WOJEWODA PODKARPACKI
ul. Grunwaldzka 15
35-959 Rzeszów

OA-IV.431.2.2025

Rzeszów, 2025-05-29

Pan

Andrzej Ślipski
Wójt Gminy Czudec

Na podstawie art. 46 ust. 1 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej, w związku ze zrealizowaną w dniach 8 i 9 kwietnia 2025 r. u Wójta Gminy w Czudcu kontrolą problemową[1], 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 oddziału) na podstawie imiennych upoważnień do kontroli (pisma z dnia 31.03.2025 r., znak OA-IV.431.2.2025) udzielonych przez działającego z upoważnienia Wojewody Podkarpackiego – Dyrektora Wydziału Organizacyjno-Administracyjnego.

Ustalenia kontrolne dokonane zostały w oparciu o stan faktyczny istniejący od 1 stycznia 2024 r. 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 Gminy w Czudcu 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, przejawiający 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 2025 r. „Planu zewnętrznej działalności kontrolnej Podkarpackiego Urzędu Wojewódzkiego w Rzeszowie na 2025 rok”).

W oparciu o poczynione ustalenia, stosownie do skali ocen przyjętej w „Programie kontroli problemowej realizowanej u Wójta Gminy Czudec”[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 Gminy w Czudcu pełnił Wójt: Pan Andrzej Ślipski. Funkcję Inspektora Ochrony Danych (IOD) powierzono wykonawcy zewnętrznemu Panu Danielowi Panek, na podstawie umowy z dnia 02.01.2023 r. z M&P Legal Services Daniel Panek (od 2024 r. MP LEGAL MIELECH, PANEK I WSPÓLNICY Sp. Komandytowa).

Wsparcie informatyczne zapewnione było przez dwóch informatyków, pracowników Urzędu Gminy. Pod ich opieką znajdywały się: środowiska sprzętowo-programowe, sieć lokalna, serwerownie, systemy i aplikacje centralne oraz własne, usprawniające pracę pracownikom Urzędu Gminy w Czudcu.

Zostały wyznaczone osoby odpowiedzialne za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa na podstawie zarządzenia nr 397/2022 Wójta Gminy Czudec z dnia 7 lipca 2022 r. Następnie, w tym samym dniu, zostało dokonane zgłoszenie jednej z osób do CSIRT NASK.

Funkcja Administratora Systemów Informatycznych (ASI) została powierzona osobie zatrudnionej na stanowisku informatyka (2013 r.).

W okresie objętym kontrolą w Urzędzie Gminy w Czudcu 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)
- Centralna Ewidencja Działalności Gospodarczej (CEIDG)

b) systemy własne lub zakupione:
- PB_EWID, PB_EWID_SRP PB_USC+EKSPORT_USC (Ewidencja Ludności i Urząd Stanu Cywilnego) – firmy Technika IT sp. z o.o.,

[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.

- Ewidencja zwrotów podatku akcyzowego – 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),
- 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 Gminy w Czudcu udostępniał elektroniczną skrzynkę podawczą (dalej: ESP) na platformie ePUAP, która pozwalała na przesłanie drogą elektroniczną pism kierowanych do urzędu, w tym pism ogólnych, skarg, wniosków, zapytań itp. Korespondencja z ePUAP nie była odbierana przez używany system obiegu dokumentów.
Na stronie www Urzędu znajdowała się informacja o adresie **elektronicznej skrzynki podawczej**.

1.2. Współpraca systemów teleinformatycznych z innymi systemami

Pracownicy Urzędu Gminy w Czudcu posiadali dostęp do rejestrów publicznych takich jak: SRP Źródło, CEIDG.
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 Gminy w Czudcu był wdrożony Proton - system Elektronicznego Obiegu Dokumentów umożliwiający częściowe zarządzanie dokumentami i wykonywanie czynności kancelaryjnych głównie w zakresie przyjmowania korespondencji. Obecnie funkcjonował on jako system archiwalny, ze względu na brak umowy serwisowej z jego opiekunem.

