WOJEWODA
ŚWIĘTOKRZYSKI

Kielce, dnia 05 grudnia 2024 r.

Znak:OK.V.431.4.2024

Pan Bogusław Kowalczyk
Wójt Gminy Michałów

WYSTĄPIENIE POKONTROLNE

Zakres kontroli:	Prawidłowość działania systemów informatycznych używanych do realizowania zadań zleconych z zakresu administracji rządowej.
Okres objęty kontrolą:	od 1 stycznia 2018 r. do dnia wszczęcia kontroli tj. 9 października 2024 r.
Kontrolerzy:	Pan Marek Rak – Główny specjalista Oddziału do spraw Informatyki w wydziale Organizacji i Kadr Świętokrzyskiego Urzędu Wojewódzkiego w Kielcach – upoważnienie do kontroli nr 744/2024 z 8 października 2024 r. Pan Maciej Terek – Główny specjalista Oddziału do spraw Informatyki w wydziale Organizacji i Kadr Świętokrzyskiego Urzędu Wojewódzkiego w Kielcach – upoważnienie do kontroli nr 743/2024 z 8 października 2024 r.
Termin przeprowadzenia kontroli:	Kontrola została przeprowadzona w dniu 9 października 2024 r. w siedzibie Urzędu Gminy w Michałowie.
Podstawa prawna do przeprowadzenia kontroli:	Kontrolę przeprowadzono na podstawie art. 6 ust. 4 pkt 3 ustawy z dnia 15 lipca 2011 r. *o kontroli w administracji rządowej*[1], art. 28 ust. 1 pkt 2 ustawy z dnia 23 stycznia 2009 r. *o Wojewodzie i Administracji rządowej w województwie*[2] oraz art. 25 ust.1 pkt 3 lit. a) ustawy z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne*[3]. Wystąpienie pokontrolne przekazano zgodnie z przepisami art. 47 ustawy o kontroli w administracji rządowej.
Ocena stanu faktycznego wynikająca z ustaleń kontroli:	Zgodnie z Rozporządzeniem Rady Ministrów z dnia 21 maja 2024 r. *w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej*

[1] Dz. U. z 2020 r. poz. 224, dalej: Ustawa o kontroli w administracji rządowej.
[2] Dz. U. z 2023 r. poz. 190
[3] Dz. U. z 2024 r. poz. 1557

oraz minimalnych wymagań dla systemów teleinformatycznych[4] ocenie podlegały czynności podejmowane w trzech obszarach tematycznych:

1. system zarządzania Bezpieczeństwem Informacji w systemach teleinformatycznych,
2. realizacja działań z zakresu bezpieczeństwa informacji,
3. Zapewnienie dostępności w tym cyfrowej informacji zawartych na stronach internetowych urzędów dla osób z niepełnosprawnościami zgodnie z ustawą z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych.

Pozytywnie z uchybieniami ocenia się prawidłowość działania systemów informatycznych używanych do realizowania zadań zleconych z zakresu administracji rządowej w Urzędzie Gminy w Michałowie w okresie objętym kontrolą. Ocena końcowa ustalona została w oparciu o przedstawione poniżej wnioski i oceny cząstkowe.

Kontrolą w przedmiotowym zakresie objęto systemy informatyczne używane do realizacji zadań zleconych z zakresu administracji rządowej tj.: System Rejestrów Państwowych Źródło (SRP Źródło), Centralna Ewidencja i Informacja o Działalności Gospodarczej (CEIDG), Sygnity (świadczenia wychowawcze) oraz RESPONS (moduł Paliwa). W toku przeprowadzonej kontroli ustalono, co następuje:

1. **System zarządzania Bezpieczeństwem Informacji w systemach teleinformatycznych**:

Oceny stanu faktycznego dokonano zgodnie z §19 ust. 1 i 2 Rozporządzenia KRI. Ustalono, że podstawowymi dokumentami z zakresu bezpieczeństwa informacji w Urzędzie Gminy jest Polityka Ochrony Danych Osobowych (PODO) wprowadzona Zarządzeniem nr K.7.2023 Wójta Gminy Michałów z dnia 22.11.2023 roku w sprawie wprowadzenia Polityki Ochrony Danych (traci moc Zarządzenie Wójta Gminy Michałów nr K.9.2018 z dnia 20.07.2018 roku), oraz Instrukcja Zarządzania Systemem Informatycznym (IZSI) służącym do przetwarzania danych osobowych w Urzędzie Gminy wprowadzona Zarządzeniem nr K.7.2022 Wójta Gminy Michałów z dnia 9.08.2022 r.

