WOJEWODA LUBUSKI

Władysław Dajczak

Gorzów Wlkp., dnia 1 kwietnia 2019 r.

NK-II.431.1.7.2018

Pani
Magdalena Szydełko
Wójt Gminy Stare Kurowo

Wystąpienie pokontrolne
z kontroli przeprowadzonej w Urzędzie Gminy Stare Kurowo

Na podstawie art. 28 ust.1 pkt 2 ustawy z dnia 23 stycznia 2009 r. o wojewodzie i administracji rządowej w województwie (Dz.U.2017.2234 ze zm.), art. 2 i art. 6 ust. 4 pkt 3 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz.U.2011.185.1092) pracownicy Wydziału Nadzoru i Kontroli oraz Biura Obsługi Urzędu i Rozwoju Systemów Informatycznych Lubuskiego Urzędu Wojewódzkiego w Gorzowie Wlkp. w składzie:

- Izabela Okonek – inspektor wojewódzki - przewodnicząca zespołu,
- Małgorzata Wołejko – starszy inspektor wojewódzki,
- Michał Piaskowski – kierownik Oddziału Informatyki,
- Izabela Milczarek – informatyk ds. administrowania systemami informatycznymi

na podstawie pisemnych upoważnień do przeprowadzenia kontroli nr: 195/1-4/2018 z dnia 10 września 2018 r., w dniach od 12 września 2018 r. do dnia 31 października 2018 r. przeprowadzili kontrolę problemową w trybie zwykłym w Urzędzie Gminy Stare Kurowo.
Kontrola została odnotowana w książce kontroli pod pozycją nr 2/2018.

Przedmiotem kontroli było: realizacja zadań administracji rządowej wynikających z ustawy z dnia 6 sierpnia 2010 r. o dowodach osobistych (Dz.U.2017.1464 ze zm.), ustawy z dnia 24 września 2010 r. o ewidencji ludności (Dz.U.2018.1382 ze zm.) oraz działanie systemów teleinformatycznych oraz rejestrów publicznych używanych do realizacji zadań zleconych z zakresu administracji rządowej na podstawie ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U.2017.570 ze zm.).

Okres objęty kontrolą, w zakresie:

- realizacji zadań administracji rządowej wynikających z ustawy o dowodach osobistych i ewidencji ludności - od 1 stycznia 2018 r. do 30 czerwca 2018 r.,
- działania systemów teleinformatycznych oraz rejestrów publicznych używanych do realizacji zadań zleconych z zakresu administracji rządowej – kontrola sprawdza stan obecny w obszarze objętym kontrolą.

Do projektu wystąpienia pokontrolnego zastrzeżenia nie zostały wniesione. Wobec powyższego stosownie do art. 47 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej przekazuję wystąpienie pokontrolne, obejmujące treść projektu wystąpienia pokontrolnego z dnia 29 stycznia 2019 r.

Ocena stanu faktycznego:

- w obszarze wykonywanie zadań wynikających z *ustawy o dowodach osobistych* i *ustawy o ewidencji ludności* oceniono **pozytywnie z nieprawidłowościami,**
- w obszarze wymiany informacji w postaci elektronicznej, w tym współpraca z innymi systemami/rejestrami informatycznymi i wspomaganie świadczenia usług drogą elektroniczną działalność urzędu oceniono **pozytywnie z uchybieniami**,
- w obszarze bezpieczeństwa informacji działalność urzędu oceniono **negatywnie,**
- w obszarze dostępności informacji zawartych na stronach internetowych urzędów dla osób niepełnosprawnych oceniono **negatywnie.**

Powyższe oceny w poszczególnych obszarach uzasadniają przedstawione poniżej ustalenia dokonane w wyniku przeprowadzonej kontroli:

W okresie objętym kontrolą funkcję Wójta Gminy Stare Kurowo pełnił Pan Wiesław Własak. Zadania z zakresu ustawy o dowodach osobistych i ustawy o ewidencji ludności w badanym okresie wykonywała Pani Monika Popek - Inspektor do spraw Ewidencji Ludności i Dowodów Osobistych.

Od 1 marca 2015 r. zadania z zakresu wydawania dowodów osobistych oraz ewidencji ludności są realizowane przy pomocy jednej wspólnej dla wszystkich gmin w Polsce aplikacji Źródło. Jest to program do przetwarzania i edycji danych gromadzonych w Systemie Rejestrów Państwowych, którego celem jest zapewnienie szybkiej i sprawnej obsługi obywatela podczas jego wizyty w urzędzie.

Od 1 stycznia 2018 r. realizacja obowiązku meldunkowego została uproszczona, aby nowe przepisy były jak najmniej uciążliwe dla obywateli. Wprowadzono możliwość zameldowania się elektronicznie o dowolnej godzinie, bez wizyty w urzędzie. Dokona tego każda osoba, która posiada profil zaufany ePUAP albo kwalifikowany podpis elektroniczny.

Mieszkańcy Gminy nie korzystali z możliwości składania wniosków w formie dokumentu elektronicznego.

Pracownicy urzędu wykonujący zadania z kontrolowanego obszaru posiadają upoważnienia Wójta Gminy do przetwarzania danych osobowych zgromadzonych w rejestrze PESEL, Rejestrze Dowodów Osobistych oraz w systemach teleinformatycznych, w których prowadzone są przedmiotowe rejestry.

Nieprawidłowość:

- zadania określone w *ustawie o dowodach osobistych* oraz *ustawie o ewidencji ludności* wykonuje organ gminy, jako zadanie zlecone z zakresu administracji rządowej, a tym właściwym organem gminy jest wójt. Stwierdzono brak stosownych upoważnień do działania w imieniu organu.

Ponadto ustalono, iż w odpowiedziach na wnioski nieprawidłowo stosowano oznaczenie aparatu pomocniczego organu (Urząd Gminy), zamiast Wójt Gminy oraz pieczątkę pracownika, zamiast pieczątkę z upoważnienia organu.