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 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 zakresie bezpieczeństwa teleinformatycznego w badanej jednostce nie został ustanowiony System Zarządzania Bezpieczeństwem Informacji (SZBI) według wymogów rozporządzenia KRI.
Kluczowe dokumenty z zakresu bezpieczeństwa informacji dotyczyły głównie ochrony danych osobowych, były to:

- Polityka Bezpieczeństwa Danych Osobowych w Urzędzie Gminy w Czudcu wraz z załącznikami, stanowiąca Załącznik Nr 1 do Zarządzenia Nr 331/2018 Wójta Gminy Czudec z dnia 23 maja 2018 r.;
- Instrukcja Bezpieczeństwa Danych Osobowych w Urzędzie Gminy w Czudcu stanowiąca Załącznik Nr 1 do Zarządzenia Nr 373/2018 Wójta Gminy Czudec z dnia 15 listopada 2018 r.;
- Regulamin Bezpieczeństwa Teleinformatycznego w Urzędzie Gminy w Czudcu stanowiący Załącznik Nr 1 do Zarządzenia Nr 374/2018 Wójta Gminy Czudec z dnia 15 listopada 2018 r.;
- Macierz upoważnień do przetwarzania danych osobowych – ustalenie zasad dostępu do przetwarzania danych osobowych dla pracowników i współpracowników Urzędu Gminy w Czudcu - Zarządzenia Nr 232/2020 Wójta Gminy Czudec z dnia 4 grudnia 2020 r.;
- Regulamin funkcjonowania, obsługi i eksploatacji monitoringu wizyjnego w Urzędzie Gminy Czudec stanowiący Załącznik nr 1 do Zarządzenia Nr 263/2021 Wójta Gminy Czudec z dnia 31 marca 2021 r.;
- Zasady dostępu do przetwarzania danych osobowych dla pracowników i współpracowników Urzędu Gminy w Czudcu stanowiące Załącznik do Zarządzenia Nr 232/2020 Wójta Gminy Czudec z dnia 4 grudnia 2020 r.;
- Instrukcja zarządzania zdarzeniami mającymi negatywny wpływ na cyberbezpieczeństwo stanowiąca Załącznik nr 1 do Zarządzenia Nr 397/2022 Wójta Gminy Czudec z dnia 7 lipca 2022 r.

2.2. Analiza zagrożeń związanych z przetwarzaniem informacji

Wymogiem skuteczności SZBI jest przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji. Na analizę ryzyka składają się: identyfikacja, szacowanie a następnie określenie sposobu postępowania z ryzykiem oraz deklaracja stosowania zabezpieczeń będących podstawą podejmowania wszelkich działań minimalizujących ryzyko stosownie do przeprowadzonej analizy.

Zarządzanie bezpieczeństwem przetwarzania danych w Urzędzie Gminy w Czudcu opierało się na zarządzaniu ryzykiem, które polegało na przeprowadzaniu okresowej analizy ryzyka i oceny skutków dla przetwarzania danych. Analiza ryzyka nie była przeprowadzana corocznie. Udostępniony Rejestr Ryzyk Bezpieczeństwa Informacji był z 2018 roku.

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, oprogramowaniach, środkach komunikacji, a także rodzaju relacji między elementami konfiguracji oraz użytkownikiem.

Regulamin Bezpieczeństwa Teleinformatycznego w Urzędzie Gminy w Czudcu w rozdziale XIX Inwentaryzacja sprzętu i oprogramowania zawierał zapisy dotyczące utrzymywania aktualności inwentaryzacji sprzętu informatycznego i oprogramowania przez Informatyka w sposób ręczny.
Ewidencja poszczególnych podzespołów oraz oprogramowania była prowadzona głównie w Ewidencji Środków Trwałych (EST) firmy SOFTRES sp. z o.o.
Jednostka nie dysponowała dedykowanym oprogramowaniem pozwalającym na identyfikację oprogramowania i komputerów w sieci.
W urzędzie do pracy bieżącej, użytkowane były komputery stacjonarne oraz szyfrowane laptopy, a do eksploatacji dopuszczone było tylko oprogramowanie autoryzowane przez Informatyka.

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.
W Urzędzie Gminy w Czudcu zarządzanie uprawnieniami i dostępu do przetwarzania danych, w systemach teleinformatycznych regulowały: Regulamin Bezpieczeństwa Teleinformatycznego, Instrukcja Bezpieczeństwa Danych Osobowych i Polityka Bezpieczeństwa Danych Osobowych. W Regulaminie Bezpieczeństwa Teleinformatycznego w zakresie zarządzania dostępem funkcjonowały zasady: zarządzania systemami oraz tworzenia i likwidacji kont użytkowników systemu informatycznego, w tym uwierzytelniania w systemie informatycznym, dorocznych przeglądów.
Dodatkowo w Polityce Bezpieczeństwa Danych Osobowych zostały zawarte zasady upoważnień do przetwarzania danych osobowych (rozdział XI).

