

 **WOJEWODA PODKARPACKI**

 ul. Grunwaldzka 15

 35-959 Rzeszów

 OA-IV.431.1.2022 Rzeszów, 2022-07-01

**Pan**

**Andrzej Głaz**

**Wójt Gminy Tuszów Narodowy**

 Na podstawie art. 46 ust. 1 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej, w związku ze zrealizowaną w dniach 12 i 18 maj 2022 r. u Wójta Gminy Tuszów Narodowy (Gmina Tuszów Narodowy, 39-332 Tuszów Narodowy 225) kontrolą problemową[[1]](#footnote-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 (kierownik) na podstawie imiennych upoważnień do kontroli (pisma z dnia 13.04.2022 r., znak OA-IV.431.1.2022) udzielonych przez Wojewodę Podkarpackiego.

Ustalenia kontrolne dokonane zostały w oparciu o stan faktyczny istniejący od 1 stycznia 2021 r.do dnia realizacji czynności kontrolnych włącznie.

Kontrola obejmuje priorytet Prezesa Rady Ministrów na 2021 r. pn. „Bezpieczeństwo teleinformatyczne oraz cyfryzacja usług i procesów w administracji”.

W toku kontroli - w oparciu o kontrolowane dokumenty (przy zastosowaniu metody niestatystycznej, losowy dobór próby) - ustalono, iż pracownicy Urzędu Gminy Tuszów Narodowy 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.

W oparciu o poczynione ustalenia, stosownie do skali ocen przyjętej w „Programie kontroli problemowej realizowanej u Wójta Gminy Tuszów Narodowy”[[2]](#footnote-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 Tuszów Narodowy pełnił Wójt: Pan Andrzej Głaz.

Funkcję Inspektora Ochrony Danych (IOD) pełnił pracownik Urzędu Gminy.

Wsparcie informatyczne zapewnione było również przez pracownika Urzędu Gminy. Pod jego opieką znajdowały się: środowiska sprzętowo-programowe, sieć lokalna i serwerownia, systemy i aplikacje centralne oraz własne, usprawniające pracę pracownikom Urzędu Gminy Tuszów Narodowy.

Informatyk pełnił funkcję Administratora Systemów Informatycznych (ASI) na podstawie Zarządzenia Nr 7/w/2013 Wójta Gminy Tuszów Narodowy z dnia 1 lipca 2013 roku w sprawie wyznaczenia Administratora Systemu Informatycznego w Urzędzie Gminy w Tuszowie Narodowym oraz określenia jego zadań.

W okresie objętym kontrolą w Urzędzie Gminy Tuszów Narodowy 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)

- SIO (System Informacji Oświatowej)

b) systemy własne lub zakupione:

 - SELWIN (Rejestr Mieszkańców, Rejestr wyborców) – firmy ARAM Software,

 - 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. Usługi elektroniczne

Urząd Gminy Tuszów Narodowy 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 odbierana była bezpośrednio w ePUAP.

Na stronie głównej oraz na stronie BIP kontrolowanej jednostki znajdowała się informacja o adresie **elektronicznej skrzynki podawczej**.

* 1. Współpraca systemów teleinformatycznych z innymi systemami

Pracownicy Urzędu Gminy Tuszów Narodowy posiadali dostęp do rejestrów publicznych takich jak: SRP Źródło, CEIDG.

System SELWIN w zakresie komunikacji z usługami sieciowymi Systemu Rejestrów Państwowych komunikował się dzięki subskrypcji inicjalnej oraz przyrostowej danych z rejestru PESEL.

* 1. Obieg dokumentów

W Urzędzie Gminy Tuszów Narodowy nie funkcjonował system Elektronicznego Zarządzania Dokumentacją umożliwiający zarządzanie dokumentami i wykonywanie czynności kancelaryjnych.

1. **Wdrożenie systemu zarządzania bezpieczeństwem informacji w systemach teleinformatycznych**
	1. Dokumenty z zakresu bezpieczeństwa informacji

Zgodnie z § 20 ust. 1 rozporządzenia KRI podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarzadzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji. 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).

