



WOJEWODA PODKARPACKI

ul. Grunwaldzka 15
35-959 Rzeszów

OA-IV.431.3.2026

Rzeszów, 2026-09-21

**Pan
Zdzisław Zadworny
Burmistrz Miasta i Gminy
Cieszanów**

Na podstawie art. 46 ust. 1 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej, w związku ze zrealizowaną w dniach 21 i 23 lipca 2026 r. u Burmistrza Miasta i Gminy Cieszanów (Urząd Miasta i Gminy Cieszanów, ul. Rynek 1, 37-611 Cieszanów) kontrolą problemową¹, której przedmiotem była ocena działania systemów teleinformatycznych używanych do realizacji zadań zleconych z zakresu administracji rządowej z minimalnymi wymaganiami dla systemów teleinformatycznych - przekazuję niniejsze **wystąpienie pokontrolne**.

Kontrolę przeprowadził zespół kontrolerów: Alicja Trygar (starszy inspektor wojewódzki), Tomasz Szmigiel (zastępca kierownika) na podstawie imiennych upoważnień do kontroli (pisma z dnia 14.07.2026 roku, znak OA-IV.431.3.2026) udzielonych przez działającego z upoważnienia Wojewody Podkarpackiego – Zastępcę Dyrektora Wydziału Organizacyjno-Administracyjnego.

Ustalenia kontrolne dokonane zostały w oparciu o stan faktyczny istniejący od 1 stycznia 2025 roku do dnia realizacji czynności kontrolnych włącznie.

W toku kontroli - w oparciu o kontrolowane dokumenty (przy zastosowaniu metody niestatystycznej, losowy dobór próby) - ustalono, iż pracownicy Urzędu Miasta i Gminy Cieszanów prawidłowo realizowali swoje zadania. Stwierdzone uchybienia w swych skutkach nie miały charakteru kluczowego (strategicznego) dla funkcjonowania kontrolowanej jednostki. W dużej mierze miały one charakter formalny, przejawiając się odstępstwami od stanu pożądanego, nie powodując jednak negatywnych następstw dla kontrolowanej działalności.

Kontrola nie wykazała okoliczności wskazujących na popełnienie przestępstwa, wykroczenia, naruszenia dyscypliny finansów publicznych lub innych czynów, za które ustawowo przewidziana jest odpowiedzialność prawna.

¹ W oparciu o zatwierdzony w dniu 7 stycznia 2026 r. „Plan zewnętrznej działalności kontrolnej Podkarpackiego Urzędu Wojewódzkiego w Rzeszowie na 2026 rok”).

W oparciu o poczynione ustalenia, stosownie do skali ocen przyjętej w „Programie kontroli problemowej realizowanej u Burmistrza Miasta i Gminy Cieszanów”², **działalność w ww. zakresie należy ocenić pozytywnie z uchybieniami.**

Na podstawie analizy dokumentacji źródłowej zespół kontrolny sformułował następującą ocenę kontrolowanych obszarów:

1. Wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami/rejestrami informatycznymi i wspomaganie świadczenia usług drogą elektroniczną – pozytywnie;
2. Wdrożenie systemu zarządzania bezpieczeństwem informacji w systemach teleinformatycznych – pozytywnie z uchybieniami;
3. Dostosowanie systemów informatycznych do standardu WCAG 2.0 – pozytywnie.

Kontekst organizacyjny

Funkcję kierownika w Urzędzie Miasta i Gminy Cieszanów pełnił Burmistrz:
Pan Zdzisław Zadworny.

Inspektor Ochrony Danych oraz Administrator Systemów Informatycznych zostali powołani na podstawie Zarządzenia Nr 90A/2021 Burmistrza Miasta i Gminy Cieszanów z dnia 1 września 2021 r.

Funkcję Inspektora Ochrony Danych (IOD) pełnił Pan Piotr Władyka w ramach umowy zlecenie. Funkcja Administratora Systemów Informatycznych (ASI) została powierzona Panu Januszowi Warcabie.

Dokonano również zgłoszenia osoby kontaktowej do CSIRT NASK w dniu 20 kwietnia 2022 r., nr zgłoszenia: 1612377.

Wsparcie informatyczne zapewnione było przez informatyka (ASI), pracownika Urzędu Miasta i Gminy. Pod jego opieką znajdowały się: środowiska sprzętowo-programowe, sieć lokalna, serwerownie, systemy i aplikacje centralne oraz własne, usprawniające pracę pracownikom Urzędu Miasta i Gminy Cieszanów i jednostek podległych.