Dokumentacja powyższa opisywała sposób dostępu do obszarów chronionych, sieci i systemów teleinformatycznych oraz nadawania, zmiany i odbierania uprawnień użytkownikom w systemach informatycznych funkcjonujących w jednostce.
Pracownicy uzyskiwali dostęp do zasobów informatycznych po przyznaniu zakresu obowiązków, nadaniu upoważnienia oraz ustanowieniu unikalnego identyfikatora i hasła w systemie teleinformatycznym.
W przypadku konieczności zmiany i odbioru uprawnień dla użytkownika w systemach informatycznych informacja przekazywana była ustnie, pomimo zapisów w Regulaminie Bezpieczeństwa Teleinformatycznego o przekazywaniu przez pracownika ds. kadr informacji za pośrednictwem poczty elektronicznej.
Zakres uprawnień użytkowników badanych systemów uniemożliwiał wykonywanie przez nich działań zastrzeżonych dla administratorów systemów.
W okresie objętym badaniem konta byłych pracowników urzędu były sukcesywnie blokowane w systemach informatycznych. Na bieżąco odbywało się monitorowanie dostępu do zasobów informatycznych zgodnie z wymaganiami § 19 ust. 2 pkt 4 rozporządzenia KRI.

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.
Polityka Bezpieczeństwa Danych Osobowych Urzędu Gminy w Czudcu w sposób ogólny regulowała, że osoby upoważnione do przetwarzania danych osobowych przed dopuszczeniem do tych danych są szkolone w zakresie obowiązujących przepisów o ochronie danych osobowych.
Kontrolującym przedstawiono informację o przeprowadzonym szkoleniu dla pracowników w 2025 roku, z zakresu: Metod zabezpieczeń nośników informacji.
Dodatkowo pracownicy byli informowani o najważniejszych zagrożeniach mailowo przez Inspektora Ochrony Danych.
Informacji o Planie szkoleń oraz zrealizowanych szkoleniach w poprzednim roku nie przedstawiono.

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. Konieczne jest opisanie zasad określających sposoby zabezpieczenia urządzeń mobilnych i danych w nich zawartych przed kradzieżą i nieuprawnionym dostępem poza siedzibą jednostki, a także zasady korzystania z ogólnodostępnych sieci.
W obowiązujących dokumentach były zawarte ogólne zasady korzystania z urządzeń mobilnych i sposoby zabezpieczenia tych urządzeń (Regulamin Bezpieczeństwa Teleinformatycznego - rozdziały: Zasady korzystania z urządzeń mobilnych, Zasady korzystania z nośników, Zasady bezpieczeństwa przy przetwarzaniu mobilnym i pracy na

odległość). Nie przedstawiono Regulaminu Pracy Zdalnej, gdyż do tej pory dla pracowników nie było potrzeby stosowania takiej możliwości.
Pracownicy nie wynosili przenośnych komputerów poza siedzibę jednostki. Laptopy nie były szyfrowane, natomiast pendrive przekazywane pracownikom były szyfrowane.

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.
W procedurach wewnętrznych dot. ochrony danych osobowych zostały określone zasady współpracy z podmiotami trzecimi jedynie w zakresie przetwarzania danych osobowych.
Dodatkowo, poziom bezpieczeństwa regulowały umowy zawierane z firmami zewnętrznymi, w przypadku serwisowania sprzętu lub oprogramowania.
Nie we wszystkich sprawdzanych umowach o asystę i opiekę autorską lub serwisową z firmami zewnętrznymi były określone zasady i czas dostępu, zwłaszcza zdalnego oraz określone SLA (Service Level Agreement), czyli gwarantowany poziom świadczenia usług oraz czas i sposób reakcji na zgłaszane problemy (udostępniono umowę licencyjną z Biurem Usług komputerowych SOFTRES sp. z o.o. – 2025 r., z ENFORMATEL Sp. z o.o. – z 2025 r., Royal Group Sp. z o.o. – z 2025 r.).
W przypadku systemów informatycznych istotnych dla jednostki zostały zawarte także umowy powierzenia przetwarzania danych osobowych (udostępniono m.in. umowę: z Biurem Usług komputerowych SOFTRES sp. z o.o., z Ideo Sp. z o.o.).

