

 **WOJEWODA PODKARPACKI**

 ul. Grunwaldzka 15

 35-959 Rzeszów

 OA-IV.431.2.2021 Rzeszów, 2021-12-07

**Pan**

**Ryszard Filipek**

**Wójt Gminy**

**Iwierzyce**

 Na podstawie art. 46 ust. 1 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej, w związku ze zrealizowaną w dniach 26 i 28 października 2021 r. u Wójta Gminy Iwierzyce (Urząd Gminy w Iwierzycach, Iwierzyce 80, 39-124 Iwierzyce) 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 20.10.2021 r., znak OA-IV.431.2.2021) udzielonych przez działającego z upoważnienia Wojewody Podkarpackiego – Dyrektora Generalnego Urzędu.

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 Iwierzyce 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 Iwierzyce”[[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 Iwierzyce pełnił Wójt: Pan Ryszard Filipek.

Funkcję Inspektora Ochrony Danych (IOD) powierzono wykonawcy zewnętrznemu na podstawie zawartej umowy.

Wsparcie informatyczne zapewnione było przez pracownika urzędu zatrudnionego jako informatyk. Pod jego opieką znajdowały się: środowiska sprzętowo-programowe, sieć lokalna i serwerownia, systemy i aplikacje centralne oraz własne, usprawniające pracę pracownikom Urzędu Gminy w Iwierzycach.

Informatyk pełnił funkcję Administratora Systemów Informatycznych (ASI).

W okresie objętym kontrolą w Urzędzie Gminy w Iwierzycach 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:

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

- system Kadry i Płace, FK, Logistyka, Majątek - Przedsiębiorstwa Informatyki „ETOB-RES” sp. z o.o.

- WIN Podatki – firmy U.I. INFO-SYSTEM Roman i Tadeusz Groszek sp. j.

- System ewidencji i rozliczania opłat za śmieci – SU - firmy „Softres” sp. z o.o.

- System eSesja i platforma PZP Zakładu Elektronicznej Techniki Obliczeniowej „ZETO” 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. Usługi elektroniczne

Urząd Gminy w Iwierzycach 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 na platformie ePUAP.

Przesyłka wpływająca przez ESP odbierana i rejestrowana była przez pracownika, a następnie przekazywana do kierowników lub pracowników.

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 w Iwierzycach 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.

* 1. Obieg dokumentów

W Urzędzie Gminy w Iwierzycach 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 i wprowadzony System Zarządzania Bezpieczeństwem Informacji (SZBI).

Kluczowe dokumenty były związane z ochroną danych osobowych:

* Instrukcja Zarządzania Systemem Informatycznym służącym do przetwarzania Danych Osobowych w Urzędzie Gminy w Iwierzycach stanowiąca Załącznik nr 2 do Zarządzenia nr 120.34.2019 Wójta Gminy Iwierzyce z dnia 18 grudnia 2019 r.;
* Polityka Bezpieczeństwa Przetwarzania Danych Osobowych w Urzędzie Gminy w Iwierzycach stanowiąca Załącznik nr 1 do Zarządzenia nr 120.34.2019 Wójta Gminy Iwierzyce z dnia 18 grudnia 2019 r.;
* Instrukcja Postępowania w Sytuacji Naruszenia Ochrony Danych Osobowych w Urzędzie Gminy w Iwierzycach stanowiąca Załącznik nr 3 do Zarządzenia nr 120.34.2019 Wójta Gminy Iwierzyce z dnia 18 grudnia 2019 r.;
* Polityka Czystego Biurka i Druku w Urzędzie Gminy w Iwierzycach stanowiąca Załącznik nr 4 do Zarządzenia nr 120.34.2019 Wójta Gminy Iwierzyce z dnia 18 grudnia 2019 r.;
* Regulamin Funkcjonowania Inspektora Ochrony Danych w Urzędzie Gminy w Iwierzycach stanowiący Załącznik nr 5 do Zarządzenia nr 120.34.2019 Wójta Gminy Iwierzyce z dnia 18 grudnia 2019 r.;
* Regulamin Retencji Danych Osobowych w Urzędzie Gminy w Iwierzycach stanowiący Załącznik nr 6 do Zarządzenia nr 120.34.2019 Wójta Gminy Iwierzyce z dnia 18 grudnia 2019 r.;
* Instrukcja przeprowadzenia oceny skutków dla danych osobowych (DPIA) oraz analizy ryzyka w Urzędzie Gminy w Iwierzycach stanowiąca Załącznik nr 7 do Zarządzenia nr 120.24.2019 Wójta Gminy Iwierzyce z dnia 18 grudnia 2019 r.;
* Zarządzenie nr 120.36.2019 Wójta Gminy Iwierzyce z dnia 18 grudnia 2019 r. w sprawie powołania Administratora Systemu Informatycznego w Urzędzie Gminy w Iwierzycach;
* Zarządzenie nr 15/2018 Wójta Gminy Iwierzyce z dnia 16 lipca 2018 r. w sprawie wyznaczenia Inspektora Ochrony Danych w Urzędzie Gminy w Iwierzycach;
* Raport analizy ryzyka dla bezpieczeństwa danych osobowych w Urzędzie Gminy w Iwierzycach z 2020 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.