W okresie objętym kontrolą w Urzędzie Miasta i Gminy Cieszanów funkcjonowały systemy teleinformatyczne własne - zakupione przez urząd oraz centralne m.in.:

a) systemy centralne:

- System Rejestrów Państwowych (SRP) - dane o obywatelach zgromadzonych w poszczególnych rejestrach (rejestr PESEL, rejestr Dowodów Osobistych, rejestr Stanu Cywilnego);
- Elektroniczna Platforma Usług Administracji Publicznej (ePUAP);

² Stosownie do § 37 ust. 2 zarządzenia Nr 1/14 Wojewody Podkarpackiego z dnia 2 stycznia 2014 r. w sprawie szczegółowych warunków i trybu prowadzenia kontroli (z późn. zm.) w ramach realizacji czynności kontrolnych stosowana była 4-stopniowa skala ocen, tj. ocena pozytywna, pozytywna z uchybieniami, pozytywna z nieprawidłowościami, negatywna.

- Centralna Ewidencja Działalności Gospodarczej (CEIDG);
- eDoręczenia.

b) systemy własne lub zakupione:

- PB_EWID, PB_EWID_SRP (System Ewidencji Ludności i Obsługi wyborów samorządowych) – firmy TECHNIKA IT sp. z o.o.,
- Ewidencja zwrotów podatku akcyzowego – w ramach zintegrowanego systemu informatycznego „Sprawny Urząd” - firmy Biuro Usług Komputerowych SOFTRES sp. z o.o.,
- Proton - Elektroniczny Obieg Dokumentów firmy Sputnik wdrożony w ramach projektu PSeAP (Podkarpacki System E-Administracji Publicznej) – obecnie serwis firma Nefeni,
- poczta elektroniczna,
- strona www,
- BIP.

Podstawą oceny są następujące ustalenia kontroli:

1. Wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami/rejestrami informatycznymi i wspomaganie świadczenia usług drogą elektroniczną

1.1. Usługi elektroniczne

Urząd Miasta i Gminy Cieszanów udostępniał elektroniczną skrzynkę podawczą (dalej: ESP) na platformie ePUAP oraz adres do eDoręczeń co umożliwiało wymianę danych i świadczenie usług elektronicznych.

Na stronie www Urzędu oraz na BIP znajdowała się informacja o adresie **elektronicznej skrzynki podawczej** ESP na ePUAP oraz adres eDoręczeń, co ułatwiało klientom składanie pism ogólnych, skarg czy wniosków drogą elektroniczną.

1.2. Współpraca systemów teleinformatycznych z innymi systemami

Pracownicy Urzędu Miasta i Gminy Cieszanów mieli dostęp do rejestrów publicznych, takich jak SRP Źródło i CEIDG, co umożliwiało efektywne przetwarzanie danych.

System PB_EWID komunikował się z usługami sieciowymi Systemu Rejestrów Państwowych w celu pobierania danych dzięki modułowi PB_EWID_SRP odpowiadającemu za transmisję danych z SRP do Systemu Ewidencji Ludności.

1.3. Obieg dokumentów

W Urzędzie Miasta i Gminy Cieszanów był wdrożony System Elektronicznego Zarządzania Dokumentacją PROTON umożliwiający zarządzanie dokumentami i wykonywanie czynności kancelaryjnych. Obecnie każda wpływająca korespondencja była rejestrowana i dekretowana w systemie PROTON.

System umożliwia cyfrowy obieg dokumentów, automatyzując rejestrację każdej korespondencji wpływowej.

2. Wdrożenie systemu zarządzania bezpieczeństwem informacji w systemach teleinformatycznych

2.1. Dokumenty z zakresu bezpieczeństwa informacji

Zgodnie z § 19 ust. 1 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, zwanego dalej Rozporządzeniem 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.

Wymaga to opracowania dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), w tym szeregu regulacji wewnętrznych oraz zapewnienia aktualizacji tych regulacji w zakresie dotyczącym zmieniającego się otoczenia. Dokumentacja jest warunkiem niezbędnym dla możliwości skutecznego zarządzania bezpieczeństwem informacji.