2.8. Procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji

Zostały określone zasady postępowania w przypadku stwierdzenia naruszenia bezpieczeństwa informacji zarówno w Polityce Bezpieczeństwa Danych Osobowych (Rozdział XV Postępowanie w przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych) jak i Instrukcji zarządzania zdarzeniami mającymi negatywny wpływ na cyberbezpieczeństwo (tzw. incydentami).
Rejestr naruszeń bezpieczeństwa danych osobowych Urzędu Gminy w Czudcu zawierał trzy wpisy od 2020 r.
Rejestru dotyczącego naruszeń bezpieczeństwa informatycznego nie przedstawiono.

2.9. Audyt wewnętrzny z zakresu 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 był wykonany w 2024 roku. Warto zwrócić uwagę, że celem audytów jest ewentualne ujawnienie słabości systemów, a także słabości zabezpieczeń lub ich stosowania. Uregulowania wewnętrzne nie zawierały zapisów dotyczących konieczności audytowania i sprawdzeń w zakresie bezpieczeństwa informacji.

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

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 Gminy w Czudcu obowiązywały wymagania określone w Regulaminie Bezpieczeństwa Teleinformatycznego (rozdział XV Zasady tworzenia kopii zapasowych).
Kopie folderów, maszyn wirtualnych były wykonywane według harmonogramu ustalonego przez ASI oraz przechowywane na serwerze NAS Synology. W jednostce było wykorzystywane dedykowane rozwiązanie do ochrony danych (dające możliwość tworzenia kopii zapasowych i odzyskiwania) - Veeam B&R.
Wykonywanie odtworzenia systemów z kopii zapasowych było testowana oraz odbywało się w razie potrzeby.

2.11. Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych

W Urzędzie Gminy w Czudcu proces administrowania technicznego i monitorowania określonych obszarów systemów, aplikacji, danych, infrastruktury sieciowej i stacji roboczych był wykonywany przez informatyków, co pozwalało na przewidywanie i zapobieganie ewentualnym problemom związanym z awariami, wyciekami bądź utratą danych.
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 Regulaminie Bezpieczeństwa Teleinformatycznego, Instrukcji Bezpieczeństwa Danych Osobowych oraz Polityce Bezpieczeństwa Danych Osobowych w Urzędzie Gminy Czudec.
Ochrona przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami realizowana była przez:

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;

c) podejmowanie czynności zmierzających do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji poprzez monitorowanie infrastruktury teleinformatycznej, kontrolę wejść i wyjść do pomieszczeń 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 Gminy w Czudcu posiadał pomieszczenia biurowe zlokalizowane w jednym budynku.
Obiekt był objęty systemem alarmowym ochrony fizycznej oraz był objęty systemem monitoringu na zewnątrz i wewnątrz budynku. Do otwierania głównych drzwi budynku oraz rozbrajania systemu alarmowego byli upoważnieni wyznaczeni pracownicy.
Urząd Gminy dysponował jedną główną serwerownią, która znajdowała się w pomieszczeniu przeznaczonym na ten cel. Dostęp do serwerowni był ograniczony i możliwy jedynie dla upoważnionych pracowników urzędu. Ważnym elementem ochrony było asystowanie osobom wchodzącym i wykonującym prace serwisowe.
Serwerownia główna posiadała system kontroli wejść (kamera). Występowało monitorowanie niektórych parametrów środowiskowych w serwerowni (temperatury). Pomieszczenie było klimatyzowane.
Drzwi do serwerowni nie były wzmocnione. Jedna z wewnętrznych ścian była z luksferami.
Bazy danych z kopiami były umieszczone w innym bezpiecznym miejscu, poza serwerownią.
W serwerowni znajdował się UPS, który podtrzymywał pracę serwera i urządzeń sieciowych.
W pomieszczeniu nie były przechowywane materiały łatwopalne.
Podstawowe urządzenie infrastruktury informatycznej: serwer, urządzenia sieciowe były zakupione w ramach Projektu.
Monitorowanie ruchu wchodzącego i wychodzącego realizowane było przez maszynę sprzętową UTM Fortigate. W ramach projektu „Cyberbezpieczny Samorząd” zaplanowany został zakup nowych UTM oraz narzędzia klasy SIEM, służącego do wykrywania, korelacji oraz analizy zdarzeń bezpieczeństwa, występujących w systemach i sieciach teleinformatycznych.
Urząd nie dysponował drugim zapasowym pomieszczeniem, jako serwerownia zapasowa oraz nie posiadał zapasowych łączy internetowych.
Wszystkie komputery oraz urządzenie sieciowe posiadały oprogramowanie systemowe zaktualizowane do wersji posiadających wsparcie producenta.

