WOJEWODA
ŚWIĘTOKRZYSKI

Kielce, dnia 23-08-2024

Znak:OK.V.431.3.2024

Pan Marcin Piszczek
Burmistrz Miasta Jędrzejowa

WYSTĄPIENIE POKONTROLNE

Zakres kontroli:	Prawidłowość działania systemów informatycznych używanych do realizowania zadań zleconych z zakresu administracji rządowej.
Okres objęty kontrolą:	od 1 stycznia 2018 r. do dnia wszczęcia kontroli tj. 19 czerwca 2024 r.
Kontrolerzy:	Marek Rak – Główny specjalista Oddziału do spraw Informatyki w wydziale Organizacji i Kadr Świętokrzyskiego Urzędu Wojewódzkiego w Kielcach – upoważnienie do kontroli nr 496/2024 z 17 czerwca 2024r. Maciej Terek – Główny specjalista Oddziału do spraw Informatyki w wydziale Organizacji i Kadr Świętokrzyskiego Urzędu Wojewódzkiego w Kielcach – upoważnienie do kontroli nr 497/2024 z 17 czerwca 2024r.
Termin przeprowadzenia kontroli:	Kontrola została przeprowadzona w dniu 19 czerwca 2024 r. w siedzibie Urzędu Miasta w Jędrzejowie, ul. 11 Listopada 33A, 28-300 Jędrzejów.
Podstawa prawna do przeprowadzenia kontroli:	Kontrolę przeprowadzono na podstawie art. 6 ust. 4 pkt 3 ustawy z dnia 15 lipca 2011 r. *o kontroli w administracji rządowej*[1], art. 28 ust. 1 pkt 2 ustawy z dnia 23 stycznia 2009 r. *o Wojewodzie i Administracji rządowej w województwie*[2] oraz art. 25 ust.1 pkt 3 lit. a) ustawy z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne*[3]. Wystąpienie pokontrolne przekazano zgodnie z przepisami art. 47 ustawy o kontroli w administracji rządowej.
Ocena stanu faktycznego wynikająca z ustaleń kontroli:	Zgodnie z Rozporządzeniem Rady Ministrów z dnia 21 maja 2024 r. *w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych*[4] ocenie

[1] Dz. U. z 2020 r. poz. 224, dalej: Ustawa o kontroli w administracji rządowej.
[2] Dz. U. z 2023 r. poz. 190
[3] Dz. U. z 2024 r. poz. 307
[4] Dz.U. z 2024 r. poz. 773, dalej Rozporządzenie KRI

podlegały czynności podejmowane w trzech obszarach tematycznych:

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

Pozytywnie z nieprawidłowościami ocenia się prawidłowość działania systemów informatycznych używanych do realizowania zadań zleconych z zakresu administracji rządowej w Urzędzie Miejskim w Jędrzejowie w okresie objętym kontrolą.

Ocena końcowa ustalona została na podstawie przedstawionych poniżej wnioski i oceny cząstkowe.

Kontrolą w przedmiotowym zakresie objęto systemy informatyczne używane do realizacji zadań zleconych z zakresu administracji rządowej tj.: SRP Źródło, CEIDG, Rejestr Wyborców oraz RESPONS(moduł Paliwa). W toku przeprowadzonej kontroli ustalono, że

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

Oceny stanu faktycznego dokonano zgodnie z §19 ust. 1 i 2 Rozporządzenia KRI. Ustalono, że podstawowymi dokumentami z zakresu bezpieczeństwa informacji w Urzędzie Miasta w Jędrzejowie jest Polityka Ochrony Danych Osobowych (PODO) składająca się z trzech dokumentów: Polityki Ochrony Danych (POD), Regulaminu Ochrony Danych (ROD), Regulaminu Monitoringu Wizyjnego (RMW), które są załącznikami do Zarządzenia Nr 183/2024 Burmistrza Miasta Jędrzejowa z dnia 6 czerwca 2024 r. *w sprawie wprowadzenia stosowania procedur związanych z ochroną danych osobowych przetwarzanych w kontrolowanej jednostce*.

