

 **WOJEWODA PODKARPACKI**

 ul. Grunwaldzka 15

 35-959 Rzeszów

 OA-IV.431.4.2024 Rzeszów, 2024-12-31

**Pan**

**Dawid Homa**

**Wójt Gminy Świlcza**

 Na podstawie art. 46 ust. 1 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej, w związku ze zrealizowaną w dniach 5 i 6 listopada 2024 r. u Wójta Gminy Świlcza (Urząd Gminy, 36-072 Świlcza 168) 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 (z-ca kierownika) na podstawie imiennych upoważnień do kontroli (pisma z dnia 25.10.2024 r., znak OA-IV.431.4.2024) udzielonych przez działającego z upoważnienia Wojewody Podkarpackiego – Dyrektora Wydziału Organizacyjno-Administracyjnego.

Ustalenia kontrolne dokonane zostały w oparciu o stan faktyczny istniejący od 1 stycznia 2023 r.do dnia realizacji czynności kontrolnych włącznie.

Kontrola obejmuje priorytet Prezesa Rady Ministrów na 2024, 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 Świlcza 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 Świlcza”[[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 Świlcza pełnił Wójt: Pan Dawid Homa.

Funkcję Inspektora Ochrony Danych (IOD) powierzono wykonawcy zewnętrznemu Panu Danielowi Panek, na podstawie umowy ORP.2151.3.2024 z dnia 02.01.2024 z MP LEGAL Mielech, Panek i Wspólnicy Sp. Komandytowa.

Wsparcie informatyczne zapewnione było przez jedną osobę będącą pracownikiem Urzędu Gminy. Pod opieką informatyka znajdowały się: środowiska sprzętowo-programowe, sieć lokalna i serwerownia, systemy i aplikacje centralne oraz własne, usprawniające pracę pracownikom Urzędu Gminy Świlcza. Dodatkowo zawarte zostały umowy z wykonawcami zewnętrznymi zapewniające wsparcie w zakresie środowiska sprzętowo-programowego, systemów i sieci.

Została wyznaczona osoba odpowiedzialna za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa (Zarządzenie nr 202.2020 Wójta Gminy Świlcza z dnia 10 listopada 2020 r.) oraz dokonano jej zgłoszenia do CSIRT NASK w dniu 17 listopada 2020 r.

W okresie objętym kontrolą w Urzędzie Gminy Świlcza funkcjonowały systemy teleinformatyczne 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)

b) systemy własne lub zakupione:

 - CLANET Lokalny Rejestr Mieszkańców– firmy Clanet,

 - Ewidencja zwrotów podatku akcyzowego – firmy Biuro Usług komputerowych SOFTRES sp. z o.o. w ramach oprogramowania Sprawny Urząd,

- 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 w Świlczy 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 internetowej oraz BIP kontrolowanej jednostki znajdowała się informacja o adresie elektronicznej skrzynki podawczej.

* 1. Współpraca systemów teleinformatycznych z innymi systemami

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

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

* 1. Obieg dokumentów

W Urzędzie Gminy Świlcza był wdrożony Proton - system Elektronicznego Obiegu Dokumentów umożliwiający częściowe zarządzanie dokumentami i wykonywanie czynności kancelaryjnych głównie w zakresie przyjmowania korespondencji.

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

Zgodnie z § 19 ust. 1 Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, zwanego dalej Rozporządzeniem KRI - podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

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 z zakresu bezpieczeństwa informacji dotyczyły głównie ochrony danych osobowych, były to:

* Polityka Bezpieczeństwa Danych Osobowych w Urzędzie Gminy Świlcza wraz z załącznikami, stanowiąca Załącznik Nr 1 do Zarządzenia Nr 140.2020 Wójta Gminy Świlcza z dnia 1 września 2020 r.;
* Instrukcja Bezpieczeństwa Danych Osobowych, stanowiąca Załącznik Nr 1 do Zarządzenia Nr 140.2020 Wójta Gminy Świlcza z dnia 1 września 2020 r.;
* Polityka Zarządzania Kluczami obowiązująca Urząd Gminy Świlcza stanowiąca Załącznik do Zarządzenia Nr 63/2012 Wójta Gminy Świlcza z dnia 6 czerwca 2012 r.;
* Zarządzenie nr 202.2020 Wójta Gminy Świlcza z dnia 10 listopada 2020 r. w sprawie wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa oraz wprowadzenia instrukcji zarządzania zdarzeniami mającymi negatywny wpływ na cyberbezpieczeństwo (tzw. incydentami);
* Zgłoszenie osób kontaktowych do CSIRT NASK z 17 listopada 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.