W trakcie trwania kontroli ww. nieprawidłowość została usunięta, wystawiono stosowne upoważnienia oraz wyrobiono właściwą pieczątkę.

1. Dowody osobiste.

1.1. Wydawanie, wymiana oraz unieważnianie dowodów osobistych

Zgodnie z założeniami programu kontroli, szczegółowym badaniem objęto 86 wybranych wniosków dowodowych, tj. 28,38 % wszystkich wydanych dowodów osobistych w okresie objętym kontrolą.

Wszystkie zbadane wnioski o wydanie dowodu osobistego złożono u bezpośrednio prowadzącego sprawę pracownika.

Nieprawidłowość:

- w dniu 30 listopada 2017 r. wszedł w życie *§ 2 rozporządzenia Ministra Spraw Wewnętrznych z dnia 29 stycznia 2015 r. w sprawie wzoru dowodu osobistego oraz sposobu i trybu postępowania w sprawie wydawania dowodów osobistych, ich utraty, uszkodzenia, unieważnienia i zwrotu (Dz.U.2017.1626)*, który określił miedzy innymi wzór wniosku o wydanie dowodu osobistego. Stwierdzono przyjęcie wniosków o wydanie dowodu osobistego na innym niż określono w ww. rozporządzeniu formularzu.

W trakcie trwania kontroli wprowadzono poprawne formularze.

Wnioski o wydanie dowodu osobistego składały uprawnione osoby, zgodnie z *art. 25 ustawy*.

Zgodnie z *§ 9 rozporządzenia*, na wszystkich wnioskach znajdowała się adnotacja urzędowa o sposobie ustalenia tożsamości osoby ubiegającej się o wydanie dowodu osobistego.

Nieprawidłowość:

- stosownie do *rozporządzenia Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitego rzeczowego wykazu akt oraz instrukcji w sprawie organizacji*

i zakresu działania archiwów zakładowych (Dz.U.2011.14.67) wnioski o wydanie dowodu osobistego, nie były opatrywane (informacja o dacie wpływu) pieczęcią wpływu, co w konsekwencji powodowało, że nie zawierały informacji o dacie ich wpływu do Urzędu. Data ta stanowi zgodnie z przepisem *art. 61 § 3 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz.U.2018.2096 ze zm.)* - zwany dalej *kpa* datę wszczęcia postępowania administracyjnego i podstawę prawidłowego obliczenia terminu załatwienia sprawy.

W trakcie trwania kontroli nieprawidłowość została usunięta. Pracownik Urzędu przyjmując nowe wnioski opatrywał je pieczęcią wpływu.

Odbiór dowodu osobistego był każdorazowo potwierdzany na formularzu odbioru dowodu osobistego. Nieprawidłowość:
- stosownie do *art. 31 ust.2 ustawy* formularz odbioru dowodu osobistego zawiera nie tylko nazwisko i imię osoby, której wydano dowód osobisty, ale również nazwisko i imię wnioskodawcy. Stwierdzono brak danych wnioskodawcy, gdy w imieniu osoby nieposiadającej zdolności do czynności prawnych lub posiadającej ograniczoną zdolność do czynności prawnych ubiegającej się o wydanie dowodu osobistego wniosek składa rodzic, opiekun prawny lub kurator.

Pracownik wykonujący to zadanie oświadczył, że dane wnioskodawcy będą wpisywane.

Osoba, która odbierała nowy dowód osobisty przedkładała dotychczasowy. Jeżeli wyrażała wolę zachowania dokumentu, otrzymywała go po unieważnieniu w systemie, a następnie fizycznym uszkodzeniu.
Zgodnie z *art. 47 ustawy* w badanym okresie 18 razy zgłoszono utratę dowodu osobistego. We wszystkich 6 zbadanych (tj. 33,33 %) przypadkach posiadacze dowodu osobistego zgłaszali jego utratę zgodnie z *art. 48 ustawy* na formularzu zgłoszenia utraty lub uszkodzenia dowodu osobistego. Utracone dowody osobiste unieważniano w dniu zgłoszenia zgodnie z *art. 50 ust. 3 pkt 1 ustawy.*
Osobie zgłaszającej utratę dowodu osobistego wydawano zaświadczenie ważne do czasu wydania nowego dowodu osobistego, nie dłużej jednak niż przez 2 miesiące.

Stwierdzone powyżej nieprawidłowości nie miały wpływu na prawidłowość wydania dowodów osobistych, miały natomiast charakter powtarzalny.

1.2. Zakres danych gromadzonych w rejestrach oraz zasady prowadzenia tego rejestru

Kontroli poddano 44 (tj. 51,16 %) wszystkich skontrolowanych wniosków i formularzy.
Kontrola wykazała prawidłowy tryb rejestracji danych. Pracownik po wprowadzeniu daty odbioru przez obywatela dowodu osobistego oraz w przypadku unieważnienia do Rejestru Dowodów Osobistych za pośrednictwem aplikacji Źródło przekazywał dane określone ustawą do rejestru PESEL. Przekazywanie danych między rejestrami następowało niezwłocznie. Poddane kontroli dowody osobiste figurowały w RDO oraz w RM.

1.3. Zasady postępowania z dokumentacją związaną z dowodami osobistymi.

Dokumentacja stanowiąca podstawę do wydania dowodu osobistego przechowywana była w kopertach dowodowych. Wytypowane do kontroli wnioski o wydanie dowodu osobistego oraz formularze utraty dowodu osobistego, przechowywane były w prawidłowo oznaczonych zgodnie z *art. 62 ust.3 ustawy* kopertach dowodowych.

W kopertach dowodowych po upływie 6 miesięcy od dnia wydania zgodnie z *art. 62 ust.4 pkt 2 ustawy* przechowywane były nieodebrane dowody osobiste.