Kontrolowany nie przedstawił oryginałów dokumentów wprowadzonych Zarządzeniem nr 207/2022 Burmistrza Miasta Jędrzejowa z dnia 20.05.2022 r. czyli PODO, ROD i RMW. Przedłożono niepodpisane elektronicznie kopie cyfrowe dokumentów oraz ich wydruki.

W omawianych dokumentach naprzemiennie stosowane są określenia: „ochrona danych osobowych" oraz „ochrona danych". Żaden z wymienionych dokumentów w swojej podstawie nie przywołuje Rozporządzenia o KRI. Część procedur z POD nie została wdrożona, wciąż nie jest stosowana lub zawiera zapisy rozbieżne względem pozostałej treści POD. Regulacje dotyczące analizy ryzyka oraz dokumentacja w zakresie przeprowadzonych audytów są dokumentami, do których zespół kontrolny wnosi wiele uwag. Uwagi te zostały opisane poniżej.

Ponadto stwierdzono brak przeglądów POD w latach 2022-2024 do których przeprowadzenia nie rzadziej niż raz w roku zobowiązany jest IODO (brak prowadzenia załącznika R2).

Przedmiotowe regulacje załączono w formie plików cyfrowych do akt kontroli (plik pn.: Dokumenty do wysłania 06.2024r.zip, pobrane-dokumenty-UM-Jedrzejow.pdf).

Ocena cząstkowa badanego zagadnienia:

Pozytywnie z nieprawidłowościami ocenia się działalność Jednostki w przedmiotowym zakresie.

2. Realizacja działań z zakresu bezpieczeństwa informacji:

Zakres kontroli przedmiotowego zagadnienia został podzielony na dwanaście obszarów badawczych:

1. Analiza zagrożeń związanych z przetwarzaniem informacji.

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

Kontrolującym przedłożono Analizy Ryzyka z lat 2022-2023. Urząd Miejski w Jędrzejowie w dniu kontroli nie przedłożył oryginalnych dokumentów. Zostały udostępnione niepodpisane elektronicznie kopie cyfrowe oraz ich wydruki. Stwierdzono, że dokumenty z kolejnych lat nie zawierają znaczących różnic, poza datą ich sporządzenia. W analizie ryzyka z roku 2022 zespół kontrolny prześledził zagrożenie zdefiniowane pod nr 36 – „zaniedbania użytkowników i administratorów". Poziom ryzyka pierwotnego w tym przypadku został określony na poziomie 75%. Wdrożenie trzech rodzajów zabezpieczeń pozwoliło zmniejszyć końcowy poziom ryzyka do wartości 25% w roku 2022. Natomiast w analizie ryzyka na kolejny rok tj. 2023 r. pomimo wdrożonych trzech zabezpieczeń w poprzednim roku, ponownie oszacowano poziom ryzyka pierwotnego na poziomie 75% tak, jak przed wdrożeniem przedmiotowych zabezpieczeń. Podobną zależność wykazują również inne określone w Jednostce ryzyka.
Porównywane zapisy z corocznie podejmowanych działań w zakresie analizy ryzyka, realizowanych w Jednostce w latach 2022 – 2023 wykazały wysoki poziom zbieżności treści. Zdaniem kontrolujących taka budowa przedmiotowych zapisów sporządzanych w następujących po sobie latach może wskazywać na brak zapewnienia odpowiedniego poziomu staranności i rzetelności podczas ich opracowania, jak również podczas czynności poprzedzających opracowanie tj. brak adekwatnego poziomu analizy ryzyka. Dokument POD wraz z załącznikami nie zawiera opisu całego procesu szacowania ryzyka; m.in. nie zamieszczono metodyki i algorytmów liczących poziom ryzyka.

