniejszych polskich rejestrów, tj. Rejestr PESEL, Rejestr Dowodów Osobistych, Rejestr Dokumentów Paszportowych, Rejestr Stanu Cywilnego, Rejestr Danych Kontaktowych, System Odznaczeń Państwowych, Centralny Rejestr Sprzeciwów, Centralny Rejestr Wyborców, a także Rejestr zastrzegania numerów PESEL.
2. PB_EWID_SRP – oprogramowanie PB_EWID wspiera prowadzenie gminnego rejestru mieszkańców oraz umożliwia tworzenie spisów i zestawień danych zaczerpniętych z ww. rejestrów. Dodatkowo oprogramowanie to dostarczane jest z oddzielnym modułem PB_EWID_SRP, który wspomaga system SRP poprzez zaciąganie danych z niego dot. ewidencji ludności oraz rejestru wyborców.
3. Karta Dużej Rodziny – jest to system służący do realizacji zadań wynikających z ustawy z dnia 5 grudnia 2014 r. o Karcie Dużej Rodziny (Dz.U. z 2014 r. poz. 1863). System umożliwia wykonywanie ustawowych zadań, np. rejestrowanie wniosków o przyznanie Karty Dużej Rodziny, w sposób elektroniczny. Dodatkowo służy do przekazywania danych do SI KDR w celu nadania uprawnień wynikających z posiadania Karty Dużej Rodziny.
4. CEIDG (Centralna Ewidencja i Informacja o Działalności Gospodarczej) – jest to elektroniczny rejestr przedsiębiorców działających w Polsce. Portal pozwala na założenie firmy, aktualizację danych, a także na zawieszenie, wznowienie lub zamknięcie działalności gospodarczej. Dodatkowo wykorzystywany jest do przekazywania informacji o wydanych zezwoleniach, koncesjach oraz wpisach do rejestrów.
5. Podatki-osoby fizyczne – jest to system mający na celu obsługę w zakresie podatku akcyzowego.

1. Elektroniczna skrzynka podawcza

Podstawa prawna:

[10] Folder „Dokumenty do UW.zip”: Plik „Zestawienie systemów teleinformatycznych używanych do realizacji zadań zleconych z zakresu administracji rządowej - podpis”

- 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.

UM w Białej posiada Elektroniczną Skrzynkę Podawczą[11]: /qnfj0i259v/SkrytkaESP, znajdującą się na Elektronicznej Platformie Usług Administracji Publicznej[12], pozwalającą na wysyłanie i odbieranie pism w formie dokumentów elektronicznych. Na stronie głównej Biuletynu Informacji Publicznej[13] UM w Białej został udostępniony zarówno adres ESP, jak i adres stosowany do doręczeń elektronicznych, tj. AE:PL-81790-69023-CJVAJ-21. Dodatkowo na portalu internetowym UM w Białej zamieszczono odnośnik do Elektronicznego Biura Obywatela, z którego istnieje możliwość przekierowania na stronę ePUAP, w celu załatwienia spraw urzędowych w sposób elektroniczny. Ponadto na stronie BIP Biała zamieszczony jest wykaz formatów danych przyjmowanych za pośrednictwem ESP, są to:

- Dane zawierające dokumenty tekstowe lub tekstowo graficzne: TXT, DOC, RTF, XLS, PDF, PPT, XPS, ODT, ODS, ODP, DOCX, XLSX, PTTX, CSV;
- Grafika: JPG(JPEG), TIF(TIFF), GEOTIFF, PNG, SVG;
- Dane zawierające informację dźwiękową lub filmową: WAV, MP3, AVI, MPG, MPEG, MP4, M4A, MPEG4, OGG, OGV;
- Dane skompresowane: ZIP, TAR, GZ(GZIP), 7Z.[14]

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.

[11] Dalej: ESP
[12] Dalej: ePUAP
[13] Dalej: BIP
[14] informacje z BIP Biała, Folder „Dokumenty do UW.zip": Plik „Ankieta dotycząca działania systemów teleinformatycznych - podpis"
[15] Dz.U. z 2024 r. poz. 773, dalej: Rozporządzenie KRI
[16] Dalej: BI

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.

Jak wynika z Zarządzenia nr OR.120.21.2020 Burmistrza Białej z dnia 3 września 2020 r. w sprawie czynności kancelaryjnych, obiegu korespondencji w Urzędzie Miejskim w Białej, podstawowym sposobem dokumentowania przebiegu załatwiania i rozstrzygania spraw jest tradycyjny (tj. papierowy) system wykonywania czynności kancelaryjnych. System elektroniczny pełni rolę systemu wspomagającego. W ramach zarządzania obiegiem dokumentacji w UM w Białej wykorzystywany jest system Elektronicznego Zarządzania Dokumentacją (EZD) - SOD 365 (System Obsługi Dokumentów).[17]

Zasady i procedury obiegu dokumentów oraz wykonywania czynności kancelaryjnych opisane zostały w § 46 - § 51 rozdziału 8 - Obieg dokumentów w Urzędzie - Regulaminu organizacyjnego.[18]

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 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;

[17] Folder „Dokumenty do UW.zip”: Folder „Dodatkowa dowodowa”: Plik „Zarządzenie nr OR.120.21.2020 w sprawie czynności kancelaryjnych i obiegu korespondencji”
[18] Folder „Dokumenty do UW.zip”: Folder „Dodatkowa dokumentacja”: Plik: „Regulamin organizacyjny”

- § 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[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.

