

**WOJEWODA PODKARPACKI**

ul. Grunwaldzka 15

35-959 Rzeszów

OA-IV.431.4.2023 Rzeszów, 2024-01-09

**Pan**

**Wojciech Bakun**

**Prezydent Miasta Przemyśla**

# Na podstawie art. 46 ust. 1 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej, w związku ze zrealizowaną w dniach 14, 16 i 29 listopada 2023 r. u Prezydenta Miasta Przemyśla 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 03.11.2023 r., znak OA-IV.431.4.2023) udzielonych przez 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 Przemyślu 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 Prezydenta Miasta Przemyśla”[[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 Przemyślu pełnił Prezydent: Pan Wojciech Bakun.

Funkcję Inspektora Ochrony Danych (IOD) powierzono pracownikowi Panu Przemysławowi Popiel na podstawie Zarządzenia nr 150/2018 Prezydenta Miasta Przemyśla z dnia 10 maja 2018 r. w sprawie wyznaczenia Inspektora ochrony danych w Urzędzie Miejskim w Przemyślu.

Wsparcie informatyczne zapewnione było przez pracowników Biura Informatycznego Urzędu Miasta. Pod ich opieką znajdowały się: środowiska sprzętowo-programowe, sieć lokalna i serwerownie, systemy i aplikacje centralne oraz własne, usprawniające pracę pracownikom Urzędu Miejskiego w Przemyślu.

Została wyznaczona osoba odpowiedzialna za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa na podstawie Zarządzenia Nr 258/2019 Prezydenta Miasta Przemyśla z dnia 15 lipca 2019 r. Funkcję tę pełnił Pełnomocnik Prezydenta ds. Ochrony Informacji Niejawnych. Zgłoszenia osoby do CSIRT NASK zostało przedstawione kontrolującym.

W okresie objętym kontrolą w Urzędzie Miejskim w Przemyślu 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:

- KSAT2000i (Internetowy Zintegrowany System Zarządzania dla jednostek samorządu terytorialnego obejmujący m.in. Ewidencję Ludności, Eksport Danych, Ewidencję zwrotów podatku akcyzowego – firmy COIG S.A.

- EZD 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 Przemyślu 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 Przemyślu posiadali dostęp do rejestrów publicznych takich jak: SRP Źródło, CEIDG, CEPIK.

System KSAT2000i komunikował się z usługami sieciowymi Systemu Rejestrów Państwowych w celu pobierania danych dzięki modułowi odpowiadającemu za transmisję danych z SRP do Lokalnej Ewidencji Ludności.

* 1. Obieg dokumentów

W Urzędzie Miejskim w Przemyślu był wdrożony Proton - system Elektronicznego Obiegu Dokumentów umożliwiający zarządzanie dokumentami i wykonywanie czynności kancelaryjnych.

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

Zgodnie z § 20 ust. 1 rozporządzenia KRI (rozporządzenie Rady Ministrów z dnia 12.04.2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych) podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarzadzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji. Wymaga to opracowania dokumentacji SZBI, w tym szeregu regulacji wewnętrznych oraz zapewnienia aktualizacji tych regulacji w zakresie dotyczącym zmieniającego się otoczenia. Dokumentacja jest warunkiem niezbędnym dla możliwości skutecznego zarządzania bezpieczeństwem informacji.

W zakresie bezpieczeństwa teleinformatycznego w badanej jednostce został ustanowiony System Zarządzania Bezpieczeństwem Informacji (SZBI) głównie według wymogów Normy ISO 27001.

Kluczowe dokumenty dotyczyły głównie ochrony danych osobowych, były to:

* Polityka Bezpieczeństwa Informacji, stanowiąca Załącznik nr 1 do Zarządzenia nr 222/2018 Prezydenta Miasta Przemyśla z dnia 29 czerwca 2018 r.;
* Polityka Bezpieczeństwa Danych Osobowych, wraz z załącznikami stanowiąca Załącznik nr 2 do Zarządzenia nr 222/2018 Prezydenta Miasta Przemyśla z dnia 29 czerwca 2018 r.;
* Instrukcja Zarządzania Systemami Informatycznymi wraz z załącznikami, stanowiąca Załącznik nr 3 do Zarządzenia nr 222/2018 Prezydenta Miasta Przemyśla z dnia 29 czerwca 2018 r.;
* Procedura Identyfikacji Wymagań, stanowiąca Załącznik nr 4 do Zarządzenia nr 222/2018 Prezydenta Miasta Przemyśla z dnia 29 czerwca 2018 r.;
* Metodyka szacowania i postępowania z ryzykiem wraz z załącznikami, stanowiąca Załącznik nr 5 do Zarządzenia nr 222/2018 Prezydenta Miasta Przemyśla z dnia 29 czerwca 2018 r.;
* Deklaracja stosowania, stanowiąca Załącznik nr 6 do Zarządzenia nr 222/2018 Prezydenta Miasta Przemyśla z dnia 29 czerwca 2018 r.;
* Plan postępowania z ryzykiem, stanowiący Załącznik nr 7 do Zarządzenia nr 222/2018 Prezydenta Miasta Przemyśla z dnia 29 czerwca 2018 r.;
* Procedura audytu wewnętrznego, stanowiąca Załącznik nr 8 do Zarządzenia nr 222/2018 Prezydenta Miasta Przemyśla z dnia 29 czerwca 2018 r.;
* Protokół z przeglądu, stanowiący Załącznik nr 9 do Zarządzenia nr 222/2018 Prezydenta Miasta Przemyśla z dnia 29 czerwca 2018 r.;
* Procedura Działań Naprawczych, stanowiąca Załącznik nr 10 do Zarządzenia nr 222/2018 Prezydenta Miasta Przemyśla z dnia 29 czerwca 2018 r.;
* Zasady ochrony danych osobowych podczas świadczenia pracy zdalnej stanowiące Załącznik nr 14 do Polityki Bezpieczeństwa Danych Osobowych;
* Instrukcja Zabezpieczenia budynków i pomieszczeń Urzędu Miejskiego w Przemyślu stanowiąca Załącznik do Zarządzenia nr 237/2023 Prezydenta Miasta Przemyśla z dnia 15 maja 2023 r.;
  1. Analiza zagrożeń związanych z przetwarzaniem informacji

Wymogiem skuteczności SZBI jest przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji. Na analizę ryzyka składają się: identyfikacja, szacowanie a następnie określenie sposobu postępowania z ryzykiem oraz deklaracja stosowania zabezpieczeń będących podstawą podejmowania wszelkich działań minimalizujących ryzyko stosownie do przeprowadzonej analizy.

Zarządzanie bezpieczeństwem ochrony danych w Urzędzie Miejskim w Przemyślu opierało się na zarządzaniu ryzykiem, które polegało m.in. na przeprowadzaniu przez Biuro Informatyczne okresowej analizy ryzyka. Kontrolującym przedstawiono Kartę celu i zadania operacyjnego wraz z ryzykami z 2023 r. oraz na 2024 r dla najważniejszych systemów w jednostce.

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

* 1. Inwentaryzacja sprzętu i oprogramowania informatycznego

Zarządzanie infrastrukturą informatyczną wymaga utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację. W praktyce oznacza to zapewnienie funkcjonowania rejestru zasobów teleinformatycznych zawierającego informacje o wszystkich zidentyfikowanych aktywach informatycznych, w tym: szczegółowe dane o urządzeniach technicznych, oprogramowaniu i środkach komunikacji, ich rodzaju, parametrach, aktualnej konfiguracji i relacjach między elementami konfiguracji oraz użytkowniku.

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

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

Ewidencja poszczególnych podzespołów oraz programów była prowadzona przy pomocy oprogramowania GLPI oraz w ewidencji wyposażenia w postaci Karty środka trwałego.

* 1. Zarządzanie uprawnieniami do pracy w systemach informatycznych

Istotnym elementem polityki bezpieczeństwa informacji jest zarządzanie dostępem do systemów teleinformatycznych przetwarzających informacje. Zarządzanie dostępem ma zapewnić, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków, a w przypadku zmiany zadań następuje również zmiana ich uprawnień.

Zarządzanie uprawnieniami dostępu do przetwarzania danych w Urzędzie Miejskim w Przemyślu regulowały: Polityka Bezpieczeństwa Danych Osobowych i Instrukcja Zarządzania Systemami Informatycznymi.

W zakresie zarządzania dostępem szczegółowe uregulowania występowały w:

- Procedurze nadawania, odbierania uprawnień do przetwarzania danych i rejestrowania oraz wyrejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności,

- Stosowanych metodach i środkach uwierzytelniania oraz procedurach związanych z ich zarządzaniem i użytkowaniem.

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 upoważnienia do przetwarzania danych osobowych.

W przypadku konieczności nadania lub zmiany uprawnień dla użytkownika stosowany był pisemny Wniosek o nadanie uprawnień do przetwarzania danych osobowych (Załącznik nr 1 do Instrukcji Zarządzania Systemami Informatycznymi). Następnie informacja, również w postaci pisemnej, była przekazywana do Biura Informatycznego celem nadania uprawnień w systemach informatycznych na podstawie wydanego upoważnienia. Korespondencja oraz wykonywane czynności były rejestrowane w Elektronicznym Obiegu Dokumentów PROTON.