Dokumentacja przechowywana jest w sposób zapewniający zabezpieczenie przed dostępem osób trzecich. Klienci przyjmowani są pojedynczo z zachowaniem wymogów o ochronie danych osobowych w wydzielonej strefie przyjęć.

1.4. Udostępnianie danych oraz wydawanie zaświadczeń z rejestru dowodów osobistych

Zgodnie z *art. 65 i art.75 ustawy* dane z rejestru dowodów osobistych i dokumentacji związanej z dowodami osobistymi udostępnia organ gminy prowadzący te rejestry.

W okresie objętym kontrolą do Urzędu Gminy wpłynął jeden wniosek o udostępnienie dokumentacji związanej z dowodami osobistymi, zgodnie z *rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 7 października 2011 r. w sprawie określenia wzorów wniosków o udostępnienie danych z Rejestru Dowodów Osobistych oraz dokumentacji związanej z dowodami osobistymi (Dz.U.2015.1604)*. Zgodnie z *art.75 ust.5 ustawy* podlegał on opłacie w wysokości określonej *rozporządzeniem Rady Ministrów z dnia 21 listopada 2011 r. w sprawie opłaty za udostępnienie danych z Rejestru Dowodów Osobistych i dokumentacji związanej z dowodami osobistymi (Dz.U.2016.319).* Zgodnie z *art.76 ustawy* opłata ta stanowi dochód budżetu państwa.

W kontrolowanym okresie nie wydawano zaświadczeń w trybie *art.63 ustawy* zawierających pełny odpis danych dotyczących tej osoby.

2. Ewidencja ludności.

2.1. Przyjmowanie zgłoszeń meldunkowych

W badanym okresie w Urzędzie Gminy Stare Kurowo przyjęto 73 zgłoszenia meldunkowe, w tym zgłoszenia pobytu stałego, zgłoszenia pobytu czasowego, zgłoszenie wymeldowania z pobytu, zgłoszenie wyjazdu za granicę oraz zgłoszenia meldunkowe cudzoziemców. Sprawdzając wyrywkowo wytypowane do kontroli 19 sztuk (tj. 26%) formularzy ustalono, że wszystkie zgłoszenia meldunkowe obywateli polskich zostały dokonane zgodnie z obowiązującym *rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 września 2011 r. w sprawie określenia wzorów i sposobu wypełniania formularzy stosowanych przy wykonywaniu obowiązku meldunkowego (Dz.U.2017.2411).*

Nieprawidłowość:

- zgodnie z *art.39 ustawy* zgłoszenia meldunkowe cudzoziemców dokonuje się na formularzach określonych *ww. rozporządzeniem*. Stwierdzono przyjęcie wszystkich zgłoszeń meldunkowych

cudzoziemców na innym niż określono w *ww. rozporządzeniu* formularzu. Nie miało to wpływu na sposób realizacji kontrolowanego zadań, miało natomiast charakter powtarzalny.

W trakcie trwania kontroli wprowadzono poprawne formularze.

Zgłoszenia meldunkowe składane były u prowadzącego sprawę pracownika, który ustalał tożsamość wnioskodawcy, weryfikował zgłoszenie w oparciu o posiadane dokumenty i rejestry, a następnie wprowadzał dane do rejestru. Stosowane przy wykonywaniu obowiązku meldunkowego formularze, zawierały wszystkie wymagane do dokonania czynności dane, każdy zawierał potwierdzenie pobytu w formie własnoręcznego podpisu właściciela lub innego podmiotu dysponującego tytułem prawnym do lokalu.

Osobie dopełniającej obowiązku zameldowania na pobyt stały zgodnie z *art. 32 ust.1 ustawy*, wydawano z urzędu zaświadczenie o zameldowaniu na pobyt stały. Osobę dokonującą innych czynności meldunkowych informowano o możliwości uzyskania na wniosek zaświadczenia potwierdzającego dokonanie czynności.

2.2. Usuwanie niezgodności

W okresie kontroli nie odnotowano przypadków otrzymania zlecenia usunięcia niezgodności na wniosek osoby, której dane dotyczyły w trybie przepisów *art.11 ust.1 ustawy*. Natomiast 7 niezgodności zostało usuniętych z urzędu. Usunięte dane nie miały wpływu na ustalenie tożsamości osoby, której dane były sprawdzane, nie stanowiły więc podstawy do zawiadomienia tej osoby.

2.3. Zasady postępowania z dokumentacją związaną z obowiązkiem meldunkowym

Wszystkie zgłoszenia meldunkowe zarejestrowano w teczce aktowej oznaczonej symbolem klasyfikacji 5343 – „sprawy meldunkowe" z podziałem na podteczki, umożliwiającej weryfikację prawidłowo dokonanej czynności materialno – technicznej oraz umożliwiającej dokonanie ustaleń danych objętych sprawozdawczością.

2.4. Wydawanie decyzji w sprawach meldunkowych

Stosownie do *art. 35 ustawy* organ gminy wydaje z urzędu lub na wniosek decyzję w sprawie wymeldowania obywatela polskiego, który opuścił miejsce pobytu stałego albo opuścił miejsce pobytu czasowego przed upływem deklarowanego okresu pobytu i nie dopełnił obowiązku wymeldowania się. W badanym okresie wydano 4 decyzje meldunkowe. Kontroli poddano wszystkie wydane decyzje z czego w 3 przypadkach orzeczono o wymeldowaniu, w 1 przypadku postępowanie umorzono.