Przedmiotowe Analizy załączono w formie plików cyfrowych do akt kontroli (Dokumenty do wysłania 06.2024r).

2. Inwentaryzacja sprzętu i oprogramowania informatycznego.

Oceny stanu faktycznego dokonano zgodnie z §19 ust. 2 pkt 2 Rozporządzenia KRI.
Ustalono, że inwentaryzacja sprzętu i oprogramowania jest prowadzona przez ASI przy pomocy oprogramowania Axence nVision. Zostały udostępnione przykładowe dwa raporty, raport dotyczący sprzętu i raport dotyczący oprogramowania. Natomiast w POD i jej załącznikach temat inwentaryzacji sprzętu i oprogramowania

w rozumieniu KRI (patrz KRI §19 ust. 2 pkt 2) został pominięty.

Przedłożone dokumenty: raporty dotyczące sprzętu i oprogramowania zostały załączone w formie skanów elektronicznych do akt kontroli (plik pobrane-dokumenty-UM-Jedrzejow.pdf).

3. Zarządzanie uprawnieniami do pracy w systemach informatycznych.

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

W §17 POD opisano procedurę nadawania uprawnień i upoważnień do przetwarzania danych (nadawanie, modyfikowanie, anulowanie uprawnień/upoważnień). Określono załączniki do tej procedury: załącznik nr 3 – Zlecenie modyfikacji uprawnień, załącznik nr 4 – upoważnienie do przetwarzania danych osobowych.
Bezpośredni przełożony, określając zakres uprawnień, o który wnioskuje dla użytkownika obowiązany jest do stosowania zasad, o których mowa w schemacie dostępu do danych, załącznik R1.
Zostały udostępnione dokumenty związane z procedurą nadawania, modyfikacji, anulowania uprawnień, upoważnień wybranych przez zespół kontrolny pracowników o inicjałach: W.C, J.L., P.P. w celu weryfikacji procedury pod względem stosowania zapisów z POD UM.

- Pracownik o inicjałach W.C.
  Przedłożono Wniosek nr 7/2022 o nadanie uprawnień do przetwarzania danych osobowych w systemie informatycznym UM w Jędrzejowie dla pracownika o inicjałach W.C. Wzór wniosku prowadzony przez ASI na własne potrzeby podpisany przez przełożonego pracownika, oraz przez ASI. Wniosek jest niezgodny ze wzorem zamieszczonym w POD. Sam wniosek dotyczy nadania uprawnień w systemie Edicta. Natomiast przedłożony załącznik nr 4 „Upoważnienie do przetwarzania danych osobowych" nr 12 w części II wymienia szereg innych zbiorów, do których użytkownik otrzyma uprawnienia. W części „Ewidencja użytkownika systemów informatycznych" wpisana jest jedynie nazwa użytkownika w systemie ESOD. Natomiast z nadanych upoważnień z części II wynika, że pracownik W.C. ma również konta w innych systemach, które nie zostały wymienione we właściwym miejscu. Część załącznika nr 4 dotycząca Ewidencji sprzętu IT nie posiada właściwych danych, jest niewypełniona. Pracownik dostał również uprawnienia do zbioru o nazwie Zakładowy Fundusz Świadczeń, zbiór ten nie jest wymieniony w załączniku R1 w pozycji Wydział Organizacyjny i Spraw Obywatelskich (pracownik W.C jest naczelnikiem tego wydziału). Przedłożono również załącznik nr 5 „Oświadczenie pracownika" oraz certyfikaty ukończenia szkolenia z zakresu „bezpieczeństwo i ochrona informacji z uwzględnieniem wymogów RPEiR(UE) 2016/679 z dnia 27 kwietnia 2016r." z 23 maja 2024r.
- Pracownik o inicjałach P.P.
  Dla pracownika o inicjałach P.P został złożony wniosek nr 29/2022