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 na podstawie stosownych zgłoszeń mimo braku

procedury przeprowadzania przeglądu uprawnień i aktualności użytkowników.

* 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 Miejskiego w Przemyślu 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 przeszkoleniu pracowników z 2023 roku, z zakresu cyberbezpieczeństwa.

* 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.

Sposoby zarządzania bezpieczną pracą na komputerach przenośnych i sposoby zabezpieczenia tych urządzeń były zawarte w Zasadach ochrony danych osobowych podczas świadczenia pracy zdalnej stanowiących załącznik do Polityki Bezpieczeństwa Danych Osobowych (Zarządzenie nr 427/2020 Prezydenta Miasta Przemyśla z dnia 10 listopada 2020 r.).

W związku z tym warto przenalizować czy wszystkie urządzenia przenośne zostały zaszyfrowane.

* 1. Serwis sprzętu informatycznego i oprogramowania

W przypadku systemów informatycznych o znaczeniu istotnym dla jednostki niezbędne jest objęcie tych systemów (w zakresie oprogramowania użytkowego, systemowego, sprzętu i rozwiązań telekomunikacyjnych) stosownymi umowami serwisowymi, gwarantującymi odpowiednio szybkie uruchomienie pracy systemu w przypadku awarii. Umowy powinny posiadać klauzule prawne zabezpieczające ochronę informacji w przypadku wejścia w ich posiadanie przez firmy serwisujące.

W procedurach wewnętrznych dot. ochrony danych osobowych ogólnie zostały określone zasady współpracy z podmiotami trzecimi głównie w zakresie przetwarzania danych osobowych.

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

Sprawdzane umowy o asystę i opiekę autorską lub serwisową z firmami zewnętrznymi miały określone SLA (Service Level Agreement), czyli gwarantowany poziom świadczenia usług oraz czas i sposób reakcji na zgłaszane problemy (Umowa serwisowa z 31 stycznia 2023 r. DU.US-60.39.23 z COIG na system KSAT2000i, Umowa na utrzymanie systemu serwisu internetowego Sky CMS z 13.01.2023 r. z NETKONCEPT sp. z o.o., Umowa nr 38/7/110 opieki autorskiej na oprogramowanie z dnia 06.12.2022 z Nefeni sp. z o.o. na system EZD PROTON).

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

* 1. Procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji

Zostały określone sposoby postępowania w przypadku stwierdzenia naruszenia bezpieczeństwa zasad ochrony danych osobowych w Polityce Bezpieczeństwa Danych Osobowych. Ewidencja naruszeń w zakresie ochrony danych osobowych zawierała stosowne wpisy (ostatni z 2022 r.). Nie przedstawiono procedur zgłaszania incydentów naruszenia bezpieczeństwa informacji związanych z pozostałymi informacjami przetwarzanymi w Urzędzie Miasta.

* 1. Audyt wewnętrzny z zakresu bezpieczeństwa informacji

Audyty 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 były wykonywane przez wykonawców zewnętrznych w 2022 r. na potrzeby diagnozy cyberbezpieczeństwa w ramach Projektu „Cyfrowa Gmina” oraz w 2023 r. – Cyberbezpieczeństwo, KRI.

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 Przemyślu obowiązywały ogólne wymagania określone w Instrukcji Zarządzania Systemami Informatycznymi (Procedura tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania).

Wykonywanie kopii zapasowych było udoskonalane przez Biuro Informatyczne, jednak szczegółowe procedury dotyczące backupów, przechowywania i odtwarzania, testowania na potrzeby zachowania ciągłości działania nie były opisane oraz prowadzone przez Biuro Informatyczne.

* 1. Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych

W Urzędzie Miejskim w Przemyślu proces administrowania technicznego i monitorowania określonych obszarów systemów, aplikacji, danych, infrastruktury sieciowej i stacji roboczych był wykonywany przez zespół informatyków, 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, poza wdrażaną aktualnie chmurową wersją systemu dziedzinowego KSAT2000i.

* 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 Systemami Informatycznymi oraz w Polityce Bezpieczeństwa Danych Osobowych.

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

1. zabezpieczenie dostępu do informacji poprzez wymuszone logowanie użytkowników za pomocą kart lub poprzez unikalny login i hasło;
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 Przemyślu posiadał lokalizację w kilku budynkach.