Powyższe regulacje zostały udostępnione w formie plików kopii cyfrowych oryginalnych dokumentów. Udostępniono dokumentację (formie notatek) związaną z weryfikacją procedur, instrukcji, procesów określonych w IZSI i PODO oraz przebiegiem ich aktualizacji przez IOD i ASI z lat 2018-2024.

Po zapoznaniu się z dokumentacją PODO zespół kontrolny stwierdza, że dokument w pewnym zakresie jest niespójny, dokładnie chodzi o załączniki numer 15, 9, 8 Rozdział III, Art. 23, strona 33 PODO. Załączniki te w swej nazwie i funkcjonalności nie zgadzają się z załącznikami opublikowanymi w PODO w rozdziale V Art. 43 – strona 48.

Niespójne są zapisy z PODO z rozdziału III Art. 23 „Zasady zarzadzania uprawnieniami użytkowników w systemach informatycznych" w stosunku do zapisów w IZSI w Rozdziale 2 „Procedury nadawania, odbierania uprawnień". W PODO mowa jest o załączniku nr 15 wniosku

[4] Dz. U. z 2017 r., poz. 2247, dalej Rozporządzenie KRI

o nadanie, zmianę, odebranie uprawnień w systemach informatycznych, natomiast w IZSI w Rozdziale 2 „Procedury nadawania, odbierania uprawnień" wniosek 15 jest pominięty. Pozostałe załączniki wymienione w Rozdziale 2 czyli załącznik numer 10, załącznik numer 13 są niespójne z zapisami w PODO. Inne nazwy załączników, inne funkcjonalności załączników. IZSI nie została zaktualizowana po wprowadzeniu nowej PODO w listopadzie 2023 r.
IZSI jest dokumentem nieaktualizowanym od sierpnia roku 2022. W tym okresie na przykład zaszła zmiana w rozporządzeniu o KRI wymienionym w podstawach prawnych tego dokumentu. Obecnie obowiązuje wersja tego rozporządzenia z 21 maja 2024 r.
Do obowiązków IOD należy systematyczne przeglądanie dokumentacji związanej z PODO i IZSI pod kątem jej aktualności oraz zastosowania w praktyce w Urzędzie.

Przedmiotowe dokumenty to jest IZSI i PODO załączono w formie plików cyfrowych do akt kontroli (Dokumenty do kontroli – Gmina Michałów.zip).

Ocena cząstkowa badanego zagadnienia:

Pozytywnie z uchybieniami ocenia się działalność Jednostki w przedmiotowym zakresie.

2. Realizacja działań z zakresu bezpieczeństwa informacji:

Zakres kontroli przedmiotowego zagadnienia został podzielony na dwanaście obszarów badawczych:

1. Analiza zagrożeń związanych z przetwarzaniem informacji.

Oceny stanu faktycznego dokonano zgodnie z §19 ust. 2 pkt 3 Rozporządzenia KRI.

Kontrolującym przedłożono „Analizy zagrożeń i ryzyka przy przetwarzaniu danych osobowych" z lat 2021-2023. W samym dokumencie zamieszczono algorytm liczenia ryzyka pierwotnego $R_{p,}$ natomiast w całym dokumencie osoba dokonująca analizy posługuje się parametrem R_k ryzyka końcowego. Brak w dokumentacji algorytmu liczącego ryzyko końcowe. Po dopytaniu pocztą elektroniczną IOD o algorytm liczenia ryzyka końcowego kontrolowany przekazał IOD informację, że algorytm liczenia ryzyka końcowego jest tajemnicą przedsiębiorstwa.
Kontrolujący przeanalizowali kilka wybranych parametrów dotyczących pomieszczenia serwerowni w analizach ryzyka z lat 2021-2023 i ustalili, że:

- brak drzwi certyfikowanych antywłamaniowych w serwerowni,
- brak systemu alarmowego w serwerowni,
- brak monitoringu w serwerowni

Na przestrzeni lat 2021-2023 parametry, które zostały wymienione powyżej są takie same, nic się w tym zakresie nie zmieniło. Dlatego zespół kontrolny pytał o algorytm liczenia ryzyka końcowego.

Należy również zwrócić uwagę na zamieszczone zalecenia. Zauważyć należy, że w badanym okresie analiza ryzyka i zagrożeń kształtują się na jednakowym poziomie, co może świadczyć o tym że Urząd Gminy, dla którego wykonywane są odpłatnie co roku analizy zagrożeń i ryzyka w praktyce swojej działalności nie bierze zaleceń pod uwagę. Od trzech lat są zalecenia wymiany drzwi w serwerowni czy zalecenia wyposażenia serwerowni w system monitorowania wejść i wyjść ale nie podjęto żadnych działań w tym zakresie.

W załączonych arkuszach zawierających analizę procesów w kolumnie „Właściciel procesu" jest tylko jedna wartość „Urząd Gminy w Michałowie". Tak ujęta analiza procesów może stwarzać ryzyko braku możliwości wskazania osoby odpowiedzialnej za dany obszar. Warto byłoby rozważyć możliwość wskazania pracowników odpowiedzialnych za dany obszar.
Przedmiotowe dokumenty tj. IZSI i PODO załączono w formie plików cyfrowych do akt kontroli (Dokumenty do kontroli – Gmina Michałów.zip).

2. Inwentaryzacja sprzętu i oprogramowania informatycznego.

Oceny stanu faktycznego dokonano zgodnie z §19 ust. 2 pkt 2 Rozporządzenia KRI. Ustalono, że inwentaryzacja sprzętu i oprogramowania jest prowadzona przez ASI przy pomocy oprogramowania GLPI. Zostały udostępnione przykładowe raporty: karta komputera, zestawienie sprzętu sieciowego, wykaz komputerów. Każdy z raportów posiada naniesiona datę wygenerowania raportu, każda pozycja w raporcie posiada wpisaną datę aktualizacji, raporty zwierają również informację na temat zainstalowanego oprogramowania.
Należy pamiętać, aby w systemie znalazły się urządzenia które na czas sporządzania raportów, wykazów, zestawień nie są podłączone do systemu informatycznego UG. Należy wówczas prowadzić dodatkowy rejestr urządzeń nie podłączonych lub czasowo odłączonych od sieci UG. ASI ma tego świadomość.

Przedłożone dokumenty: zrzuty ekranów z oprogramowania GLPI załączono w formie plików cyfrowych do akt kontroli Pobrane-dokumenty-UG-Michalow.pdf).

3. Zarządzanie uprawnieniami do pracy w systemach informatycznych.

Oceny stanu faktycznego dokonano zgodnie z §19 ust. 2 pkt 4 oraz 5 Rozporządzenia KRI.

W Rozdziale III, Art. 23 PODO opisano zasady zarządzania uprawnieniami użytkowników w systemach informatycznych.
Na potrzeby procedury zdefiniowano załączniki:
Załącznik nr 15 wniosek o nadanie, zmianę, odebranie uprawnień w systemach informatycznych. Załącznik nr 9 ewidencja osób upoważnionych do przetwarzania danych osobowych. Załącznik nr 7 dostęp do systemów informatycznych.

W Rozdziale 2 IZSI opisano również procedurę zarządzania uprawnieniami użytkowników w systemach informatycznych Urzędu. Procedura została wdrożona w sierpniu 2022 r.

