NAJWYŻSZA IZBA KONTROLI
Delegatura we Wrocławiu

LWR.410.015.03.2018
P/18/006

WYSTĄPIENIE POKONTROLNE

NAJWYŻSZA IZBA KONTROLI
Delegatura we Wrocławiu
ul. Marszałka J. Piłsudskiego 15/17, 50-044 Wrocław
T +48 71 711 83 00, F +48 71 711 83 50
lwr@nik.gov.pl

I. Dane identyfikacyjne kontroli

Numer i tytuł kontroli

P/18/006 – Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego.

Jednostka przeprowadzająca kontrolę

Najwyższa Izba Kontroli
Delegatura we Wrocławiu

Kontroler

Cezary Mazik – specjalista kontroli państwowej, upoważnienie do kontroli nr LWR/157/2018 z dnia 27 czerwca 2018 r.

(dowód: akta kontroli str. 1)

Jednostka kontrolowana

Starostwo Powiatowe w Górze, ul. A. Mickiewicza 1, 56-200 Góra (dalej: „Starostwo").

Kierownik jednostki kontrolowanej

Pan Piotr Tomasz Wołowicz – Starosta Górowski[1].

(dowód: akta kontroli str. 2-4)

II. Ocena kontrolowanej działalności

Ocena ogólna

Najwyższa Izba Kontroli ocenia negatywnie działalność kontrolowanej jednostki w zakresie zarządzania bezpieczeństwem informacji.

Uzasadnienie oceny ogólnej

Podstawą oceny ogólnej były negatywne oceny cząstkowe dotyczące wszystkich trzech badanych obszarów, tj. organizacji bezpieczeństwa informacji, wdrożonych i wykorzystywanych rozwiązań organizacyjnych i technicznych zapewniających bezpieczeństwo informacji oraz działań podejmowanych w celu zapobiegania incydentom bezpieczeństwa informacji.

Stwierdzone w toku kontroli nieprawidłowości dotyczyły: **[1]** nieopracowania i niewdrożenia systemu zarządzania bezpieczeństwem informacji, w szczególności polityki bezpieczeństwa informacji (dalej: „PBI"), wymaganego przepisem § 20 ust. 3 w związku z ust. 1 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*[2] (dalej: *„rozporządzenie KRI"*); **[2]** nieprowadzenia inwentaryzacji zasobów informatycznych, która zawierałaby pełne i aktualne informacje w zakresie posiadanego sprzętu informatycznego oraz jego konfiguracji, co było niezgodne z § 20 ust. 2 pkt 2 *rozporządzenia KRI*; **[3]** niewskazania po dniu 17 października 2017 r. Administratora Bezpieczeństwa Informacji (dalej: „ABI"), którego zadaniem winien być – zgodnie z § 2 Zarządzenia Nr 23/12 Starosty Górowskiego z dnia 12 grudnia 2012 r. *w sprawie ochrony danych osobowych przetwarzanych w Starostwie Powiatowym* – nadzór nad wprowadzaniem PBI i przestrzeganiem zasad w niej zawartych, co było działaniem nierzetelnym; **[4]** przypadków braku ograniczenia i właściwego nadzorowania przydzielania oraz wykorzystywania prawa uprzywilejowanego dostępu do systemów informatycznych, co stanowiło naruszenie § 20 ust. 2 pkt 4 *rozporządzenia KRI;* **[5]** stosowania haseł dostępowych użytkowników do systemu informatycznego niezapewniających właściwej ochrony informacji przed nieuprawnionym dostępem, co naruszało § 20 ust. 2 pkt 7 *rozporządzenia KRI*;

[1] Od dnia 9 grudnia 2010 r.
[2] Dz. U. z 2017 r. poz. 2247.

[6] braku formalnej procedury nadawania i odbierania uprawnień pracownikom Starostwa w dostępie do systemów informatycznych, co powodowało naruszenie § 20 ust. 2 pkt 4 w związku z ust. 3 *rozporządzenia KRI*; **[7]** nieprawidłowego zabezpieczenia serwerowni Starostwa, co stanowiło naruszenie § 20 ust. 2 pkt 9 *rozporządzenia KRI*; **[8]** sporządzania i przechowywania kopii zapasowych serwerów baz danych w sposób niezapewniający wystarczającej ochrony przed utratą informacji, co było niezgodne z § 20 ust. 2 pkt 12 lit. b i e *rozporządzenia KRI;* **[9]** braku zapisów zobowiązujących wykonawcę do zachowania tajemnicy informacji w zawartej umowie na dostawę i serwis zestawów komputerowych, co było niezgodne z postanowieniami § 20 ust. 2 pkt 10 *rozporządzenia KRI;* **[10]** niestosowania szyfrowania dysków twardych komputerów przenośnych, co prowadziło do naruszenia postanowień § 20 ust. 2 pkt 9 *rozporządzenia KRI;* **[11]** nieprowadzenia okresowych analiz ryzyka utraty integralności, poufności lub dostępności informacji, co było niezgodne z § 20 ust. 2 pkt 3 *rozporządzenia KRI*; **[12]** nieprzeprowadzania audytów wewnętrznych w zakresie bezpieczeństwa informacji, co było sprzeczne z § 20 ust. 2 pkt 14 *rozporządzenia KRI*; **[13]** braku szkoleń osób zaangażowanych w proces przetwarzania informacji, ze szczególnym uwzględnieniem zagrożenia bezpieczeństwa informacji, skutków naruszenia tych zasad, w tym odpowiedzialności prawnej za te czyny, oraz stosowania środków zapewniających bezpieczeństwo informacji, co stanowiło naruszenie § 20 ust. 2 pkt 6 *rozporządzenia KRI*.

Ponadto Najwyższa Izba Kontroli sformułowała uwagi dotyczące: **[1]** udostępnienia szczegółów technicznych stosowanych procedur i zabezpieczeń wszystkim pracownikom Starostwa; **[2]** braku możliwości zarządzania z poziomu aplikacji ochroną przetwarzanych informacji przed nieautoryzowanym dostępem poprzez ustanawianie zasad złożoności hasła dostępowego i okresu, po jakim hasło użytkownika powinno być zmienione, co stwierdzono w przypadku trzech poddanym oględzinom systemów informatycznych; **[3]** użytkowania przez Starostwo 20,4% komputerów i laptopów posiadających niewspierany już przez producenta system informatyczny.