Obiekty były objęte systemem alarmowym i systemem monitoringu na zewnątrz i wewnątrz budynku ochrony fizycznej. Główny budynek był objęty również ochroną fizyczną przez strażników miejskich. Do pobierania kluczy do budynków byli uprawnieni pracownicy tych budynków.

Urząd Miasta dysponował jedną serwerownią w budynku głównym oraz w pozostałych budynkach w zależności od wykonywanych w nich zadań. Serwerownie znajdowały się w pomieszczeniach zaadaptowanych na ten cel. Dostęp do serwerowni był ograniczony i możliwy jedynie dla upoważnionych pracowników urzędu. Ważnym elementem ochrony było asystowanie osobom wchodzącym i wykonującym prace serwisowe.

Serwerownie posiadały czujki ruchu i dymu. Pomieszczenia były klimatyzowane.

Główna serwerownia posiadała system kontroli dostępu oraz wzmocnione drzwi wejściowe.

W jednym z pomieszczeń serwerowni były przechowywane materiały łatwopalne typu opakowania i kartony oraz wycofane sprzęty komputerowe, ze względu na brak magazynu.

Praca serwerów i urządzeń sieciowych w razie zaników prądu mogła być podtrzymywana przez UPS.

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

Bazy danych z kopiami były umieszczone w kilku miejscach, jednak nie było to opisane lub zdeponowane na potrzeby Planu Zachowania Ciągłości Działania.

* 1. Zabezpieczenia techniczno-organizacyjne systemów informatycznych

Stosowanie zabezpieczeń techniczno-organizacyjnych również powinno wynikać z analizy ryzyka i powstałego w jej wyniku planu postępowania z ryzykiem i deklaracji stosowania zabezpieczeń.

Poziom bezpieczeństwa systemów teleinformatycznych zapewniono poprzez:

1. aktualizację oprogramowania oraz redukcję ryzyk wynikających z wykorzystywania opublikowanych podatności technicznych systemów teleinformatycznych (w tym oprogramowania antywirusowego);
2. minimalizację ryzyka utraty informacji w wyniku awarii oraz ochronę przed błędami, utratą i nieuprawnioną modyfikacją, a także zapewnienie bezpieczeństwa plików systemowych, zastosowania systemu kopii zapasowych, systemu kontroli dostępu do zasobów informatycznych, systemu monitorowania funkcjonowania systemów teleinformatycznych i sieci.

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

* 1. Rozliczalność działań w systemach informatycznych

Przetwarzanie informacji w systemach wymagało dostępu do danych przez uprawnionych użytkowników. Wszelkie działania związane z przetwarzaniem informacji, a także działania administratorów muszą podlegać dokumentowaniu w postaci zapisów w dziennikach systemów (logi), co zapewnia rozliczalność operacji. Informacje zawarte w logach (tj. kto, kiedy i co wykonał w systemie teleinformatycznym) powinny być regularnie przeglądane w celu wykrycia działań niepożądanych i muszą być przechowywane w bezpieczny sposób, co najmniej dwa lata. Świadomość użytkowników, że żadne działanie nie zostanie anonimowe podnosi poziom bezpieczeństwa informacji.

Urząd Miejski w Przemyślu 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 7,7 pkt na 10 możliwych, natomiast strona www uzyskała wynik 5,5 pkt na 10 możliwych.

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

Przy czym do ww. ustaleń kontrolnych (przekazanych do wiadomości w dniu 11 grudnia 2023 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 następujące wnioski, zalecenia pokontrolne:

1. Zgodnie z wymogami § 20 ust. 1-3 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych niezbędne jest ustanowienie i wdrożenie, a następnie eksploatowanie, monitorowanie, przeglądanie i doskonalenie pełnego systemu bezpieczeństwa informacji uwzględniającego m.in. ciągłość działania systemów.
2. Ustanowić i wdrożyć pozostałe procedury, o których mowa w niniejszym dokumencie (m.in. zgłaszania incydentów naruszenia bezpieczeństwa informacji, systemu backupu, sposobu zarządzania sprzętem informatycznym i oprogramowaniem, rozliczalności działań).
3. Przeanalizować wdrożenie usługi katalogowej Active Directory, która pozwalałaby na zarządzanie tożsamościami i relacjami w sieci, przez co umożliwiałaby sprawniejszą kontrolę nad całą siecią.

O sposobie wykonania powyższych wniosków pokontrolnych, bądź działaniach podjętych w celu ich realizacji, oczekuję od Pana odpowiedzi na piśmie, w terminie **21 dni** od dnia otrzymania niniejszego wystąpienia.

**WOJEWODA PODKARPACKI**

**(-)**

**Teresa Kubas-Hul**

(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)