Obie instrukcje są niespójne jeżeli chodzi o treść i sam przebieg procedury. Procedura zawarta w IZSI w Rozdziale 2 nie została poddana aktualizacji po wdrożeniu nowej PODO w listopadzie 2023 roku. Wymieniony załącznik numer 10 z POD (obowiązuje PODO) nie jest tożsamy, jeżeli chodzi o nazwę i funkcjonalność z załącznikiem numer 10 z PODO, Rozdział III, Art.43.

Również procedura opisana w PODO z Rozdziału III, Art. 23 jest niespójna z samą dokumentacja PODO. W Rozdziale V, Art. 43 „Wykaz załączników", opublikowane zostały inne załączniki jeżeli chodzi o nazwy i ich funkcjonalności (załączniki numer 15, 9 i 7). Zespołowi kontrolnemu został przedłożony dokument, załącznik numer 8 „*Ewidencja osób upoważnionych do przetwarzania danych osobowych*". W PODO w Rozdziale III, Art. 23 wspomniany załącznik ma numer 9.
Zespołowi kontrolnemu został przedłożony „Wniosek o nadanie, zmianę, odebranie uprawnień" pracownika o inicjałach M.G. Sam dokument nie nosi żadnych znaczników mówiących o tym, iż jest to załącznik numer 15 z PODO. Wzór tego załącznika nie został dołączony do PODO.

Z przedłożonych dokumentów wynika, że IOD prowadzi dość systematycznie przeglądy PODO i IZSI. „*Raport z czynności audytowych wykonanych przez IOD*" z maja 2024 roku, z raportu wynika, że weryfikacji podlegała stosowana POD w zakresie nadanych upoważnień do przetwarzania danych osobowych. Tym samym między innymi powinien zostać zweryfikowany załącznik numer 9 „Ewidencja osób upoważnionych do przetwarzania danych osobowych" jego prowadzenie i bieżące użytkowanie, oraz jego zgodność z zapisami w PODO. Wygląda na to, że żadna z tych czynności nie została wykonana właściwie przez IOD.

Podobnie jest z przeglądem przeprowadzonym przez IOD z dnia 4 grudnia 2023 roku. POD została zaktualizowana, zatwierdzona i ostatecznie wdrożona. W dniu kontroli jednak zespół kontrolny stwierdził w niej opisane wyżej nieścisłości.

Przedłożone dokumenty: załącznik numer 8, załącznik numer 15 załączono w formie plików cyfrowych do akt kontroli (Pobrane-dokumenty-UG-Michalow.pdf). Dokumenty PODO i IZSI załączono w formie plików cyfrowych do akt kontroli (Dokumenty do kontroli - Gmina Michałów.zip).

4. Szkolenia pracowników zaangażowanych w proces przetwarzania danych.

Oceny stanu faktycznego dokonano zgodnie z §19 ust. 2 pkt 6 Rozporządzenia KRI.

Kontrolowana Jednostka przedłożyła listy obecności z własnoręcznymi podpisami uczestników szkoleń wewnętrznych na przestrzeni lat 2018-2024. Szkolenia odbywają się raz w roku. W każdym z tych szkoleń bierze udział tylko cześć pracowników Urzędu. Brak dodatkowych terminów szkoleń dla pracowników, którzy z różnych względów nie mogli uczestniczyć w szkoleniu w wyznaczonym terminie.

Przedłożono certyfikaty pracowników ze szkolenia w zakresie „Ochrona danych osobowych w jednostkach samorządu terytorialnego". Szkolenie odbyło się w dniu 26.01.2024 online.

Przedmiotowe listy szkoleń, konspekty szkoleń, certyfikaty ze szkoleń zostały załączone w formie skanów elektronicznych do akt kontroli (Dokumenty do kontroli - Gmina Michałów.zip).

5. Praca na odległość i mobilne przetwarzanie danych.

Oceny stanu faktycznego dokonano zgodnie z §19 ust. 2 pkt 8 Rozporządzenia KRI.