Jednocześnie NIK ocenia pozytywnie działania Starostwa podejmowane w związku z wejściem w życie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. *w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)*[3] (dalej: „*RODO*").

III. Opis ustalonego stanu faktycznego

1. Organizacja bezpieczeństwa informacji

Opis stanu faktycznego

W Starostwie nie było opracowanego i wdrożonego systemu zarządzania bezpieczeństwem informacji, o którym mowa w § 20 ust. 1 w zw. z ust. 3 *rozporządzenia KRI*.

W okresie objętym kontrolą obowiązywały dokumenty dotyczące bezpieczeństwa przetwarzania danych osobowych. W tym zakresie przyjęto Zarządzenie nr 23/12 Starosty Górowskiego z dnia 12 grudnia 2012 r. *w sprawie ochrony danych osobowych przetwarzanych w Starostwie Powiatowym w Górze,* które wprowadzało*:*

- „Politykę Bezpieczeństwa Informacji w zakresie przetwarzania danych osobowych w Starostwie Powiatowym w Górze";

[3] Dz. Urz. UE L 119 z 04.05.2016, str. 1, ze zm.

- „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Starostwie Powiatowym w Górze";
- „Instrukcję postępowania w sytuacjach naruszenia systemu ochrony danych osobowych w Starostwie Powiatowym w Górze".

(dowód: akta kontroli str. 5-63; 94-95)

Dokumentacja związana z ochroną danych osobowych uwzględniająca wymogi *RODO* została wprowadzona Zarządzeniem Nr 19/2018 Starosty Górowskiego z dnia 23 lipca 2018 r. *w sprawie wprowadzenia dokumentacji związanej z ochroną danych osobowych służącej do przetwarzania danych osobowych w Starostwie Powiatowym w Górze*. Powyższy dokument został przedstawiony do zapoznania się wszystkim pracownikom jednostki i obejmował:

- „Politykę Bezpieczeństwa Danych Osobowych"[4];
- procedury[5];
- „Plan ciągłości działania";
- „Regulamin Ochrony Danych Osobowych w Starostwie Powiatowym w Górze"[6];
- procedurę sporządzania analizy ryzyka.

Wskazane wyżej procedury oraz regulamin zawierały elementy PBI w zakresie systemów przetwarzających dane osobowe, ale ze względu na wprowadzenie ich pod koniec czynności kontrolnych, już po przeprowadzeniu większości badań i oględzin oraz fakt, że nie zastępowały one wprost PBI wprowadzonej Zarządzeniem nr 23/12 Starosty Górowskiego, nie były przedmiotem kontroli opisanej w pkt. 2 niniejszego wystąpienia.

(dowód: akta kontroli str. 123-126)

Zgodnie z obowiązującymi w Starostwie regulacjami dotyczącymi bezpieczeństwa danych osobowych nadzór nad przestrzeganiem PBI i przestrzeganiem zasad w nich zawartych pełnił ABI. Od dnia 17 października 2017 r. nie było formalnie wyznaczonego pracownika, do którego zadań należały kwestie zapewnienia bezpieczeństwa informacji przetwarzanych w Starostwie.

(dowód: akta kontroli str. 113-114)

W dniu 18 czerwca 2018 r. Starosta Górowski wyznaczył Inspektora Ochrony Danych (dalej: „IOD")[7], co było zgodne z art. 37 ust. 1 *RODO*. W dniu 5 lipca 2018 r. jednostka przekazała informację o wyznaczeniu IOD do Prezesa Urzędu Ochrony Danych Osobowych, co było zgodne z art. 158 ust. 5 ustawy z dnia 10 maja 2018 r. *o ochronie danych osobowych*[8] (dalej: „*uodo*").

(dowód: akta kontroli str. 64-65)

---

[4] Zawierającą m.in.: zapisy dotyczące inwentaryzacji danych, zgodności z prawem i upoważnienia do ich przetwarzania; analizy ryzyka i oceny skutków; instrukcji postępowania z incydentami; prowadzenia szkoleń; prowadzenia rejestrów czynności przetwarzania przez Administratora; stosowanych procedur audytu; obszarów przetwarzania danych osobowych; obowiązku zachowania poufności; sposobu udostępniania danych osobowych oraz postępowania dyscyplinarnego.

[5] Procedury: audytu; niszczenia danych; tworzenia kopii zapasowych; zarządzania uprawnieniami i napraw w serwisach zewnętrznych.

[6] Zawierający m.in.: uregulowania dotyczące zasad bezpiecznego użytkowania sprzętu IT, dysków i programów; użytkowania komputerów przenośnych; polityki haseł; zabezpieczenia dokumentacji papierowej z danymi osobowymi; zasady wynoszenia nośników z danymi poza obszar przetwarzania danych; zasady korzystania z Internetu; zasady korzystania z poczty elektronicznej; ochrony przeciwwirusowej; sposób wyznaczenia Administratora System Informatycznego; procedury nadawania i zmiany uprawnień użytkowników uprzywilejowanych; procedury wykonywania połączeń zdalnych, procedury archiwizacji danych oraz procedury dostępu do pomieszczenia serwerowni.

[7] Zarządzeniem nr 11/2018 Starosty Górowskiego z dnia 18 czerwca 2018 r. w sprawie wyznaczenia *inspektora ochrony danych.*

[8] Dz. U. poz. 1000.

Osoba wyznaczona IOD była pracownikiem zewnętrznym, posiadającym fachową wiedzę i będąca praktykiem w dziedzinie danych osobowych. Jej kandydatura została zaakceptowana przez Starostwo. IOD swoje zadania realizował na mocy umowy *na wdrożenie dokumentacji i procedur związanych z ochroną danych osobowych (RODO) oraz świadczenie usługi inspektora ochrony danych* zawartej w dniu 25 maja 2018 r. przez Starostwo z firmą zewnętrzną. Umowa ta została zawarta na czas określony do dnia 24 maja 2019 r. Wykonywanie zadań IOD na podstawie umowy o świadczenie usług było zgodne z art. 37 ust. 6 *RODO*.