W Urzędzie Miasta i Gminy Cieszanów ustanowiono Systemu Zarządzania Bezpieczeństwem Informacji na podstawie Zarządzenia Nr 22/2026 z 17 lutego 2026 r. wraz kompleksową dokumentacją (108 dokumentów) wdrożoną pod nadzorem Pełnomocnika ds. Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).

Kluczowe dokumenty stanowiące SZBI to:

- System Zarządzania Bezpieczeństwem Informacji ustanowiony Zarządzeniem Nr 22/2026 z 17 lutego 2026 r. Burmistrza Miasta i Gminy Cieszanów;
- Polityka Bezpieczeństwa Informacji (załącznik nr 1 do Zarządzenia);
- Polityka Ochrony Danych Osobowych (załącznik nr 2 do Zarządzenia);
- Polityka Bezpieczeństwa Teleinformatycznego (załącznik nr 3 do Zarządzenia);
- Polityka Ciągłości Działania (załącznik nr 4 do Zarządzenia);
- Wykaz dokumentów, druków, formularzy i zapisów SZBI (załącznik nr 5 do Zarządzenia);

2.2. Analiza zagrożeń związanych z przetwarzaniem informacji

Wymogiem skuteczności SZBI jest przeprowadzanie okresowych analiz ryzyka.

Analiza zagrożeń w ramach SZBI wymaga ocen ryzyka utraty poufności, integralności lub dostępności informacji, obejmujących identyfikację, szacowanie, plan i deklarację zabezpieczeń zgodnie z §19 Rozporządzenia KRI.

W Urzędzie Miasta i Gminy Cieszanów zarządzanie ryzykiem opierało się na Procedurze Analizy Ryzyka w Urzędzie Miasta i Gminy Cieszanów i jego analizie wraz z omówieniem obszarów o podniesionym ryzyku przeprowadzonej w grudniu 2025 roku, zrealizowanej przez wykonawcę zewnętrznego EX LEGE Szkolenia Prawnicze Outsourcing Usług IOD Rafał Andrzejewski. Systematycznie należy dokonywać weryfikacji aktualności i wdrożenia działań.

Wyniki analizy ryzyka mają wpływać na decyzje odnośnie podniesienia bezpieczeństwa funkcjonowania jednostki, np. poprzez wzmocnienie kontroli zarządczej, system zastępstw na strategicznych stanowiskach, szkolenia pracowników w stosunku do zagrożonych obszarów eksploatacji systemów informatycznych. Dokonując analizy ryzyka warto wziąć pod uwagę utratę integralności, dostępności lub poufności wszystkich informacji.

2.3. Inwentaryzacja sprzętu i oprogramowania informatycznego

Zarządzanie infrastrukturą informatyczną wymaga utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację. W praktyce oznacza to zapewnienie funkcjonowania rejestru zasobów teleinformatycznych zawierającego informacje o wszystkich zidentyfikowanych aktywach informatycznych, w tym: szczegółowe dane o urządzeniach technicznych, parametrach, aktualnej konfiguracji, oprogramowaniu, środkach komunikacji, a także rodzaju relacji między elementami konfiguracji oraz użytkownikiem. Inwentaryzacja sprzętu i oprogramowania informatycznego jest kluczowym elementem zarządzania infrastrukturą w ramach SZBI, wymagając aktualnego rejestru zasobów z danymi o rodzajach, konfiguracjach, relacjach i użytkownikach zgodnie z §19 ust. 2 pkt 2 Rozporządzenia KRI.

W UMiG Cieszanów regulacje wewnętrzne przewidywały utrzymywanie ewidencji sprzętu i oprogramowania w postaci rejestru zasobów teleinformatycznych, za który odpowiadał ASI.

Inwentaryzacja sprzętu i oprogramowania uwzględniająca rodzaj i konfigurację była prowadzona w postaci Załącznika nr 1 i nr 2 do Procedury zapewnienia prawidłowego przetwarzania danych przy korzystaniu ze sprzętu IT i systemów u Administratora. Na potrzeby odtworzenia zasobów ewidencjonowanie odbywało się częściowo przez program antywirusowy Arcabit, dodatkowo ma się odbywać przez wdrażane narzędzie SIEM.

Sposób zabezpieczenia systemów informatycznych został przedstawiony w Polityce Bezpieczeństwa Teleinformatycznego w rozdziale Zarządzanie Zasobami Teleinformatycznymi.

