

**WOJEWODA PODKARPACKI**

ul. Grunwaldzka 15

35-959 Rzeszów

OA-IV.431.2.2023 Rzeszów, 2023-06-15

**Pan**

**Wojciech Piękoś**

**Wójt Gminy**

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 13 kwietnia 2023 r. u Wójta Gminy Jasło (Gmina Jasło, ul. Słowackiego 4, 38-200 Jasło) 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 31.03.2023 r., znak OA-IV.431.2.2023) udzielonych przez działającego z upoważnienia Wojewody Podkarpackiego – Dyrektora Wydziału Organizacyjno - Administracyjnego.

Ustalenia kontrolne dokonane zostały w oparciu o stan faktyczny istniejący od 1 stycznia 2022 r.do dnia realizacji czynności kontrolnych włącznie.

Kontrola obejmuje priorytet Prezesa Rady Ministrów na 2023, 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 Jasło 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 Jasło”[[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 Jasło pełnił Wójt: Pan Wojciech Piękoś.

Funkcję Inspektora Ochrony Danych (IOD) powierzono na podstawie umowy zlecenia Panu Rafałowi Cichoń.

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 Jasło.

Informatyk został wyznaczony jako osoba kontaktowa do CSIRT NASK na podstawie Zarządzenie Wójta Gminy Jasło Nr 17/2021 z dnia 09.02.2021, natomiast dane wyznaczonej osoby zostały zgłoszone przez ePUAP do CSIRT NASK w dniu 22.02.2021.

W okresie objętym kontrolą w Urzędzie Gminy Jasło 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:

- Respons (Ewidencja Ludności, Eksport Danych i Wyborcy) – firmy ZETO SOFTWARE Sp. z o.o.,

- 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. Usługi elektroniczne

Urząd Gminy Jasło 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 odbierana była poprzez system Proton.

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 Jasło posiadali dostęp do rejestrów publicznych takich jak: SRP Źródło, CEIDG.

System Respons komunikował się z usługami sieciowymi Systemu Rejestrów Państwowych w celu pobierania danych przy pomocy modułu odpowiadającego za transmisję danych z SRP do Lokalnej Ewidencji Ludności.

* 1. Obieg dokumentów

W Urzędzie Gminy Jasło był wdrożony Proton - system Elektronicznego Obiegu Dokumentów 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 (rozporządzenie 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) 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) według wymogów powyższego rozporządzenia KRI.

Kluczowe dokumenty dotyczyły głównie ochrony danych osobowych, były to:

* Polityka Bezpieczeństwa Danych Osobowych wraz z załącznikami, stanowiąca Załącznik do Zarządzenia nr 32/2018 Wójta Gminy Jasło z dnia 25 maja 2018 r.;
* Instrukcja Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych w Urzędzie Gminy Jasło wraz z załącznikami;
* Regulamin pracy zdalnej w Urzędzie Gminy Jasło stanowiący załącznik do Zarządzenia nr 38/2023 Wójta Gminy Jasło z dnia 7 kwietnia 2023 r.
  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.

Zarządzanie bezpieczeństwem ochrony danych osobowych w Urzędzie Gminy w Jaśle opierało się na zarządzaniu ryzykiem, które polegało m.in. na przeprowadzaniu przez Informatyka okresowej analizy ryzyka. Kontrolującym przedstawiono Rejestr Ryzyka z 2021 r.

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.

* 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 urzędzie do pracy bieżącej, użytkowane były komputery stacjonarne oraz laptopy.

Regulacje wewnętrzne nie zawierały zapisów dotyczących sposobu zarządzania sprzętem informatycznym i oprogramowaniem (w tym licencjami na oprogramowanie). Jednak do eksploatacji dopuszczone było tylko oprogramowanie autoryzowane przez ASI.

Ewidencja poszczególnych podzespołów oraz oprogramowania była prowadzona przy pomocy oprogramowania STATlook.

* 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.

Zarządzanie uprawnieniami dostępu do przetwarzania danych w Urzędzie Gminy Jasło regulowały: Polityka Bezpieczeństwa Danych Osobowych i Instrukcja Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych w Urzędzie Gminy Jasło. W zakresie zarządzania dostępem szczegółowe uregulowania występowały w: Procedurze nadawania i rejestrowania uprawnień do przetwarzania danych osobowych w systemie informatycznym, Metodach i środkach uwierzytelniania oraz procedurze związanej z ich zarządzaniem.

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.

Pracownicy uzyskiwali dostęp do zasobów informatycznych po przyznaniu zakresu obowiązków i nadaniu unikalnego identyfikatora 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 nadania i zmiany uprawnień dla użytkownika w systemach informatycznych informacja przekazywana była ustnie, a uprawnienia nadawane na podstawie upoważnienia. Odbiór uprawnień/dostępów następował po przedstawieniu karty obiegowej w przypadku pracowników lub na podstawie ustnego zgłoszenia Kierownika Referatu w przypadku stażystów (pracowników tymczasowych). Obowiązująca dokumentacja wskazywała w takich przypadkach na stosowanie formularza wniosku o nadanie/odebranie uprawnień w systemie informatycznym (Załącznik nr 1 do Instrukcji Zarządzania Systemem Informatycznymi Służącym do Przetwarzania Danych Osobowych), jednak nie był on stosowany.

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 funkcjonująca w Urzędzie Gminy Jasło regulowała zakres podnoszenia świadomości pracowników poprzez: konieczność zapoznania wszystkich osób przetwarzających informację z procedurami bezpieczeństwa informacji w zakresie niezbędnym do wykonywania pracy, a także obowiązek ich przestrzegania.