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. Zazwyczaj w ramach SZBI funkcjonują inne polityki, regulaminy i procedury, np.:

- Polityka bezpieczeństwa teleinformatycznego;
- Polityka bezpieczeństwa fizycznego;
- Polityka bezpieczeństwa danych osobowych;
- Procedura zarządzania ryzykiem;
- Regulamin korzystania z zasobów informatycznych;
- Procedura zarządzania sprzętem i oprogramowaniem;
- Procedura zarządzania konfiguracją;
- Procedura zarządzania uprawnieniami do pracy w systemach teleinformatycznych;
- Procedura monitorowania poziomu świadczenia usług;
- Procedura bezpiecznej utylizacji sprzętu elektronicznego;
- Procedura zarządzania zmianami i wykonywania testów;
- Procedura stosowania środków kryptograficznych;
- Procedura określania specyfikacji technicznych wymagań odbioru systemów IT;

[19] Dalej: SZBI
[20] Dalej: PBI

- Procedura zgłaszania i obsługi incydentów naruszenia bezpieczeństwa informacji;
- Procedura wykonywania i testowania kopii bezpieczeństwa;
- Procedura monitoringu i kontroli dostępu do zasobów teleinformatycznych, prowadzenia logów systemowych.

Dodatkową dokumentację SZBI stanowią także:

- Dokumentacja z przeglądów SZBI;
- Dokumentacja z szacowania ryzyka bezpieczeństwa informacji;
- Dokumentacja postępowania z ryzykiem;
- Dokumentacja akceptacji ryzyka;
- Dokumentacja audytów z zakresu BI;
- Dokumentacja incydentów naruszania BI;
- Dokumentacja zarządzania uprawnieniami do pracy w systemach teleinformatycznych;
- Dokumentacja zarządzania sprzętem i oprogramowaniem teleinformatycznym;
- Dokumentacja szkolenia pracowników zaangażowanych w proces przetwarzania informacji.

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 UM w Białej został opracowany i ustanowiony, wdrożony i eksploatowany, monitorowany i przeglądany oraz utrzymywany i doskonalony System Zarządzania Bezpieczeństwem Informacji, który został wprowadzony zarządzeniem nr OR.120.8.2021 Burmistrza Białej z dnia 1 marca 2021 r. w sprawie ustanowienia Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miejskim w Białej[21]. Ponadto w związku z aktualizacją normy PN-EN ISO/IEC 27001:2023, w UM w Białej obowiązuje nowa wersja SZBI wprowadzona zarządzeniem nr OR.120.1.2025 Burmistrza Białej z dnia 2 stycznia 2025 r. w sprawie ustanowienia Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miejskim w Białej.[22] Z Raportu z przeglądu dokumentacji wymagań Systemu Zarządzania Bezpieczeństwem Informacji oraz Raportu

[21] Folder „Dokumenty do UW.zip”: Folder „Dokumentacja wymagań SZBI 27001_2023”, Folder „Dodatkowa dowodowa”: Plik: „Zarządzenie w sprawie ustanowienia Systemu Zarządzania Bezpieczeństwem Informacji z dnia 1 marca 2021”,
[22] Folder „Dokumenty do UW.zip”: Folder „Dodatkowa dowodowa”: Pliki: „Zarządzenie w sprawie ustanowienia Systemu Zarządzania Bezpieczeństwem Informacji z dnia 2 stycznia 2025”

z przeglądu udokumentowanych informacji systemu zarządzania bezpieczeństwem informacji wynika, że ostatni przegląd SZBI odbył się w marcu 2025 r.[23] Dodatkowo w październiku 2024 r. został sporządzony Raport z przeglądu zarządzania[24].

Z dokumentacji przekazanej kontrolerom wynika, że na SZBI składają się Polityka Ochrony Danych Osobowych oraz Polityka Bezpieczeństwa Informacji wraz z politykami towarzyszącymi i inni dokumentami, m.in. Polityką Zarządzania Ryzykiem w Bezpieczeństwie Informacji, Polityką Bezpieczeństwa Fizycznego i Środowiskowego, Polityką Kontroli Dostępu do Systemów Informatycznych, Polityką Zapasowych Kopii Informacji, itp.

Dodatkowo w dokumentacji przekazanej kontrolerom znalazły się oświadczenia o przestrzeganiu wymagań dotyczących bezpieczeństwa informacji.[25]

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 na przeciwdziałanie zagrożeniom oraz ograniczenie skutków zmaterializowanych ryzyk, a także wpływa na racjonalne zarządzenie środkami finansowymi poprzez stosowanie zabezpieczeń adekwatnych do oszacowanego poziomu ryzyka. Jednocześnie należy zaznaczyć, że prawidłowość przeprowadzenia analizy ryzyka polega na jego regularnym i ciągłym monitorowaniu.

