Warszawa, 23 maja 2019 r.

WOJEWODA MAZOWIECKI

WK-I.431.4.7.2019

Pan
Krzysztof Kapusta
Starosta Nowodworski

Starostwo Powiatowe
w Nowym Dworze Mazowieckim
ul. Ignacego Paderewskiego 1B
05-100 Nowy Dwór Mazowiecki

WYSTĄPIENIE POKONTROLNE

Na podstawie art. 28 ust. 1 pkt 2 ustawy o wojewodzie i administracji rządowej w województwie[1], art. 6 ust. 4 pkt 3 ustawy o kontroli w administracji rządowej[2], art. 25 ust. 1 pkt 3 lit. a ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne[3], Katarzyna Możdżyńska – starszy inspektor wojewódzki, Andrzej Nieszporek – inspektor wojewódzki, Renata Syska – I zastępca kierownika w Oddziale Kontroli Finansowej i Jednostek Samorządu Terytorialnego Wydziału Kontroli, a także Marek Lenarcik – kierownik Oddziału Administrowania Systemami i Zarządzania Sprzętem Informatycznym w Biurze Informatyki i Łukasz Plaskot – starszy inspektor wojewódzki w Oddziale Eksploatacji Systemów Informatycznych i Infrastruktury Serwerowej w Biurze Informatyki, przeprowadzili w dniach od 4 do 22 marca 2019 r. kontrolę w Starostwie Powiatowym w Nowym Dworze Mazowieckim, z siedzibą przy ul. Ignacego Paderewskiego 1B.

Nawiązując do projektu wystąpienia pokontrolnego z 25 kwietnia 2019 r., do którego nie wniesiono zastrzeżeń, przekazuję Panu Staroście wystąpienie pokontrolne.

---

[1] Ustawa z dnia 23 stycznia 2009 r. o wojewodzie i administracji rządowej w województwie (Dz. U. z 2017 r. poz. 2234, ze zm.).
[2] Ustawa z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz. U. Nr 185, poz. 1092, ze zm.).
[3] Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2019 r. poz. 700, ze zm.).

Przedmiot kontroli obejmował realizację zadań w zakresie działania systemów teleinformatycznych używanych do realizacji zadań publicznych albo realizacji obowiązków wynikających z art. 13 ust. 2 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne pod względem zgodności z minimalnymi wymaganiami dla systemów teleinformatycznych lub minimalnymi wymaganiami dla rejestrów publicznych i wymiany informacji w postaci elektronicznej[4].

Kontrolą objęto okres od 1 stycznia 2017 r. do 4 marca 2019 r.

I. Działanie systemów teleinformatycznych używanych do realizacji zadań zleconych z zakresu administracji rządowej albo realizacji obowiązków wynikających z art. 13 ust. 2 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne pod względem zgodności z minimalnymi wymaganiami dla systemów teleinformatycznych lub minimalnymi wymaganiami dla rejestrów publicznych i wymiany informacji w postaci elektronicznej

Ocenie poddano trzy główne obszary kontroli, tj. wymianę informacji w postaci elektronicznej, w tym współpracę z innymi systemami informatycznymi oraz wspomaganie usług drogą elektroniczną, zarządzanie bezpieczeństwem informacji w systemach teleinformatycznych oraz zapewnienie dostępności informacji zawartych na stronach internetowych urzędu dla osób niepełnosprawnych.

W jednostce prowadzono rejestry publiczne, o których mowa w art. 14 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne. W prowadzonych rejestrach publicznych wyróżniono typy obiektów oraz ustalono strukturę ich identyfikatorów, zgodnie z wymogami § 10 ust. 1, 2 i 3 rozporządzenia w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[5] (dalej rozporządzenie w sprawie KRI).

Kontroli poddano system teleinformatyczny [redacted] używany w Starostwie do realizacji zadań publicznych.

[4] Zgodnie z art. 25 ust. 3 przedmiotowej ustawy kontrola dotyczyła wyłącznie systemów teleinformatycznych oraz rejestrów publicznych, które są używane do realizacji zadań zleconych z zakresu administracji rządowej.