Zgodnie z § 1 pkt 2 lit. i zawartej umowy zagwarantowano niezależne wykonywanie obowiązków przez IOD poprzez jego bezpośrednie podporządkowanie administratorowi danych osobowych Staroście w zakresie należytego wykonania postanowień umowy. Nie stwierdzono także wystąpienia konfliktu interesów, o którym mowa w art. 38 ust. 6 RODO, gdyż osoba ta nie uczestniczyła w określaniu celów i sposobów przetwarzania danych osobowych.

(dowód: akta kontroli str. 66-72; 115-116)

Obowiązujące w Starostwie regulacje w zakresie bezpieczeństwa danych osobowych[9] zawierały także procedury:

- nadawania uprawnień w systemie informatycznym;
- przydziału haseł dla administratorów systemów, użytkowników oraz częstotliwość ich zmiany;
- rozpoczęcia i zakończenia pracy w systemie informatycznym;
- postępowania z nośnikami informacji zawierającymi dane osobowe;
- korzystania z komputerów przenośnych;
- korzystania z poczty elektronicznej;
- sporządzania i przechowywania kopii zapasowych;
- zabezpieczeń systemu informatycznego przed oprogramowaniem złośliwym;
- przygotowywania systemu informatycznego do napraw, przeglądów i konserwacji;
- zapewnienia bezpieczeństwa i prawidłowej eksploatacji urządzeń w serwerowni.

(dowód: akta kontroli str. 5-63)

Przytoczone powyżej regulacje składały się wyłącznie z części deklaratywnej i były w całości dostępne dla wszystkich pracowników Starostwa. Pracownicy jednostki zostali zapoznani z tymi regulacjami.

(dowód: akta kontroli str. 114)

Jednostka przeprowadziła identyfikację zbiorów danych i sporządziła dla nich wykaz składający się z 87 podzbiorów. Dla każdego z nich wyodrębniono: nazwę podzbioru danych; aktywa w podziale na informacje, programy i systemy operacyjne, Infrastrukturę IT, Infrastrukturę Starostwa (obszar przetwarzania), pracowników i współpracowników oraz outsourcing; podstawę prawną przetwarzania danego podzbioru; zaznaczenie konieczności prowadzenia rejestru czynności przetwarzania; zaznaczenie konieczności dokonywania oceny skutków; opis celu przetwarzania, kategorii osób, kategorii danych osobowych oraz odbiorców; opis operacji przetwarzania; czas przechowywania danych.

(dowód: akta kontroli str. 123-126)

[9] Zarządzenie nr 23/12 Starosty Górowskiego z dnia 12 grudnia 2012 r. *w sprawie ochrony danych osobowych przetwarzanych w Starostwie Powiatowym w Górze*, wraz z załącznikami.

Starostwo nie posiadało informacji o zasobach informatycznych jednostki obejmujących ich rodzaj i konfigurację, wynikających z § 20 ust. 2 pkt 2 *rozporządzenia KRI.*

(dowód: akta kontroli str. 97)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następujące nieprawidłowości:

1. W Starostwie nie opracowano i nie wdrożono systemu zarządzania bezpieczeństwem informacji, w szczególności PBI. Było to niezgodne z wymaganiami § 20 ust. 1 *rozporządzenia KRI*, stanowiącym, że 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. Ponadto § 20 ust. 3 *rozporządzenia KRI* wskazuje, że wymagania określone w ww. ust. 1 uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001 *„Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania"* (dalej: „ISO 27001"), a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą[10]. Starosta przyznał, że w dokumencie tym odniesiono się głównie do ochrony danych osobowych, a pominięto system zarządzania bezpieczeństwem informacji, nie umiał jednak wyjaśnić, z jakich stało się to przyczyn.

(dowód: akta kontroli str. 94; 113-114)

2. W Starostwie nie prowadzono inwentaryzacji zasobów informatycznych, która zawierałaby pełne i aktualne informacje w zakresie posiadanego sprzętu informatycznego oraz jego konfiguracji, co było niezgodne z § 20 ust. 2 pkt 2 *rozporządzenia KRI*. W złożonych wyjaśnieniach Starosta jako powód braku takiego rejestru wskazał trudną sytuację powiatu górowskiego. W ocenie NIK taka argumentacja nie znajduje potwierdzenia w stanie faktycznym, ponieważ na rynku istnieją także bezpłatne aplikacje typu „open source[11]" posiadające funkcjonalności z ww. zakresu.

(dowód: akta kontroli str. 97; 115)

3. W Urzędzie nie wskazano osoby odpowiedzialnej za bezpieczeństwo informacji, co było działaniem nierzetelnym. Zgodnie z treścią pkt A.6.1.1 *Role i odpowiedzialność za bezpieczeństwo informacji* normy ISO 27001 zadania w zakresie bezpieczeństwa informacji powinny zostać precyzyjnie określone i przypisane konkretnym osobom. NIK zauważa, że po dniu 17 października 2017 r. nie powołano w Starostwie ABI, którego zadaniem miał być – zgodnie z § 2 Zarządzenia Nr 23/12 Starosty Górowskiego z dnia 12 grudnia 2012 r. *w sprawie ochrony danych osobowych przetwarzanych w Starostwie Powiatowym* – nadzór nad wprowadzaniem PBI i przestrzeganiem zasad w niej zawartych. Zdaniem NIK brak odpowiedzialnej za to osoby spowodował, że akt ten był nieaktualny, niepełny oraz w wielu aspektach nieprzestrzegany. Według wyjaśnień złożonych przez

---

[10] W tym: PN-ISO/IEC 27002 - w odniesieniu do ustanawiania zabezpieczeń, PN-ISO/IEC 27005 – w odniesieniu do zarządzania ryzykiem, PN-ISO/IEC 24762 - w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.

[11] Idei wolnego oprogramowania, która zapewnia swoim użytkownikom prawo do legalnego oraz darmowego uruchamiania, kopiowania, rozpowszechniania, analizowania, modyfikacji oraz ulepszania i rozbudowy istniejących produktów.

Wicestarostę, proponował on tą funkcję kilku pracownikom, ale żaden z nich jej nie przyjął.