W Urzędzie Gminy obowiązywała od 2019 r. Instrukcja przeprowadzenia oceny skutków dla danych osobowych (DPIA) oraz analizy ryzyka, która opisywała metodologię przeprowadzenia Oceny Ryzyka naruszenia praw lub wolności osób fizycznych.

W 2020 r. został dokonany Raport Analizy Ryzyka dla bezpieczeństwa danych osobowych w Urzędzie Gminy w Iwierzycach przez Inspektora Ochrony Danych, w którym została wskazana akceptacja ryzyka na poziomie średnim.

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.

Regulacje wewnętrzne nie zawierały zapisów dotyczących sposobu zarządzania sprzętem informatycznym i oprogramowaniem (w tym licencjami na oprogramowanie) oraz funkcjonowania rejestru zasobów teleinformatycznych.

Ewidencja poszczególnych podzespołów oraz oprogramowania prowadzona była przez informatyka.

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

* 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:

* Instrukcja Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych;
* Polityka Bezpieczeństwa Przetwarzania Danych Osobowych.

Dokumentacja powyższa szczegółowo opisywała sposób 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.

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 w Iwierzycach regulowała zakres podnoszenia świadomości pracowników poprzez konieczność zapoznania pracownika z treścią polityk, instrukcji, a także o zobowiązaniu się do ich przestrzegania.

W 2019 roku w Urzędzie Gminy było przeprowadzane szkolenie pracowników z zakresu „Ochrony danych osobowych”.

* 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.

W obowiązujących dokumentach nie były zawarte podstawowe zasady zarządzania bezpieczną pracą na komputerach przenośnych i sposoby zabezpieczenia tych urządzeń.

Pracownicy nie wynosili przenośnych komputerów poza siedzibę jednostki, w związku z tym praca zdalna nie występowała.

* 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 w ogólny sposób określone zostały zasady współpracy z podmiotami trzecimi w zakresie przetwarzania danych osobowych i serwisu sprzętu teleinformatycznego.

Dodatkowy poziom bezpieczeństwa regulowały umowy zawierane z firmami zewnętrznymi.

Jednak tylko niektóre 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.

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

* 1. Procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji

Zostały określone zasady postepowania w przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych w Polityce Bezpieczeństwa Przetwarzania Danych Osobowych (rozdział VII pkt E) oraz w Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych (Rozdział VII § 26). W zakresie bezpieczeństwa pozostałych informacji nie funkcjonowały procedury ani rejestr incydentów 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 nie był wykonywany.

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 Iwierzyce obowiązywały wymagania określone w Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych (rozdział V – Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania).