2.4. Zarządzanie uprawnieniami do pracy w systemach informatycznych

Istotnym elementem polityki bezpieczeństwa informacji jest zarządzanie dostępem do systemów teleinformatycznych przetwarzających informacje. Zarządzanie 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 następuje również zmiana ich uprawnień.

Zarządzanie uprawnieniami dostępu w Urzędzie Miasta i Gminy Cieszanów regulowała Polityka Bezpieczeństwa Teleinformatycznego oraz Załącznik 11 Procedura Zarządzania Dostępem i Uprawnieniami.

Pracownicy uzyskiwali dostęp do zasobów informatycznych po przypisaniu przyznaniu zakresu obowiązków i nadaniu unikalnego identyfikatora i hasła w systemie teleinformatycznym.

Ustalono, że proces nadawania, zmiany i odbierania uprawnień do systemów informatycznych nie był w pełni sformalizowany. W szczególności nie stosowano udokumentowanych wniosków obejmujących nadanie, zmianę lub odebranie uprawnień

oraz ich zatwierdzenie przez osoby uprawnione. Nie prowadzono również bieżącego, udokumentowanego przeglądu uprawnień użytkowników. Powyższe ograniczało możliwość wykazania adekwatności i aktualności przyznanych dostępów oraz zwiększało ryzyko utrzymania uprawnień po zmianie zakresu obowiązków.

Zakres uprawnień użytkowników badanych systemów uniemożliwiał wykonywanie przez nich działań zastrzeżonych dla administratorów systemów.

2.5. Szkolenia pracowników zaangażowanych w proces przetwarzania informacji

Istotnym elementem SZBI jest świadomość pracowników współodpowiedzialności za bezpieczeństwo informacji, zagrożeń i konsekwencji zaistnienia incydentów związanych z naruszeniem bezpieczeństwa.

Szkolenia z zakresu bezpieczeństwa informacji powinny obejmować wszystkie osoby uczestniczące w procesie przetwarzania informacji oraz dostarczać aktualnej wiedzy o nowych zagrożeniach, adekwatnych zabezpieczeniach oraz skutkach ewentualnych incydentów związanych z bezpieczeństwem informacji.

Dokumentacja wewnętrzna Urzędu Miasta i Gminy w Cieszanowie regulowała zakres podnoszenia świadomości pracowników poprzez szkolenia wstępne i cykliczne z zakresu bezpieczeństwa (Procedura Szkoleń i Działań na Rzecz Podnoszenia Świadomości Personelu Urzędu - zał. 14 do Polityki Bezpieczeństwa Informacji). Kontrolującym przedstawiono informację o szkoleniach pracowników zrealizowanych w ramach projektu Cyberbezpieczny Samorząd przeprowadzonych w sierpniu i we wrześniu 2025 roku, z zakresu cyberbezpieczeństwa i SZBI.

2.6. Praca na odległość i mobilne przetwarzanie danych

Wobec możliwości technicznych związanych z telepracą (pracą poza siedzibą podmiotu publicznego z wykorzystaniem urządzeń mobilnych takich jak laptopy, tablety, smartfony) pojawiają się nowe zagrożenia bezpieczeństwa informacji.

Zarządzanie bezpieczeństwem urządzeń mobilnych jest istotnym elementem SZBI, wymagającym regulacji zasad ochrony przed kradzieżą, nieautoryzowanym dostępem i zagrożeniami sieci Wi-Fi, szczególnie w kontekście przetwarzania danych publicznych. Konieczne jest więc opisanie zasad określających sposoby zabezpieczenia urządzeń mobilnych i danych w nich zawartych.

W obowiązujących dokumentach były zawarte ogólne zasady Ochrony Kryptograficznej jako załącznik do Polityki bezpieczeństwa teleinformatycznego. Zasady pracy mobilnej uregulowane zostały w Polityce Bezpieczeństwa Teleinformatycznego w rozdziale Bezpieczeństwo Pracy Mobilnej.

Urządzenia przenośne pendrive były szyfrowane, natomiast laptopy nie. Według wyjaśnień przedstawionych zespołowi kontrolnemu pracownicy nie wynosili komputerów przenośnych poza siedzibę Urzędu. Ograniczało to ekspozycję na ryzyka związane z utratą lub kradzieżą urządzeń poza siedzibą, jednak nie zastępowało potrzeby określenia wymagań dotyczących szyfrowania urządzeń przenośnych, w szczególności na wypadek naruszenia przyjętych zasad.