(dowód: akta kontroli str. 113-114; 130)

Uwaga dotycząca badanej działalności

NIK zwraca uwagę, że szczegóły techniczne stosowanych procedur i zabezpieczeń zawarte w załącznikach do obowiązującej w Starostwie PBI powinny być dostępne wyłącznie pracownikom odpowiedzialnym za ich realizacji i nie powinny być częścią deklaratywną tego dokumentu. Udostępnienie tych dokumentów wszystkim pracownikom Starostwa stwarza ryzyko, że informacje w nich zawarte zostaną wykorzystane do przełamania ustanowionych zabezpieczeń.

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia negatywnie działalność Starostwa w zakresie organizacji bezpieczeństwa informacji, w szczególności ze względu na brak ustanowienia PBI zgodnej z wymogami *rozporządzenia KRI*.

2. Wdrożone i wykorzystywane rozwiązania organizacyjne i techniczne zapewniające bezpieczeństwo informacji

Opis stanu faktycznego

Na dwóch z 10 poddanych oględzinom stanowiskach komputerowych stwierdzono, że pracownicy Starostwa posiadali uprawnienia administratora, mimo iż nie byli oni administratorami systemów informatycznych. Pracownikom tym wbrew wymogom § 20 ust. 2 pkt 4 *rozporządzenia KRI*, umożliwiono instalowanie dowolnego oprogramowania.

(dowód: akta kontroli str. 109-111)

W Starostwie brak było formalnej procedury nadawania i odbierania uprawnień dla pracowników w dostępie do systemów informatycznych. Uprawnienia dostępu do systemów informatycznych, ich zmiana lub cofnięcie następowało w formie polecenia ustnego[12]. Badanie uprawnień 15 pracowników wykonujących zadania w systemach informatycznych[13], wykazało, że były one zgodne z realizowanymi czynnościami zapisanymi w ich zakresach czynności[14].

(dowód: akta kontroli str. 115; 122)

W okresie po 1 czerwca 2017 r. w Starostwie Powiatowym w Górze zakończyło pracę sześć osób, a cztery inne zmieniło swoje miejsce pracy. W żadnym z powyższych przypadków zmiana jak i pozbawienie uprawnień w dostępie do systemów komputerowych nie zostało udokumentowane. Osobom, które zakończyły zatrudnienie w badanym okresie zostały odebrane uprawnienia do systemów informatycznych.

(dowód: akta kontroli str. 120-121)

„Procedura przydziału haseł dla administratorów systemów, użytkowników oraz częstotliwość ich zmiany", stanowiąca część „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Starostwie Powiatowym w Górze"[15] wprowadzała obowiązek stosowania przez pracowników

---

[12] Procedurę zarządzania uprawnieniami wprowadzono Zarządzeniem nr 19/2018 Starosty Górowskiego z dnia 23 lipca 2018 r. *w sprawie wprowadzenia dokumentacji związanej z ochroną danych osobowych służącej do przetwarzania danych osobowych w Starostwie Powiatowym w Górze*. Dotyczy ona systemów przetwarzających dane osobowe i wymaga pisemnych wniosków do dostęp/zmianę lub odebranie uprawnień, wprowadza ona także zasady tworzenia, ewidencjonowania i korzystania z loginów (identyfikatorów).

[13] W tym 4 na stanowiskach kierowniczych.

[14] Badanie przeprowadzone w dniach 6-7 sierpnia 2018 r., obejmujące pracowników obsługujących systemy Bestia (2 osoby) oraz EWOPIS (13 pracowników).

[15] Zarządzenie nr 23/12 Starosty Górowskiego z dnia 12 grudnia 2012 r. *w sprawie ochrony danych osobowych przetwarzanych w Starostwie Powiatowym w Górze.*

jednostki co najmniej 8-znakowych haseł dostępowych do systemów informatycznych, o odpowiedniej budowie i złożoności.

W toku przeprowadzonych w dniu 9 lipca 2018 r. oględzin trzech systemów informatycznych[16] stwierdzono, że nie posiadały one funkcjonalności umożliwiających zarządzanie ochroną przetwarzanych informacji przed nieautoryzowanym dostępem poprzez ustanawianie zasad złożoności haseł dostępowych oraz okresów po jakich hasła powinny być zmienione. Komputery użytkowane w Starostwie nie były zarządzane centralnie w oparciu o mechanizmy np. *Microsoft Active Directory*[17].

Badanie polegające na dokonaniu oględzin czynności logowania do systemów informatycznych na 10 stanowiskach komputerowych wykazało, że:

- trzech przypadkach użytkownicy nie musieli wprowadzać żadnego hasła dostępowego – następowało automatyczne zalogowanie;
- sześciu przypadkach hasła miały od 1 do 7 znaków;
- jednym przypadku hasło miało 8 znaków.

(dowód: akta kontroli str. 107-111)

Starostwo w badanym okresie[18] na podstawie zawartych umów korzystało z adresów poczty elektronicznej zlokalizowanych na komercyjnych serwerach. Umowy te zobowiązywały dostawcę usług do zachowania w tajemnicy wszelkich informacji, których ujawnienie byłoby sprzeczne z interesem zleceniodawcy oraz jego zobowiązanie o nie udostępnianie osobom trzecim jakichkolwiek informacji uzyskanych w związku z wykonywaniem umowy bez pisemnej zgody zleceniodawcy. Przytoczone postanowienia umowy wypełniały postanowienia § 20 ust. 2 pkt 7 *rozporządzenia KRI.*

(dowód: akta kontroli str. 74-81)

Oględziny pięciu stanowisk pracy[19] realizujących zadania związane z rejestracją pojazdów oraz wydawaniem praw jazdy wykazały, że ich monitory były usytuowane w sposób uniemożliwiający wgląd do danych przez osoby nieuprawnione. Powyższe działania spełniały wymogi § 20 ust. 2 pkt 7 *rozporządzenia KRI.*

(dowód: akta kontroli str. 112)

Zasady pracy z komputerami przenośnymi w Starostwie określała „Procedura korzystania z komputerów przenośnych" stanowiąca część „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Starostwie Powiatowym w Górze"[20]. Wymagała on przede wszystkim zabezpieczenia fizycznego użytkowanego komputera, nie pozostawiania go bez nadzoru, nie udostępniania osobom nieupoważnionych oraz zapisywania danych tylko w folderach dysków twardych zabezpieczonych przez szyfrowanie. Procedura ta wymagała również założenia hasła na komputer przenośny, wygaszacz ekranu oraz stosowanie środków ochrony kryptograficznej w postaci szyfrowania informacji zawierających dane osobowe.