Kluczowe dokumenty dotyczyły głównie ochrony danych osobowych, były to:

* Polityka Bezpieczeństwa wprowadzona Zarządzeniem nr 10/W/2021 Wójta Gminy Tuszów Narodowy z dnia 02 listopada 2021 r. wraz z załącznikami;
* Instrukcja Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Tuszów Narodowy stanowiąca Załącznik do Zarządzenia nr 7/W/2021 Wójta Gminy Tuszów Narodowy z dnia 01 września 2021 roku wraz z załącznikami;
* Instrukcja Naruszenia Ochrony Danych Osobowych w Urzędzie Gminy w Tuszowie Narodowym stanowiąca Załącznik nr 1 do Zarządzenia nr 6/W/2018 Wójta Gminy Tuszów Narodowy z dnia 30 lipca 2018 roku;
* Regulamin Pracy Zdalnej w Urzędzie Gminy Tuszów Narodowy stanowiący Załącznik do Zarządzenia nr 16.W.2020 Wójta gminy Tuszów Narodowy z dnia 30 czerwca 2020 r. wraz z załącznikami;
* Regulamin funkcjonowania monitoringu wizyjnego w Urzędzie Gminy Tuszów Narodowy stanowiąca Załącznik nr 1 do Zarządzenia nr 12/W/2018 Wójta Gminy Tuszów Narodowy z dnia 26 listopada 2018 roku;
* Instrukcja postępowania z kluczami oraz zabezpieczenia pomieszczeń w Urzędzie Gminy w Tuszowie Narodowym stanowiąca Załącznik do Zarządzenia nr 9/W/2017 Wójta Gminy Tuszów Narodowy z dnia 15 grudnia 2017 r. wraz z załącznikiem;
* Polityka czystego biurka i czystego ekranu stanowiąca Załącznik nr 1 do Zarządzenia nr 10/W/2017 Wójta Gminy Tuszów Narodowy z dnia 15 grudnia 2017 roku;
* Instrukcja postępowania w przypadku naruszenia ochrony danych osobowych w systemach informatycznych stanowiąca Załącznik nr 1 do Zarządzenia nr 22/W/2012 Wójta Gminy Tuszów Narodowy z dnia 27 grudnia 2012 r.;
* Procedura Zarządzania ryzykiem w obszarze ochrony danych osobowych stanowiąca załącznik nr 1 do Zarządzenia nr 5/W/2018 Wójta Gminy Tuszów Narodowy z dnia 10 lipca 2018 roku.
	1. 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.

W Urzędzie Gminy Tuszów Narodowy wprowadzona została Procedura Zarządzania ryzykiem w obszarze ochrony danych osobowych i na jej podstawie dokonywana była analiza identyfikacji ryzyka, obejmująca plan postepowania z ryzykiem. Analiza identyfikacji ryzyka ograniczała się do ochrony danych osobowych, nie obejmowała wszystkich zagadnień bezpieczeństwa informacji.

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.

* 1. 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, oprogramowaniu i środkach komunikacji, ich rodzaju, parametrach, aktualnej konfiguracji i relacjach między elementami konfiguracji oraz użytkowniku.

W Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Tuszów Narodowy został zawarty krótki zapis dotyczący procesu inwentaryzacji sprzętu oraz wprowadzony został formularz Ewidencja urządzeń elektronicznych przetwarzających dane osobowe (Rozdział XV).

Kontrola inwentaryzacji sprzętu powinna być przeprowadzana na koniec roku kalendarzowego przez ASI. Kontrolującym przekazano specyfikację ze stanem na 1.09.2020 r. w postaci Karty technicznej sprzętu komputerowego zgodną z formularzem.

* 1. 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 badanym okresie zarządzanie uprawnieniami dostępu do przetwarzania danych w Urzędzie Gminy regulowały: Polityka Bezpieczeństwa i Instrukcja Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych.

Dokumentacja powyższa szczegółowo opisywała sposób dostępu do obszarów chronionych, sieci i systemów teleinformatycznych oraz nadawania, zmiany i odbierania uprawnień użytkownikom w systemach informatycznych funkcjonujących w jednostce.