modyfikacja uprawnień, wykorzystujący wzór prowadzony przez ASI na własne potrzeby podpisany przez przełożonego pracownika, oraz przez ASI. Wniosek jest niezgodny ze wzorem zamieszczonym w PODO. Przedłożono również załącznik nr 4 „Upoważnienie do przetwarzania danych osobowych" o numerze 84. Cześć załącznika nr 4 dotycząca ewidencji sprzętu IT nie została uzupełniona wymaganymi danymi. Przedłożono również załącznik nr 5 „Oświadczenie pracownika" oraz certyfikaty ukończenia szkolenia z zakresu „bezpieczeństwo i ochrona informacji z uwzględnieniem wymogów RPEiR(UE) 2016/679 z dnia 27 kwietnia 2016r." z lat 2022-2024.

- Pracownik o inicjałach J.L.
  Dla pracownika o inicjałach J.L. nie przedłożono wniosku bezpośredniego przełożonego o odebranie upoważnienia jak również wniosku o nadanie upoważnienia (załącznik nr 3). Przedłożono załącznik nr 4 „Upoważnienie do przetwarzania danych osobowych" o numerze 42 nadanie upoważnienia. Cześć załącznika nr 4 dotycząca ewidencji sprzętu IT nie została uzupełniona wymaganymi danymi. Brak złożonego podpisu pracownika o inicjałach J.L. Przedłożono załącznik nr 4 „Upoważnienie do przetwarzania danych osobowych" o numerze 42 anulowanie upoważnienia. Przedłożono również załącznik nr 5 „Oświadczenie pracownika".

W załączniku nr 4 jeżeli chodzi o uprawnienia, mamy podział na wersję papierową i wersję elektroniczną (przetwarzania danych). Nie jest jasne, które uprawnienia odnoszą się do danych przetwarzanych w wersji papierowej, a które uprawnienia dotyczą danych przetwarzanych w wersji elektronicznej. Wątpliwość budzi również uprawnienie PZ – praca poza siedzibą Administratora – w którym nie zostało jednoznacznie określone czy uprawnienie to dotyczy pracy zdalnej w odniesieniu do przetwarzania danych w wersji elektronicznej, czy do pracy w terenie poza siedzibą Urzędu. Podobne wątpliwości powstają również w kwestii uprawnienia A – archiwizacja. Z upoważnienia nie wynika jednoznacznie czy ma zastosowanie do robienia kopii archiwalnych, bezpieczeństwa, zapasowych w systemach informatycznych, czy sposobu przechowywania dokumentacji papierowej.

Proces nadawania, modyfikacji, odbierania uprawnień i upoważnień w znacznym stopniu odbiega od instrukcji przewidzianej w POD.
Brak przestrzegania w pełnym zakresie procedury opisanej w §17 POD w codziennej pracy począwszy od bezpośredniego przełożonego, dalej przez ASI i IODO.

Przedmiotowe dokumenty: załączniki nr 3 i 4, załącznik R1 zostały załączone w formie skanów elektronicznych do akt kontroli (plik pobrane-dokumenty-UM-Jedrzejow.pdf).

4. **Szkolenia pracowników zaangażowanych w proces przetwarzania danych.**

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

Kontrolowana Jednostka przedłożyła listy obecności z własnoręcznymi podpisami uczestników szkolenia z roku 2024 (załącznik nr 10). W dokumentacji dotyczącej nadawania, modyfikacji, odbierania uprawnień dla dwóch wybranych pracowników znajdowały się certyfikaty ze szkoleń odbytych w roku 2024. Na odwrocie certyfikatu znajduje się wypisana tematyka szkolenia. Brak prowadzenia załącznika nr 10 „Lista uczestników szkoleń" w latach 2022-2023.

Przedmiotowe listy szkoleń, konspekty szkoleń, certyfikaty ze szkoleń zostały załączone w formie skanów elektronicznych do akt kontroli (plik pobrane-dokumenty-UM-Jedrzejow.pdf).