(dowód: akta kontroli str. 41)

---

[16] EWOPIS; Radix System FKJ i Radix Kadry.

[17] Usługa Active Directory używa strukturalnego magazynu danych jako podstawy dla logicznej i hierarchicznej organizacji informacji katalogowych, przechowuje informacje dotyczące obiektów w sieci i ułatwia administratorom i użytkownikom znaleźć i używać tych informacji.

[18] Od dnia 1 czerwca 2017 r. do dnia 28 sierpnia 2018 r.

[19] 100% wykorzystywanych stanowisk do tych celów.

[20] Zarządzenie nr 23/12 Starosty Górowskiego z dnia 12 grudnia 2012 r. *w sprawie ochrony danych osobowych przetwarzanych w Starostwie Powiatowym w Górze.*

Serwerownia Starostwa była zlokalizowana w odrębnym zamykanym pomieszczeniu, wyposażonym w klimatyzację, dedykowane zasilanie elektryczne oraz system zasilania zapasowego. Część zastosowanych zabezpieczeń fizycznych serwerowni w zakresie zapewnienia bezpieczeństwa przeciwpożarowego w niewystarczającym stopniu chroniła to pomieszczenie.

(dowód: akta kontroli str. 92-93)

W okresie objętym kontrolą obowiązywała jedna umowa dotycząca zakupu i serwisowania sprzętu komputerowego. Nie zawierała ona zapisów gwarantujących zachowanie odpowiedniego poziomu bezpieczeństwa informacji.

(dowód: akta kontroli str. 82-91)

Obowiązująca w badanym okresie „Procedura przygotowania systemu informatycznego do napraw, przeglądów i konserwacji"[21] wymagała naprawy dysków twardych w miejscu użytkowania. W przypadku konieczności dostarczenia dysku do serwisu, zgodnie z tymi regulacjami powinien być on dostarczony po wymontowaniu dysków twardych. Wszystkie serwery i komputery serwisowane były w tym okresie przez Informatyka Starostwa bez korzystania z usług serwisu zewnętrznego.

(dowód: akta kontroli str. 116)

Według stanu na dzień 17 lipca 2017 r. Starostwo posiadało 11 komputerów z zainstalowanym systemem operacyjnym Windows XP Pro, co stanowiło 20,4% wszystkich komputerów i laptopów.

(dowód: akta kontroli str. 116, 120-121)

Obowiązek tworzenia kopii zapasowej w Starostwie został uregulowany w „Procedurze sporządzania i przechowywania kopii zapasowych", stanowiącej część „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Starostwie Powiatowym w Górze"[22]. Zgodnie z nią pełna kopia danych powinna być tworzona co tydzień, a przyrostowa codziennie. Wykonane w ten sposób kopie powinny być przechowywane pod zamknięciem, poza pomieszczeniem serwerowni. W toku przeprowadzonych w dniu 9 lipca 2018 r. oględzin stwierdzono, że kopie zapasowe były wykonywane na dostępnych zasobach dyskowych znajdujących się w serwerowni Starostwa i tam przechowywane. Kopie zapasowe były tworzone w zależności od aplikacji/zasobu którego dotyczyły.

Ponadto dodatkowe kopie zapasowe były przechowywane na dysku zewnętrznym w kasie pancernej poza pomieszczeniem serwerowni i zawierały kopie zapasowe utworzone odpowiednio: 11 miesięcy[23] oraz 2-3 tygodni[24]. Wcześniej. Kopie zapasowe były sprawdzane przynajmniej raz w miesiącu pod kątem ich przydatności do odtworzenia danych w przypadku awarii systemu.

(dowód: akta kontroli str. 97; 107-108)

Starostwo dla ochrony swoich zasobów informacyjnych stosowało oprogramowanie antywirusowe. W toku przeprowadzonych w dniu 11 lipca 2018 r. oględzin 10 komputerów stwierdzono, że w dziewięciu badanych przypadkach

---

[21] Zarządzenie nr 23/12 Starosty Górowskiego z dnia 12 grudnia 2012 r. *w sprawie ochrony danych osobowych przetwarzanych w Starostwie Powiatowym w Górze.*

[22] Zarządzenie nr 23/12 Starosty Górowskiego z dnia 12 grudnia 2012 r. *w sprawie ochrony danych osobowych przetwarzanych w Starostwie Powiatowym w Górze.*

[23] Według oględzin przeprowadzonych w dniu 6 sierpnia 2018 r. kopie zapasowe bazy ewidencji i budynków oraz systemu PZGiK według stanu na dzień 30 września 2017 r.

[24] Według oględzin przeprowadzonych w dniu 6 sierpnia 2018 r. dla serwerów geodezyjnych, serwerów Redix oraz Bestia z 10 lipca 2018 r.

oprogramowanie to posiadało definicje wirusów pochodzące z dnia badania, a w jednym przypadku definicje te były sprzed dwóch dni.

(dowód: akta kontroli str. 109-111)

W Starostwie nie obowiązywały procedury dotyczące monitorowania pojemności nośników pamięci systemów urzędu, a także nie stosowano oprogramowania automatyzującego monitorowanie pojemności pamięci masowych (dysków twardych) wykorzystywanych w serwerach. Monitoring taki był prowadzony ręcznie przez Informatyka. W toku przeprowadzonych w dniu 9 lipca 2018 r. oględzin trzech serwerów wykorzystywanych przez tą jednostkę ustalono, że ich dyski twarde były zajęte w od 1,8% do 38,2% pojemności.

(dowód: akta kontroli str. 107-108)

W jednostce nie funkcjonowały procedury dotyczące zarządzania zmianą oprogramowania. Według udzielonych wyjaśnień w Starostwie nie występują zmiany oprogramowania, a jedynie jego aktualizacje. Ze względu na niski poziom infrastruktury informatycznej jednostki, te ostatnie nie wywołują zakłóceń i dotyczą najczęściej systemów operacyjnych.

