

 **WOJEWODA PODKARPACKI**

 ul. Grunwaldzka 15

 35-959 Rzeszów

 OA-IV.431.1.2023 Rzeszów, 2023-04-25

**Pani**

**Renata Siembab**

**Burmistrz Przecławia**

 Na podstawie art. 46 ust. 1 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej, w związku ze zrealizowaną w dniach 9, 10 i 22 luty 2023 r. u Burmistrza Przecławia (Urząd Miejski w Przecławiu, ul. Kilińskiego 7, 39-320 Przecław) kontrolą problemową[[1]](#footnote-1), której przedmiotem była ocena działania systemów teleinformatycznych używanych do realizacji zadań zleconych z zakresu administracji rządowej z minimalnymi wymaganiami dla systemów teleinformatycznych - przekazuję niniejsze **wystąpienie pokontrolne.**

# Kontrolę przeprowadził zespół kontrolerów: Alicja Trygar (starszy inspektor wojewódzki), Tomasz Szmigiel (kierownik) na podstawie imiennych upoważnień do kontroli (pisma z dnia 01.02.2023 r., znak OA-IV.431.1.2023) udzielonych przez działającego z upoważnienia Wojewody Podkarpackiego – Dyrektora Generalnego Urzędu.

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 Miejskiego w Przecławiu 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 Burmistrza Przecławia”[[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 Miejskim w Przecławiu pełniła Burmistrz: Pani Renata Siembab.

Funkcję Inspektora Ochrony Danych (IOD) powierzono pracownikowi zatrudnionemu w Urzędzie Miejskim w Przecławiu Pani Sabinie Piecuch, na podstawie Zarządzenia nr 80/2018 Burmistrza Przecławia z dnia 31 lipca 2018 r. w sprawie powołania wspólnego Inspektora Ochrony Danych.

Wsparcie informatyczne zapewnione było również przez pracownika Urzędu Miejskiego. Pod jego opieką znajdowały się: środowiska sprzętowo-programowe, sieć lokalna i serwerownia, systemy i aplikacje centralne oraz własne, usprawniające pracę pracownikom Urzędu Miejskiego Przecławia.

Informatyk pełnił także funkcję Administratora Systemów Informatycznych (ASI) na podstawie zakresu obowiązków, uprawnień i odpowiedzialności z dnia 04 maja 2021 r. oraz został wyznaczony jako osoba kontaktowa do CSIRT NASK w dniu 13 maja 2021 r.

W okresie objętym kontrolą w Urzędzie Miejskim w Przecławiu 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:

 - PB\_EWID (Rejestr Mieszkańców) – firmy Technika IT,

 - PB\_EWID\_SRP (synchronizacja danych między systemami) – firmy Technika IT

 - 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 Miejski w Przecławiu 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 Miejskiego w Przecławiu posiadali dostęp do rejestrów publicznych takich jak: SRP Źródło, CEIDG.

System PB\_EWID\_SRP 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 Miejskim w Przecławiu 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 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) 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 został ustanowiony System Zarządzania Bezpieczeństwem Informacji (SZBI) – zarządzenie Nr 213/2022 Burmistrza Przecławia z dnia 30 grudnia 2022 r. w sprawie wprowadzenia „Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miejskim w Przecławiu”.

Kluczowe dokumenty SZBI to:

* Polityka Ochrony Danych Osobowych wraz z załącznikami, stanowiąca Załącznik nr 2 do Zarządzenia nr 213/2022 Burmistrza Przecławia z dnia 30 grudnia 2022 r.;
* Polityka Zarządzania Systemami Informatycznymi wraz z Procedurami, stanowiąca Załącznik nr 1 do Systemu Zarządzania Bezpieczeństwem Informacji Urzędu Miejskiego w Przecławiu;
* Instrukcja postępowania z kluczami oraz zabezpieczenia pomieszczeń i obiektu Urzędu Miejskiego w Przecławiu wprowadzona na podstawie regulaminu pracy Urzędu Miejskiego - Zarządzenie nr 129/2018 Burmistrza Przecławia z dnia 17 grudnia 2018 r.;
* Regulamin pracy zdalnej dla pracowników Urzędu Miejskiego w Przecławiu stanowiący załącznik do Zarządzenia nr 145.2020 Burmistrza Przecławia z dnia 22 października 2020 r.

