NAJWYŻSZA IZBA KONTROLI
Departament Administracji Publicznej

KAP.410.3.4.2024

Pan
Artur Ludew
Burmistrz Szydłowca
Rynek Wielki 1
26-500 Szydłowiec

# WYSTĄPIENIE POKONTROLNE

P/24/004 Zapewnienie bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych w jednostkach samorządu terytorialnego

NAJWYŻSZA IZBA KONTROLI
Departament Administracji Publicznej
ul. Filtrowa 57, 02-056 Warszawa
T +48 22 444 53 08, kap@nik.gov.pl

# I. Dane identyfikacyjne

| | |
|---|---|
| Jednostka kontrolowana | Urząd Miejski w Szydłowcu Rynek Wielki 1, 26-500 Szydłowiec (dalej: UM lub Urząd). |
| Kierownik jednostki kontrolowanej | Pan Artur Ludew Burmistrz Szydłowca od 9 grudnia 2014 r. do - obecnie. |
| Zakres przedmiotowy kontroli | Rozwiązania organizacyjne i techniczne w zakresie zapewnienia bezpieczeństwa przetwarzania informacji oraz zapewnienia ciągłości działania w Urzędzie i ich stosowanie. |
| Okres objęty kontrolą | Od 1 stycznia 2023 r. do dnia zakończenia czynności kontrolnych, tj. do 1 sierpnia 2024 r. (także okresy wcześniejsze w zakresie uczestnictwa w programie Cyfrowa Gmina). |
| Podstawa prawna podjęcia kontroli | Art. 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[1]. |
| Jednostka przeprowadzająca kontrolę | Najwyższa Izba Kontroli<br>Departament Administracji Publicznej |
| Kontrolerzy | 1. Marek Bieńkowski, doradca ekonomiczny, upoważnienie do kontroli nr KAP/44/2023 z 24 maja 2024 r.<br>2. Krzysztof Matuszek, doradca ekonomiczny, upoważnienie do kontroli nr KAP/44/2023 z 24 maja 2024 r.<br>(akta kontroli str. 1-2) |

[1] Dz. U. z 2022 r. poz. 623.

# II. Ocena ogólna[2] kontrolowanej działalności

**OCENA OGÓLNA**

W Urzędzie w okresie objętym kontrolą, ustanowiono i wdrożono System Zarządzania Bezpieczeństwem Informacji, jednak stwierdzono nieprawidłowości dotyczące nieopracowania niektórych szczegółowych procedur oraz ustanowienia polityki ciągłości działania w zakresie systemów informatycznych.

Uzasadnienie oceny ogólnej

W Urzędzie ustanowiono i wdrożono Politykę Bezpieczeństwa Informacji wraz z procedurami i instrukcjami[3], która podlegała regularnym przeglądom, co było zgodne z § 20 ust. 1 w zw. z ust. 3 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[4] (dalej: stare rozporządzenie KRI), a obecnie z § 19 ust. 1 w zw. z ust. 3 rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[5] (dalej: rozporządzenie KRI).

W Urzędzie prawidłowo realizowano zadania dotyczące opracowania dokumentacji z zakresu ochrony danych osobowych spełniającej wymogi 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/WE6 (dalej: RODO). Prawidłowo również realizowano zadania w zakresie gromadzenia aktualnych informacji o zasobach informatycznych obejmujących ich rodzaj i konfigurację, zgodnie z § 19 ust. 2 pkt 2 rozporządzenia KRI.

Ponadto, w Urzędzie w okresie objętym kontrolą, podejmowano działania zapewniające bezpieczeństwo przetwarzania informacji, m.in. poprzez testowanie kopii zapasowych, nadawanie uprawnień pracownikom adekwatnie do realizowanych przez nich zadań oraz zgodnie z § 20 ust. 2 pkt 10 rozporządzenia KRI stosowano w umowach serwisowych postanowienia gwarantujące odpowiedni poziom bezpieczeństwa informacji. Wprowadzono również procedury dotyczące pracy zdalnej oraz procedury uniemożliwiające instalowanie przez nieuprawnionego pracownika nieautoryzowanego oprogramowania. W toku kontroli stwierdzono, że określono wymagania dla haseł dostępu oraz blokowania kont byłych pracowników w systemach informatycznych wykorzystywanych przez Urząd. W Urzędzie zgodnie z § 19 ust. 2 pkt 13 rozporządzenia KRI opracowano procedurę w zakresie zgłaszania incydentów naruszenia bezpieczeństwa informacji.

W okresie objętym kontrolą w Urzędzie podjęto działania w celu zapobiegania incydentom bezpieczeństwa informacji, tj. stosownie do § 19 ust. 2 pkt 6 rozporządzenia KRI zorganizowano szkolenia pracowników oraz zgodnie z § 19 ust. 2 pkt 14 rozporządzenia KRI przeprowadzono audyt w zakresie bezpieczeństwa informacji. Nie prowadzono natomiast okresowych analiz ryzyka utraty integralności, poufności lub dostępności informacji, o których mowa w § 19 ust. 2 pkt 3 rozporządzenia KRI.

W Urzędzie nie zidentyfikowano zbiorów danych (oprócz danych osobowych). Ponadto nie ustanowiono polityki ciągłości działania, planów ciągłości działania i

---

[2] Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.

[3] Dalej: SZBI.

[4] Dz. U. z 2017 r. poz. 2247. Uchylone z dniem 23 maja 2024 r.

[5] Dz. U. poz. 773. Obowiązuje od dnia 23 maja 2024 r.

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

planów odtworzeniowych, nie przeprowadzono także analizy ryzyka w zakresie zapewnienia ciągłości działania, co należy uznać za nierzetelne.