Uprawnienia w systemie informatycznym nadawane były przez Administratora Systemu Informatycznego na podstawie Upoważnienia do przetwarzania danych osobowych.

Dostęp do zasobów informatycznych zależny był od zakresu obowiązków.

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.

W przypadku konieczności nadania, zmiany i odbioru uprawnień dla użytkownika w systemach informatycznych informacja przekazywana była ustnie, pomimo powołania się w dokumentach na wprowadzenie Upoważnienia do pracy w systemie informatycznym Urzędu Gminy oraz wzoru wniosku o nadanie, modyfikację lub odebranie uprawnień w systemie (Rozdział III Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Tuszów Narodowy).

Na bieżąco odbywało się monitorowanie dostępu do zasobów informatycznych zgodnie z wymaganiami § 20 ust. 2 pkt 4 rozporządzenia KRI.

* 1. 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 Gminy Tuszów Narodowy regulowała zakres podnoszenia świadomości pracowników poprzez konieczność zapoznania wszystkich osób przetwarzających dane osobowe w zakresie zabezpieczeń systemu informatycznego, a także o obowiązku do ich przestrzegania.

Z zakresu bezpieczeństwa informatycznego było przeprowadzane szkolenie wewnętrzne dla nowo przyjętych pracowników (notatka z dnia 4 marca 2022 r., i 19 sierpnia 2021 r.).

Natomiast dla pozostałych pracowników zostało przeprowadzone spotkanie w 2021 r., dotyczące tematów z bezpieczeństwa informatycznego oraz sprawdzenia ich wiedzy nt. przestrzegania zasad ochrony danych osobowych (test wykonało 23 pracowników).

* 1. 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.

Został ustanowiony Regulamin Pracy Zdalnej w Urzędzie Gminy Tuszów, który określał szczegółowe zasady takiej pracy spowodowanej możliwością wystąpienia sytuacji kryzysowej.

Jednak w żadnym dokumencie nie zostały ustanowione zasady zarządzania bezpieczną pracą na komputerach przenośnych i sposoby zabezpieczenia tych urządzeń.

Pracownicy wynosili przenośne komputery poza siedzibę jednostki, laptopy były szyfrowane a dostęp zdalny był możliwy przez mechanizm VPN.

* 1. 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 nie określono zasad współpracy z podmiotami trzecimi w zakresie przetwarzania informacji i serwisu sprzętu teleinformatycznego.

W przypadku umów zawieranych z firmami zewnętrznymi o asystę i opiekę autorską lub serwisową nie wszystkie miały określony poziom SLA (Service Level Agreement), czyli gwarantowany poziom świadczenia usług oraz czas i sposób reakcji na zgłaszane problemy (udostępniono umowę z firmą Usługi Informatyczne i Projektowe „Admin-Comp” oraz z firmą INTERmedi@ Ł. Czekała T. Frąckowiak spółka jawna.).

W przypadku systemów informatycznych istotnych dla jednostki zostały zawarte umowy powierzenia przetwarzania danych osobowych (udostępniono umowę z: firmą Usługi Informatyczne i Projektowe „Admin-Comp” i firmą INTERmedi@). Niemniej w umowach zawartych w 2022 roku były nieaktualne wpisy dot. podstawy prawnej oraz serwisowanych baz.

* 1. Procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji

Zostały określone zasady postepowania w przypadku stwierdzenia naruszenia bezpieczeństwa informacji w Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Tuszów Narodowy (Rozdział XI) oraz w Instrukcji Naruszenia Ochrony Danych Osobowych w Urzędzie Gminy w Tuszowie Narodowym. Według wyjaśnień rejestr incydentów nie zawierał wpisów dotyczących naruszenia bezpieczeństwa informacji.

* 1. Audyt wewnętrzny z zakresu bezpieczeństwa informacji

Audyt z zakresu bezpieczeństwa informacji nie rzadziej niż raz na rok, w rozumieniu § 20 ust. 14 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych był wykonywany w 2020 roku przez firmę zewnętrzną. Tematem Sprawozdania z zadania audytowego przeprowadzonego w Urzędzie Gminy Tuszów Narodowy była „Ocena 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.