(dowód: akta kontroli str. 116)

Dla każdego z 87 zidentyfikowanych podzbiorów, zawartych w „Wykazie zbiorów danych osobowych Starostwa Powiatowego w Górze" prowadzono rejestr czynności przetwarzania danych. Dla każdego z nich określono zgodnie z wymaganiami art. 30 ust. 1 *RODO*: nazwę administratora i jego dane kontaktowe; nazwę współadministratora i jego dane kontaktowe; przedstawiciela administratora; dane IOD wraz z jego adresem mailowym; cel przetwarzania danych; kategorię osób; kategorię danych osobowych; kategorię odbiorców, którym dane osobowe zostaną ujawnione; odbiorców w państwach trzecich; odbiorców w organizacjach międzynarodowych; nazwę państwa trzeciego lub organizacji międzynarodowej oraz informację czy wymagana jest dokumentacja odpowiednich zabezpieczeń; planowane terminy usunięcia poszczególnych kategorii danych; opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 *RODO.*

(dowód: akta kontroli str. 123-126)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następujące nieprawidłowości:

1. W dwóch z 10 badanych przypadków stanowisk komputerowych istniała możliwość zainstalowania na tym sprzęcie dowolnego oprogramowania przez użytkownika niebędącego informatykiem. Sprawdzenie uprawnień kont użytkowników w systemie operacyjnym wykazało, że mieli oni nadane uprawnienia administratora. Było to niezgodne z § 20 ust. 2 pkt 4 *rozporządzenia KRI*, stanowiącym że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie m.in. podejmowania 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. Według wyjaśnień Wicestarosty na tych komputerach były przeprowadzane aktualizacje i konta użytkowników musiały być przełączone na tryb administratora. NIK nie podziela powyższych argumentów, ponieważ takie aktualizacje można było wykonać z konta informatyka lub pod jego nadzorem. W toku przeprowadzonych oględzin uczestniczący w nich informatyk Starostwa dokonał korekty uprawnień dla tych kont zmieniając je na standardowe użytkownika.

(dowód: akta kontroli str. 109-111; 132)

2. W dziewięciu z 10 badanych przypadków stanowisk komputerowych hasła dostępowe użytkowników do systemu operacyjnego nie były stosowane lub zawierały mniej niż 8 znaków. Było to niezgodne z „Procedurą przydziału haseł dla administratorów systemów, użytkowników oraz częstotliwość ich zmiany", będącej częścią „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Starostwie Powiatowym w Górze", w myśl której minimalna długość hasła powinna wynosić co najmniej 8 znaków. Według wyjaśnień przedłożonych przez Wicestarostę zmiana haseł leżała w gestii samych użytkowników, a długość haseł została już dostosowana do zaleceń.

(dowód: akta kontroli str. 109-111;132)

3. W Starostwie brak było formalnej procedury nadawania i odbierania uprawnień użytkownikom systemów informatycznych. Ich nadanie, zmiana lub cofnięcie następowało w formie ustnej. Było to niezgodne z § 20 ust. 2 pkt 4 rozporządzenia KRI, który stanowi, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie m.in. podejmowania 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. Brak formalnej procedury w tym zakresie był niezgodny z pkt A.9.2.1 ISO 27001, powodując jednocześnie naruszenie przepisu § 20 ust. 2 pkt 4 w związku z ust. 3 rozporządzenia KRI. Zgodnie z wyjaśnieniami złożonymi przez Wicestarostę wynikało to z błędnej interpretacji przepisów.

(dowód: akta kontroli str. 115;130)

4. Serwerownia Starostwa nie posiadała dostatecznego zabezpieczenia w zakresie bezpieczeństwa przeciwpożarowego, wypełniającego zalecenia pkt 11.1.1 i 11.2.1 ISO 27002, jak również nie prowadzono dla tego obiektu ewidencji wejść/wyjść gości, o której mowa w pkt 11.1.2 ISO 27002. Powyższe stanowiło naruszenie przepisu § 20 ust. 2 pkt 9 *rozporządzenia KRI* w zakresie nieprawidłowego zabezpieczenia informacji. Według wyjaśnień Wicestarosty niedostateczne zabezpieczenie w zakresie bezpieczeństwa przeciwpożarowego wynikało z braku środków finansowych, a brak ewidencji z niedopilnowania obowiązków przez pracownika.

(dowód: akta kontroli str. 92-93; 132)

Kopie zapasowe serwerów i baz danych były przechowywane w serwerowni Starostwa, tj. w miejscu gdzie zlokalizowane były serwery z danymi źródłowymi. Ponadto, w przypadku serwera SQL Redix kopie zapasowe wykonano w 2018 r. tylko trzykrotnie (tj. w dniach: 5 stycznia, 17 stycznia i 15 maja), co było niezgodne z regulacjami wewnętrznymi Starostwa[25], w myśl których sporządzanie kopii pełnych powinno następować raz w tygodniu, a przyrostowych codziennie. W myśl tych uregulowań kopie zapasowe powinny być przechowywane pod zamknięciem poza pomieszczeniem serwerowni. Takie postępowanie stanowiło również naruszenie § 20 ust. 2 pkt 12 lit. b i e *rozporządzenia KRI*, ponieważ nie zapewniało wystarczającej ochrony przed utratą informacji. Ponadto, w myśl postanowień pkt 12.3.1 normy PN-ISO/IEC 27002:2014, kopie zapasowe należy przechowywać w innej lokalizacji, w odległości pozwalającej uniknąć uszkodzeń spowodowanych katastrofą, która dotknęła ośrodek podstawowy. Według wyjaśnień Starosty kopie

[25] „Procedura sporządzania i przechowywania kopii zapasowych", stanowiąca część „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Starostwie Powiatowym w Górze".

zapasowe były przechowywane na dyskach zewnętrznych w kasie pancernej poza serwerownią. Przeprowadzone w dniu 6 sierpnia 2018 r. oględziny tych dysków wykazały, że kopie te zawierały nieaktualne bazy danych, tj. sprzed od 2 tygodni do nawet 11 miesięcy, co zdaniem NIK sprawia, że nie można ich traktować jako w pełni przydatnych do odzyskania informacji.

