

 **WOJEWODA PODKARPACKI**

 ul. Grunwaldzka 15

 35-959 Rzeszów

 OA-IV.431.1.2021 Rzeszów, 2021-11-09

**Pan**

**Andrzej Ożóg**

**Burmistrz Gminy i Miasta**

**Sokołowa Małopolskiego**

 Na podstawie art. 46 ust. 1 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej, w związku ze zrealizowaną w dniach 13 i 15 września 2021 r. u Burmistrza Gminy i Miasta (Urząd Gminy i Miasta w Sokołowie Małopolskim, ul. Rynek 1, 36-050 Sokołów Małopolski) 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 01.09.2021 r., znak OA-IV.431.1.2021) udzielonych przez działającego z upoważnienia Wojewody Podkarpackiego – Dyrektora Wydziału Organizacyjno-Administracyjnego.

Ustalenia kontrolne dokonane zostały w oparciu o stan faktyczny istniejący od 1 stycznia 2020 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 i Miasta w Sokołowie Małopolskim 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.

W oparciu o poczynione ustalenia, stosownie do skali ocen przyjętej w „Programie kontroli problemowej realizowanej u Burmistrza Gminy i Miasta Sokołowa Małopolskiego”[[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 i Miasta w Sokołowie Małopolskim pełnił Burmistrz: Pan Andrzej Ożóg.

Funkcję Inspektora Ochrony Danych (IOD) powierzono pracownikowi Urzędu Gminy i Miasta Sokołów Małopolski Panu Piotrowi Rafińskiemu, który był zatrudniony w Urzędzie jako Informatyk.

Wsparcie informatyczne zapewnione było przez informatyka i kierownika Referatu Organizacyjno - Administracyjnego. Pod ich opieką znajdowało się: środowisko sprzętowo-programowe, sieć lokalna i serwerownia, systemy i aplikacje centralne oraz własne, usprawniające pracę pracownikom Urzędu Gminy i Miasta.

Kierownik referatu Organizacyjno - Administracyjnego pełnił funkcję Administratora Systemu Informatycznego (ASI).

W okresie objętym kontrolą w Urzędzie Gminy i Miasta użytkowane były systemy teleinformatyczne zakupione przez urząd oraz tzw. 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:

- Lokalny Rejestr Mieszkańców wraz z modułem ImportSRP – firmy Clanet – Klaudiusz Gatys

- Proton - Elektroniczny Obieg Dokumentów firmy Sputnik wdrożony w ramach projektu PSeAP (Podkarpacki System E-Administracji Publicznej)

- Ewidencja wniosków o Zwrot Podatku Akcyzowego (AKC) – Biura Usług Komputerowych „Softres” sp. z o.o.

- pozostałe moduły firmy „Softres” sp. z o.o.

- 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 i Miasta w Sokołowie Małopolskim 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. System Proton komunikował się z systemem zewnętrznym ePUAP w celu odbierania i wysyłania korespondencji w postaci elektronicznej. Korespondencja wpływająca przez ESP była rejestrowana w systemie Proton i kierowana do kierowników referatów lub pracowników.

Na stronie głównej oraz na stronie BIP kontrolowanej jednostki była informacja o adresie elektronicznej skrzynki podawczej.

1.2. Obieg dokumentów

W Urzędzie Gminy i Miasta w Sokołowie Małopolskim funkcjonował system – Proton umożliwiający zarządzanie dokumentami i wykonywanie czynności kancelaryjnych. Był to system pomocniczy w sposobie dokumentowania przebiegu załatwiania spraw.

1.3. Współpraca systemów teleinformatycznych z innymi systemami

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

System ImportSRP komunikował się z usługami sieciowymi Systemu Rejestrów Państwowych w celu pobierania danych dzięki modułowi odpowiadającemu za transmisję danych z SRP do Lokalnego Rejestru Mieszkańców.

2. **Wdrożenie systemu zarządzania bezpieczeństwem informacji w systemach teleinformatycznych**

2.1. 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 i wprowadzony pełny System Zarządzania Bezpieczeństwem Informacji (SZBI).