[23] Folder „dokumenty kontrolne.7z": Pliki: „Raport z przeglądu dokumentacji – 2025", „Raport z przeglądu dokumentacji – 2024"
[24] Folder „Dokumenty do UW.zip": Folder „Dodatkowa dowodowa": Plik „Raport z przeglądu zarządzania"
[25] Folder „Dokumenty do UW.zip": Folder „Dodatkowa dowodowa": Plik „Oświadczenia o przestrzeganiu wymagań dotyczących bezpieczeństwa informacji"

W UM w Białej została wprowadzona Polityka Zarządzania Ryzykiem w Bezpieczeństwie Informacji stanowiąca część SZBI, w której zostały określone zasady identyfikacji, oceny i postępowania z ryzykiem związanym z bezpieczeństwem informacji[26].

Ponadto z dokumentacji przedstawionej kontrolerom wynika, że w marcu 2024 r. została przeprowadzona analiza ryzyka utraty integralności, dostępności lub poufności informacji w bezpieczeństwie informacji dla każdego z referatów osobno, uwzględniając przy tym rodzaj zagrożenia i podatność na nie. Dodatkowo w styczniu 2025 r. został sporządzony Raport z Szacowania i Postępowania z Ryzykiem w Bezpieczeństwie Informacji – Szacowanie Ryzyka Identyfikacja Ryzyka, także zawierający dane o właścicielu ryzyka, zagrożeniach, ich podatności oraz zagrożonych aktywach.[27]

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, 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.

Zasady inwentaryzacji zostały określone w SZBI - Wymagania Dotyczące Inwentaryzacji Aktywów.[28]

[26] Folder „Dokumenty do UW.zip”: Folder „Dokumentacja wymagań SZBI 27001_2023”: Plik „6.1.2-6.1.3-8.1-POL-PZRBI-v25_1”
[27] Folder „Dokumenty do UW.zip”: Folder „Dodatkowa dowodowa”: Folder „Szacowanie ryzyka 2024 i 2025” - wszystkie dokumenty
[28] Folder „Dokumenty do UW.zip”: Folder „Dokumentacja wymagań SZBI 27001_2023”: Plik „A.5.9-WYM-WDIA-v25_1”

Z wyjaśnień UM w Białej wynika, że „inwentaryzacja sprzętu przeprowadzana jest w czasie rzeczywistym, wykorzystując [redacted][29] (…) Dodatkowo ewidencja prowadzona jest również w arkuszu kalkulacyjnym zawierającym niezbędne informacje o sprzęcie. (…) Inwentaryzacja oprogramowania również prowadzona jest w [redacted], który monitoruje oprogramowanie zainstalowane na komputerach oraz powiadamia o wszelkich aktualizacjach.[30]" Ponadto z przedstawionej dokumentacji wynika, że oprogramowanie jest ewidencjonowane na dodatkowej liście stanowiącej załącznik do SZBI, którą prowadzi ASI.[31] Załącznikiem do wyjaśnień są dokumenty potwierdzające posiadanie aktualnego oprogramowania antywirusowego oraz aktualnych licencji na wsparcie urządzeń sieciowych w UM w Białej.[32]

Powyższe wyjaśnienia złożone przez Burmistrza Białej zostały przyjęte przez zespół kontrolny.

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;
- § 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

[29] Folder „Dokumenty kontrolne.zip": Pliki: „licencja-axence", „axence - ewidencja sprzętu-1", „axence - ewidencja sprzętu-2", „axence - ewidencja sprzętu-3"
[30] Folder „Dokumenty kontrolne.zip": Pliki: „arkusz_ewidencja sprzętu", „axence - ewidencja oprogramowania", Pismo „pismo z wyjaśnieniami" z dnia 4 kwietnia 2025 r.
[31] Folder „Dokumenty kontrolne.zip": Plik „biala_lista"
[32] Folder „Dokumenty kontrolne.zip": Pliki: „FortiAnalyzer", „FortiGate", „WithSecure Elements EDR and EPP for Computers Premium", „WithSecure Elements EDR and EPP for Servers", „WithSecure Elements Vulnerability Management"

realizowanych przez nie zadań oraz obowiązków, a w przypadku zmiany zadań lub zakończenia stosunku pracy następuje zmiana lub odebranie uprawnień.

Zasady zarządzania uprawnieniami w systemach informatycznych określone zostały w SZBI w Wymaganiach Dotyczących Warunków Zatrudnienia oraz Wymaganiach Dotyczących Obowiązków po Zakończeniu lub Zmianie Zatrudnienia. Dodatkowo w Polityce Kontroli Dostępu do Systemów Informatycznych określono zasady dostępu i ograniczeń do systemów[33].

Z dokumentacji oraz informacji powziętych z UM w Białej wynika, że osobom, które zostały nowo zatrudnione, zmieniły stanowisko pracy lub zakończyły stosunek pracy w UM w Białej, sporządzane są wnioski o nadanie, zmianę lub odebranie dostępu do systemów informatycznych wraz z adnotacją ASI o zrealizowaniu zadania.[34].