Pomimo ustanowienia dokumentów związanych z SZBI, system ten nie został wdrożony w pełnym zakresie. Nie wszystkie dokumenty wskazane w dokumentacji SZBI zostały wprowadzone w życie, (np. nie przedstawiono dziennika systemów, czy instrukcji dla działania systemów na wypadek wdrożenia planu zachowania ciągłości działania), natomiast niektóre z dokumentów wymagały aktualizacji zapisów do bieżącej sytuacji.

Dodatkowo warto zwrócić uwagę, że cała dokumentacja powinna być zgodna i zawierać wymogi określone głównie w rozporządzeniu 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.

* 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 Miejskim w Przecławiu zarządzanie ryzykiem polegające na przeprowadzaniu przez Inspektora Ochrony Danych okresowej analizy ryzyka i oceny skutków dla przetwarzania danych w stosunku do przeprowadzanych czynności przetwarzania wspierało głównie bezpieczeństwo ochrony danych osobowych.

Wyniki analizy ryzyka mają wpływać na decyzje odnośnie podniesienia bezpieczeństwa funkcjonowania jednostki, np. poprzez wzmocnienie kontroli zarządczej, system zastępstw na strategicznych stanowiskach, szkolenia pracowników w stosunku do zagrożonych obszarów eksploatacji systemów informatycznych. Dokonując analizy ryzyka warto wziąć pod uwagę utratę integralności, dostępności lub poufności wszystkich informacji, nie tylko tych związanych z danymi osobowymi.

* 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). Niemniej do eksploatacji dopuszczone były tylko komputery i laptopy wraz z oprogramowaniem autoryzowanym i skonfigurowanym przez ASI.

Ewidencja poszczególnych podzespołów oraz oprogramowania prowadzona była przy pomocy zakupionego oprogramowania ESET PROTECT.

* 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 Urzędzie Miejskim zarządzanie uprawnieniami dostępu do przetwarzania danych regulowały: Polityka Zarządzania Bezpieczeństwem Informacji i Polityka Ochrony Danych Osobowych.

W zakresie zarządzania dostępem dodatkowo funkcjonowały: Procedura nadawania, odbierania uprawnień (Załącznik nr 2 do Polityki Zarządzania Systemem Informatycznym), Procedura blokowania, odblokowania i usuwania kont użytkowników (Załącznik nr 3 do Polityki Zarządzania Systemem Informatycznym) oraz Procedura zmiany haseł dla kont użytkowników (Załącznik nr 4 do Polityki Zarządzania Systemem Informatycznym).

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 zmiany i odbioru uprawnień dla użytkownika w systemach informatycznych informacja przekazywana była telefonicznie lub mailowo do informatyka, który po konsultacji z IOD dokonywał zmian.

W urzędzie obowiązywała dokumentacja, która wskazywała w takich przypadkach na stosowanie formularza wniosku o przyznanie upoważnienia do przetwarzania danych osobowych oraz przydzielenie uprawnień w systemie informatycznym przetwarzającym dane osobowe (Załącznik nr 3 do Polityki Ochrony Danych Osobowych).

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 regulowała zakres podnoszenia świadomości pracowników poprzez konieczność zapoznania wszystkich osób przetwarzających informację z procedurami bezpieczeństwa informacji w zakresie niezbędnym do wykonywania pracy, a także o obowiązku do ich przestrzegania.

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

Kontrolującym przedstawiono informację o szkoleniach pracowników z 2020 i 2022 roku, z zakresu bezpieczeństwa informacji oraz ochrony danych osobowych. Dokumentacja związana z bezpieczeństwem informacji była umieszczona na zasobie sieciowym, dostępnym dla wszystkich pracowników.

* 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.

Pracownicy nie wynosili przenośnych komputerów poza siedzibę jednostki.

* 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 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.

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 (udostępniono umowę z Biurem Usług komputerowych SOFTRES sp. z o.o.).

W przypadku systemów informatycznych istotnych dla jednostki zostały zawarte także umowy powierzenia przetwarzania danych osobowych (udostępniono m.in. umowę: z Technika IT Sp. z o.o. i 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 informacji w Urzędzie Miejskim w Przecławiu w:

- Polityce Zarządzania Systemami Informatycznymi,

- Polityce Ochrony Danych Osobowych.

Według wyjaśnień rejestr incydentów nie zawierał wpisów dotyczących naruszenia bezpieczeństwa informacji.