Kontrola wykazała, że w podjętych przez organ postępowaniach prawidłowo zawiadamiano strony o wszczęciu postępowania na podstawie *art. 61 § 4 kpa.* W postępowaniach wszczętych na wniosek pobrano opłatę skarbową zgodnie z *art. 1 ust. 1 ustawy z dnia 16 listopada 2006 r. o opłacie skarbowej (Dz.U.2018.1044 ze zm.)*. W jednym przypadku postępowanie było wszczęte z urzędu. Przed wydaniem decyzji strony zostały powiadomione o uprawnieniach wynikających z zapisów *art.10 kpa*, co potwierdzają zwrotne potwierdzenia odbioru załączone do akt poszczególnych spraw.

Nieprawidłowość:

- zgodnie z *art. 107 § 1 pkt 6 i § 3 kpa* jednym z elementów decyzji jest uzasadnienie prawne. We wszystkich poddanych kontroli decyzjach stwierdzono brak uzasadnienia prawnego.

Pracownik wykonujący to zadanie oświadczył, że będzie w decyzjach umieszczał uzasadnienie prawne.

Ww. decyzje zawierają pouczenie o środkach odwoławczych, jak również wydane są przez osobę uprawnioną do ich wydania. Decyzje zostały prawidłowo dostarczone stronom postępowania.
Akta prowadzonych spraw zawierały metrykę zgodnie z *art. 66a kpa* i *rozporządzeniem Ministra Administracji i Cyfryzacji z dnia 6 marca 2012 r. w sprawie wzoru i sposobu prowadzenia metryki sprawy (Dz.U.2012.250).*
Nieprawidłowość:
- zgodnie z *art. 35 § 3* załatwienie sprawy wymagającej postępowania wyjaśniającego powinno nastąpić nie później niż w ciągu miesiąca, a sprawy szczególnie skomplikowanej – nie później niż w ciągu dwóch miesięcy od dnia wszczęcia postępowania. W jednym przypadku przekroczono termin załatwienia sprawy. Nie dopełniono też obowiązku zawiadomienia stron o przyczynach zwłoki oraz wyznaczenia nowego terminu załatwienia sprawy, co koliduje z *art. 36 § 1 kpa.*

Powyższe sprawy były chronologicznie rejestrowane w spisie spraw założonym dla teczki aktowej oznaczonej symbolem klasyfikacji 5343 - „sprawy meldunkowe". Na poszczególnych podaniach umieszczano wynikający ze spisu spraw znak sprawy.

2.5. Nadawanie numeru PESEL

W badanym okresie wydano 21 numerów PESEL zgodnie z *art.17 ust.1 pkt 2 ustawy* z urzędu przy wykonywaniu obowiązku meldunkowego, w tym 20 numerów PESEL przez cudzoziemców na terenie gminy. Osoby te zostały powiadomione o nadaniu numeru PESEL.

2.6. Wymiana danych między rejestrami

Kontroli poddano 19 (tj. 100 %) wszystkich skontrolowanych wniosków i formularzy.
Kontrola wykazała prawidłowy tryb rejestracji danych wszystkich skontrolowanych formularzy zgodnie z *rozporządzeniem Ministra Spraw Wewnętrznych z dnia 16 lutego 2012 r. w sprawie trybu rejestracji danych w rejestrze PESEL oraz w rejestrach mieszkańców i rejestrach zamieszkania cudzoziemców (Dz.U.2018.2484).* Pracownik po dokonaniu zameldowania lub wymeldowania za pośrednictwem aplikacji Źródło rejestrował dane w rejestrze PESEL. Przekazywanie danych z rejestru PESEL do Rejestru Mieszkańców następowało niezwłocznie.

2.7. Udostępnianie danych z rejestru mieszkańców

Zgodnie z *art.50 ust.2 ustawy* dane z rejestru mieszkańców udostępnia organ gminy prowadzący rejestr. W kontrolowanym okresie 74 razy udostępniono nieodpłatnie zgodnie z *art. 53 pkt 1 ustawy* dane z rejestru mieszkańców podmiotom, wskazanym w *art. 46 ust.1 ustawy*. Badanie wszystkich (100 %) wniosków wykazało, że dwa wnioski nie zostały złożone na odpowiednich formularzach

określonych *rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 5 października 2011 r. w sprawie określenia wzoru wniosków o udostępnianie danych z rejestru mieszkańców, rejestru zamieszkania cudzoziemców i rejestru PESEL oraz trybu uzyskiwania zgody na udostępnianie danych po wykazaniu interesu faktycznego (Dz.U.2018.2523).* Powyższe uznano jednak za uchybienie, które nie wpłynęło na prawidłowe załatwienie sprawy. Odpowiedzi udzielano terminowo, zgodnie z zakresem żądania wnioskodawcy w formie wydruku z systemu lub odrębnego pisma. Kopię udzielonej odpowiedzi dołączano do wniosku.

Nieprawidłowość:

- zgodnie z *art. 55 ustawy* opłaty za udostępnianie danych stanowią dochód budżetu państwa;
- zgodnie z *art. 53 ustawy* udostępnienie danych następuje dla podmiotów, o których mowa w *art. 46 ustawy*. Odpłatnie podmiotom określonym w *ust.2 pkt 1 – 3*, nieodpłatnie podmiotom określonym w u*st.2 pkt.4 ustawy.*

Stwierdzono stosowanie pieczątki z adnotacją: „o zwolnieniu z opłaty skarbowej". Zwolnienia wynikające z *ustawy o opłacie skarbowej* nie mają w ww. przypadkach zastosowania.

Odrębnie rejestrowano i udzielano odpowiedzi własnym jednostkom organizacyjnym oraz tzw. udostępnień masowych.

2.8. Wydawanie zaświadczeń z rejestru mieszkańców

Zgodnie z *art.45 ust.2 ustawy* zaświadczenia z rejestru mieszkańców organ wydaje na wniosek zainteresowanej osoby. Kontrolując wszystkie 43 zarejestrowane sprawy stwierdzono, że Urząd po ich rozpatrzeniu wydawał zaświadczenia (poświadczenia zameldowania) w formie wydruku z systemu. W sytuacji gdy o wydanie zaświadczenia zwracała się osoba, której dane miały być wykorzystane do celów innych niż wynika to z *ustawy o opłacie skarbowej* pobierano opłatę w wysokości 17 zł. Zaświadczenia wydawano terminowo, kopie udzielonej odpowiedzi dołączano do wniosku.