W kontrolowanym okresie zdarzyły się przypadki odebrania oraz nadania uprawnień do systemów informatycznych. W sprawie Burmistrz Białej złożył stosowne wyjaśnienia, które zostały przyjęte przez zespół kontrolny. [35]

Ponadto pracownikom UM w Białej realizującym zadania zlecone z zakresu administracji rządowej wystawiane są upoważnienia do przetwarzania informacji, które są zgodne ze wzorem zawartym w dokumentacji SZBI.[36] Jednocześnie w trakcie analizy upoważnień dot. wykonywania zadań z zakresu Centralnej Ewidencji i Informacji o Działalności Gospodarczej zespół kontrolny ustalił, że nie zostały one podpisane przez osoby, którym udzielano upoważnień, co zakwalifikowano jako uchybienie.[37]

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

[33] Folder „Dokumenty do UW.zip”: Folder „Dokumentacja wymagań SZBI 27001_2023”: Pliki: „A.6.2-WYM-WDWZ”, „A.6.5-WYM-WDOZZZ”, „A.8.2-5-POL-PKDSI”
[34] Folder „dokumenty kontrolne.7z”: Pliki: „A.6.2 - Wnioski o nadanie uprawnień (NOWE)”, „Wnioski o nadanie uprawnień”, „wniosek_srp1”, „wniosek_srp2”
[35] Folder „dokumenty kontrolne.7z”: Pliki: „CEIDG-odebranie uprawnień”, „CEIDG-nadanie uprawnień”, „podatki-odebranie”, „podatki-nadanie”, Pismo „wyjaśnienie do kontroli” z dnia 15 kwietnia 2025 r.
[36] Folder „Dokumenty do UW.zip”: Folder „Dodatkowa dowodowa”: Plik „Upoważnienia do przetwarzania informacji”
[37] Folder „Dokumenty do UW.zip”: Folder „Dodatkowa dowodowa”: Pliki: „Upoważnienie - CEIDG – 2011 r.”, „Upoważnienie - CEIDG – 2012 r.”, „Upoważnienie – CEIDG”

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 SZBI zostały określone nie tylko wymagania dotyczące zapewnienia świadomości, edukacji i szkoleń w zakresie bezpieczeństwa informacji, ale także wzór rejestru zrealizowanych działań uświadamiających, edukacyjnych i szkoleń w zakresie bezpieczeństwa informacji. Dodatkowo został przesłany przedmiotowy rejestr za okres objęty kontrolą, w którym wykazane są przeprowadzone szkolenia wraz z liczbą uczestników[38].

Z wyjaśnień Burmistrz Białej wynika, że „Ostatnie szkolenia z zakresu bezpieczeństwa informacji w tym ochrony danych osobowych z elementami tematu cyberbezpieczeństwa odbyły się: 11 marca 2024 r., 9 stycznia 2025 r., 16 stycznia 2025 r. i obejmowały wszystkich pracowników Urzędu. Ponadto w dniu 23 stycznia 2025 r. przeprowadzono szkolenie dla kierowników referatów i pracowników na samodzielnym stanowisku pracy w temacie System Zarządzania Bezpieczeństwem Informacji – realizacja wymogów. (…) W tematyce cyberbezpieczeństwa zostało przeprowadzone szkolenie w dniu 18 lutego 2025 r. Szkolenie to przeprowadzone zostało w ramach realizowanego w tut. Urzędzie projektu „Zwiększenie cyberbezpieczeństwa w instytucjach samorządowych Gminy Biała”. W ramach tegoż projektu odbędą się jeszcze 3 szkolenia dla pracowników. (…) Do celów szkoleniowych z powyższego zakresu pracownicy mają również udostępnioną platformę szkoleniową (…).”[39] Ponadto UM w Białej

[38] Folder „Dokumenty do UW.zip”: Folder „Dodatkowa dowodowa”: Plik „Rejestr zrealizowanych działań uświadamiających - 2024-2025”
[39] Pismo „wyjaśnienie do kontroli” z dnia 15 kwietnia 2025 r.

przesłał dokumentację potwierdzającą zakresy tematyczne szkoleń[40] wraz z listami obecności pracowników[41].

Powyższe wyjaśnienia złożone przez Burmistrza Białej zostały przyjęte przez zespół kontrolny.

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.

Zasady pracy zdalnej wraz z prawami i obowiązkami pracodawcy i pracownika zostały określone w SZBI w Polityce Pracy Zdalnej[42]. Dodatkowe zasady określające bezpieczny sposób korzystania z komputerów zawarte są w polityce Bezpieczeństwa Fizycznego i Środowiskowego oraz Polityce Konfiguracji i Obsługi Urządzeń Końcowych Użytkownika.

Z informacji uzyskanych z UM w Białej wynika, że w okresie objętym kontrolą nie miały miejsca przypadki przejścia pracownika na pracę zdalną[43].

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) 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.

---

[40] Folder „dokumenty kontrolne.7z": Pliki: „2025-01-09 - Program szkolenia", „2025-01-16 - Program szkolenia", „2025-01-23 - Program szkolenia", „2025-01-23 - Program szkolenia", 2025-01-23 - Program szkolenia"

[41] Folder „Dokumenty do UW.zip": Folder „Dodatkowa dowodowa": Plik: „Lista obecności - 2025-01-09", „Lista obecności - 2025-01-16", „Lista obecności - 2025-01-23"

[42] Folder „Dokumenty do UW.zip": Folder „Dokumentacja wymagań SZBI 27001_2023": Plik „A.6.7-POL-PPZ"

[43] Pismo „wyjaśnienie do kontroli" z dnia 15 kwietnia 2025 r.