Każdy nowozatrudniony pracownik zobowiązany był do odbycia szkolenia ze stosowania zasad bezpieczeństwa informacji.

Kontrolującym przedstawiono informację o przeszkoleniu pracowników z 2022 roku, z zakresu bezpieczeństwa informacji oraz ochrony danych osobowych. Dla pracowników dokumentacja związana z bezpieczeństwem informacji była umieszczona na zasobie sieciowym.

* 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.

Zasady zarządzania bezpieczną pracą na komputerach przenośnych i sposoby zabezpieczenia tych urządzeń były zawarte w Regulaminie pracy zdalnej w Urzędzie Gminy Jasło, stanowiącym załącznik do Zarządzenia nr 38/2023 Wójta Gminy Jasło z dnia 7 kwietnia 2023 r.

* 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 dot. ochrony danych osobowych ogólnie zostały określone zasady współpracy z podmiotami trzecimi w zakresie przetwarzania danych osobowych.

Dodatkowo poziom bezpieczeństwa regulowały umowy zawierane z firmami zewnętrznymi, w przypadku serwisowania sprzętu lub oprogramowania.

Sprawdzane 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 (udostępniono umowy z ZETO SOFTWARE sp. z o.o., ZETO-RZESZÓW SP. z o.o., Techup Sp. z o.o., Agnat Sp. z o.o.).

W przypadku systemów informatycznych istotnych dla jednostki zostały zawarte także umowy powierzenia przetwarzania danych osobowych (udostępniono umowę: z Agnat Sp. z o.o.).

* 1. Procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji

Zostały określone zasady postępowania w przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych w Polityce Bezpieczeństwa Danych Osobowych. 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 12.04.2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych był wykonywany. W 2022 r. dodatkowo była przeprowadzona diagnoza cyberbezpieczeństwa w ramach Projektu „Cyfrowa Gmina”.

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.

W okresie objętym kontrolą w zakresie wykonywania kopii zapasowych w Urzędzie Gminy Jasło obowiązywały ogólne wymagania określone w Instrukcji Zarządzania Systemem Informatycznym (Procedura tworzenia kopii zapasowych zbioru danych oraz programów i narzędzi programowych służących do ich przetwarzania).

Wykonywanie kopii zapasowych od 2018 roku zostało udoskonalone co zostało opisane przez informatyka w dodatkowej notatce dotyczącej backupów.

Przechowywanie kopii zapasowych w innej lokalizacji niż serwery było w trakcie wdrożenia.

Wykonywanie odtworzenia systemów z kopii zapasowych występowało w razie potrzeby.

* 1. Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych

W Urzędzie Gminy Jasło 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 oraz w Polityce Bezpieczeństwa Danych Osobowych.

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

1. zabezpieczenie dostępu do informacji poprzez wymuszone logowanie 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 Jasło posiadał lokalizację w jednym budynku.

Obiekt nie był objęty systemem alarmowym ochrony fizycznej, natomiast był objęty systemem monitoringu na zewnątrz i wewnątrz budynku. Do otwierania głównych drzwi budynku byli upoważnieni wyznaczeni pracownicy.

Urząd Gminy dysponował jedną serwerownią główną oraz drugą serwerownią, która mogła pełnić rolę centrum zapasowego. Serwerownie znajdowały się w pomieszczeniach zaadaptowanych 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.

Serwerownie posiadały czujki ruchu i dymu, jednak brakowało systemu ppoż. Pomieszczenia były klimatyzowane.

Drzwi do głównej serwerowni były wzmocnione.

Bazy danych z kopiami były umieszczone w jednej z serwerowni. Praca serwera i urządzeń sieciowych w razie zaników prądu mogła być podtrzymywana przez UPS.

Strategiczne stanowiska komputerowe, także wyposażone były w urządzenia UPS podtrzymujące pracę komputera podczas zaników prądu.

W pomieszczeniu nie były przechowywane materiały łatwopalne.

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

* 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.

Nie było wdrożonej usługi katalogowej Active Directory, która pozwalałaby na zarządzanie tożsamościami i relacjami w sieci, przez co umożliwiałaby sprawniejszą 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 Jaśle 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.

Ze względu na to, że strony www i BIP były umieszczone w domenie rządowej: samorząd.gov.pl. nie jest możliwe przeprowadzenie analizy stron poprzez walidator dostępny pod adresem: <https://validator.utilitia.pl/>.

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 17 maja 2023 r.) przysługiwało Panu, na podstawie ww. ustawy o kontroli w administracji rządowej, prawo zgłoszenia umotywowanych pisemnych zastrzeżeń, z którego Pan nie skorzystała.

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 ustanowienie i wdrożenie, a następnie eksploatowanie, monitorowanie, przeglądanie i doskonalenie pełnego systemu bezpieczeństwa informacji uwzględniającego zarządzanie ryzykiem i ciągłość działania systemu bezpieczeństwa informacji oraz ujednolicenie stosowania dokumentacji dot. danych osobowych.
2. Ustanowić procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji.
3. Kopie zapasowe przechowywać w innej lokalizacji niż serwerownia.
4. Przeanalizować wdrożenie usługi katalogowej Active Directory, która pozwalałaby na zarządzanie tożsamościami i relacjami w sieci, przez co umożliwiałaby sprawniejszą kontrolę nad całą siecią.

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**

**(-)**

**Ewa Leniart**

(Podpisane bezpiecznym podpisem elektronicznym)

1. W oparciu o zatwierdzony w dniu 21 grudnia 2022 r. „Plan zewnętrznej działalności kontrolnej Podkarpackiego Urzędu Wojewódzkiego w Rzeszowie na 2023 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)