(dowód: akta kontroli str. 97; 107)

5. W umowie nr 2/2017, zawartej w dniu 19 lipca 2017 r. na dostawę i serwis zestawów komputerowych, Starostwo nie zawarło zapisów zobowiązujących wykonawcę do zachowania tajemnicy informacji, co było niezgodne z postanowieniami § 20 ust. 2 pkt 10 *rozporządzenia KRI.* Według wyjaśnień złożonych przez Starostę w umowie tej zastosowano zapis o ochronie danych osobowych, a umowa ta została parafowana przez radcę prawnego. NIK wskazuje jednak, że zobligowanie wykonawcy umowy do zapewnienia ochrony wyłącznie danych osobowych jest niewystarczające, gdyż realizując umowę wykonawca może mieć dostęp do wielu informacji o funkcjonowaniu m.in. środowiska informatycznego Starostwa, które nie są danymi osobowymi, a winny podlegać ochronie.

(dowód: akta kontroli str. 82-91; 116)

6. Dyski twarde użytkowanych przez Starostwo komputerów przenośnych nie były szyfrowane, czego wymagała „Procedura korzystania z komputerów przenośnych" będąca elementem „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Starostwie Powiatowym w Górze"[26]. Według wyjaśnień przedłożonych przez Wicestarostę wynikało to z braku spójnego oprogramowania szyfrującego.

(dowód: akta kontroli str. 115; 132)

Uwagi dotyczące badanej działalności

NIK zwraca uwagę, że:

1) poddane oględzinom trzy systemy informatyczne nie pozwalały (z poziomu aplikacji) na zarządzanie ochroną przetwarzanych informacji przed nieautoryzowanym dostępem poprzez ustanawianie zasad złożoności hasła dostępowego oraz okresów po jakim hasło użytkownika powinno być zmienione. Rodzi to ryzyko, że stosowane bezpośrednio przez użytkowników hasła będą niezgodne z prowadzoną przez Starostwo polityką w zakresie złożoności haseł;

2) 20,4% komputerów i laptopów użytkowanych przez Starostwo posiada system informatyczny, który nie jest już wspierany przez producenta. Taki stan rzeczy znacząco obniża poziom bezpieczeństwa informatycznego i zdaniem NIK należy dążyć do jak najszybszej wymiany takiego oprogramowania na nowsze, posiadające wsparcie techniczne.

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia negatywnie wdrożone i wykorzystywane przez Starostwo rozwiązania organizacyjne i techniczne zapewniające bezpieczeństwo informacji.

3. Działania w celu zapobiegania incydentom bezpieczeństwa informacji

Opis stanu faktycznego

W objętym kontrolą okresie w Starostwie nie prowadzono okresowych analiz ryzyka utraty integralności, poufności lub dostępności informacji, o których mowa w § 20 ust. 2 pkt 3 *rozporządzenia KRI.*

[26] Zarządzeniem nr 11/2018 Starosty Górowskiego z dnia 18 czerwca 2018 r. w sprawie wyznaczenia *inspektora ochrony danych.*

Procedura w zakresie zgłaszania incydentów naruszenia bezpieczeństwa informacji w Starostwie odnosiły się wyłącznie do danych osobowych. Wymagała ona pisemnego zgłaszania incydentów i opisywała postępowanie w przypadku ich wystąpienia[27]. Pracownicy Starostwa zostali zapoznani w ww. regulacjami. Według informacji udzielonych przez Starostę w badanym okresie nie wystąpiły incydenty związane z bezpieczeństwem informacji.

W Starostwie nie prowadzono szkoleń osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem zagrożenia bezpieczeństwa informacji, skutków naruszenia tych zasad, w tym odpowiedzialność prawna za te czyny oraz stosowania środków zapewniających bezpieczeństwo informacji.

(dowód: akta kontroli str. 59-63; 116; 121-126)

W badanym okresie w Starostwie nie przeprowadzano audytów wewnętrznych z zakresu bezpieczeństwa informacji.

(dowód: akta kontroli str. 97-98; 116)

Realizując wymogi określone w art. 32 ust. 1 *RODO* Starostwo dokonało analizy ryzyk istniejących w procesach przetwarzania danych osobowych w jednostce. Przyjęto w niej założenie, że dane w zbiorach informatycznych przetwarzane są przez te same aktywa (pracownicy, sprzęt, oprogramowanie, infrastruktura Starostwa), w związku z czym są one obarczone tymi samymi ryzykami, których prawdopodobieństwo wystąpienia oraz skutki są również wspólne. W analizie tej opisano 41 zagrożeń, wyznaczono dla nich zabezpieczenia oraz określono prawdopodobieństwo wystąpienia (w skali 1-3), skutek wystąpienia (w skali 1-3); istotność ryzyka (jako iloczyn prawdopodobieństwa i skutku), a także sposób reakcji na ryzyko.

(dowód: akta kontroli str. 123-126)

Według stanu na dzień 8 sierpnia 2018 r. szkoleniem podstawowym z zakresu ochrony danych osobowych, uwzględniającym regulacje wprowadzone przez *RODO,* zostało objętych łącznie 51 pracowników[28]. Dodatkowo sześciu pracowników brało udział w szkoleniu dotyczącym zasad wystawiania upoważnień do przetwarzania danych osobowych w systemach informatycznych. Oba te szkolenia prowadził IOD.

(dowód: akta kontroli str. 123-126; 131)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następujące nieprawidłowości:

1. W Starostwie nie prowadzono okresowych analiz ryzyka utraty integralności, poufności lub dostępności informacji. Było to niezgodne z wymogiem § 20 ust. 2 pkt 3 *rozporządzenia KRI*, zobowiązującym do wykonywania takich analiz oraz do podejmowania działań minimalizujących te ryzyka. W złożonych wyjaśnieniach Starosta stwierdził, że analiz takich nie prowadzono z powodu trudnej sytuacji finansowej jednostki.

(dowód: akta kontroli str. 116)

---

[27] Załącznik nr 3 do Zarządzenia nr 23/12 Starosty Górowskiego z dnia 12 grudnia 2012 r. *w sprawie ochrony danych osobowych przetwarzanych w Starostwie Powiatowym w Górze* oraz „Instrukcja postępowania z incydentami" stanowiąca część „Polityki Ochrony Danych Osobowych" wprowadzona Zarządzeniem Nr 19/2018 Starosty Górowskiego z dnia 23 lipca 2018 r. *w sprawie wprowadzenia dokumentacji związanej z ochroną danych osobowych służącej do przetwarzania danych osobowych w Starostwie Powiatowym w Górze.* Pracownicy Starostwa zostali zapoznani z tymi dokumentami.