W IZSI w rozdziale 2, §7, punkt 11 znajduje się bardzo ogólny zapis, iż dostęp do systemu informatycznego Urzędu Gminy mają również inne podmioty tylko i wyłącznie w zakresie i na zasadach określonych w umowach powierzenia przetwarzania danych osobowych. Dostęp do danych tylko i wyłącznie pod nadzorem ASI. W umowie przetwarzania danych osobowych z dnia 2.01.2018 z firmą Asseco Data System S.A. w §3 w punkcie 15 zapisano, że dostęp do danych osobowych odbywać się będzie za pośrednictwem szyfrowanego łącza. Z rozmowy przeprowadzonej z ASI wynika, że istotnie tak jest. Całość procesu połączenia zdalnego odbywa się pod jego nadzorem i bez jego obecności w tym procesie połączenie zdalne z systemem informatycznym UG firm zewnętrznych nie jest możliwe. W PODO Art. 30, strona 38 znajduje się więcej szczegółów dotyczących pracy na odległość, pracy zdalnej podmiotów zewnętrznych.

Część pracowników ma odstęp do poczty Urzędu poprzez przeglądarkę (zdalnie). Brak w IZSI i PODO procedury uzyskania dostępu przez pracowników Urzędu do zdalnej poczty, brak w dokumentacji informacji, kto z pracowników ma dostęp do poczty zdalnej.

Przedmiotowe regulacje załączono w formie plików cyfrowych do akt kontroli (Dokumenty do kontroli - Gmina Michałów.zip oraz Pobrane-dokumenty-UG-Michalow.pdf).

6. Serwis sprzętu komputerowego i oprogramowania.

Oceny stanu faktycznego dokonano zgodnie z §19 ust. 2 pkt 10 Rozporządzenia KRI.

Z rozmowy przeprowadzonej z ASI wynika, że przeważającą większość prac serwisowych wykonuje sam we własnym zakresie. Niewielka część czynności serwisowych wykonywana jest przez firmy zewnętrzne które mają aktualne umowy z Urzędem.
Zespół kontrolny nie znalazł zapisów w PODO i IZSI związanych z wykonaniem czynności serwisowych przez firmy zewnętrzne.
Zostały przedłożone kopie cyfrowe oryginałów dokumentów związanych z przeglądem infrastruktury teleinformatycznej z roku 2024 wykonanych przez ASI.

Przedmiotowe regulacje załączono w formie plików cyfrowych do akt kontroli (Dokumenty do kontroli - Gmina Michałów.zip).

7. Procedury zgłaszania incydentów naruszenia Bezpieczeństwa Informacji.

Oceny stanu faktycznego dokonano zgodnie z §19 ust. 2 pkt 13 Rozporządzenia KRI.

Procedurę związaną z szeroko pojętymi incydentami w zakresie bezpieczeństwa informacji w Urzędzie Gminy wprowadza Zarządzenie Wójta Gminy Michałów nr K.8.2022 z dnia 09.08.2022 roku w sprawie wprowadzenia do stosowania procedury zarządzenia incydentami związanymi z bezpieczeństwem informacji i cyberbezpieczeństwem.
Jest to dokument zawierający szereg informacji w zakresie bezpieczeństwa informacji poczynając od kategorii incydentów, procedury zgłaszania incydentów, podejmowania działań związanych z naruszeniami bezpieczeństwa informacji oraz procedurami reagowania na zaistniały incydent.

Przedmiotowe regulacje załączono w formie plików cyfrowych do akt kontroli (Dokumenty do kontroli - Gmina Michałów.zip).

8. Audyt wewnętrzny z zakresu bezpieczeństwa informacji.

Oceny stanu faktycznego dokonano zgodnie z §19 ust. 2 pkt 14 Rozporządzenia KRI.

Przedłożono kopie cyfrowe oryginalnych dokumentów związanych z przeprowadzonymi audytami w latach 2019-2023. Jako podstawę prawną wykonywanych audytów podano między innymi Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie KRI.

Przedmiotowe regulacje załączono w formie plików cyfrowych do akt kontroli (Dokumenty do kontroli - Gmina Michałów.zip).

9. Kopie zapasowe.

Oceny stanu faktycznego dokonano zgodnie z §19 ust. 2 pkt 12 Rozporządzenia KRI.