Powyższe sprawy były chronologicznie rejestrowane w spisie spraw założonym dla teczki aktowej: NK.II.5345 – „Udostępnianie danych i wydawanie zaświadczeń z ewidencji ludności i dowodów osobistych". Na poszczególnych podaniach umieszczano wynikający ze spisu spraw znak sprawy.

3. Wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami/rejestrami informatycznymi i wspomaganie świadczenia usług drogą elektroniczną.

3.1. Usługi elektroniczne.

Zgodnie z *art. 16 ust. 1a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne*: Podmiot publiczny udostępnia elektroniczną skrzynkę podawczą, spełniającą standardy określone i opublikowane na ePUAP przez ministra właściwego do spraw informatyzacji, oraz zapewnia jej obsługę.

Zgodnie z *§ 5 ust. 2 pkt 1 i 4 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*.
Interoperacyjność na poziomie organizacyjnym osiągana jest przez, m.in.:
- informowanie przez podmioty realizujące zadania publiczne, w sposób umożliwiający skuteczne zapoznanie się, o sposobie dostępu oraz zakresie użytkowym serwisów dla usług realizowanych przez te podmioty;
- publikowanie i uaktualnianie w Biuletynie Informacji Publicznej przez podmiot realizujący zadania publiczne opisów procedur obowiązujących przy załatwianiu spraw z zakresu jego właściwości drogą elektroniczną.

Urząd Gminy Stare Kurowo dla wybranych usług publikuje na stronach BIP sposób załatwienia spraw. Na stronie głównej jest przekierowanie na platformę ePUAP, gdzie wystawiona jest jedna usługa elektroniczna – „Pismo ogólne do Urzędu".

3.2. Centralne repozytorium wzorów dokumentów elektronicznych.

Zgodnie z *art. 19 b ust. 3 ustawy*: Organy administracji publicznej przekazują do centralnego repozytorium oraz udostępniają w Biuletynie Informacji Publicznej wzory dokumentów elektronicznych. Przy sporządzaniu wzorów dokumentów elektronicznych stosuje się międzynarodowe standardy dotyczące sporządzania dokumentów elektronicznych przez organy administracji publicznej, z uwzględnieniem konieczności podpisywania ich bezpiecznym podpisem elektronicznym.
W trakcie kontroli ustalono, że Urząd w badanym okresie do centralnego repozytorium wzorów dokumentów ePUAP nie przekazywał wzorów dokumentów elektronicznych.

3.3. Model usługowy

Zgodnie z *§ 15 ust. 2 rozporządzenia*: Zarządzanie usługami realizowanymi przez systemy teleinformatyczne ma na celu dostarczanie tych usług na deklarowanym poziomie dostępności i odbywa się w oparciu o udokumentowane procedury.
Na stronie BIP Urzędu Gminy Stare Kurowo zamieszczane są karty informacyjne świadczonych usług, zawierające także dokumenty do pobrania. Elektroniczne załatwienie sprawy kończy się na etapie urzędu, gdzie dokumenty są drukowane i podlegają papierowemu obiegowi wewnątrz instytucji.
Nieprawidłowość:
- brak formalnych procedur zarządzania usługami.

3.4. Współpraca systemów teleinformatycznych z innymi systemami

Zgodnie z *§ 5 ust. 3 pkt 3 rozporządzenia*: Interoperacyjność na poziomie semantycznym osiągana jest przez m.in. stosowanie w rejestrach prowadzonych przez podmioty publiczne odwołań do rejestrów zawierających dane referencyjne w zakresie niezbędnym do realizacji zadań.
Według *§ 16 ust. 1 rozporządzenia*: Systemy teleinformatyczne używane przez podmioty realizujące

zadania publiczne wyposaża się składniki sprzętowe lub oprogramowanie umożliwiające wymianę danych z innymi systemami teleinformatycznymi za pomocą protokołów komunikacyjnych i szyfrujących określonych w obowiązujących przepisach, normach, standardach lub rekomendacjach ustanowionych przez krajową jednostkę normalizacyjną lub jednostkę normalizacyjną Unii Europejskiej.

Urząd Gminy posiada zintegrowany system do zarządzania gminą i na tym poziomie interoperacyjność systemów jest na odpowiednim poziomie.

3.5. Obieg dokumentów w Urzędzie.

Zgodnie z *§ 20 ust. 2 pkt 9 rozporządzenia*: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie m.in. zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu, jej ujawnienie, modyfikacje, usunięcie lub zniszczenie.

W Urzędzie Gminy Stare Kurowo w celu zarządzania obiegiem dokumentów i dokumentacją stosowane są procedury i zasady postępowania z dokumentami wpływającymi do Urzędu zawarte w Instrukcji Kancelaryjnej, stanowiącej załącznik do *rozporządzenia Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych i rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych.* W Urzędzie obowiązuje tradycyjny („papierowy") system wykonywania czynności kancelaryjnych, jako podstawowy sposób dokumentowania spraw w Urzędzie.

3.6. Formaty danych udostępniane przez systemy teleinformatyczne.

Zgodnie z *§ 17 ust. 1 rozporządzenia*: Kodowanie znaków w dokumentach wysyłanych z systemów teleinformatycznych podmiotów realizujących zadania publiczne lub odbieranych przez takie systemy, także w odniesieniu do informacji wymienianej przez te systemy z innymi systemami na drodze teletransmisji, o ile wymiana ta ma charakter wymiany znaków, odbywa się według standardu Unicode UTF-8 określonego przez normę ISO/1EC 10646 wraz ze zmianami lub normę ją zastępującą.