Kluczowym dokumentem ramowym w zakresie bezpieczeństwa infrastruktury oraz systemów informatycznych była Instrukcja Zarządzania Systemami Informatycznymi, stanowiąca odzwierciedlenie deklarowanych przez Burmistrza Gminy i Miasta w Sokołowie Małopolskim wytycznych w zakresie bezpieczeństwa informacji. Kolejne dokumenty, które obowiązywały związane były także wdrożeniem ochrony danych osobowych:

• Polityka Bezpieczeństwa Danych Osobowych w Urzędzie Gminy i Miasta Sokołów Małopolski stanowiąca załącznik nr 1 do Zarządzenia Nr 733/2018 Burmistrza Gminy i Miasta Sokołów Małopolski z dnia 23 lipca 2018 r. w sprawie zmiany Zarządzenia Nr 705/2018 dot. określenia zasad bezpieczeństwa danych osobowych w Urzędzie Gminy i Miasta w Sokołowie Małopolskim;

• Polityka Zarządzania Kluczami w Urzędzie Gminy i Miasta Sokołów Małopolski stanowiąca Załącznik nr 2 do Zarządzenia Nr 733/2018 Burmistrza Gminy i Miasta Sokołów Małopolski z dnia 23 lipca 2018 r.;

• Instrukcja Zarządzania Systemami Informatycznymi w Urzędzie Gminy i Miasta Sokołów Małopolski stanowiąca Załącznik nr 3 do Zarządzenia Nr 705/2018 Burmistrza Gminy i Miasta Sokołów Małopolski z dnia 23 maja 2018 r.;

• Analiza poufności, integralności i rozliczalności systemów informatycznych pod kątem zagrożeń i ryzyka przy przetwarzaniu danych osobowych z dnia 12.06.2019 r.;

• Plan ciągłości działania na wypadek dysfunkcji systemu informatycznego w Urzędzie Gminy i Miasta Sokołów Małopolski stanowiący Załącznik nr 1 do Zarządzenia Nr 11/2018 Burmistrza Gminy i Miasta Sokołów Małopolski z dnia 6 grudnia 2018 r.;

• Procedura Oceny Powagi Naruszenia Ochrony Danych Osobowych z dnia 3 lutego 2020 r. Burmistrza Gminy i Miasta Sokołów Małopolski;

• Regulamin Pracy Zdalnej w Urzędzie Gminy i Miasta Sokołów Małopolski stanowiący Załącznik nr 1 do Zarządzenia Nr 394a/2020 Burmistrza Gminy i Miasta Sokołów Małopolski z dnia 22 grudnia 2020 r.;

• Procedura Awaryjna na wypadek absencji Administratora Systemu Informatycznego w Urzędzie Gminy i Miasta w Sokołowie Małopolskim stanowiąca Załącznik do Zarządzenia Nr 480/2021 Burmistrza Gminy i Miasta Sokołów Małopolski z dnia 23 czerwca 2021 r.;

• Regulamin korzystania z poczty elektronicznej przez pracowników w Urzędzie Gminy i Miasta w Sokołowie Małopolskim stanowiąca Załącznik do Zarządzenia Nr 634/2017 Burmistrza Gminy i Miasta Sokołów Małopolski z dnia 13 grudnia 2017 r.

Za wdrożenie dokumentacji związanej z ochroną danych osobowych, jej monitorowanie i poddawanie przeglądom odpowiedzialny był Inspektor Ochrony Danych.

Natomiast Administrator Systemu Informatycznego odpowiadał za wdrażanie procedur bezpieczeństwa oraz nadzór nad funkcjonowaniem systemów i sieci teleinformatycznej.

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.

W Urzędzie Gminy i Miasta w Sokołowie Małopolskim przyjęta była analiza poufności, integralności i rozliczalności systemów informatycznych pod kątem zagrożeń i ryzyka przy przetwarzaniu danych osobowych z 12.06.2019 r. na podstawie uchylonej ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych.

Załącznik nr 7 analizy zawierał tabelę szacowania ryzyka dla bezpieczeństwa informacji (w tym: poufność, rozliczalność i integralność) uwzględniającą:

- zasoby

- rodzaje zagrożeń

- szacowanie.

Szacowana wartość ryzyka określona została jako niskie ryzyko utraty bezpieczeństwa danych osobowych.

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.