2.7. Serwis sprzętu informatycznego i oprogramowania

W przypadku systemów informatycznych o znaczeniu istotnym dla jednostki niezbędne jest objęcie tych systemów (w zakresie oprogramowania użytkowego, systemowego, sprzętu i rozwiązań telekomunikacyjnych) stosownymi umowami serwisowymi, gwarantującymi odpowiednio szybkie uruchomienie pracy systemu w przypadku awarii. Umowy powinny posiadać klauzule prawne zabezpieczające ochronę informacji w przypadku wejścia w ich posiadanie przez firmy serwisujące.

Serwis sprzętu i oprogramowania w systemach kluczowych dla jednostki publicznej wymaga umów z SLA, klauzulami poufności i regulacjami dostępu, aby zapewnić szybką reakcję na awarie i ochronę danych.

Procedura Zarządzania Umowami (zał. 17 do Polityki Bezpieczeństwa Informacji) określała ogólne ramy współpracy oraz konieczność monitorowania realizacji umowy pod kątem przestrzegania zasad bezpieczeństwa informacji i ochrony danych przez Pełnomocnika ds. SZBI. W dokumentacji została również określona Procedura Zarządzania Dostawcami ICT oraz wprowadzony do uzupełnienia wzór Rejestru Dostawców Usług ICT.

W sprawdzanych umowach o asystę i opiekę autorską lub serwisową z firmami zewnętrznymi powyższe zapisy Procedur nie były stosowane, zachowany został dotychczasowy wzór umowy. W sprawdzanych umowach z wykonawcami zostały określone zasady i czas dostępu, zwłaszcza zdalnego oraz określono SLA (Service Level Agreement), czyli gwarantowany poziom świadczenia usług oraz czas i sposób reakcji na zgłaszane problemy (udostępniono umowę o asystę techniczną z Biurem Usług komputerowych SOFTRES sp. z o.o. – 2026 r. na oprogramowanie PB_EWID, PB_EWID_SRP oraz umowę opieki autorskiej na 2026 r. z Nefeni Sp. z o.o. na oprogramowanie EZD PROTON).

W przypadku tego systemu została również przedstawiona umowa powierzenia przetwarzania danych osobowych.

2.8. Procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji

Zasady postępowania w przypadku wystąpienia zdarzenia związanego z bezpieczeństwem informacji oraz słabością systemów informacyjnych zostały określone w Polityce Zarządzania Zdarzeniami, Incydentami Cyberbezpieczeństwa i Naruszeniami (zał. 10 do Polityki Bezpieczeństwa Informacji) oraz w Procedurze Zarządzania Incydentami (zał. 8 do Polityki Ochrony Danych Osobowych). Procedury umożliwiały szybkie i najbardziej efektywne podjęcie działań korygujących przez wskazanie m.in. osób odpowiedzialnych i kanałów zgłaszania incydentu lub naruszenia.

Rejestr incydentów i działań korygujących w Urzędzie Miasta i Gminy Cieszanów nie zawierał wpisów.

2.9. Audyt wewnętrzny z zakresu bezpieczeństwa informacji

W obowiązującej dokumentacji zawarte zostały ogólne Procedury Audytów Wewnętrznych dotyczące konieczności audytowania i sprawdzeń w zakresie bezpieczeństwa informacji. Warto zwrócić uwagę, że celem audytów jest ewentualne ujawnienie słabości systemów, a także słabości zabezpieczeń lub ich stosowania.

Wyniki audytu powinny wpłynąć na doskonalenie tych zabezpieczeń, sposobów ich stosowania, a także na program szkoleń z bezpieczeństwa informacji. Audyt z zakresu

bezpieczeństwa informacji nie rzadziej niż raz na rok, w rozumieniu § 19 ust. 14 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 w Urzędzie Miasta i Gminy Cieszanów był wykonany w 2026 roku w ramach projektu Cyberbezpieczny Samorząd - pn. Audyt Bezpieczeństwa Informacji wg. wymagań Krajowych Ram Interoperacyjności.

2.10. Kopie zapasowe

Wykonywanie kopii zapasowych zapobiega utracie informacji w wyniku awarii.

Kopie powinny być właściwie tworzone, przechowywane i testowane.

W okresie objętym kontrolą w zakresie wykonywania kopii zapasowych w Urzędzie Miasta i Gminy Cieszanów obowiązywały wymagania określone w Procedurze Zarządzania Kopiami Zapasowymi (zał. 4 do Polityki Zarządzania Ciągłością Działania).