Zgodnie z *§ 18 ust. 1 rozporządzenia*: Systemy teleinformatyczne podmiotów realizujących zadania publiczne udostępniają zasoby informacyjne co najmniej w jednym z formatów danych określonych w załączniku nr 2 do rozporządzenia.

Wg *§ 18 ust. 2 rozporządzenia*: Jeżeli z przepisów szczegółowych albo opublikowanych w repozytorium interoperacyjności schematów XML lub innych wzorów nie wynika inaczej, podmioty realizujące zadania publiczne umożliwiają przyjmowanie dokumentów elektronicznych służących do załatwiania spraw należących do zakresu ich działania w formatach danych określonych w załącznikach nr 2 i 3 do rozporządzenia.

W toku kontroli dokonano weryfikacji kodowania znaków, w odniesieniu do informacji wymienianych przez systemy Urzędu z innymi systemami zewnętrznymi, na drodze teletransmisji, która wykazała stosowanie standardu Unicode UTF-8.

4. System zarządzania bezpieczeństwem informacji w systemach informatycznych.

4.1. Dokumenty z zakresu bezpieczeństwa informacji. Zaangażowanie kierownictwa podmiotu.

Zgodnie z *§ 20 ust. 1 rozporządzenia*: 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.

Zgodnie z *§ 20 ust. 2 rozporządzenia*: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie działań związanych z bezpieczeństwem informacji.

Zgodnie z *§ 20 ust. 2 pkt 1 rozporządzenia*: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez m.in. zapewnienie aktualizacji regulacji wewnętrznych w zakresie - dotyczącym zmieniającego się otoczenia.

Wójt Gminy Stare Kurowo wydał Zarządzenie Nr 120.25.2018 z dnia 03 sierpnia 2018 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji w Urzędzie Gminy w Starym Kurowie. Polityka bezpieczeństwa informacji jest skonstruowana poprawnie.

Nieprawidłowość:

- stwierdzono jednak, że nie została ona wdrożona w rzeczywistość. Istnieją duże rozbieżności pomiędzy zapisami polityki a stanem faktycznym. Polityka została ustanowiona na 2 miesiące przed rozpoczęciem kontroli, więc nie można stwierdzić czy były dokonywane jej przeglądy. Nie ma dowodów, że były one dokonywane w stosunku do wcześniejszych wersji dokumentu.

4.2. Analiza zagrożeń związanych z przetwarzaniem informacji.

Zgodnie z *§ 20 ust. 2 pkt 3 rozporządzenia*: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez, m.in. przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy.

Przedstawiony kontrolującym dokument „Szacowania ryzyka dla bezpieczeństwa danych osobowych" z dnia 19 czerwca 2018 r. odnosi się do szacowania ryzyka wyłącznie w obszarze danych osobowych.

Nieprawidłowość:

- pominięte zostały podatności i zagrożenia dla kluczowych systemów używanych w gminie. Nie przedstawiono planu postępowania z ryzykiem na żadnym poziomie ryzyka.

4.3. Inwentaryzacja sprzętu i oprogramowania informatycznego.

Zgodnie z *§ 20 ust. 2 pkt 2 rozporządzenia*: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez m.in. utrzymanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.

Nieprawidłowość:

- w wyniku kontroli ustalono, że inwentaryzacja zasobów informatycznych w Urzędzie Gminy Stare Kurowo nie jest prowadzona. Dane z ewidencji środków trwałych nie zawierają bardziej szczegółowych danych odnośnie konfiguracji sprzętowej oraz zainstalowanego oprogramowania.

4.4. Zarządzanie uprawnieniami.

Zgodnie z *§ 20 ust. 2 pkt 4 rozporządzenia*: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez m.in. podejmowanie działań zapewniających, 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 mających na celu zapewnienie bezpieczeństwa informacji.

Zgodnie z *§ 20 ust. 2 pkt 5 rozporządzenia*: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez m.in. zapewnienie bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4.

W trakcie kontroli stwierdzono, że ewidencja ujawnień jest prowadzona na zasadzie wystawiania pracownikom upoważnień do systemów informatycznych. Prowadzony jest także rejestr zbiorczy wystawionych upoważnień. Procedury odbierania i nadawania uprawnień są opracowane w Polityce Bezpieczeństwa Informacji.

Nieprawidłowość:

- stwierdzono jednak, że nie są one stosowane w rzeczywistości. Firma zewnętrzna obsługująca urząd w zakresie obsługi informatycznej nie zna tych procedur. Wnioskowanie o nadanie lub odebranie uprawnień przekazywane jest tylko w formie ustnej. W tej sytuacji niemożliwe jest prawidłowe zarządzanie uprawnieniami.

4.5. Szkolenia pracowników zaangażowanych w proces przetwarzania informacji.

Zgodnie z *§ 20 ust. 2 pkt 6 rozporządzenia*: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez m.in. zapewnienie szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:

a) zagrożenia bezpieczeństwa informacji,

b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,

c) stosowanie środków zapewniających bezpieczeństwo informacji w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich.

Urząd Gminy Stare Kurowo przeprowadził szkolenia z zakresu bezpieczeństwa informacji na etapie wdrażania polityki bezpieczeństwa informacji. W czerwcu 2018 r. przeprowadzono szkolenie dla wszystkich pracowników potwierdzone listami obecności. Z uwagi na incydenty stwierdzone podczas kontroli warto rozważyć pogłębienie szkoleń pracowników w tej tematyce oraz przeszkolenie pracowników firmy zewnętrznej obsługującej informatycznie urząd.

4.6. Praca na odległość i mobilne przetwarzanie danych.

Zgodnie z *§ 20 ust. 2 pkt 8 rozporządzenia*: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez m.in. ustanowienie podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość.