W załączniku nr 14 „Opis środków technicznych stosowanych do zabezpieczenia danych osobowych i wykaz obszaru przetwarzania" w punkcie 3 zamieszczono informację o procesie wykonywania kopii zapasowych. ASI przedłożył zrzuty ekranu harmonogramów wykonywania kopii zapasowych z właściwego oprogramowania. W pomieszczeniu serwerowni w certyfikowanej szafie pancernej przechowywane są kopie zapasowe.

Zespołowi kontrolnemu został przedłożony protokół z przeprowadzonych testów kopii zapasowych systemów Urzędu Gminy w Michałowie z dnia 9 stycznia 2024 roku.

Kopie zapasowe jeżeli jest to możliwe należy przechowywać w innej strefie pożarowej niż strefa w której fizycznie są wykonane. W Urzędzie kopie przechowywane są a tej samej strefie pożarowej. Zespół kontrolny nie znalazł zapisów w IZSI i PODO mówiących o tym kiedy, w jakich odstępach czasowych ASI ma wykonywać testy kopii zapasowych.

Przedmiotowe regulacje załączono w formie plików cyfrowych do akt (Pobrane-dokumenty-UG-Michalow.pdf).

10. Bezpieczeństwo techniczno-organizacyjne dostępu do informacji.

Oceny stanu faktycznego dokonano zgodnie z §19 ust. 2 pkt 7, 9 oraz 11 Rozporządzenia KRI.

Ustalono, że Urząd Gminy w Michałowie posiada trzy wejścia do budynku. Oprócz Urzędu Gminy w tym samym budynku znajduje się jeszcze GOPS i bank spółdzielczy. Wejścia do budynku zabezpieczone są oszklonymi, metalowymi drzwiami z zamkiem. Dodatkowo wejścia do budynku zabezpieczone są roletami zewnętrznymi. Budynek wyposażony jest w system antywłamaniowy, w pomieszczeniach budynku rozmieszczone są urządzenia systemu przeciwpożarowego. Pomieszczenie serwerowni wyposażone jest w urządzenie systemu klimatyzacji, kontroli temperatury i wilgotności oraz system przeciwpożarowy.

Na ścianach budynku zamieszczone są kamery monitoringu wizyjnego. Dostęp do konsoli monitoringu wizyjnego w pokoju ASI. Dane z monitoringu przechowywane są przez okres dwóch tygodni, (Regulamin funkcjonowania monitoringu wizyjnego na terenie Urzędu Gminy jest z roku 2018).

Zespołowi kontrolnemu przedłożono załącznik nr 14 do PODO „Opis środków technicznych stosowanych do zabezpieczenia danych osobowych i wykaz obszaru przetwarzania". Przedłożono również Protokół potwierdzający bezpieczne niszczenie nośników danych z maja 2021 roku oraz protokół z wykonania przeglądów infrastruktury

technicznej Urzędu Gminy z września 2024 roku.
Wdrożono politykę kluczy (Zarządzenie k.3A.2024 Wójta Gminy Michałów z dnia 24 czerwca 2024 r.)

Przedmiotowe regulacje załączono w formie plików cyfrowych do akt kontroli (Dokumenty do kontroli - Gmina Michałów.zip).

11. Zabezpieczenia techniczno-organizacyjne systemów informatycznych.

Oceny stanu faktycznego dokonano zgodnie z §19 ust. 2 pkt 12, oraz ust. 4 Rozporządzenia KRI.

Ustalono i sprawdzono, że ustawienia dotyczące polityki haseł (częstotliwości zmian hasła, złożoności) oparte są o Active Directory. Hasła przechowywane są w tzw. bezpiecznej kopercie, w pomieszczeniu serwerowni w certyfikowanym sejfie.
Urząd Gminy posiada sprawne, podłączone i skonfigurowane urządzenie UTM umieszczone w szafie dystrybucyjnej w serwerowni. ASI udostępnił zrzut z konsoli urządzenia z podstawowymi parametrami, certyfikatami. Stacje robocze wyposażone są urządzenia podtrzymujące napięcie, oprogramowanie antywirusowe aktualizowane na bieżąco, włączona jest blokada portów USB dla nośników zewnętrznych na stacjach roboczych.