Kopie baz danych wykonywane były przez ASI z częstotliwością do 7 dni na dysk zewnętrzny.

Nośniki kopii zapasowych były przechowywane w innym pomieszczeniu niż serwerownia.

Wykonywanie odtworzenia systemów z kopii zapasowych występowało w razie potrzeby.

* 1. Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych

W Urzędzie Gminy w Iwierzycach 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 w Iwierzycach oraz w Polityce Bezpieczeństwa Przetwarzania Danych Osobowych w Urzędzie Gminy w Iwierzycach.

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 Iwierzycach posiadał lokalizację w jednym budynku.

Obiekt był objęty systemem alarmowym ochrony fizycznej, natomiast nie był objęty systemem monitoringu.

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

Serwerownia posiadała system alarmowy. Nie występowało monitorowanie parametrów środowiskowych w serwerowni (np. temperatury, wilgotności). Drzwi do serwerowni posiadały wzmocniony zamek.

Nośniki z kopiami były umieszczone w innym miejscu niż serwerownia.

W serwerowni znajdował się UPS, który podtrzymywał pracę serwerów 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.

Podstawowe urządzenia sieciowe oraz łącze nie posiadały tzw. zapasu.

Stosowane zapory sieciowe typu firewall były skonfigurowane domyślnie przez firmę zewnętrzną.

Nie wszystkie komputery oraz urządzenie sieciowe posiadały oprogramowanie systemowe zaktualizowane do wersji posiadających wsparcie producenta.

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

* 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 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 Iwierzycach 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 poprzez walidator dostępny pod adresem: https://validator.utilitia.pl/ badana strona uzyskała wynik 3,2 pkt na 10 możliwych, natomiast strona www uzyskała wynik 7,3 pkt na 10 możliwych.

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

Przy czym do ww. ustaleń kontrolnych (przekazanych do wiadomości w dniu 22 listopada 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 ustanowienie i wdrożenie, a następnie eksploatowanie, monitorowanie, przeglądanie i doskonalenie pełnego systemu bezpieczeństwa informacji wraz z uzupełnieniem dokumentacji o niezbędne elementy, w tym Plan Zachowania Ciągłości Działania.
2. W umowach serwisowych ze stronami trzecimi zawierać zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji, w tym połączeń zdalnych i określić poziom SLA.
3. Ustanowić podstawowe zasady gwarantujące bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość.
4. Zapewnić okresowe audyty wewnętrzne w zakresie bezpieczeństwa informacji 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.
5. Przeprowadzać cyklicznie szkolenia z zakresu nie tylko ochrony danych osobowych lecz również z zakresu bezpieczeństwa informacji, obejmujące wszystkie osoby uczestniczące w procesie przetwarzania informacji. Szkolenia te powinny dostarczać aktualnej wiedzy o nowych zagrożeniach, adekwatnych zabezpieczeniach oraz skutkach ewentualnych incydentów naruszenia bezpieczeństwa informacji.
6. Z uwagi na brak wsparcia dla systemu operacyjnego Windows 7 od 15 stycznia 2020 r. przez firmę Microsoft należy w pierwszej kolejności wyeliminować ww. oprogramowanie.
7. Należy zaktualizować posiadane zabezpieczenia sieciowe do wersji posiadających wsparcie producenta lub zadbać o ich wymianę.
8. Zadbać, aby wszystkie istotne dla jednostki oprogramowania miały możliwość rejestracji zdarzeń.
9. Należy rozważyć montaż urządzeń badających warunki środowiskowe (temperatura, wilgotność, dym, otwarcie drzwi serwerowni). Urządzenia te można skonfigurować tak, aby informacje o wystąpieniu w pomieszczeniu serwerowni niekorzystnych warunków środowiskowych wysyłane były poprzez np. e-mail, SMS.
10. W miarę możliwości przenieść programy instalowane lokalnie, np. księgowy, kadrowy na odpowiednio zabezpieczony serwer.

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)