5. **Praca na odległość i mobilne przetwarzanie danych.**

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

W dokumentach z zakresu bezpieczeństwa informacji wymienionych w części 1 wystąpienia nie poruszono tematu pracy zdalnej . *(W KRI §19 ust. 2 pkt 8 mówi o ustanowieniu podstawowych zasad pracy przy przetwarzaniu mobilnym i pracy zdalnej.)*Z rozmowy przeprowadzonej z ASI wynika, że firmy zewnętrzne współpracujące w ramach różnych umów z Urzędem nie dysponują dostępem do połączenia zdalnego z siecią Urzędu.
Przedmiotowe regulacje załączono w formie plików cyfrowych do akt kontroli (Dokumenty do wysłania 06.2024r.zip, pobrane-dokumenty-UM-Jedrzejow.pdf).

6. **Serwis sprzętu komputerowego i oprogramowania.**

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

W dokumentach z zakresu bezpieczeństwa informacji wymienionych w części 1 wystąpienia nie poruszono zagadnień związanych z serwisem sprzętu i oprogramowania. Przedłożono umowę z firmą ZETO SOFTWARE Sp. z o.o., która całościowo określa sposób serwisowania oprogramowania tej firmy. Z rozmowy przeprowadzonej z ASI wynika, że serwis sprzętu komputerowego i aktualizacje oprogramowania wykonuje ASI we własnym zakresie.

Przedmiotowe regulacje załączono w formie plików cyfrowych do akt kontroli (Dokumenty do wysłania 06.2024r.zip, pobrane-dokumenty-UM-Jedrzejow.pdf).

7. **Procedury zgłaszania incydentów naruszenia Bezpieczeństwa Informacji.**

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

Powyższe zagadnienie jest opisane w §33 POD – Postępowanie i procedury na wypadek zaistnienia zagrożenia, naruszeń tzw. Incydenty. Na potrzeby wspomnianej procedury zdefiniowano dwa załączniki. Załącznik nr 13 – Raport z naruszenia danych i załącznik nr 14 – Rejestr incydentów. Do dnia kontroli w Urzędzie Miasta obydwa załączniki nie zawierały wpisów dotyczących naruszeń/incydentów. Omawiana procedura dotyczy wyłącznie danych szczególnych – tj. danych osobowych. Procedura nie obejmuje innych danych przetwarzanych w Urzędzie Miasta niż dane osobowe. To może sugerować brak świadomości konieczności ochrony innych danych niż dane osobowe.

Przedmiotową POD wraz z załącznikami nr 13 i 14 załączono w formie plików cyfrowych do akt kontroli (Dokumenty do wysłania 06.2024r.zip, pobrane-dokumenty-UM-Jedrzejow.pdf)

8. Audyt wewnętrzny z zakresu bezpieczeństwa informacji.

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

W §36 POD w niewystarczający sposób została opisana procedura dotycząca audytów wewnętrznych w zakresie bezpieczeństwa informacji. Określono jedynie częstotliwość wykonywania audytów. Mają być wykonywane nie rzadziej niż raz w roku. Kontrolującym przedłożono dokumentację dotyczącą audytów wewnętrznych przeprowadzonych przez IODO w latach 2022-2023. Udostępniona dokumentacja posiada jedynie znacznik czasu w postaci daty wpisanej komputerowo, bez podpisu osoby, która przeprowadziła audyt. UM do dnia kontroli nie przedstawił oryginałów dokumentów dotyczących audytów z lat 2022-2023, a jedynie niepodpisane elektronicznie kopie cyfrowe, z których na potrzeby kontroli wykonano wydruk dokumentacji.

Audyty z lat 2022-2023 dotyczyły obszaru działania związanego z Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2016 w sprawie KRI. W obu audytach z lat 2022-2023 zadano jednakowe pytania kontrolne, w ten sam sposób oceniono spełnione wymogi, udzielono tych samych komentarzy, wniosków, uwag, w ten sam sposób uzasadniono oceny.