Kopie folderów, maszyn wirtualnych były wykonywane według harmonogramu ustalonego przez ASI oraz przechowywane na serwerze.

Ustalono, że kopie zapasowe były przechowywane wyłącznie w serwerowni Urzędu. Nie zapewniono zatem przechowywania co najmniej jednej kopii w lokalizacji odseparowanej od podstawowego środowiska przetwarzania. Ograniczało to odporność procesu odtwarzania danych na zdarzenia powodujące jednocześnie uszkodzenie serwerowni i przechowywanych w niej kopii.

Wykonywanie odtworzenia systemów z kopii zapasowych było testowane oraz odbywało się w razie potrzeby.

2.11. Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych

W Urzędzie Miasta i Gminy Cieszanów proces administrowania technicznego i monitorowania określonych obszarów systemów, aplikacji, danych, infrastruktury sieciowej i stacji roboczych był wykonywany przez Administratora Systemów Informatycznych (informatyka), co pozwalało na przewidywanie i zapobieganie ewentualnym problemom związanym z awariami, wyciekami bądź utratą danych.

Ustalono, że dla osoby realizującej zadania Administratora Systemów Informatycznych nie wyznaczono formalnego zastępstwa. W przypadku jej nieobecności mogło to ograniczyć zdolność Urzędu do terminowego reagowania na awarie, incydenty bezpieczeństwa oraz zdarzenia wymagające uprawnień administracyjnych.

Systemy centralne, w ramach kontroli podlegały badaniu w ograniczonym zakresie, ze względu na centralne polityki, procedury, wdrożenia i dostępy.

Wybrane systemy własne lub zakupione podlegały sprawdzeniu w zakresie zgodności z rozdz. IV 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.

Najistotniejsze systemy były objęte opieką na podstawie umów opieki autorskiej lub serwisowej.

Pracownicy nie zgłaszali problemów z funkcjonalnością badanych systemów.

2.12. Zabezpieczenia techniczno-organizacyjne dostępu do informacji

Celem zabezpieczeń jest uzyskanie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, a także np. kradzieżą środków przetwarzania informacji. Zastosowane zabezpieczenia powinny być adekwatne do poziomu ryzyka wynikającego z analizy ryzyka bezpieczeństwa informacji. Szereg zabezpieczeń techniczno-organizacyjnych dostępu do informacji opisano w dokumencie Bezpieczeństwo fizyczne i środowiskowe (zał. 5 do Polityki Bezpieczeństwa Informacji).

Ochrona informacji przed kradzieżą, nieautoryzowanym dostępem, uszkodzeniami czy zakłóceniami w UMiG Cieszanów realizowana była poprzez wielowarstwowe zabezpieczenia logiczne, fizyczne i monitorujące, zgodne z wymogami ustanowionego SZBI oraz rozporządzenia KRI §19:

- a) zabezpieczenie dostępu do informacji poprzez wymuszone logowanie użytkowników za pomocą kart lub poprzez podanie unikalnego hasła do badanych systemów;
- b) kontrolę i monitorowanie zabezpieczenia fizycznego dostępu do pomieszczeń oraz zabezpieczenie budynku w system alarmowy;
- c) podejmowanie czynności zmierzających do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji poprzez monitorowanie infrastruktury teleinformatycznej, kontrolę wejść i wyjść do pomieszczenia serwerowni uprawnionych osób;
- d) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji poprzez system autoryzacji dostępu do systemów operacyjnych, sieci i aplikacji, stosowania systemów antywirusowych i antyspamowych.

Urząd Miasta i Gminy Cieszanów posiadał pomieszczenia biurowe zlokalizowane w jednym budynku. W budynku Urzędu Miasta i Gminy mieścił się również Miejsko-Gminny Ośrodek Pomocy Społecznej.

Nowa część obiektu była objęta systemem alarmowym ochrony fizycznej oraz systemem monitoringu wizyjnego. Do otwierania głównych drzwi budynku oraz rozbrajania systemu alarmowego byli upoważnieni wyznaczeni pracownicy. W Urzędzie stosowana była Polityka Kluczy jako załącznik do Polityki Bezpieczeństwo Fizyczne i Środowiskowe.

Ustanowiono strefy bezpieczne z ograniczonym dostępem, takie jak serwerownia, archiwum).