2.13. Zabezpieczenia techniczno-organizacyjne systemów informatycznych

Stosowanie zabezpieczeń techniczno-organizacyjnych również powinno wynikać z analizy ryzyka i powstałego w jej wyniku planu postępowania z ryzykiem i deklaracji stosowania zabezpieczeń.
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 wymagało dostępu do danych przez uprawnionych użytkowników. Wszelkie działania związane z przetwarzaniem informacji, a także działania administratorów muszą podlegać dokumentowaniu w postaci zapisów w dziennikach systemów (logi), co zapewnia rozliczalność operacji. Informacje zawarte w logach (tj. kto, kiedy i co wykonał w systemie teleinformatycznym) powinny być regularnie przeglądane w celu wykrycia działań niepożądanych i muszą być przechowywane w bezpieczny sposób, co najmniej dwa lata. Świadomość użytkowników, że żadne działanie nie zostanie anonimowe podnosi poziom bezpieczeństwa informacji.

Urząd Gminy w Czudcu nie dysponował regulacjami wewnętrznymi, w których określone byłyby zasady polityki zarządzania logami oraz rozliczalności działań poszczególnych obiektów.
Sprawdzane systemy informatyczne użytkowe miały udokumentowane rozliczalności.

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.

Systemy informatyczne wspomagające realizację zadań urzędu nie były objęte wymogami WCAG 2.0 w zakresie dostępności ze względu na brak interakcji z klientami za pośrednictwem sieci publicznej.
Analizując poprawność kodu strony BIP poprzez walidator dostępny pod adresem: https://validator.utilitia.pl/ badana strona uzyskała wynik 5,5 pkt na 10 możliwych, natomiast strona www uzyskała wynik 7,3 pkt na 10 możliwych.

Ww. ustalenia, w tym ocena kontrolowanej działalności, zostały udokumentowane w aktach kontroli, na które składają się kopie dokumentów.

Przy czym do ww. ustaleń kontrolnych (przekazanych do wiadomości w dniu 8 maja 2025 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. Dokonać analizy wszystkich umów serwisowych ze stronami trzecimi i w razie potrzeby uzupełnić je o zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji, w tym określić SLA (Service Level Agreement), czyli gwarantowany poziom świadczenia usług, ciągłość działania, zasady i czas dostępu zdalnego, czas i sposób reakcji na zgłaszane problemy oraz prowadzić nadzór nad wykonawcami w zakresie zgodności z regulacjami i zapisami.
2. Dążyć do wzmocnienia zabezpieczeń techniczno-organizacyjnych (drzwi, ściany) pomieszczenia pełniącego rolę serwerowni.
3. Niezbędne jest ustalenie, wdrożenie, a następnie eksploatowanie, monitorowanie, przeglądanie i doskonalenie pełnego systemu zarządzania bezpieczeństwem informacji uwzględniającego zarządzanie ryzykiem (wziąć pod uwagę utratę integralności, dostępności lub poufności wszystkich informacji oraz ciągłość działania systemu bezpieczeństwa informacji).
4. Wprowadzić inwentaryzację sprzętu i oprogramowania informatycznego służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację (§ 19 ust. 2 pkt 2 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).
5. Wdrożyć szyfrowanie wszystkich urządzeń przenośnych.

O sposobie wykonania powyższych wniosków pokontrolnych, bądź działaniach podjętych w celu ich realizacji, oczekuję od Pana odpowiedzi na piśmie wraz ze skanami dokumentów lub innych potwierdzeń dotyczących sposobu wdrożenia zaleceń, w terminie **21 dni** od dnia otrzymania niniejszego wystąpienia.

WOJEWODA PODKARPACKI
(-)

Teresa Kubas-Hul
(Podpisane bezpiecznym podpisem elektronicznym)