Zarządzanie bezpieczeństwem opierało się na analizie ryzykiem związanym z ochroną danych osobowych. W tym celu stosowana była procedura określająca zasady przeprowadzenia analizy ryzyka w celu zabezpieczenia danych osobowych adekwatnych do zidentyfikowanych zagrożeń.

Arkusz analizy ryzyka - szacowania z 31.06.2022 r. został udostępniony na potrzeby kontroli. Były w nim opisane zagrożenia oraz adekwatne zabezpieczenia dotyczące czynności przetwarzania w zbiorach danych. Arkusz, od tego czasu nie był aktualizowany. Innych analiz zagrożeń związanych z przetwarzaniem informacji nie przedstawiono.

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.

Regulacje wewnętrzne w Urzędzie Gminy nie zawierały zapisów dotyczących utrzymania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji.

Ewidencja poszczególnych podzespołów oraz oprogramowania była prowadzona głównie w Ewidencji Środków Trwałych (EST) firmy SOFTRES sp. z o.o.

Jednostka nie dysponowała oprogramowaniem pozwalającym na identyfikację oprogramowania i komputerów w sieci.

W urzędzie do pracy bieżącej, użytkowane były komputery stacjonarne oraz laptopy, a do eksploatacji dopuszczone było tylko oprogramowanie autoryzowane przez ASI.

* 1. Zarządzanie uprawnieniami do pracy w systemach informatycznych

Istotnym elementem polityki bezpieczeństwa informacji jest zarządzanie dostępem do systemów teleinformatycznych przetwarzających informacje. Zarządzanie dostępem ma na celu 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 regulowały: Polityka Bezpieczeństwa Danych Osobowych i Instrukcja Bezpieczeństwa Danych Osobowych. W zakresie zarządzania dostępem istotne procedury to: Zarządzanie dostępem do danych osobowych oraz Procedura określająca środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych.

Dokumentacja powyższa opisywała sposób dostępu do obszarów chronionych, sieci i systemów teleinformatycznych, a także nadawanie uprawnień użytkownikom oraz ich pracy w systemach informatycznych funkcjonujących w jednostce. Instrukcja i Polityka nie regulowały sposobu odbierania uprawnień użytkownikom lub ich zmiany w przypadku innego zakresu obowiązków.

Pracownicy uzyskiwali dostęp do zasobów informatycznych po przyznaniu zakresu obowiązków, zapoznaniu z obowiązującymi dokumentami, nadaniu unikalnego identyfikatora i hasła w systemie teleinformatycznym zgodnie z zakresem obowiązków.

Zakres uprawnień użytkowników badanych systemów uniemożliwiał wykonywanie przez nich działań zastrzeżonych dla administratorów systemów.

Na bieżąco odbywało się monitorowanie dostępu do zasobów informatycznych zgodnie z wymaganiami § 19 ust. 2 pkt 4 rozporządzenia KRI.

Konta byłych pracowników urzędu były sukcesywnie blokowane w systemach informatycznych.

Informacja o konieczności zgłoszenia zmiany i odbioru uprawnień dla użytkownika w systemach informatycznych przekazywana była ustnie. Nie wykorzystywano do tego celu np. formularza wniosków o nadanie/odebranie uprawnień w systemie informatycznym.

* 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.

W Polityce Bezpieczeństwa Danych Osobowych uregulowany był zakres podnoszenia świadomości pracowników.

Kontrolującym przedstawiono informację o szkoleniach pracowników z 2024 roku, z zakresu bezpieczeństwa i ochrony danych osobowych. Wcześniejsze szkolenia nie zostały przedstawione. Nie przedstawiono również szkoleń odbytych przez Informatyka (poza tym z 2024 r.)