Wytyczne dotyczące zachowania bezpieczeństwa informacji podczas zawierania umów serwisowych ze stronami trzecimi znajdują się w Polityce bezpieczeństwa informacji w relacjach z dostawcami, Wymaganiach dotyczących uwzględnienia bezpieczeństwa informacji w umowach z dostawcami, wymaganiach dotyczących zarządzania bezpieczeństwem informacji w łańcuchu dostaw ICT oraz w Zasadach monitorowania, przeglądu i zarządzania zmianami usług dostawców, które stanowią elementu SZBI[44]. Dodatkowo prowadzony jest Rejestr Umów Przetwarzania Danych Osobowych w Imieniu Administratora, w którym określony jest kontrahent wraz z okresem obowiązywania umowy i zadaniami przez niego wykonywanymi[45].

W UM w Białej wykorzystywane są dwa systemy teleinformatyczne przeznaczone do realizacji zadań zaleconych z zakresu administracji rządowej zakupione u zewnętrznego dostawcy. W związku z powyższym zostały podpisane stosowane umowy licencyjne, umożliwiające prawidłową eksploatację i rozwój poprzez zgłaszanie występujących błędów oraz świadczenie pomocy przez dystrybutora. Dodatkowo zawarte zostały adekwatne umowy powierzenia przetwarzania danych osobowych gwarantujące właściwe zabezpieczenie danych w przypadku awarii systemu, a także zapewniające bezpieczeństwo przetwarzanych informacji uzyskanych przez wykonawców w związku z realizacją umów[46].

Ponadto w dokumentacji przekazanej przez UM w Białej znajdują się także inne umowy dot. prawidłowego funkcjonowania systemów teleinformatycznych, do których również zostały zawarte stosowane umowy powierzenia przetwarzania danych osobowych.[47]

Została także podpisana umowa z osobą prowadzącą działalność gospodarczą na świadczenie usługi pełnienia funkcji Inspektora ochrony danych oraz pełnienia funkcji Pełnomocnika ds. bezpieczeństwa informacji, do której nie została zawarta umowa powierzenia przetwarzania danych osobowych[48].

Burmistrz Białej złożył wyjaśnień w tym przedmiocie: „Zgodnie z obowiązującymi, mającymi zastosowanie przepisami prawa, w szczególności

[44] Folder „Dokumenty do UW.zip”: Folder „Dokumentacja wymagań SZBI 27001_2023”: Pliki: „A.5.19-POL-PBIRD”, „A.5.20-WYM-WDUBIUD”, „A.5.21-WYM-WDZBILDICT”, „A.5.22-ZAS-ZMPZZUD”
[45] Folder „Dokumenty do UW.zip”: Folder „Dodatkowa dowodowa”: Plik „Rejestr umów przetwarzania danych osobowych w imieniu administratora”
[46] Folder „Dokumenty kontrolne.zip”: Folder „Umowy”: Pliki: „umowa1”, „umowa6”
[47] Folder „Dokumenty kontrolne.zip”: Folder „Umowy”: Pliki: „umowa2”, „umowa3”, „umowa4”, „umowa5”
[48] Folder „Dokumenty do UW.zip”: Folder „Dodatkowa dokumentacja”: Pliki: „umowa IOD i PBI – 2024”, „Umowa IOD i PBI – 2025”, „Zarządzenie OR.120.12.2020 w sprawie powołania pełnomocnika i zespołu ds. SZBI”

ogólnym Rozporządzeniem o Ochronie Danych Osobowych, z zewnętrznym inspektorem ochrony danych, administrator ani podmiot przetwarzający nie zawierają umów powierzenia przetwarzania, gdyż przetwarzanie danych osobowych, do którego dochodzi w związku z pełnieniem funkcji IOD jest prawnie regulowane zakresem obowiązków IOD określonym w art. 39 RODO. Świadczenie usług zewnętrznego IOD jest realizowane w oparciu o ww. przepis i dokumentowane stosowaną umową cywilnoprawną na usługi w tym zakresie, jaką administrator i podmiot przetwarzający zawierają z IOD. (…) W analogi do funkcji IOD, w ramach jednej umowy cywilnoprawnej zawarto również zapisy dotyczące świadczenia usług Pełnomocnika, gdzie w § 1 pkt 2 powołano świadczeniodawcę do pełnienia funkcji Pełnomocnika ds. Bezpieczeństwa Informacji, wskazując jednocześnie zakres zadań realizowanych dla tej funkcji, czym uznano że dopełniony został obowiązek upoważnienia Pełnomocnika do działania w imieniu Burmistrza – administratora. Dodatkowo wydane zostało zarządzenie Burmistrza nr OR.120.12.2020 z dnia 28 maja 2020 r. w sprawie powołania w Urzędzie Pełnomocnika oraz Zespołu do spraw Systemu Zarządzania Bezpieczeństwem Informacji, które również upoważnia do realizacji funkcji w zakresie określonym w ww. umowie oraz w zabezpieczeniu A.5.2 dokumentacji wymagań SZBI.”[49]