[5] Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247, ze zm.).

I.A. Wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami teleinformatycznymi oraz wspomaganie usług drogą elektroniczną

Starostwo Powiatowe w Nowym Dworze Mazowieckim udostępnia elektroniczną skrzynkę podawczą (dalej ESP). Starostwo w systemie [redacted] umożliwia udostępnianie danych w formacie gml, tj. określonym w załączniku nr 2 i 3 rozporządzenia w sprawie KRI.

Ustalono, że Starostwo nie przekazywało wzorów dokumentów elektronicznych do Centralnego Repozytorium Wzorów Dokumentów Elektronicznych[6].

Stwierdzono, że system [redacted] powiązany jest z platformą ePUAP. Wymiana danych odbywa się za pomocą platformy ePUAP, która narzuca protokoły komunikacyjne i szyfrujące. Współpraca pomiędzy systemami jest możliwa dzięki wyposażaniu Starostwa w odpowiedni sprzęt oraz oprogramowanie umożliwiające wymianę danych między systemami, zgodnie z § 16 ust. 1 rozporządzenia w sprawie KRI. Kodowanie znaków w wysyłanych z systemów lub odbieranych przez te systemy dokumentach odbywa się zgodnie z normą ISO/IEC 10646, co jest zgodne z § 17 ust. 1 ww. rozporządzenia. W Starostwie nie udostępnia się zasobów zgromadzonych w systemie [redacted] przez usługi sieciowe, więc nie opisywano usług sieciowych za pomocą języka WSDL[7].

Zgodnie z zarządzeniem Nr 7/11 Starosty Nowodworskiego z dnia 24 stycznia 2011 roku w sprawie wyboru systemu wykonywania czynności kancelaryjnych, ustalono, że podstawowym sposobem dokumentowania przebiegu załatwiania i rozstrzygania spraw jest system tradycyjny. Zarządzeniem nr 33/15 Starosty Nowodworskiego z dnia 31 sierpnia 2015 r. w sprawie stosowania w Starostwie Powiatowym w Nowym Dworze Mazowieckim Systemu [redacted] ustanowiono, że wprowadza się System [redacted], wdrożony w ramach [redacted] jako oprogramowanie wspomagające wykonywanie czynności kancelaryjnych w systemie tradycyjnym.

W wyniku kontroli stwierdzono następujące nieprawidłowości:

1. Udostępnienie ESP niezgodnie z wymogami art. 16 ust. 1a ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz nie zamieszczenie na stronie Biuletynu Informacji Publicznej (dalej BIP) informacji określonych w § 3 ust. 1 rozporządzenia w sprawie

[6] Zgodnie z wyjaśnieniami Starosty Nowodworskiego z 12 marca 2019 r. cyt.: *„Organ nie sporządzał własnych wzorów dokumentów, korzysta ze wzorów udostępnionych przez Serwis ePUAP – Ministerstwo Cyfryzacji – Portal gov.pl”.*

[7] Web Services Description Language (dalej WSDL). Ustalenie zostało zawarte w notatce z przeprowadzonych w dniach 13, 19, 21 i 22 marca 2019 r. rozmów z informatykiem.

[8] [redacted]

sporządzania i doręczania dokumentów elektronicznych oraz udostępnia formularzy, wzorów i kopii dokumentów elektronicznych[9], zgodnie z którym cyt.: „(*…) udostępnionym adresie elektronicznej skrzynki podawczej, podanym w formie identyfikatora URI; maksymalnym rozmiarze dokumentu elektronicznego wraz z załącznikami, wyrażonym w megabajtach, możliwym do doręczenia za pomocą elektronicznej skrzynki podawczej, nie mniejszym niż 5 megabajtów; zakresach użytkowych dokumentów elektronicznych (…); rodzajach informatycznych nośników danych na których może zostać im doręczony dokument elektroniczny; rodzajach informatycznych nośników danych, na których może zostać zapisane urzędowe poświadczenie odbioru; innych wymagań określonych przepisami prawa dotyczących doręczania dokumentów elektronicznych”.*