Zespół kontrolny przeanalizował trzy pierwsze obszary badania.

Punkt 1 „Dokumenty z zakresu bezpieczeństwa informacji”.

Dokumenty z zakresu bezpieczeństwa informacji w rozumieniu KRI.

Czy polityk bezpieczeństwa podlegają aktualizacji w zakresie dotyczącym zmieniającego się otoczenia? TAK.

W obu audytach z lat 2022-2023 autor powołuje się na §37 z POD pomijając Regulamin Ochrony Danych, w którym jest napisane, że należy wdrożyć załącznik nr R2 – przegląd i aktualizacja POD. Za aktualizowanie tego załącznika odpowiada Administrator i IOD. Załącznik R2 do dnia kontroli nie był aktualizowany, procedura nie

została wdrożona. Oba audyty pomijają brak wdrożenia załącznika R2. Tym samym nie można uznać, że cała procedura dotycząca aktualizacji POD została wdrożona i spełnia wymogi KRI posiadając atrybuty autentyczności, rozliczalności, niezaprzeczalności i niezawodności.

Punkt 2 *„Inwentaryzacja sprzętu i oprogramowania informatycznego".* Audytor powołuje się we wszystkich przypadkach na §15, §16, §17 POD oraz na prowadzone: załączniki 3 zlecenie modyfikacji uprawnień, oraz załącznik 4 upoważnienia do przetwarzania danych osobowych.

W POD w żadnym miejscu nie został poruszony temat inwentaryzacji sprzętu i oprogramowania w rozumieniu KRI. Zespół kontrolny analizując procedurę nadawania, modyfikacji, odebrania uprawnień w systemach informatycznych (gdzie załączniki 3 i 4 mają zastosowanie) ustalił, że procedura realizowana w jednostce w znacznym stopniu odbiega od procesu zdefiniowanego w POD. Zespół kontrolny zwrócił uwagę na nie wypełnione części załącznika nr 4 dotyczące „Ewidencji sprzętu IT" we wszystkich załącznikach nr 4, które zostały udostępnione kontrolującym. ASI przedłożył dokumentację (przykładowe raporty) z oprogramowania, które służy mu do inwentaryzacji sprzętu i oprogramowania prowadząc inwentaryzację we własnym zakresie.

Punkt 3 Analiza zagrożeń związanych z przetwarzaniem informacji. Uwagi kontrolujących w tym zakresie znajdują się w punkcie 2.1 niniejszego dokumentu.

Zarządzenie Burmistrza Miasta Jędrzejowa nr 207/2022 z dnia 20 maja 2020 w §1 mówi o tym, że „Wprowadza się procedury postępowania i zabezpieczenia danych osobowych przetwarzanych w Urzędzie Miejskim w Jędrzejowie stanowiące Politykę Bezpieczeństwa Ochrony Danych Osobowych". §2 Nadzór i kontrolę nad realizacją zarządzenia powierza się Inspektorowi Ochrony Danych Osobowych w Urzędzie Miejskim w Jędrzejowie.

Audyty z lat 2022-2023 przeprowadziła ta sama osoba, która odpowiada za wdrożenie procedur wprowadzonych Zarządzeniem nr 207/2022 Burmistrza Miasta Jędrzejowa. Z Audytów z lat 2022-2023 wynika, że zaledwie około 43% zadań objętych audytem zostało wdrożonych na przestrzeni 2 lat. Pozostałe zadania, procesy, procedury są od dwóch lat w realizacji, nie wiadomo, w jakim stopniu zostały wdrożone, nie wiadomo kiedy zakończy się wdrożenie.

UM posiada dokumentację z audytów przeprowadzonych przez audytora wewnętrznego z roku 2017-2022.