* 1. Kopie zapasowe

Wykonywanie kopii zapasowych zapobiega utracie informacji w wyniku awarii.

Kopie powinny być właściwie tworzone, przechowywane i testowane.

Zakres wykonywania kopii zapasowych był określony w wewnętrznej dokumentacji: Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Tuszów Narodowy. Zapisy odbiegały od rzeczywistego sposobu wykonywania kopii zapasowych dlatego informacja została zaktualizowane na potrzeby kontroli w notatce z dnia 18.05.2022 r. sporządzonej przez ASI.

Wykonywanie odtworzenia systemów z kopii zapasowych występowało w razie potrzeby.

* 1. Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych

W Urzędzie Gminy Tuszów Narodowy proces administrowania technicznego i monitorowania określonych obszarów systemów, aplikacji, danych, infrastruktury sieciowej i stacji roboczych był wykonywany przez informatyka, 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 12 kwietnia 2012 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.

* 1. 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 Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Tuszów Narodowy oraz w Polityce Bezpieczeństwa.

Ochrona przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami realizowana była przez:

1. zabezpieczenie dostępu do informacji poprzez wymuszone logowanie u użytkowników za pomocą kart lub poprzez podanie unikalnego hasła do badanych systemów;
2. kontrolę i monitorowanie zabezpieczenia fizycznego dostępu do pomieszczeń;
3. podejmowanie czynności zmierzających do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji poprzez monitorowanie infrastruktury teleinformatycznej, kontrolę wejść i wyjść do pomieszczeń serwerowni uprawnionych osób;
4. 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 Tuszowie Narodowym posiadał lokalizację w jednym budynku.

Obiekt był objęty systemem monitoringu oraz był objęty systemem alarmowym ochrony fizycznej, natomiast system ppoż. obejmował tylko archiwum.

Klucze do budynku były zabezpieczone i przechowywane przez pracowników uprawnionych do otwierania budynku oraz rozkodowywania systemu alarmowego. W tym celu opracowana i wdrożona została Instrukcja postępowania z kluczami oraz zabezpieczenia pomieszczeń w Urzędzie Gminy w Tuszowie Narodowym (Zarządzenie Nr 9/W/2017 Wójta Gminy Tuszów Narodowy z dnia 15 grudnia 2017 r.).

W tym samym budynku miał również siedzibę Gminny Ośrodek Pomocy Społecznej oraz znajdowały się delikatesy spożywcze.

Urząd Gminy dysponował jedną serwerownią, która umieszczona była w pomieszczeniu zaadaptowanym na ten cel. To pomieszczenie było także pokojem informatyka. Dostęp do serwerowni był ograniczony i możliwy jedynie dla upoważnionych pracowników urzędu. Ważnym elementem ochrony było asystowanie osobom wchodzącym i wykonującym prace serwisowe.

Serwerownia posiadała zainstalowany system alarmowy. Nie występowało monitorowanie parametrów środowiskowych w serwerowni (np. temperatury, wilgotności). Pomieszczenie było klimatyzowane.

Drzwi do serwerowni były wzmocnione i ognioodporne.

Bazy danych z kopiami były umieszczone w tym samym miejscu.

W serwerowni znajdował się UPS, który podtrzymywał pracę serwera i urządzeń sieciowych. Strategiczne stanowiska komputerowe także wyposażone były w urządzenia UPS podtrzymujące pracę komputera podczas zaników prądu.

W pomieszczeniu nie były przechowywane materiały łatwopalne.

Do połączeń internetowych było wykorzystywane łącze główne oraz przygotowane drugie jako zapasowe.

Sieć bezprzewodowa nie była wykorzystywana przez pracowników do pracy w urzędzie.

Podstawowe urządzenie infrastruktury informatycznej – to dwa serwery fizyczne oraz cztery wirtualne.