Urząd dysponował jedną główną serwerownią, która znajdowała się w pomieszczeniu przeznaczonym na ten cel. Serwerownia znajdowała się w części budynku przeznaczonej w najbliższym czasie do remontu. W związku z czym nie były podejmowane inwestycje wzmocnienia zabezpieczeń fizycznych lub modernizacji tego pomieszczenia.

Dostęp do serwerowni był ograniczony i możliwy jedynie dla upoważnionych pracowników urzędu. Ważnym elementem ochrony było asystowanie osobom wchodzącym i wykonującym prace serwisowe.

W serwerowni występowało monitorowanie parametrów środowiskowych (temperatury, wilgotności).

Pomieszczenie było klimatyzowane.

Drzwi do serwerowni były wzmocnione, jednak dostęp do pomieszczenia odbywał się przy użyciu zwykłego klucza bez zastosowania dodatkowej kontroli dostępu.

W badanym okresie kopie zapasowe systemów krytycznych nie były przechowywane w odrębnej lokalizacji. Kopie znajdowały się w pomieszczeniu serwerowni, na dedykowanym urządzeniu odseparowanym od środowiska produkcyjnego.

W serwerowni znajdował się UPS, który podtrzymywał pracę serwera i urządzeń sieciowych. Na potrzeby ochrony infrastruktury i zabezpieczenia urządzeń na wypadek przerw w dostawie energii elektrycznej w jednostce wykorzystywane było zasilanie poprzez: agregat prądotwórczy.

Podstawowe urządzenie infrastruktury informatycznej: serwer, urządzenia sieciowe były zakupione w ramach Projektu.

W budynku udostępniona była zabezpieczona sieć bezprzewodowa Wi-Fi, wykorzystywana również do pracy na stanowiskach, na których nie było możliwości podłączenia przewodowego. Oprócz łącza głównego funkcjonowało zapasowe łącze DSL, zapewniające utrzymanie ciągłości działania w przypadku awarii łącza podstawowego.

Monitorowanie ruchu sieciowego wchodzącego i wychodzącego realizowane było przez maszynę sprzętową UTM Fortigate, zakupioną w ramach projektu.

Wszystkie komputery oraz urządzenie sieciowe posiadały oprogramowanie systemowe zaktualizowane do wersji posiadających wsparcie producenta. W ramach projektu Urząd zakupił narzędzie iS SEC klasy SIEM z elementami XDR, EDR oraz monitoringiem infrastruktury IT - służące do wykrywania, korelacji oraz analizy zdarzeń bezpieczeństwa, występujących w systemach i sieciach teleinformatycznych.

Urząd nie dysponował drugim zapasowym pomieszczeniem, jako serwerownia zapasowa. Nośniki uszkodzone lub niezdolne do ponownego użycia były trwale niszczone.

2.13. Zabezpieczenia techniczno-organizacyjne systemów informatycznych

Zabezpieczenia techniczno-organizacyjne systemów informatycznych w UMiG Cieszanów wynikały z analizy ryzyka przeprowadzonej w grudniu 2025 r.

Poziom bezpieczeństwa systemów teleinformatycznych zapewniono poprzez:

- a) aktualizację oprogramowania oraz redukcję ryzyk wynikających z wykorzystywania opublikowanych podatności technicznych systemów teleinformatycznych (w tym oprogramowania antywirusowego);
- b) minimalizację ryzyka utraty informacji w wyniku awarii oraz ochronę przed błędami, utratą i nieuprawnioną modyfikacją, a także zapewnienie bezpieczeństwa plików systemowych, zastosowania systemu kopii zapasowych, systemu kontroli dostępu do zasobów informatycznych, systemu monitorowania funkcjonowania systemów teleinformatycznych i sieci.

Była wdrożona usługa katalogowa Active Directory, która pozwalała na zarządzanie tożsamościami i relacjami w sieci, przez co umożliwiała sprawniejszą kontrolę nad całą siecią oraz użytkownikami.

2.14. Rozliczalność działań w systemach informatycznych

Przetwarzanie informacji w systemach teleinformatycznych urzędów publicznych wymaga obowiązkowego logowania działań użytkowników i administratorów, co zapewnia rozliczalność i wykrywanie incydentów.