2.3. Inwentaryzacja sprzętu i oprogramowania informatycznego

Regulacje wewnętrzne zawierały zapisy dotyczące konieczności rejestru zasobów teleinformatycznych, w tym: podstawowej konfiguracji komputera. Szczegóły dot. inwentaryzacji zawierał rozdział 19 Instrukcji Zarządzania Systemami Informatycznymi w Urzędzie Gminy i Miasta Sokołów Małopolski. Ewidencja sprzętu, oprogramowania oraz podzespołów prowadzona była przez aplikację IT Manager. Każdy komputer posiadał Kartę konfiguracji sprzętowo-systemowej.

W jednostce, do pracy bieżącej, użytkowane były komputery stacjonarne oraz laptopy.

2.4. Zarządzanie uprawnieniami do pracy w systemach informatycznych

Zarządzanie uprawnieniami dostępu do systemów w Urzędzie Gminy i Miasta regulowały:

• Instrukcja Zarządzania Systemami Informatycznymi w Urzędzie Gminy i Miasta Sokołów Małopolski;

• Polityka Bezpieczeństwa Danych Osobowych w Urzędzie Gminy i Miasta Sokołów Małopolski.

Dokumentacja powyższa szczegółowo opisywała sposób tworzenia kont, nadawania, zmiany i odbierania uprawnień użytkownikom w systemach informatycznych funkcjonujących w jednostce.

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

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 zmiany i odbioru uprawnień dla użytkownika w systemach informatycznych informacja przekazywana była ustnie lub na formularzu „Wniosek o utworzenie/likwidację/modyfikację konta w domenie/systemie informatycznym”.

Na bieżąco odbywało się monitorowanie dostępu do zasobów informatycznych zgodnie z wymaganiami § 20 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.

Dokumentacja wewnętrzna Urzędu Gminy i Miasta zobowiązywała do ochrony danych osobowych każdego pracownika, który uzyskał upoważnienie do przetwarzania danych osobowych. Regulowała także zakres podnoszenia świadomości pracowników poprzez konieczność zapoznania się nowego pracownika z treścią polityk, instrukcji.

Instrukcje, polityki, procedury umieszczone były na zasobie wewnętrznym dostępnym dla każdego pracownika.

W Urzędzie było przeprowadzane szkolenie dla pracowników w 2019 roku z ochrony danych osobowych i bezpieczeństwa informacji. Na bieżąco użytkownicy byli powiadamiani przez pracowników IT o nowych zagrożeniach przez system mailowy.

2.6. Praca na odległość i mobilne przetwarzanie danych

W obowiązującej Polityce Bezpieczeństwa Danych Osobowych (Rozdział X) oraz Instrukcji Zarządzania Systemami Informatycznymi (Rozdział 13) były zawarte podstawowe zasady zarządzania zabezpieczeniem komputerów przenośnych.

Dodatkowo w 2020 roku został ustanowiony Regulamin Pracy Zdalnej określający szczegółowe zasady pracy zdalnej spowodowanej możliwością wystąpienia sytuacji kryzysowej.

W procedurach pracy zdalnej dla pracowników Urzędu nie uwzględniono zabezpieczenia wynoszonych urządzeń za pomocą mechanizmów szyfrowania.

Pracownicy Urzędu korzystali z przygotowanych laptopów przy pracy zdalnej, praca wykonywana była na zasobach serwerowych, bez umieszczania danych na dyskach laptopów.

Sprawdzane umowy serwisowe zawierane z wykonawcą zewnętrznym nie zawsze miały określone zasady bezpiecznych połączeń zdalnych na wypadek wykonywania usługi opieki przez takie połączenie (np. z Clanet).

2.7. Serwis sprzętu informatycznego i oprogramowania

W przypadku systemów informatycznych o istotnym znaczeniu 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.

Jednak nie wszystkie umowy o asystę i opiekę autorską lub serwisową z firmami zewnętrznymi miały określone SLA (Service Level Agreement), czyli gwarantowany poziom świadczenia usług oraz czas i sposób reakcji na zgłaszane problemy (np. z Clanet).

W przypadku systemów informatycznych istotnych dla jednostki zostały zawarte umowy powierzenia przetwarzania danych osobowych.

2.8. Procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji

W Instrukcji Zarządzania Systemami Informatycznymi w Urzędzie Gminy i Miasta Sokołów Małopolski oraz Polityce Bezpieczeństwa Danych Osobowych w Urzędzie Gminy i Miasta Sokołów Małopolski zostały określone zasady postępowania w przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych (Rozdział XV). Dodatkowo obowiązywała także Procedura Oceny Powagi Naruszenia Ochrony Danych Osobowych Burmistrza Gminy i Miasta Sokołów Małopolski.