Powyższe wyjaśnienia złożone przez Burmistrza Białej zostały przyjęte, jednakże zespół kontrolny zwraca uwagę, że funkcja Inspektora Ochrony Danych Osobowych została połączona z funkcją Pełnomocnika ds. Systemu Zarządzania Bezpieczeństwem Informacji. Zgodnie z art. 38 ust. 6 RODO – IOD może wykonywać inne zadania i obowiązki po warunkiem, że nie powodują one konfliktu interesów. W przypadku połączenia funkcji IOD z zadaniami związanymi z nadzorem lub bezpośrednim zarządzaniem systemem bezpieczeństwa informacji istnieje ryzyko, że powołana na te stanowiska osoba będzie zobowiązana do monitorowania i oceniania procesów, za których realizację sama odpowiada. Może to podważyć niezależność i bezstronność IOD, co jest kluczowe dla skutecznego wykonywania tej funkcji. W związku z powyższym zasadnym jest przeprowadzenie precyzyjnej, udokumentowanej analizy ryzyka co do ewentualnego konfliktu interesów w obecnym modelu organizacyjnym. Analiza ta powinna obejmować szczegółowy zakres obowiązków przypisanych IOD oraz ocenę ich potencjalnego wpływu na zdolność do niezależnego sprawowania nadzoru nad przetwarzaniem danych osobowych.

[49] Pismo „pismo z wyjaśnieniami” z dnia 4 kwietnia 2025 r.

Dodatkowo zespół kontrolny rekomenduje, aby umowa o świadczenie usług w wyżej opisanym zakresie, została sformułowana w sposób bardziej precyzyjny i szczegółowy, a to poprzez wyraźne określenie i rozdzielenie obowiązków wynikających z pełnienia funkcji IOD oraz pełnomocnika ds. SZBI; określenie zasad wykonywania poszczególnych zadań jeżeli chodzi o pełnomocnika ds. SZBI, uwzględnienie zasad przetwarzania danych osobowych na tle realizacji umowy oraz doprecyzowanie zasad odpowiedzialności. W obecnym brzmieniu umowa ta nie precyzuje bowiem w sposób wystarczający zakresu zadań, obowiązków oraz odpowiedzialności wykonawcy, co może prowadzić do niejasności w zakresie zgodności z przepisami o ochronie danych osobowych, w tym co do konieczności ewentualnego zawarcia umowy powierzenia przetwarzania danych osobowych (art. 28 RODO). Doprecyzowanie zapisów umownych przyczyni się do zwiększenia przejrzystości relacji między stronami oraz zapewnienia zgodności z zasadą rozliczalności, minimalizacji ryzyka konfliktu interesów i prawidłowego określenia ról oraz obowiązków stron w procesie przetwarzania danych osobowych.

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 Procedurze zgłaszania zdarzeń związanych z bezpieczeństwem informacji oraz Polityce zarządzania incydentami związanymi z bezpieczeństwem informacji zostały określone wytyczne oraz sposób postępowania ze zdarzeniami związanymi z naruszeniem bezpieczeństwa informacji, które mają na celu zapewnienie ciągłości operacyjnej oraz ograniczenie występowania takich incydentów w przyszłości. Dodatkowo zostały sporządzone dokumenty ułatwiające zgłoszenie, identyfikację oraz nadzór nad występującymi incydentami, tj. Zgłoszenie zdarzenia związanego z bezpieczeństwem informacji, Informacja o incydencie związanym z bezpieczeństwem informacji oraz Rejestr incydentów związanych z bezpieczeństwem informacji[50].

[50] Folder „Dokumenty do UW.zip”: Folder „Dokumentacja wymagań SZBI 27001_2023”: Pliki: „A.6.8-PRO-PZZZBI”, „A.5.24-28-POL-PZIZBI”, „A.6.8-Z-ZZZBI”, „A.5.24-INF-IIZBI”, „A.5.24-RE-RIZBI”

Z informacji uzyskanych z UM w Białej wynika, że w okresie objętym kontrolą nie miały miejsca przypadki wystąpienia incydentów naruszenia bezpieczeństwa informacji.[51]

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 Systemu Zarządzania Bezpieczeństwem Informacji jednostki z kryteriami audytu.

W celu prawidłowego przeprowadzania audytów wewnętrznych z zakresu bezpieczeństwa informacji w UM w Białej zostały opracowane Wymagania dotyczące audytów wewnętrznych wraz z dodatkową dokumentacją, tj. Programem audytów wewnętrznych, Planem audytu wewnętrznego oraz Raportem z audytu wewnętrznego. Ponadto sporządzono Wymagania dotyczące niezależnych przeglądów bezpieczeństwa informacji oraz Monitorowanie zgodności z wymaganiami systemu zarządzania bezpieczeństwem informacji.[52]

Na podstawie dokumentacji przekazanej kontrolerom ustalono, że w okresie objętym kontrolą, w jednostce przeprowadzono obligatoryjny audyt wewnętrzny z zakresu bezpieczeństwa informacji, który został zaplanowany w Programie audytów wewnętrznych na rok 2024 oraz opisany w Planie audytu wewnętrznego[53]. Ponadto z przedstawionej dokumentacji wynika, że na IV kwartał 2025 r. został zaplanowany coroczny obligatoryjny audyt wewnętrzny

[51] Pismo „wyjaśnienie do kontroli" z dnia 15 kwietnia 2025 r.
[52] Folder „Dokumenty do UW.zip": Folder „Dokumentacja wymagań SZBI 27001_2023": Pliki: „9.2-WYM-WDAW", „9.2.2-PRG-PAW", „9.2.2-PLN-PAW", „9.2.2-RA-RAW", „A.5.35-WYM-WDNPBI", „A.5.36-WYM-MZWSZBI"
[53] Folder „Dokumenty do UW.zip": Folder „Dodatkowa dowodowa": Plik „Raport z audytu wewnętrznego 1-2024", Folder „dokumenty kontrolne.7z": Pliki: „Program audytów wewnętrznych na rok 2024", „Plan audytu wewnętrznego 2024"

w przedmiotowym zakresie[54] oraz w styczniu 2025 r. został sporządzony Raport z monitorowania, pomiarów, analizy i oceny bezpieczeństwa informacji[55].