2. Niezamieszczenie na stronie BIP odesłania do opisu usług załatwianych drogą elektroniczną[10], co jest niezgodnie z § 5 ust. 2 pkt 1 i 4 rozporządzenia w sprawie KRI, zgodnie z którym cyt.: *„(…) 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 udostępnianie w Biuletynie informacji Publicznej (…) opisów procedur obowiązujących przy załatwianiu spraw z zakresu jego właściwości drogą elektroniczną”.*
3. Brak procedur dotyczących dostarczania i zarządzania usługami na deklarowanym poziomie dostępności, co jest niezgodne z § 15 ust. 2 ww. rozporządzenia, zgodnie z którym cyt.: *„Zarządzanie usługami realizowanymi przez systemy teleinformatyczne ma na celu dostarczanie tych usług na deklarowanym poziomie dostępności i odbywa się w oparciu o udokumentowane procedury”.*

Przedstawiając powyższe informuję, że realizację zadań dotyczących wymiany informacji w postaci elektronicznej, w tym współpracy z innymi systemami oraz wspomaganie usług drogą elektroniczną **ocenia się negatywnie.**

Ustalenia kontroli wykazały, że udostępniona została ESP, w jednostce zarządzano obiegiem dokumentacji, a funkcjonujące w Starostwie systemy współpracowały z innymi systemami. Mając natomiast na uwadze: udostępnienie ESP niezgodnie z zapisami ustawy

[9] Rozporządzenie Prezesa Rady Ministrów z dnia 14 września 2011 r. w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych (Dz. U. z 2018 r. poz. 180).

[10] Zgodnie z wyjaśnieniami Starosty Nowodworskiego z 12 marca 2019 r. cyt.: *„Starostwo Powiatowe w Nowym Dworze Mazowieckim świadczy usługi w formie elektronicznej poprzez ePUAP (…) oraz za pośrednictwem strony powiatu nowodworskiego (…)”.*

o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niezamieszczenie na BIP informacji dotyczących jej funkcjonowania, niezamieszczenie na stronie BIP odesłania do opisu usług, a także brak procedur dotyczących dostarczania i zarządzania usługami na deklarowanym poziomie dostępności, uzasadnione jest sformułowanie oceny negatywnej.

I.B. Systemy zarządzania bezpieczeństwem informacji w systemach teleinformatycznych

Zgodnie z § 20 ust. 1 rozporządzenia w sprawie KRI, w okresie objętym kontrolą w jednostce obowiązywały *Polityki Bezpieczeństwa Informacji* wprowadzone Zarządzeniami Starosty Nowodworskiego, odpowiednio: nr 18/2016 z dnia 11 kwietnia 2016 r.[11], nr 32/2017 z dnia 24 lipca 2017 r.[12], nr 13/2018 z dnia 21 maja 2018 r.[13].

Obowiązujące w okresie kontrolowanym *Polityki Bezpieczeństwa Informacji* opisują sposoby nadawania/odbierania uprawnień użytkownikom, określają sposoby pracy w systemie informatycznym, procedury zarządzania oraz czynności mające wpływ na zapewnienie bezpieczeństwa systemu informatycznego.

W toku kontroli potwierdzono zaangażowanie kierownictwa jednostki w proces ustanawiania i funkcjonowania systemu bezpieczeństwa informacji m.in. poprzez wprowadzenie *Polityk Bezpieczeństwa Informacji*, *Procedur corocznej samooceny kontroli zarządczej*, zwoływanie narad i spotkań poświęconych m.in. tematyce dotyczącej bezpieczeństwa informacji, zmian

---

[11] *Polityka* opisuje zagadnienia takie jak:
- identyfikacja zasobów systemu informatycznego,
- środki techniczne i organizacyjne służące zapewnieniu poufności, integralności i rozliczalności przetwarzania danych,
- instrukcja zarzadzania systemem informatycznym służącym do przetwarzania danych osobowych,
- instrukcja zarzadzania systemem informatycznym służącym do przetwarzania danych osobowych w systemie Pojazd i Kierowca,
- instrukcja bezpieczeństwa użytkownika systemu informatycznego,
- wykaz budynków i pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe,
- wzór – upoważnienie do przetwarzania danych osobowych,
- wzór – ewidencja osób upoważnionych do przetwarzania danych osobowych,
- wzór – zobowiązanie do zachowania tajemnicy danych osobowych,
- wzór – raport stwierdzenia naruszenia bezpieczeństwa systemu informatycznego administratora danych.