Urządzenia mobilne w Urzędzie Gminy Stare Kurowo nie są wynoszone poza siedzibę Urzędu. Poza pocztą elektroniczną nie ma zdalnego dostępu do zasobów Urzędu Gminy Stare Kurowo.

Nieprawidłowość:

- urządzenia mobilne nie są szyfrowane (pomimo zapisów w Polityce Bezpieczeństwa Informacji).

4.7. Serwis sprzętu informatycznego i oprogramowania.

Wg § 20 ust. 2 pkt 10 rozporządzenia: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez, m.in. zawieranie w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.

Urząd Gminy Stare Kurowo posiada umowę w zakresie obsługi informatycznej z firmą zewnętrzną.

Nieprawidłowość:

- Firma zewnętrzna w zakresie umowy nie posiada żadnych zapisów związanych z powierzeniem przetwarzania danych osobowych.

4.8. Procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji.

Zgodnie z *§ 20 ust. 2 pkt 13 rozporządzenia*: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez m.in. bezzwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.

Podczas kontroli pracownicy Urzędu Gminy wyjaśnili, że incydenty prawie nie występują. Rejestr incydentów nie zawiera żadnych wpisów.

Nieprawidłowość:

- w wyniku działań kontrolnych ujawniono co najmniej kilka incydentów. Pracownicy pomimo, że w polityce bezpieczeństwa informacji jest zdefiniowane pojęcie incydentu oraz występuje protokół obsługi incydentu, nie wiedzą jak mają się zachować w przypadku jego wystąpienia.

Zarządzanie incydentami jest bardzo ważnym aspektem systemu zarządzania bezpieczeństwem informacji. Jest to podstawowe narzędzie przy badaniu podatności systemów informatycznych. Brak zarejestrowanych incydentów świadczy o braku monitorowania systemów w kontekście występowania incydentów, a także o niewystarczającej wiedzy pracowników na temat definicji i sposobu zgłaszania incydentu.

4.9. Audyt wewnętrzny w zakresie bezpieczeństwa informacji.

Zgodnie z *§ 20 ust. 2 pkt 14 rozporządzenia*: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez m.in. zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

Dokumentacja polityki bezpieczeństwa informacji powstała w 2018 r. Można przyjąć, że analiza wdrożeniowa spełniła wymogi audytu bezpieczeństwa na ten rok.

4.10. Kopie zapasowe.

Zgodnie z *§ 20 ust. 2 pkt 12 lit. B rozporządzenia*: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez, m.in. minimalizowanie ryzyka utraty informacji w wyniku awarii.

Formalne procedury zarządzania bezpieczeństwem informacji są opisane w Polityce Bezpieczeństwa Informacji.

Nieprawidłowość:

- stwierdzono, iż kopie bezpieczeństwa są wykonywane codziennie ale na serwerach produkcyjnych oraz odbiegają one od zapisów w dokumentacji. Kopie zapasowe powinny być testowo odtwarzane, jednakże brak jest na to jednoznacznych dowodów.

4.11. Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych.

Zgodnie z *§ 15 ust. 1 rozporządzenia*: Systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne projektuje się, wdraża oraz eksploatuje z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności przenoszalności i pielęgnowalności, przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk.

Nieprawidłowość:

- Urząd Gminy Stare Kurowo nie posiada żadnych formalnych regulacji wewnętrznych dotyczących projektowania, wdrażania, wprowadzania zmian i monitorowania systemów informatycznych.

4.12. Zabezpieczenia techniczno-organizacyjne informacji.

Zgodnie z *§ 20 ust. 2 rozporządzenia*: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez, m.in.:

pkt 7: zapewnienie ochrony przetwarzania informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:

a) monitorowanie dostępu do informacji;

b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,

c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji,

pkt 9: zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie,

pkt 11 rozporządzenia: ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji środków przetwarzania informacji, w tym urządzeń mobilnych.

W Urzędzie Gminy Stare Kurowo istnieją zabezpieczenia fizyczne minimalizujące wystąpienie ryzyka kradzieży informacji i środków przetwarzania informacji.

Nieprawidłowości:

- dostęp do pomieszczenia serwerowni jest ograniczony tylko dla zewnętrznych klientów. Brakuje wykazu osób uprawnionych do wejścia. W rzeczywistości pracownicy korzystają z tego pomieszczenia z uwagi na umieszczenie tam urządzenia ksero. Na zapleczu serwerowni zlokalizowane jest pomieszczenie gospodarcze wykorzystywane przez pracownika zajmującego się sprzątaniem pomieszczeń. Przebywanie osób nieuprawnionych nie jest nadzorowane. Do stacji komputerowych pracowników założone są loginy i hasła dostępu, ale brakuje mechanizmu wymuszenia zmiany haseł. Dotyczy to także dostępu do poczty elektronicznej.

4.13. Zabezpieczenia techniczno-organizacyjne systemów informatycznych

Wg *§ 20 ust. 2 pkt 12 rozporządzenia***:** Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez, m.in. zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:

a) dbałości o aktualizację oprogramowania;

b) minimalizowaniu ryzyka utraty informacji w wyniku awarii;

c) ochronie przed błędami, utratą, nieuprawnioną modyfikacją;

d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa;

e) zapewnieniu bezpieczeństwa plików systemowych;

f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych;

g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa;

h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa.

Wg § 20 ust. 4 rozporządzenia: Niezależnie od zapewnienia działań, o których mowa w ust. 2, w przypadkach uzasadnionych analizą ryzyka w systemach teleinformatycznych podmiotów realizujących zadania publiczne należy ustanowić dodatkowe zabezpieczenia.

Na wszystkich komputerach w Urzędzie Gminy jest zainstalowane oprogramowanie antywirusowe.