* 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 były zawarte ogólne zasady zarządzania bezpieczną pracą na komputerach przenośnych i sposoby zabezpieczenia tych urządzeń (Zasady korzystania z komputerów przenośnych).

W pracy bieżącej wykorzystywane były pendrive, które nie były szyfrowane.

Laptopy były szyfrowane.

* 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 dokumentacji wewnętrznej zostały określone zasady współpracy z podmiotami trzecimi w zakresie naprawy sprzętu komputerowego.

Poziom bezpieczeństwa regulowały przede wszystkim umowy zawierane z firmami zewnętrznymi, w przypadku serwisowania sprzętu lub oprogramowania.

W sprawdzanych umowach z firmami zewnętrznymi o asystę i opiekę autorską lub serwisową nie zawsze były określone SLA (Service Level Agreement), czyli gwarantowany poziom świadczenia usług oraz czas i sposób reakcji na zgłaszane problemy (udostępniono umowę z Biurem Usług komputerowych SOFTRES sp. z o.o. – 2024 r., oraz z CLANET Sp. z o.o. – na 2024 r.).

W przypadku systemów informatycznych istotnych dla jednostki nie zawsze zostały zawarte umowy powierzenia przetwarzania danych osobowych (np. stosowne zapisy w umowie z Biurem Usług komputerowych SOFTRES 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 (Postępowanie w przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych) oraz w Instrukcji Bezpieczeństwa Danych Osobowych (Zgłaszanie zdarzeń mogących świadczyć o naruszeniu bezpieczeństwa). W przypadku naruszenia bezpieczeństwa pozostałych informacji została ustanowiona Instrukcja zarządzania zdarzeniami mającymi negatywny wpływ na cyberbezpieczeństwo (tzw. incydentami).

W Urzędzie Gminy rejestr incydentów bezpieczeństwa nie zawierał wpisów.

* 1. Audyt wewnętrzny z zakresu bezpieczeństwa informacji

Audyt z zakresu bezpieczeństwa informacji nie rzadziej niż raz na rok, w rozumieniu § 19 ust. 14 rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych był wykonany corocznie. Ostatni audyt odbył się w 2024 r. Została także przeprowadzona diagnoza cyberbezpieczeństwa w ramach Projektu „Cyfrowa Gmina” w 2022 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.

* 1. Kopie zapasowe

Wykonywanie kopii zapasowych zapobiega utracie informacji w wyniku awarii.

Kopie powinny być właściwie tworzone, przechowywane i testowane.

W sprawdzanej Polityce i Instrukcji nie było informacji w zakresie obowiązku tworzenia kopii zapasowych oraz ich testowego przywracania mających na celu zapewnienie ciągłości pracy i bezpieczeństwa w systemach informatycznych. Na potrzeby kontroli została sporządzona przez Informatyka notatka zawierająca Procedurę tworzenia kopii zapasowych wraz z testowym przywracaniem maszyn wirtualnych.

Wykonywanie kopii zapasowych było prowadzone przy pomocy specjalistycznego oprogramowania do backupu.

Kopie zapasowe były przechowywane w innej lokalizacji niż serwerownia.

Dostęp do kopii bezpieczeństwa miały tylko osoby upoważnione przez Administratora Danych Osobowych.

Wykonywanie odtworzenia systemów z kopii zapasowych było przeprowadzane przez Informatyka lub firmy nadzorujące użytkowane systemy.

* 1. Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych

W Urzędzie Gminy Świlcza 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 21 maja 2024 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 Polityce Bezpieczeństwa Danych Osobowych (Określenie środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych, Zarządzania dostępem do danych osobowych) i Instrukcji 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.

Monitorowanie ruchu wchodzącego i wychodzącego realizowane było przez maszynę sprzętową UTM Fortigate. Konfiguracja i nadzór nad urządzeniem zostało powierzony wykonawcy zewnętrznemu.

W Urzędzie Gminy Świlcza pomieszczenia biurowe pracowników zlokalizowane były w głównym budynku, częściowo w sąsiednim budynku.

Obiekt był objęty systemem alarmowym ochrony oraz był objęty systemem monitoringu. Do otwierania głównych drzwi budynku byli upoważnieni wyznaczeni pracownicy.