[12] *Polityka* opisuje zagadnienia takie jak:
- identyfikację zasobów systemu informatycznego,
- środki techniczne i organizacyjne służące zapewnieniu poufności, integralności i rozliczalności przetwarzania danych,
- wzór – upoważnienie do przetwarzania danych osobowych,
- wzór – ewidencja osób upoważnionych do przetwarzania danych osobowych,
- wzór – zobowiązanie do zachowania tajemnicy danych osobowych.

[13] *Polityka* opisuje zagadnienia takie jak:
- informacje ogólne,
- osoby odpowiedzialne za ochronę danych osobowych,
- zasady przetwarzania danych osobowych.

Regulaminu organizacyjnego. Wszyscy pracownicy Starostwa zostali zapoznani z obowiązującymi w okresie kontrolowanym *Politykami Bezpieczeństwa Informacji* i zobowiązani do stosowania określonych w nich zasad.

Zgodnie z zapisem § 20 ust. 2 pkt 2 rozporządzenia w sprawie KRI w jednostce prowadzony jest Rejestr zasobów teleinformatycznych (baza konfiguracji CMDB) zawierający informacje o zmianach konfiguracji wszystkich aktywów informatycznych w wersji elektronicznej przy pomocy oprogramowania [redacted]

W Starostwie obowiązuje *Procedura oceny ryzyka bezpieczeństwa informacji* stanowiąca załącznik nr 5 do *Polityki Bezpieczeństwa Informacji w Starostwie Powiatowym w Nowym Dworze Mazowieckim,* wprowadzonej Zarządzeniem Starosty Nowodworskiego nr 32/2017 z 24 lipca 2017 r. Celem tej procedury jest oszacowanie ryzyka w oparciu o wskazane w niej kryteria. Ponadto ma ona zapewnić zidentyfikowanie ryzyk, udokumentowanie ich oraz cykliczne przeglądanie dokumentacji. Procedura obejmuje wszystkie wydziały Starostwa.

Pracownicy wykonujący zadania w badanym systemie teleinformatycznym uczestniczyli w procesie przetwarzania informacji w stopniu adekwatnym do przypisanych obowiązków, zgodnie z § 20 ust. 2 pkt 4 rozporządzenia w sprawie KRI.

W okresie objętym kontrolą nie wystąpiły przypadki projektowania i wdrażania systemów teleinformatycznych.

Stosownie do zapisów § 20 ust. 2 pkt 13 ww. rozporządzenia, w Starostwie obowiązywały zasady zgłaszania i postępowania z incydentami naruszenia bezpieczeństwa informacji, uregulowane w *Politykach Bezpieczeństwa Informacji* obowiązującymi w okresie kontrolowanym. Zgodnie z udzielonymi wyjaśnieniami w okresie kontrolowanym nie wystąpiły incydenty naruszenia bezpieczeństwa informacji [14].

W Starostwie stworzona jest procedura odnosząca się do tworzenia i przechowywania kopii zapasowych. Procedura opisana została w *Politykach Bezpieczeństwa Informacji* wprowadzonych zarządzeniem Starosty nr 18/2016 z dnia 11 kwietnia 2016 r. oraz nr 32/2017 z dnia 24 lipca 2017 r. i spełniała wymogi określone w § 20 ust. 2 pkt 12 lit. b rozporządzenia w sprawie KRI.