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 UM w Białej została sporządzona Polityka zapasowych kopii informacji, która określa m.in. ich rodzaj, osoby odpowiedzialne oraz wytyczne dot. prawidłowego zarządzania nimi[56]. Ponadto w dokumentacji kontrolnej został przekazany Plan zapasowych kopii informacji określający najistotniejsze dane tego procesu, a także zrzut ekranu z odpowiedniego programu komputerowego ukazujący ostatnią datę modyfikacji oraz czas wykonania kolejnej[57].

Zgodnie z § 6 Polityki Zapasowych Kopii Informacji każda wymagająca tego kopia zapasowa systemu, oprogramowania i danych, przechowywana jest co najmniej w jednej, bezpiecznej, dodatkowej lokalizacji zdalnej, w wystarczającej odległości od miejsc przetwarzania informacji objętych kopią zapasową.

---

[54] Folder „Dokumenty do UW.zip”: Folder „Dodatkowa dowodowa”: Plik „Program audytów wewnętrznych na rok 2025”

[55] Folder „Dokumenty do UW.zip”: Folder „Dodatkowa dowodowa”: Plik „Raport z monitorowania pomiarów analizy i oceny bezpieczeństwa informacji”

[56] Folder „Dokumenty do UW.zip”: Folder „Dokumentacja wymagań SZBI 27001_2023”: Pliki: „A.8.13-POL-PZKI”

[57] Folder „dokumenty kontrolne.7z”: Pliki: „xopero”, „A.8.13-PLN-PZKI-v25_1 - Plan Zapasowej Kopi informacji”,

Z wyjaśnień złożonych przez Burmistrza Białej wynika, że kopie zapasowe tworzone są przy wykorzystaniu systemu backup'u polskiej firmy, a przechowywane są w serwerowni innego państwa znajdującego się na terenie Unii Europejskiej. Dodatkowo serwery wirtualne replikowane są na serwery znajdujące się w drugiej serwerowni[58]. Powyższe wyjaśnienia złożone przez Burmistrza Białej zostały przyjęte przez zespół kontrolny.

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 Białej do realizacji zadań z zakresu administracji rządowej wykorzystywane są wspomagające systemy teleinformatyczne, które dzielą się na systemy centralne, tj. SRP, Karta Dużej Rodziny, CEIDG, oraz te zakupione u dostawcy zewnętrznego – PB_EWID_SRP (Technika IT Sp. z o.o.), Podatki-osoby fizyczne (U.I. INFOSYSTEM sp.j). Na obsługę zakupionych systemów informatycznych zawarte zostały stosowne umowy licencyjne, gwarantujące rozwój i dostosowanie do obowiązujących przepisów prawa. Ponadto w SZBI UM w Białej zawarta jest Polityka bezpieczeństwa systemów i aplikacji w procesach rozwoju i wsparcia, która określa wytyczne w zakresie bezpieczeństwa informacji podczas rozwoju oprogramowania i aplikacji[59]. 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:
  pkt 7 - zapewnienie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez: a)

[58] Folder „dokumenty kontrolne.7z": Plik „xopero_cloud", Pismo „wyjaśnienie do kontroli" z dnia 15 kwietnia 2025 r.
[59] Folder „Dokumenty do UW.zip": Folder „Dokumentacja wymagań SZBI 27001_2023": Pliki: „A.8.25-34-POL-PBSAPRW"

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.

Z kontrolowanej dokumentacji wynika, że w UM w Białej stosowane są zabezpieczenia dostępu do informacji, które zostały określone m.in. w Polityce Kontroli Dostępu, Polityce Kontroli Dostępu do Systemów Informatycznych, Wymaganiach Dotyczących Monitorowania Sieci, Systemów i Aplikacji, Polityce Bezpieczeństwa Sieci i Usług Sieciowych[60].

W UM w Białej opracowano Instrukcję w sprawie określenia procedury postępowania z kluczami oraz zabezpieczenia pomieszczeń i obiektu Urzędu Miejskiego w Białej wprowadzonej Zarządzeniem nr OR.120.29.2013 Burmistrza Białej z dnia 24 czerwca 2013 r. w sprawie wprowadzenia Instrukcji postępowania z kluczami oraz zabezpieczenia pomieszczeń i obiektu Urzędu Miejskiego w Białej[61]. Dodatkowo zespół kontrolny wniósł o opisanie faktycznej procedury postępowania z kluczami do serwerowni oraz pomieszczeń, w których realizowane są zadania zlecone z zakresu administracji rządowej. W dokumentacji przekazanej kontrolom znajdują się także upoważnienia osób uprawnionych do wynoszenia kluczy do całego budynku lub też poszczególnych biur w budynku poza siedzibę UM w Białej[62]. Z analizy dokumentacji wynika, że faktyczna procedura