W ramach zabezpieczenia dostępu stosowana była zapora sieciowa typu firewall z nowo zakupioną licencją.

Komputery oraz urządzenie sieciowe posiadały oprogramowanie systemowe zaktualizowane do wersji posiadających wsparcie producenta.

Sprzęt komputerowy był ubezpieczony.

W ramach programu „Polska Cyfrowa”, jest planowany m.in. zakup serwera z oprogramowaniem oraz urządzenia do backupu.

* 1. 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:

1. aktualizację oprogramowania oraz redukcję ryzyk wynikających z wykorzystywania opublikowanych podatności technicznych systemów teleinformatycznych (w tym oprogramowania antywirusowego);
2. 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.

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

* 1. 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 Tuszowie Narodowym nie dysponował regulacjami wewnętrznymi, w których określone byłyby zasady rozliczalności działań wykonywanych w systemach informatycznych.

Sprawdzane systemy informatyczne użytkowe miały udokumentowaną rozliczalność.

1. **Zapewnienie dostępności informacji zawartych na stronach internetowych 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 i strony www poprzez walidator dostępny pod adresem: https://validator.utilitia.pl/ badane strony uzyskały wynik 5,5 pkt na 10 możliwych.

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

Przy czym do ww. ustaleń kontrolnych (przekazanych do wiadomości w dniu 13 czerwca 2022 r.) przysługiwało Panu, na podstawie ww. ustawy o kontroli w administracji rządowej, prawo zgłoszenia umotywowanych pisemnych zastrzeżeń, z których Pan nie skorzystał. W ramach ww. uprawnienia nie skorzystał Pan również z prawa skierowania wniosku o przedłużenie terminu do złożenia zastrzeżeń.

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.

Przedstawiając powyższe uwagi i oceny, dokonane m.in. w oparciu o projekt wystąpienia pokontrolnego oraz ww. akta kontroli, w celu usunięcia stwierdzonych uchybień oraz usprawnienia badanej działalności, przekazuję Panu następujące wnioski, zalecenia pokontrolne:

1. W umowach serwisowych ze stronami trzecimi zawierać zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji, w tym połączeń zdalnych i określić poziom SLA oraz zadbać aktualność zapisów w obowiązujących umowach.
2. Należy rozważyć montaż urządzeń badających warunki środowiskowe w serwerowni (temperatura, wilgotność, dym, otwarcie drzwi). Urządzenia te można skonfigurować tak, aby informacje o wystąpieniu w pomieszczeniu serwerowni niekorzystnych warunków środowiskowych wysyłane były poprzez np. e-mail, SMS.
3. Nośniki kopii zapasowych przechowywać w innym pomieszczeniu niż serwerownia.
4. Zgodnie z wymogami § 20 ust. 1-3 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych niezbędne jest opracowanie dokumentacji, ustanowienie, wdrożenie, a następnie eksploatowanie, monitorowanie, przeglądanie i doskonalenie pełnego systemu bezpieczeństwa informacji wraz z uzupełnieniem dokumentacji o niezbędne elementy, jej sprawdzenie i ujednolicenie.
5. Przeprowadzić okresowe analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz utworzyć plan zachowania ciągłości działania.
6. Ustanowić podstawowe zasady gwarantujące bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość.
7. Wdrożyć i ujednolicić zasady nadawania uprawnień do pracy w systemach informatycznych.

O sposobie wykonania powyższych wniosków pokontrolnych, bądź działaniach podjętych w celu ich realizacji, oczekuję od Pana odpowiedzi na piśmie, w terminie **30 dni** od dnia otrzymania niniejszego wystąpienia.

**WOJEWODA PODKARPACKI**

**(-)**

**Ewa Leniart**

(Podpisane bezpiecznym podpisem elektronicznym)

1. W oparciu o zatwierdzony w dniu 22 grudnia 2021 r. „Plan zewnętrznej działalności kontrolnej Podkarpackiego Urzędu Wojewódzkiego w Rzeszowie na 2022 rok”. [↑](#footnote-ref-1)
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. [↑](#footnote-ref-2)