Regulacje wewnętrzne, w których ustalono zasady postępowania z informacjami w jednostce, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków

[14] W trakcie kontroli przedłożono do wglądu *„Rejestr incydentów bezpieczeństwa*" – brak zapisów w rejestrze w okresie kontrolowanym. Wzór rejestru zgodny jest z wzorem stanowiącym załącznik do *Polityki Bezpieczeństwa Informacji.*

przetwarzania informacji, w tym urządzeń oraz zasady dotyczące zapewnienia ochrony przetwarzanych informacji, zostały zawarte w *Politykach Bezpieczeństwa Informacji* obowiązujących w okresie kontrolowanym. W toku kontroli ustalono, że zgodnie z § 20 ust. 2 pkt 7, 9 i 12 ww. rozporządzenia, Starostwo zapewnia ochronę przetwarzanych informacji przed kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, a także zabezpieczenie informacji w sposób uniemożliwiający osobom nieuprawnionym jej ujawnienie, modyfikację, usunięcie lub zniszczenie, poprzez:

- stosowanie zabezpieczeń budynku i pomieszczeń, [redacted]
- nadawanie użytkownikom uprawnień do systemów [redacted]
- wymóg logowania się do systemu [redacted]
- ograniczenie uprawnień użytkowników na stacjach roboczych,
- automatyczną aktualizację oprogramowania systemów operacyjnych komputerów,
- aktualizację systemów operacyjnych serwerów,
- funkcjonowanie urządzeń brzegowych typu firewall,
- zabezpieczenie komputerów użytkowników aktualnym oprogramowaniem antywirusowym, automatycznie aktualizującym sygnatury wirusów,
- wyposażenie serwerów i urządzeń sieciowych w zasilanie awaryjne zabezpieczające system przed przepięciami i chwilowymi zanikami napięcia,
- ustanowienie regulacji dotyczących konserwacji, napraw i utylizacji sprzętu i oprogramowania.

[15] Kontrolującym przedłożone zostały umowy nr WAO.273.37.2016 z 23 grudnia 2016 r. oraz WAO.273.35.2018 z 28 grudnia 2018 r. w sprawie serwisu pogwarancyjnego i konserwacji, a także umowy nr WAO.273.35.2016 z 21 grudnia 2016 r. oraz WAO.273.36.2018 z 31 grudnia 2018 r. w sprawie monitorowania lokalnego systemu Alarmowego.

[16] [redacted]

[17] [redacted]

W wyniku kontroli stwierdzono następujące nieprawidłowości:

1. Nieprzeprowadzenie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji mimo obowiązku wynikającego z § 20 ust. 2 pkt 3 rozporządzenia w sprawie KRI, zgodnie z którym cyt.: *„Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań (…) przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji (…)”*.
2. Nieprzeprowadzenie w 2018 r. okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji. Działaniem takim naruszono dyspozycję § 20 ust. 2 pkt 14 ww. rozporządzenia, zgodnie z którym kierownictwo umożliwia realizację i egzekwowanie działań w zakresie cyt.: *„(…) zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji nie rzadziej niż raz na rok”*[18].
3. Niezapewnienie osobom zaangażowanym w proces przetwarzania informacji, szkoleń ze szczególnym uwzględnieniem zagadnień takich jak zagrożenia bezpieczeństwa informacji, skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna czy stosowanie środków zapewniających bezpieczeństwo informacji, czym naruszono wymogi § 20 ust. 2 pkt 6 rozporządzenia w sprawie KRI.
4. W umowach zawartych pomiędzy Starostwem a podmiotami zewnętrznymi[19], niezawarto zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji. Działaniem takim naruszono wymóg § 20 ust. 2 pkt 10 ww. rozporządzenia.

Ponadto w toku kontroli ustalono, że:

– nadawanie, zmiana i odbieranie uprawnień w [redacted] i systemie [redacted] odbywa się niezgodnie z zapisami *Polityk Bezpieczeństwa Informacji* obowiązującymi w okresie kontrolowanym. W jednostce brak jest dokumentów potwierdzających kiedy nadano, zmieniono lub odebrano ww. uprawnienia[20],

[18] Kontrolującym przedłożony został Raport z przeprowadzonego w 2017 r. audytu bezpieczeństwa informacji dla Starostwa Powiatowego w Nowym Dworze Mazowieckim.