Przedmiotowe regulacje załączono w formie plików cyfrowych do akt kontroli (Dokumenty do wysłania 06.2024r.zip, pobrane-dokumenty-UM-Jedrzejow.pdf).

9. Kopie zapasowe.

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

W §26 POD – Zasady tworzenia kopii bezpieczeństwa i kopii archiwalnych opisano procedurę wykonywania kopii danych w systemach informatycznych. ASI zapisuje kopie zapasowe na nośnikach zewnętrznych, które przechowuje w certyfikowanym sejfie znajdującym się w serwerowni. Kopie wykonywane są automatycznie według wcześniej ustalonego harmonogramu. Kopie przechowywane są również na urządzeniu NAS, które zamontowane jest w serwerowni w szafie dystrybucyjnej. ASI prowadzi załącznik 17 – Rejestr nośników komputerowych zawierających dane. Systemy, dane oraz ich kopie przechowywane są w tej samej strefie pożarowej.

Przedmiotowe regulacje załączono w formie plików cyfrowych do akt kontroli (Dokumenty do wysłania 06.2024r.zip).

10. Bezpieczeństwo techniczno-organizacyjne dostępu do informacji.

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

Ustalono, że Urząd Miasta w Jędrzejowie zajmuje dwa budynki. Budynek z wejściem głównym posiada drzwi metalowe oszklone. W pobliżu na ścianie budynku umieszczona jest kamera monitoringu wizyjnego. Budynek wyposażony jest w system antywłamaniowy. Pomieszczenie serwerowni znajduje się na parterze budynku głównego, wyposażone jest w urządzenie systemu klimatyzacji oraz czujkę alarmu antywłamaniowego. Gaśnica systemu przeciwpożarowego znajduje się na zewnątrz przy wejściu do pomieszczenia serwerowni. Serwerownia wyposażona jest w szafy dystrybucyjne, w których zamontowane zostały urządzenia aktywne. Są one podpięte są do urządzeń UPS, zapewniających podtrzymanie napięcia przez około 15 minut. Budynek wyposażony jest w system monitoringu wizyjnego. Opracowano Regulamin monitoringu wizyjnego, który jest częścią PBODO Urzędu. Opracowano i wdrożono politykę kluczy, prowadzony jest rejestr pobrań kluczy. ASI przedłożył „Protokół zniszczenia uszkodzonych nośników komputerowych" z 2019 roku.

Przedmiotowe regulacje załączono w formie plików cyfrowych do akt kontroli (Dokumenty do wysłania 06.2024r.zip).