Nieprawidłowość:

- w czasie kontroli stacje robocze oraz serwery nie posiadały bieżących aktualizacji systemowych, a oprogramowanie antywirusowe nie miało bieżących definicji wirusów.

Poświadczenia administracyjne do serwerów i systemów, znane są firmie zewnętrznej i przechowywane u sekretarza gminy.

4.14. Rozliczalność działań w systemach informatycznych.

Zgodnie z *§ 21 ust 2 rozporządzenia*: W dziennikach systemów odnotowuje się obligatoryjnie działania użytkowników lub obiektów systemowych polegające na dostępie do:

1) systemu z uprawnieniami administracyjnymi;

2) konfiguracji systemu, w tym konfiguracji zabezpieczeń;

3) przetwarzanych w systemach danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa.

Zgodnie z *§ 21 ust. 3 rozporządzenia*: W zakresie wynikającym z analizy ryzyka poza informacjami wymienionymi w *§ 21 ust. 2 rozporządzenia KRI* są odnotowywane działania użytkowników lub obiektów systemowych, a także inne zdarzenia związane z eksploatacją systemu w postaci:

1) działań użytkowników nieposiadających uprawnień administracyjnych,

2) zdarzeń systemowych nieposiadających krytycznego znaczenia dla funkcjonowania systemu,

3) zdarzeń i parametrów środowiska, w którym eksploatowany jest system teleinformatyczny - w zakresie wynikającym z analizy ryzyka.

Zgodnie z *§ 21 ust. 4 rozporządzenia*: informacje w dziennikach systemów przechowywane są od dnia ich zapisu, przez okres wskazany w przepisach odrębnych, a w przypadku braku przepisów odrębnych przez dwa lata.

Wszystkie systemy informatyczne stosowane w Urzędzie Gminy posiadają logi systemowe.

Nieprawidłowość:

- brak kopii zapewniających możliwość ich przechowywania przez okres minimum 2 lat. Stwierdzono także, iż niektóre z nich ulegają nadpisaniu.

5. **Zapewnienie dostępności informacji zawartych na stronach internetowych urzędów dla osób niepełnosprawnych.**

Zgodnie z *§ 19 rozporządzenia*: W systemie teleinformatycznym podmiotu realizującego zadania publiczne służące prezentacji zasobów informacji należy zapewnić spełnienie przez ten system wymagań Web Content Accessibility Guidelines (WCAG 2.0), z uwzględnieniem poziomu AA, określonych w załączniku nr 4 do rozporządzenia.

W toku kontroli dokonano weryfikacji zgodności strony internetowej Urzędu oraz BIP Urzędu ze standardem WCAG 2.0 poprzez wykorzystanie narzędzi dostępnych na stronie internetowej https://validator.w3.org. Strona BIP jest zgodna ze standardem WCAG 2.0.

Nieprawidłowość:

- strona Urzędu Gminy zawiera szereg błędów związanych z kodowaniem i brakiem odpowiedniej formy prezentacji strony (CSS). Brakuje także elementów ułatwiających odbiór strony dla osób niepełnosprawnych (brak zmiany kontrastu i wielkości czcionki).

Przedstawiając powyższe ustalenia, zalecam:

1. wydawać decyzje administracyjne w terminach wynikających z kpa, a w razie przedłużenia terminu poinformować stronę postępowania o tym fakcie,
2. umieszczać w decyzjach administracyjnych uzasadnienie prawne zgodnie z wymogami kpa,

3. dokonać kompleksowego wdrożenia Systemu zarządzania bezpieczeństwem informacji, uwzględniając wszystkie informacje przetwarzane oraz przechowywane w Urzędzie,
4. przeprowadzać okresową aktualizację dokumentacji SZBI, w tym „Polityki Bezpieczeństwa", „Instrukcji zarządzania systemem informatycznym" oraz innych dokumentów stanowiących SZBI zgodnie z wymogami wskazanymi w § 20 ust. 2 pkt 1 rozporządzenia KRI,
5. badać podatności systemów informatycznych np. na postawie występujących incydentów i określać zagrożenia oraz przeprowadzać okresowe udokumentowane analizy ryzyka i przedstawiać sposób postępowania z ryzykiem,
6. wykonywać audyty wewnętrzne przynajmniej raz w roku,
7. wdrożyć procedurę zarządzania uprawnieniami,
8. właściwie zarządzać urządzeniami mobilnymi podczas pracy poza siedzibą urzędu,
9. uaktualnić ewidencję sprzętu i oprogramowania oraz dokumentować inwentaryzację zasobów teleinformatycznych,
10. prowadzić rejestr incydentów, opracować procedurę zgłaszania incydentów oraz przeszkolić pracowników w tym zakresie,
11. stworzyć procedurę wykonywania kopii zapasowych, testować i dokumentować okresowe odtwarzanie danych, dostosować rozwiązania teleinformatyczne dla użytkowników przy wykonywaniu kopii zapasowych stacji roboczych oraz opracować plany zapewnienia ciągłości działania,
12. wdrożyć rozwiązania teleinformatyczne zapewniające możliwość przechowywania logów systemowych przez okres minimum 2 lat,
13. wdrożyć regulacje wewnętrzne dotyczących projektowania, wdrażania, wprowadzania zmian i monitorowania systemów informatycznych,
14. wdrożyć procedury umożliwiające zarządzanie usługami realizowanymi przez systemy teleinformatyczne, stosować szczegółowe opisy usług na stronach internetowych urzędu.

Na podstawie art. 49 ustawy proszę o przekazanie w terminie 30 dni od daty otrzymania niniejszego wystąpienia pokontrolnego, informacji o sposobie wykonania zaleceń, wykorzystaniu wniosków lub przyczynach ich niewykorzystania albo o innym sposobie usunięcia stwierdzonych nieprawidłowości.

WOJEWODA LUBUSKI

Władysław Dajczak