[19] Dotyczy umów wdrażających stronę internetową Starostwa nr: N/0089.1/2015, N/0089/2016, N/0089/2017, N/0089/2018 i N/0089/2019 odpowiednio z 4 listopada 2015 r., 11 stycznia 2016 r., 10 stycznia 2017 r., 10 stycznia 2018 r. i 11 stycznia 2019 r., umów określających zasady udostępniania BIP nr: BIP/0056/2016, BIP/0056/2017, BIP/0056/2018 i BIP/0056/2019 odpowiednio z 11 stycznia 2016 r., 10 stycznia 2017 r., 9 stycznia 2018 r. i 11 stycznia 2019 r., umów dotyczących pakietu kont e-mail i świadczenia poczty elektronicznej nr: U/0024/2017, U/0024/2018, U/0024/2019 odpowiednio z 10 stycznia 2017 r., 9 stycznia 2018 r. oraz z 11 stycznia 2019 r.

[20] Zgodnie z protokołem z przeprowadzonych w dniach 13, 19, 21 i 22 marca 2019 r. rozmów z Administratorem Systemu [redacted]

- nie było wykonywane przywrócenie systemów z kopii zapasowych, jak również nie były wykonywane okresowe testy odtworzeniowe[21],
- nie zapewniono bezpieczeństwa kopiom baz danych – zminimalizowania ryzyka utraty informacji, np. w wyniku awarii. [redacted][22],
- w jednostce nie ustanowiono podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość[23], czym naruszono zapis § 20 ust. 2 pkt 8 rozporządzenia w sprawie KRI,
- informacje w dziennikach systemów przechowywane są przez okres krótszy[24] niż wskazany w § 21 powyższego rozporządzenia. Kontrolerom nie przedstawiono dowodów na fakt zapisywania logów przez system [redacted] ani też z jakiego okresu są one zapisywane i jakiego zakresu dotyczą[25].

Przedstawiając powyższe informuję, że realizację zadań w zakresie działania systemu zarządzania bezpieczeństwem informacji w systemach teleinformatycznych **ocenia się negatywnie.**

Ustalenia kontroli wykazały, że w Starostwie opracowano dokumentację systemu zarządzania bezpieczeństwem informacji, z którą pracownicy zostali zapoznani, zapewniono aktualizację inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji, a osoby zaangażowane w proces przetwarzania informacji posiadały stosowne uprawnienia. Ponadto systemy teleinformatyczne funkcjonujące w Starostwie posiadały wymagane zabezpieczenia techniczno-organizacyjne. Mając natomiast na uwadze: nieprzeprowadzenie okresowej analizy ryzyka utraty integralności, dostępności lub poufności informacji, nieprzeprowadzenie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, niezapewnienia szkolenia osobom zaangażowanym w proces przetwarzania informacji,

[21] Zgodnie z protokołem z przeprowadzonych w dniach 13, 19, 21 i 22 marca 2019 r. rozmów z informatykiem i z Administratorem Systemu [redacted]

[22] Zgodnie z protokołem z przeprowadzonych w dniach 13, 19, 21 i 22 marca 2019 r. rozmów z informatykiem i z Administratorem Systemu [redacted]

[23] Zgodnie z wyjaśnieniami Starosty Nowodworskiego z 12 marca 2019 r. cyt.: *"W okresie objętym kontrolą nie zaistniały przypadki korzystania z przenośnych nośników danych oraz laptopów i innych urządzeń mobilnych poza budynkiem Starostwa".*

[24] [redacted]

[25] Zgodnie z protokołem z przeprowadzonych w dniach 13, 19, 21 i 22 marca 2019 r. rozmów z informatykiem.

niezawarcie w umowach serwisowych zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji oraz inne opisane powyższej uchybienia uzasadnione jest sformułowanie oceny negatywnej.

I.C. Zapewnienie dostępności informacji zawartych na stronach internetowych jednostki dla osób niepełnosprawnych

Strony internetowe Starostwa działające pod adresami www.nowodworski.pl oraz www.bip.nowodworski.pl poddano weryfikacji zgodności ze standardem WCAG 2.0 za pomocą walidatorów http://validator.w3.org oraz http://jigsaw.w3.org/css-validator/. Po weryfikacji ww. stron stwierdzono spełnienie wymagań WCAG 2.0 określonych w załączniku nr 4 rozporządzenia w sprawie KRI. W wyniku kontroli stwierdzono, że dostępna strona internetowa i strona BIP jednostki zawierają rozwiązania techniczne umożliwiające osobom niepełnosprawnym zapoznanie się z treścią informacji, czym spełniono wymogi określone w § 19 ww. rozporządzenia.