11. Zabezpieczenia techniczno-organizacyjne systemów informatycznych.

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

	Ustalono, że ustawienia dotyczące polityki haseł (częstotliwości zmian hasła, złożoności) oparte są o Active Directory. Zostały udostępnione zrzuty ekranu z konsoli systemu Windows Serwer z parametrami haseł. ASI prowadzi „Rejestr kopert z hasłami administracyjnymi" (załącznik nr 16 do POD). Hasła przechowywane są w tzw. bezpiecznej kopercie, w pomieszczeniu serwerowni w certyfikowanym sejfie. Urząd posiada sprawne, podłączone i skonfigurowane urządzenie UTM umieszczone w szafie dystrybucyjnej w serwerowni. ASI udostępnił zrzut z konsoli urządzenia z podstawowymi parametrami i certyfikatami. **12. Rozliczalność działań w systemach teleinformatycznych.** Oceny stanu faktycznego dokonano zgodnie z §21 ust. 2, 3 oraz 4 Rozporządzenia KRI. Ustalono, że oprogramowanie wspomagające oraz systemy operacyjne używane w UM posiadają funkcjonalności monitorujące prace użytkowników. Nie ma procedury, narzędzi czy oprogramowania do systematycznego przeglądania logów systemowych co w efekcie końcowym skutkuje brakiem przeglądania logów a tym samym brakiem monitorowania zdarzeń. Przedmiotowe informacje załączono w formie skanów elektronicznych do akt kontroli (pobrane-dokumenty-UM-Jedrzejow.pdf).
Ocena cząstkowa badanego zagadnienia:	Pozytywnie z nieprawidłowościami ocenia się działalność Jednostki w przedmiotowym zakresie.
3. Zapewnienie dostępności cyfrowej informacji zawartych na stronach internetowych urzędów dla osób z niepełnosprawnościami zgodnie z ustawą z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych:	**Czy sporządzono i opublikowano deklarację dostępności oraz zawarto w deklaracji dostępności elementy wskazane w art. 10 ust. 3-5 ustawy dla stron internetowych podmiotu.** Oceny stanu faktycznego dokonano zgodnie z §10 ust. 3, 4 i 5 ustawy. Ustawy z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych[5]. Ustalono, że obydwie kontrolowane strony posiadają stosowne deklaracje dostępności: – https://jedrzejow.eu – Deklaracja dostępności aktualizowana 2023-11-20 – http://jedrzejow.eobip.pl – Deklaracja dostępności aktualizowana 2020-09-22 Deklaracje dostępności nie zawierają informacji na temat skrótów klawiszowych służących przemieszczaniu się po elementach strony internetowej.
Ocena cząstkowa badanego zagadnienia:	Pozytywnie z uchybieniami ocenia się działalność Jednostki w przedmiotowym zakresie.

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

Wnioski, zalecenia oraz dodatkowe informacje:

Reasumując powyższe ustalenia, zwracam się z prośbą do Pana Burmistrza o niedopuszczenie do powstania nieprawidłowości wykazanych w toku kontroli w przyszłej działalności w podległej Panu Jednostce. Wobec powyższego sformułowano następujące zalecenia:

1. Wdrożyć wszystkie procedury opisane w POD lub zmienić POD tak, aby uwzględniała to co jest faktycznie wykonywane.

2. Wykonywać regularnie przeglądy POD do których zobowiązany jest IODO.

3. Rzetelnie przeprowadzać analizę ryzyka.

4. Uwzględnić zagadnienie inwentaryzacji sprzętu i oprogramowania w dokumentacji SZBI.

5. Dopracować proces nadawania, modyfikacji, odbierania uprawnień i upoważnień i zapewnić aby dokumentacja opisywała to co faktycznie jest wykonywane.

6. Opisać w dokumentacji SZBI zasady pracy przy przetwarzaniu mobilnym i pracy zdalnej zgodnie z zaleceniami zawartymi w KRI.

7. Uwzględnić w dokumentacji SZBI zagadnienia związane z serwisem sprzętu i oprogramowania.

8. Zapewnić, aby zarządzanie incydentami obejmowało wszystkie dane przetwarzane w jednostce a nie tylko dane osobowe.

9. Opisać szczegółowo w dokumentacji SZBI procedurę dotyczącą przeprowadzania audytów wewnętrznych w zakresie bezpieczeństwa informacji.

10. Rzetelnie przeprowadzać audyty wewnętrzne.

11. Systematycznie przeglądać logi systemowe.

12. W deklaracjach dostępności uzupełnić informacje na temat skrótów klawiszowych służących przemieszczaniu się po elementach strony internetowej.

Jednocześnie na podstawie art. 49 ustawy o kontroli w administracji rządowej, proszę poinformować Wojewodę Świętokrzyskiego w terminie 30 dni od daty otrzymania niniejszego wystąpienia pokontrolnego o sposobie wykorzystania wyżej wymienionych uwag i wniosków oraz o wykonaniu zaleceń, a także o podjętych działaniach lub przyczynach niepodjęcia działań.

Ponadto informuję, iż zgodnie z art. 48 ustawy o kontroli w administracji rządowej od niniejszego wystąpienia pokontrolnego nie

przysługują środki odwoławcze.

Józef Bryk
Wojewoda Świętokrzyski