12. Rozliczalność działań w systemach teleinformatycznych.

Oceny stanu faktycznego dokonano zgodnie z §19 ust. 2, 3 oraz 4 Rozporządzenia KRI. Ustalono, że oprogramowanie wspomagające oraz systemy operacyjne używane w Urzędzie Gminy posiadają funkcjonalności monitorujące prace użytkowników. Nie ma natomiast procedury, narzędzi czy oprogramowania do systematycznego przeglądania logów systemowych co w efekcie końcowym skutkuje brakiem przeglądania logów a tym samym brakiem monitorowania zdarzeń. Podjęto działania w celu pozyskania specjalistycznego oprogramowania do analizy logów.

Przedmiotowe regulacje załączono w formie plików cyfrowych do akt kontroli (Dokumenty do kontroli - Gmina Michałów.zip).

Ocena cząstkowa badanego zagadnienia:

Pozytywnie z uchybieniami ocenia się działalność Jednostki w przedmiotowym zakresie.

3. Zapewnienie dostępności cyfrowej informacji zawartych na stronach internetowych urzędów dla osób z niepełnosprawnościami

Czy sporządzono i opublikowano deklarację dostępności oraz zawarto w deklaracji dostępności elementy wskazane w art. 10 ust. 3-5 ustawy dla stron internetowych podmiotu.

Oceny stanu faktycznego dokonano zgodnie z §10 ust. 3, 4 i 5 ustawy z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych

zgodnie z ustawą z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych:	i aplikacji mobilnych podmiotów publicznych[5]. Ustalono, że obydwie kontrolowane strony posiadają stosowne deklaracje dostępności: – https://www.michalow.pl – Deklaracja dostępności aktualizowana 2023-01-13 – https://bip.michalow.pl – Deklaracja dostępności aktualizowana 2022-10-24
Ocena cząstkowa badanego zagadnienia:	Pozytywnie ocenia się działalność Jednostki w przedmiotowym zakresie.
Wnioski, zalecenia oraz dodatkowe informacje:	Reasumując powyższe ustalenia, zwracam się z prośbą do Pana Wójta o niedopuszczenie do powstania nieprawidłowości wykazanych w toku kontroli w przyszłej działalności w podległej Panu Jednostce. Wobec powyższego sformułowano następujące zalecenia: 1. Regularnie przeprowadzać przeglądy i aktualizację dokumentacji z zakresu bezpieczeństwa informacji. 2. Uporządkować zapisy w dokumentacji aby zapewnić spójność procedur i załączników. 3. Rzetelnie przeprowadzać analizę ryzyka. 4. W analizie procesów rozważyć wskazanie osób odpowiedzialnych za poszczególne obszary. 5. Zapewnić szkolenia wszystkim pracownikom. 6. Opisać w dokumentacji procedurę zdalnego dostępu do poczty elektronicznej Urzędu. 7. W miarę możliwości przechowywać kopie zapasowe w innej strefie pożarowej niż strefa w której fizycznie są wykonane. 8. Opisać w dokumentacji w jakich odstępach czasowych ASI ma wykonywać testy kopii zapasowych. 9. Opisać w dokumentacji procedurę przeglądania logów systemowych i w miarę możliwości systematycznie je monitorować. Jednocześnie na podstawie art. 49 ustawy o kontroli w administracji rządowej, proszę poinformować Wojewodę Świętokrzyskiego w terminie 30 dni od daty otrzymania niniejszego wystąpienia pokontrolnego o sposobie wykorzystania wyżej wymienionych uwag i wniosków oraz o wykonaniu zaleceń, a także o podjętych działaniach lub przyczynach niepodjęcia działań. Ponadto informuję, iż zgodnie z art. 48 ustawy o kontroli

[5] Dz. U. z 2023 r. poz. 1440

w administracji rządowej od niniejszego wystąpienia pokontrolnego nie przysługują środki odwoławcze.

Józef Bryk
Wojewoda Świętokrzyski