Logi muszą rejestrować co najmniej: tożsamość użytkownika, datę, godzinę i rodzaj operacji (kto, kiedy, co), z przeglądem okresowym w celu identyfikacji anomalii oraz przechowywaniem minimum 2 lata w sposób chroniący przed nieautoryzowanym dostępem. Świadomość użytkowników o pełnej identyfikowalności podnosi dyscyplinę bezpieczeństwa.

Urząd posiadał regulacje wewnętrzne określające politykę logów i rozliczalności - Logowanie Zdarzeń w Systemach Informatycznych (zał. 3 do Polityki Bezpieczeństwa Teleinformatycznego). Systemy użytkowe miały udokumentowaną rozliczalność.

3. Zapewnienie dostępności informacji zawartych na stronie BIP oraz internetowej urzędów dla osób niepełnosprawnych

W udostępnianych systemach teleinformatycznych powinny zostać zastosowane rozwiązania techniczne umożliwiające osobom niedosłyszącym lub niedowidzącym zapoznanie z treścią informacji m.in. poprzez powiększenie czcionki, obrazu, zmianę kontrastu, czy też odsłuchanie wyświetlanej treści – zgodnie ze standardem WCAG 2.0.

Podmioty publiczne są zobowiązane zapewnić dostępność cyfrową stron internetowych i aplikacji mobilnych zgodnie z wymaganiami określonymi w ustawie o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych. Wymagania te odpowiadają, co do zasady, standardowi WCAG 2.1 na poziomie AA.

W wyniku automatycznej weryfikacji wybranych stron internetowych, przeprowadzonej przy użyciu polskiego walidatora Utilitia <https://validator.utilitia.pl/> wykazano 4 błędy dla strony BIP oraz 40 błędów dla strony internetowej Urzędu. Wyniki te stanowią przesłankę do przeprowadzenia pogłębionej analizy zgodności z wymaganiami dostępności cyfrowej, ponieważ sama liczba błędów automatycznych nie przesądza o liczbie i wadze naruszonych kryteriów sukcesu WCAG.

Ww. ustalenia, w tym ocena kontrolowanej działalności, zostały udokumentowane w aktach kontroli, na które składają się kopie dokumentów oraz dokumenty przesłane przez urząd drogą elektroniczną.

Przy czym do ww. ustaleń kontrolnych (przekazanych do wiadomości w dniu 26 sierpnia 2026 r.) przysługiwało Panu, na podstawie ww. ustawy o kontroli w administracji rządowej, prawo zgłoszenia umotywowanych pisemnych zastrzeżeń, z którego Pan nie skorzystał.

W związku z powyższym, stosownie do art. 46 ust. 1 ustawy o kontroli w administracji rządowej, sporządzono niniejsze wystąpienie pokontrolne, obejmujące m.in. treść projektu wystąpienia pokontrolnego.

Zgodnie z wymogami § 19 ust. 1-14 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:

1. Wdrożyć i udokumentować proces nadawania, zmiany, przeglądu oraz odbierania uprawnień do systemów informatycznych, obejmujący wnioski, akceptacje, zakres uprawnień oraz potwierdzenie ich odebrania. Przeprowadzać okresowe, udokumentowane przeglądy uprawnień użytkowników i administratorów, w szczególności po zmianie stanowiska, zakresu obowiązków lub ustaniu zatrudnienia.
2. Zapewnić przechowywanie co najmniej jednej kopii w lokalizacji odseparowanej od podstawowego środowiska przetwarzania.
3. Wyznaczyć formalne zastępstwo dla osoby realizującej zadania Administratora Systemów Informatycznych.
4. Dokonać szyfrowania wszystkich urządzeń przenośnych.
5. W związku z planowanym remontem pomieszczenia serwerowni zaleca się przeprowadzenie weryfikacji i odpowiednie zaplanowanie zabezpieczeń fizycznych, środowiskowych oraz technicznych pomieszczenia, z uwzględnieniem charakteru i znaczenia przetwarzanych informacji, lokalizacji serwerowni, wyników analizy ryzyka oraz wymagań dotyczących zapewnienia poufności, integralności, dostępności i rozliczalności informacji.

O sposobie wykonania powyższych wniosków pokontrolnych, bądź działaniach podjętych w celu ich realizacji, oczekuję od Pana odpowiedzi na piśmie, w terminie **21 dni** od dnia otrzymania niniejszego wystąpienia.

WOJEWODA PODKARPACKI

(-)

Teresa Kubas-Hul

(Podpisane bezpiecznym podpisem elektronicznym)