2.9. 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 12.04.2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych nie był wykonany w 2019 i 2020 r.

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.

2.10. Kopie zapasowe

Wykonywanie kopii zapasowych zapobiega utracie informacji w wyniku awarii.

Kopie powinny być właściwie tworzone, przechowywane i testowane.

W zakresie wykonywania kopii zapasowych w Urzędzie Gminy i Miasta w Sokołowie Małopolskim obowiązywały wymagania określone w Instrukcji Zarządzania Systemami Informatycznymi w Urzędzie Gminy i Miasta Sokołów Małopolski.

Kopie wykonywane były w sposób automatyczny według zdefiniowanego kalendarza przy pomocy specjalistycznego oprogramowania do tworzenia kopii zapasowych i odzyskiwania danych po awarii. Na bieżąco analizowane były raporty z wykonywania kopii zapasowych.

Kopie baz danych były przechowywane w innej lokalizacji.

Wykonywanie odtworzenia systemów z kopii zapasowych występowało w razie potrzeby.

2.11. Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych

W Urzędzie Gminy i Miasta Sokołów Małopolski proces administrowania technicznego i monitorowania określonych obszarów systemów, aplikacji, danych, infrastruktury sieciowej i stacji roboczych był wykonywany przez informatyka oraz kierownika Referatu Organizacyjno - Administracyjnego, 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.

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:

Instrukcji Zarządzania Systemami Informatycznymi w Urzędzie Gminy i Miasta Sokołów Małopolski oraz Polityce Bezpieczeństwa Danych Osobowych w Urzędzie Gminy i Miasta Sokołów Małopolski.

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

a) zabezpieczenie dostępu do informacji poprzez wymuszone logowanie u 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.

Obiekt Urzędu Gminy i Miasta był objęty systemem monitoringu. Był także objęty systemem alarmowym ochrony fizycznej.

Urząd dysponował jedną serwerownią, która znajdowała się w pomieszczeniu odpowiednio przygotowanym 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.

W serwerowni zostało wdrożone monitorowanie parametrów środowiskowych. Drzwi do serwerowni posiadały specjalne wzmocnienia i zamki.

W serwerowni przechowywane były serwery i urządzenia sieciowe. Nośniki z kopiami zapasowymi były umieszczone w innym miejscu niż serwerownia.

W serwerowni znajdował się UPS, który podtrzymywał pracę serwerów i urządzeń sieciowych. Strategiczne stanowiska komputerowe były wyposażone w urządzenia UPS podtrzymujące pracę komputera podczas zaników prądu. W posiadaniu urzędu był również agregat prądotwórczy.

W pomieszczeniu nie były przechowywane materiały łatwopalne.

Podstawowe urządzenia sieciowe posiadały tzw. zapas (poza łączem internetowym).

Konfiguracja zapór sieciowych i pozostałych urządzeń była przemyślana i aktualizowana w zależności od posiadanej wiedzy i specjalistycznych szkoleń.

Zastosowane zabezpieczenia techniczno-organizacyjne wynikały częściowo z analizy ryzyka i planu postępowania z ryzykiem.

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.

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

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.

Podczas kontroli przedstawiono kontrolującym zasady rozliczalności w następujących systemach: Clanet, BIP i Zwrot Podatku Akcyzowego (AKC).

**3**. **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 poprzez walidator dostępny pod adresem: https://validator.utilitia.pl/ badana strona uzyskała wynik 5,0 pkt na 10 możliwych, a strona www 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 11 października 2021 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. 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, ustanowienie, wdrożenie, a następnie eksploatowanie, monitorowanie, przeglądanie i doskonalenie pełnego systemu bezpieczeństwa informacji wraz z przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji.
2. We wszystkich umowach serwisowych ze stronami trzecimi zawierać zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji, w tym połączeń zdalnych i określić poziom SLA.
3. Ustanowić, wdrożyć i zapewnić funkcjonowanie procedury wewnętrznej w zakresie wykonywania corocznych audytów bezpieczeństwa informacji.

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 21 grudnia 2020 r. „Plan zewnętrznej działalności kontrolnej Podkarpackiego Urzędu Wojewódzkiego w Rzeszowie na 2021 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)