Przedstawiając powyższe informuję, że realizację zadania w przedmiocie zapewnienia dostępności informacji zawartych na stronach internetowych urzędu dla osób niepełnosprawnych ocenia się **pozytywnie**.

Ustalenia kontroli wykazały, że w Starostwie zapewniono dostępność informacji zawartych na stronie internetowej oraz stronie BIP urzędu dla osób niepełnosprawnych. Mając na uwadze powyższe uzasadnionym jest sformułowanie oceny pozytywnej.

Przedstawiając powyższe ustalenia, zobowiązuję Pana Starostę do podjęcia działań w celu wyeliminowania stwierdzonych nieprawidłowości, a w szczególności do:

1. Udostępnienia ESP zgodnie z wymogami art. 16 ust. 1a ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz zamieszczenia na stronie BIP Starostwa informacji określonych w § 3 ust. 1 rozporządzenia w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych.
2. Zamieszczenia na stronie BIP Starostwa odesłania do opisu usług załatwianych drogą elektroniczną, zgodnie z § 5 ust. 2 pkt 1 i 4 rozporządzenia w sprawie KRI.
3. Stworzenia procedur dotyczących dostarczania i zarządzania usługami na deklarowanym poziomie dostępności, zgodnie z § 15 ust. 2 ww. rozporządzenia.

4. Przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, zgodnie z obowiązkiem wynikającym z § 20 ust. 2 pkt 3 rozporządzenia w sprawie KRI.
5. Przeprowadzania okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, zgodnie z dyspozycją § 20 ust. 2 pkt 14 ww. rozporządzenia.
6. Zapewnienia osobom zaangażowanym w proces przetwarzania informacji, szkoleń ze szczególnym uwzględnieniem zagadnień takich jak zagrożenia bezpieczeństwa informacji, skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna czy stosowanie środków zapewniających bezpieczeństwo informacji, zgodnie z wymogami § 20 ust. 2 pkt 6 rozporządzenia w sprawie KRI.
7. Zawierania w umowach zawartych pomiędzy Starostwem a podmiotami zewnętrznymi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji, zgodnie z wymogiem określonym w § 20 ust. 2 pkt 10 ww. rozporządzenia.

Ponadto wskazuję na konieczność:

- nadawania, zmiany i odbierania uprawnień [redacted] i systemie [redacted] zgodnie z zapisami obowiązujących w Starostwie *Polityk Bezpieczeństwa Informacji*,
- wykonywania przywróceń systemów z kopii zapasowych oraz wykonywania okresowych testów odtworzeniowych,
- zapewnienia bezpieczeństwa kopiom baz danych – zminimalizowania ryzyka utraty informacji, poprzez [redacted]
- ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracę na odległość, zgodnie z zapisem § 20 ust. 2 pkt 8 rozporządzenia w sprawie KRI,
- przechowywania informacji w dziennikach systemów przez okres wskazany w § 21 ww. rozporządzenia.

Przedstawiając powyższe informuję, że zgodnie z art. 48 ustawy o kontroli w administracji rządowej od wystąpienia pokontrolnego nie przysługują środki odwoławcze oraz zobowiązuję Pana Starostę na podstawie art. 49 ww. ustawy do przekazania, w terminie 14 dni od daty otrzymania niniejszego wystąpienia pokontrolnego, pisemnej informacji

o sposobie wykonania zaleceń, wykorzystaniu wniosków pokontrolnych lub przyczynach ich niewykorzystania albo o innym sposobie usunięcia stwierdzonych nieprawidłowości.

z up. WOJEWODY MAZOWIECKIEGO

Bogusław Krupa
Zastępca Dyrektora
Wydziału Kontroli