Urząd Gminy dysponował jedną serwerownią główną, która znajdowała się w pomieszczeniu przeznaczonym na ten cel oraz dodatkowym miejscem, znajdującym się w niewielkim pomieszczeniu, na infrastrukturę sprzętową dedykowaną dla drugiego budynku. Dostęp do serwerowni był ograniczony i możliwy jedynie dla upoważnionych pracowników urzędu. Nie występowała kontrola dostępu. Ważnym elementem ochrony było asystowanie osobom wchodzącym i wykonującym prace serwisowe.

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

Drzwi do serwerowni były wzmocnione, natomiast okno znajdujące się w pomieszczeniu nie było zabezpieczone.

W serwerowni znajdował się UPS, który podtrzymywał pracę serwera, urządzeń sieciowych oraz komputerów. Dodatkowo przy stanowiskach komputerowych również znajdowały się UPSy.

W pomieszczeniu nie były przechowywane materiały łatwopalne.

Podstawowe urządzenie infrastruktury informatycznej: serwer, urządzenia sieciowe były zakupione w ramach Projektów.

Wszystkie 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.

Była wdrożona usługa katalogowa Active Directory, która pozwalała na zarządzanie tożsamościami i relacjami w sieci, przez co umożliwiała 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 Świlcza nie dysponował regulacjami wewnętrznymi, określającymi zasady rozliczalności działań użytkowników wykonywanych w systemach informatycznych.

Sprawdzane systemy informatyczne użytkowe nie miały udokumentowanej rozliczalności.

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 5,5 pkt na 10 możliwych, natomiast strona www uzyskała wynik 3,2 pkt na 10 możliwych.

Ww. ustalenia, w tym ocena kontrolowanej działalności, zostały udokumentowane w aktach kontroli, na które składają się kopie dokumentów oraz dokumenty przesłane przez urząd drogą elektroniczną.

Przy czym do ww. ustaleń kontrolnych (przekazanych do wiadomości w dniu 6 grudnia 2024 r.) przysługiwało Panu, na podstawie ww. ustawy o kontroli w administracji rządowej, prawo zgłoszenia umotywowanych pisemnych zastrzeżeń, z którego Pan nie skorzystał.

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 poniższe wnioski, zalecenia pokontrolne.

Zgodnie z wymogami § 19 ust. 1-14 Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych:

1. Dokonać analizy wszystkich umów serwisowych ze stronami trzecimi i w razie potrzeby uzupełnić je o zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji, w tym określić SLA (ciągłość działania) oraz prowadzić nadzór nad wykonawcami w zakresie zgodności z regulacjami i zapisami.
2. Dążyć do wzmocnienia zabezpieczeń techniczno-organizacyjnych pomieszczenia pełniącego rolę serwerowni.
3. Niezbędne jest ustalenie, wdrożenie, a następnie eksploatowanie, monitorowanie, przeglądanie i doskonalenie pełnego systemu zarządzania bezpieczeństwem informacji uwzględniającego zarządzanie ryzykiem i ciągłość działania systemu bezpieczeństwa informacji.
4. Wdrożyć szyfrowanie wszystkich urządzeń przenośnych.
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. Ustanowić w procedurze i uruchomić rozliczalność działań w systemach informatycznych użytkowników i obiektów oraz ich regularny przegląd.
7. Wprowadzić inwentaryzację sprzętu i oprogramowania informatycznego służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację (§ 19 ust. 2 pkt 2 Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych).
8. W celu zapewnienie bezpieczeństwa informacji podejmować działania zapewniające, 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. Te działania powinny uprawnić proces przekazywania informacji m. in. w przypadku bezzwłocznej zmiany uprawnień lub ich odebrania np. poprzez system obiegu korespondencji.

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**

 **(-)**

 **Teresa Kubas-Hul**

(Podpisane bezpiecznym podpisem elektronicznym)

1. W oparciu o zatwierdzony w dniu 13 grudnia 2023 r. „Plan zewnętrznej działalności kontrolnej Podkarpackiego Urzędu Wojewódzkiego w Rzeszowie na 2024 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)