[28] Według informacji Wicestarosty przeszkolenie przeszli wszyscy pracownicy na stanowiskach urzędniczych z wyjątkiem przebywających na długotrwałym zwolnieniu lekarskim bądź na świadczeniu rehabilitacyjnym.

2. W Starostwie nie ustanowiono procedur w zakresie zgłaszania incydentów naruszenia bezpieczeństwa informacji. Funkcjonujące w Starostwie procedury odniosły się wyłącznie do incydentów w zakresie danych osobowych. Było to niezgodne z § 20 ust. 2 pkt 13 *rozporządzenia KRI*, który stanowi, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo warunków umożliwiających realizację i egzekwowanie bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących. Według składanych przez Wicestarostę wyjaśnień wynikało to z błędnej interpretacji przepisów, a także braku opracowanego i wdrożonego systemu zarządzania bezpieczeństwem informacji.

(dowód: akta kontroli str. 59-63; 116; 121-126; 130)

3. W okresie objętym kontrolą w Starostwie nie przeprowadzano audytów wewnętrznych w zakresie bezpieczeństwa informacji, co było sprzeczne z § 20 ust. 2 pkt 14 *rozporządzenia KRI*. W złożonych wyjaśnieniach Starosta stwierdził, że audytów nie prowadzono z powodu trudnej sytuacji finansowej jednostki.

(dowód: akta kontroli str. 97; 116)

4. W Starostwie nie prowadzono szkoleń osób zaangażowanych w proces przetwarzania informacji, ze szczególnym uwzględnieniem zagrożenia bezpieczeństwa informacji, skutków naruszenia tych zasad, w tym odpowiedzialność prawna za te czyny, oraz stosowania środków zapewniających bezpieczeństwo informacji, co stanowiło naruszenie § 20 ust. 2 pkt 6 *rozporządzenia KRI*. W złożonych wyjaśnieniach Starosta stwierdził, że przedmiotowych szkoleń nie prowadzono z powodu trudnej sytuacji finansowej jednostki.

(dowód: akta kontroli str. 116)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia negatywnie działania Starostwa podejmowane w celu zapobiegania incydentom bezpieczeństwa informacji, szczególnie ze względu na brak prowadzenia audytów wewnętrznych bezpieczeństwa informacji oraz szkoleń z tego zakresu.

IV. Wnioski

Wnioski pokontrolne

Przedstawiając powyższe oceny wynikające z ustaleń kontroli, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy z dnia 23 grudnia 1994 r. *o Najwyższej Izbie Kontroli*[29] (dalej: „*ustawa o NIK*"), wnosi o:

1. Opracowanie i wdrożenie systemu zarządzania bezpieczeństwem informacji, uwzględniającego zalecenia normy ISO 27001 i norm z nią związanych (PN-EN ISO/IEC 27002, PN-EN ISO/IEC 27005, PN-EN ISO/IEC 24762).
2. Wyznaczenie osoby (lub osób) odpowiedzialnej za realizację zadań związanych z bezpieczeństwem informacji.
3. Prowadzenie aktualnej i kompletnej elektronicznej ewidencji sprzętu informatycznego, obejmującej jego rodzaj i konfigurację.
4. Ustanowienie obowiązku pisemnego dokumentowania przydzielania uprawnień do systemów informatycznych Starostwa.
5. Wdrożenie rozwiązań zapewniających odpowiednie zabezpieczenie pomieszczenia serwerowni.

[29] Dz. U. z 2017 r. poz. 524, ze zm.

6. Przechowywanie kopii zapasowych baz danych poza serwerownią oraz sporządzanie takich kopii zgodnie z uregulowaniami obowiązującymi w Starostwie.
7. Zawieranie w umowach serwisowych z podmiotami zewnętrznymi, świadczącymi usługi informatyczne dla Starostwa, zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.
8. Zapewnienie szyfrowania danych na komputerach przenośnych.
9. Wykonywanie okresowych analiz ryzyka utraty integralności, poufności lub dostępności informacji.
10. Ustanowienie procedur w zakresie zgłaszania incydentów naruszenia bezpieczeństwa informacji.
11. Zapewnienie szkoleń osób dla zaangażowanych w proces przetwarzania informacji.
12. Coroczne przeprowadzanie audytów wewnętrznych z zakresu bezpieczeństwa informacji.

V. Pozostałe informacje i pouczenia

Prawo zgłoszenia zastrzeżeń

Wystąpienie pokontrolne zostało sporządzone w dwóch egzemplarzach; jeden dla kierownika jednostki kontrolowanej, drugi do akt kontroli.

Zgodnie z art. 54 *ustawy o NIK* kierownikowi jednostki kontrolowanej przysługuje prawo zgłoszenia na piśmie umotywowanych zastrzeżeń do wystąpienia pokontrolnego, w terminie 21 dni od dnia jego przekazania. Zastrzeżenia zgłasza się do Dyrektora Delegatury NIK we Wrocławiu.

Obowiązek poinformowania NIK o sposobie wykorzystania uwag i wykonania wniosków pokontrolnych

Zgodnie z art. 62 *ustawy o NIK* proszę o poinformowanie Najwyższej Izby Kontroli, w terminie 21 dni od otrzymania wystąpienia pokontrolnego, o sposobie wykorzystania uwag i wykonania wniosków pokontrolnych oraz o podjętych działaniach lub przyczynach niepodjęcia tych działań.

W przypadku wniesienia zastrzeżeń do wystąpienia pokontrolnego, termin przedstawienia informacji liczy się od dnia otrzymania uchwały o oddaleniu zastrzeżeń w całości lub zmienionego wystąpienia pokontrolnego.

Wrocław, dnia 06 września 2018 r.

Kontroler:
Cezary Mazik
Specjalista kontroli państwowej

.....
podpis

Najwyższa Izba Kontroli
Delegatura we Wrocławiu
Dyrektor

DYREKTOR
Delegatura Najwyższej Izby Kontroli
we Wrocławiu

.....
z up. *podpis*
Ziemowit Florkowski
Wicedyrektor