[60] Folder „Dokumenty do UW.zip”: Folder „Dokumentacja wymagań SZBI 27001_2023”: Pliki: „A.5.15-POL-PKD”, „A.8.2-5-POL-PKDSI”, „A.8.16-WYM-WDMSSA”, „A.8.20-23-POL-PBSUS”
[61] Folder „Dokumenty do UW.zip”: Folder „Dodatkowa dowodowa”: Plik „Zarządzenie nr OR.120.29.2013 w sprawie wprowadzenia Instrukcji postępowania z kluczami oraz zabezpieczenia pomieszczeń”
[62] Folder „Dokumenty kontrolne.zip”: Pliki: „upoważnienia do kluczy 1d”

postępowania z kluczami opisana przez Burmistrza Białej jest tożsama z wytycznymi określonymi ww. Instrukcji postępowania z kluczami.

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.

W dokumentach stanowiących SZBI, tj. Wymaganiach Dotyczących Instalacji Oprogramowania w Systemach Produkcyjnych, Wymaganiach Dotyczących Bezpieczeństwa Informacji Podczas Zakłóceń, Planie Zarządzania Ciągłością Działania Podczas Zakłóceń, Wymaganiach Dotyczących Gotowości ICT do Zapewnienia Ciągłości Działania, Polityce Zapasowych Kopii Informacji, Zasadach Stosowania Kryptografii, Polityce Zarządzania Podatnościami Technicznymi i Polityce Kontroli Dostępu do Systemów Informatycznych, zostały wykazane mechanizmy jakie kontrolowana jednostka zastosowała w celu zapewnienia ochrony przetwarzanych informacji, w ramach badanych systemów teleinformatycznych przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami[63].

Dodatkowo zapewniono także środki uniemożliwiające nieautoryzowany dostęp oraz zapewniające kontrolę dostępu do systemów teleinformatycznych służących do realizacji zadań zleconych z zakresu administracji rządowej poprzez

[63] Folder „Dokumenty do UW.zip”: Folder „Dokumentacja wymagań SZBI 27001_2023”: Pliki: „A.8.19-WYM-WDIOSP”, „A.5.29-WYM-WDBIPZ”, „A.5.29-PLN-PZCDPZ”, „A.5.30-WYM-WDGICTZCD”, „A.8.13-POL-PZKI”, „A.8.24-ZAS-ZSK”, „A.8.8-POL-PZPT”, „A.8.2-5-POL-PKDSI”

indywidualne logowanie do wybranych systemów, np. za pomocą loginu i hasła, karty dostępowej i numeru PIN[64].

Podczas kontroli dokonano oględzin pomieszczenia serwerowni w UM w Białej. Czynność ta została przeprowadzona w obecności Pracownika na stanowisku ds. informatycznych zajmującego samodzielne stanowisko pracy. W toku oględzin dokonano ustalenia stanu faktycznego i stwierdzono, że główny budynek UM w Białej posiada zabezpieczenie alarmowe oraz monitoring w najistotniejszych punktach. W siedzibie UM w Białej znajdują się dwie serwerownie, które są pomieszczeniami oddzielnymi[65]. W celu zapewnienia bezpieczeństwa fizycznego serwerowni zespół kontrolny rekomenduje, [redacted].

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 informacji uzyskanych podczas kontroli wynika, że w przypadku systemu Podatki, rozliczalność odnotowywana jest w dzienniku zdarzeń, który zapisuje

[64] Pismo „wyjaśnienie do kontroli” z dnia 15 kwietnia 2025 r.
[65] Plik: „Protokół oględzin serwerowni”

wszelkie działania, w tym nazwę zalogowanego użytkownika, dokonaną czynność oraz czas jej wykonania. W zakresie systemu PB_EWID wszystkie czynności użytkownika odnotowywane są w przedmiotowym systemie. W przypadku systemów centralnych, tj. SRP, Karta Dużej Rodziny oraz CEIDG dostęp do dzienników zdarzeń mają odpowiednio: Centralny Ośrodek Informatyki, Ministerstwo Rodziny, Pracy i Polityki Społecznej oraz Ministerstwo Rozwoju i Technologii[66].

Z analizy przedkontrolnej wynika, że „W systemach dziedzinowych wykorzystanych w UM Biała informacje w dziennikach systemowych przechowywane są od dnia ich zapisu przez okres co najmniej dwóch lat".

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

W wyniku kontroli stwierdzono następujące uchybienie:

1. Brak podpisów osób, którym udzielano upoważnień na upoważnieniach dot. wykonywania zadań z zakresu Centralnej Ewidencji i Informacji o Działalności Gospodarczej.

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. Podpisywanie upoważnień dot. wykonywania zadań z zakresu Centralnej Ewidencji i Informacji o Działalności Gospodarczej przez osoby, którym upoważnienie zostało udzielone.

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,

[66] Folder „dokumenty kontrolne.7z": Pliki: „podatki", „podatki"

wykorzystaniu wniosków lub przyczynach ich niewykorzystania, o podjętych działaniach lub przyczynach ich niepodjęcia, albo o innym sposobie usunięcia stwierdzonych nieprawidłowości, w terminie 7 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