* 1. Audyt wewnętrzny z zakresu bezpieczeństwa informacji

Nie był wykonywany coroczny audyt z zakresu bezpieczeństwa informacji w rozumieniu § 20 ust. 14 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. Poprzednie audyty odbyły się w 2019 r. oraz w 2022 r. - 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 Miejskim w Przecławiu obowiązywały ogólne wymagania określone w Polityce Bezpieczeństwa Informacji i Ochrony Danych Osobowych (Procedura tworzenia kopii).

Wykonywanie kopii zapasowych miało być udoskonalone przy pomocy nowo zakupionego oprogramowania do backupu.

Kopie zapasowe nie były przechowywane w innej lokalizacji niż serwerownia.

Wykonywanie odtworzenia systemów z kopii zapasowych występowało w razie potrzeby.

* 1. Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych

W Urzędzie Miejskim w Przecławiu 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, a współpraca w ramach serwisu układała się poprawnie.

Pracownicy nie zgłaszali podczas audytu 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 Zarządzania Systemami Informatycznymi oraz w Polityce Ochrony Danych Osobowych w Urzędzie Miejskim w Przecławiu.

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 Miejski w Przecławiu posiadał lokalizację w jednym budynku.

Obiekt był objęty systemem alarmowym ochrony fizycznej oraz był objęty systemem monitoringu na zewnątrz budynku. Do otwierania głównych drzwi budynku oraz rozkodowania systemu alarmowego byli upoważnieni wyznaczeni pracownicy.

Urząd Miejski 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 również posiadała system alarmowy. Występowało monitorowanie niektórych parametrów środowiskowych w serwerowni (temperatury), jednak brakowało systemu ppoż. Pomieszczenie było klimatyzowane.

Drzwi do serwerowni były wzmocnione, w oknie były kraty.

Bazy danych z kopiami były umieszczone w tym samym miejscu.

W serwerowni znajdował się UPS, który podtrzymywał pracę serwera 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 urządzenie infrastruktury informatycznej – nowo zakupiony serwer był przed konfiguracją.

Zapora sieciowa typu firewall także w ramach Projektu była nowo zakupiona i informatyk przygotowywał się do jej konfiguracji.

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.

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

Takie wdrożenie jest planowane po dokonaniu instalacji serwera, jego konfiguracji i odbyciu szkolenia przez pracownika z zakresu zarządzania usługą Active Directory – w ramach projektu „Cyfrowa Gmina”.

* 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 Miejski w Przecławiu nie dysponował regulacjami wewnętrznymi, w których określone byłyby zasady rozliczalności działań wykonywanych w systemach informatycznych.

Sprawdzane systemy informatyczne użytkowe miały wprowadzoną rozliczalność działań.

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 7,7 pkt na 10 możliwych. W ramach projektu „Cyfrowa Gmina” jest przewidziane dostosowanie strony internetowej oraz BIP do wymogów dostępności cyfrowej.

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 ePUAP.

Przy czym do ww. ustaleń kontrolnych (przekazanych do wiadomości w dniu 28 marca 2023 r.) przysługiwało Pani, na podstawie ww. ustawy o kontroli w administracji rządowej, prawo zgłoszenia umotywowanych pisemnych zastrzeżeń, z którego Pani 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 Pani 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 wdrożenie, a następnie eksploatowanie, monitorowanie, przeglądanie i doskonalenie pełnego systemu bezpieczeństwa informacji wraz z dostosowaniem, a następnie stosowaniem bieżącej dokumentacji w tym zakresie uwzględniającej zarządzanie ryzykiem i ciągłość działania systemu bezpieczeństwa informacji.
2. Dokonać analizy wszystkich umów serwisowych ze stronami trzecimi i w razie potrzeby uzupełnić je o zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji oraz określić SLA.
3. Kopie zapasowe przechowywać w innej lokalizacji niż serwerownia.
4. Wykonywać audyt z zakresu bezpieczeństwa informacji nie rzadziej niż raz na rok, w rozumieniu § 20 ust. 14 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.
5. Przeanalizować wdrożenie usługi katalogowej Active Directory, która pozwalałaby na zarządzanie tożsamościami i relacjami w sieci, przez co umożliwiałaby sprawniejszą kontrolę nad całą siecią.
6. Wdrożyć szyfrowanie wszystkich urządzeń przenośnych.

O sposobie wykonania powyższych wniosków pokontrolnych, bądź działaniach podjętych w celu ich realizacji, oczekuję od Pani 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)