W Urzędzie nie opracowano:

1) Regulaminu korzystania z zasobów informatycznych.
2) Procedury zarządzania sprzętem i oprogramowaniem.
3) Procedury zarządzania konfiguracją.
4) Procedury bezpiecznej utylizacji sprzętu elektronicznego.
5) Procedury zarządzania zmianami i wykonywaniem testów.
6) Polityka fizycznego dostępu do pomieszczeń (w tym serwerowni).
7) Polityki dostępu do infrastruktury informatycznej zewnętrznych podmiotów w związku z realizacją procedur serwisowych.
8) Procedury zarządzania pojemnością przestrzenią dyskową,

co w ocenie NIK było nierzetelne.

NIK zauważa, że w trakcie kontroli część stwierdzonych nieprawidłowości została usunięta w wyniku podjętych w Urzędzie działań.

# III. Opis ustalonego stanu faktycznego kontrolowanej działalności

OBSZAR

## 1. Organizacja bezpieczeństwa informacji i zapewnienia ciągłości działania systemów informatycznych

Opis stanu faktycznego

1. W Urzędzie nie zidentyfikowano poza danymi osobowymi innych zbiorów danych wymagających ochrony, które były przez Urząd przetwarzane[7]. Zbiorom danych nie przypisano w konsekwencji odpowiedniego poziomu ochrony (*dalszy opis w sekcji Stwierdzone nieprawidłowości*).

(akta kontroli str. 435-442)

W Urzędzie prowadzony był *Rejestr czynności przetwarzania danych osobowych* (dalej: RCPD)[8]. Ostatnia jego aktualizacja została sporządzona dnia 2 stycznia 2024r.[9]. Dla każdego zdefiniowanego procesu przetwarzania przeprowadzono szacowanie ryzyka w związku z ochroną danych osobowych. W odniesieniu do danych osobowych Administrator nie kategoryzował danych ze względu na ich wartość, stosując podejście oparte na ryzyku naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.

(akta kontroli str. 4-14)

2. W Urzędzie opracowano, ustanowiono i wdrożono System Zarządzania Bezpieczeństwem Informacji w rozumieniu § 20 ust. 1 w związku z ust. 3 starego rozporządzenia KRI, a obecnie § 19 ust. 1 w związku z ust. 3 rozporządzenia KRI. Dokumentacja została opracowana przez pracownika Urzędu[10], a następnie zatwierdzona przez Burmistrza Szydłowca[11] i zakomunikowana pracownikom Urzędu.

W Urzędzie opracowano procedury w formie załączników do SZBI, które zostały zatwierdzone i zakomunikowane pracownikom Urzędu odpowiedzialnym za realizację

---

7 Informacje takie klasyfikuje się z uwzględnieniem wymagań prawnych wartości, krytyczności i wrażliwości na nieuprawnione ujawnienie lub modyfikację.

8 Na podstawie art. 30 RODO.

9 W RCPD, poza informacjami wynikającymi z art. 30 ust. 1 lit. a-g RODO, uwzględniono: nazwę komórki organizacyjnej przetwarzającej dane, podstawę prawną przetwarzania, źródło pozyskania danych osobowych, nazwę systemu lub oprogramowania służących do przetwarzania danych, decyzję Administratora danych o przeprowadzeniu oceny skutków dla ochrony danych osobowych (DPIA)- RCPD nr 14.

10 Informatyk Urzędu odpowiadał również za jej wdrożenie, ocenę, przegląd i modyfikację.

11 Zarządzenie Burmistrza Szydłowca nr 126/22 z dnia 30 września 2022 r.

zadań określonych tymi dokumentami. Załączniki do SZBI stanowiły następujące procedury:

1) Procedura monitorowania dostępu do informacji;
2) Procedura analizy ryzyka;
3) Procedura zarządzania podatnościami;
4) Procedura bezpiecznej pracy zdalnej;
5) Procedura wykonywania kopii zapasowych;
6) Procedura przywracania systemów informatycznych po awarii;
7) Procedura zarządzania incydentem i zapewnienie obsługi;
8) Procedura zarządzania uprawnieniami i dostępem.

(akta kontroli str. 17-101, 221-234, płyta cd-1 pliki 001-039)

3. W Urzędzie opracowano, ustanowiono i wdrożono *Politykę ochrony danych osobowych* uwzględniającą wymogi RODO wprowadzoną Zarządzeniem Burmistrza Szydłowca[12], z którą zapoznano pracowników Urzędu.

(akta kontroli str. 226-227)

Dokument *Polityka ochrony danych osobowych* był aktualizowany i poddawany przeglądom. Ostatnia aktualizacja została przeprowadzona w marcu 2024 r. Dokumentacja ochrony danych osobowych w Urzędzie obejmowała następujące procedury, polityki i instrukcje:

- Polityka retencji danych osobowych,
- Procedura przetwarzania szczególnych kategorii danych,
- Polityka ochrony danych osobowych,
- Procedura postępowania w sytuacji naruszenia ochrony danych osobowych,
- Procedura nadawania uprawnień do przetwarzania danych osobowych w UM w Szydłowcu,
- Formularze służące realizacji praw osób, których dane dotyczą żądania sprostowania, usunięcia, ograniczenia oraz wniesienia sprzeciwu, będące załącznikiem do Procedury realizacji praw osób, których dane dotyczą zatwierdzonej przez Burmistrza Szydłowca. *Procedura realizacji praw,*
- Procedura publikacji, aktualizacji oraz okresowych przeglądów danych zamieszczanych w Biuletynie Informacji Publicznej Urzędu Miejskiego w Szydłowcu,
- Instrukcja anonimizacji danych osobowych w UM w Szydłowcu[13] (*Instrukcja Anonimizacja danych osobowych w dokumentach papierowych i elektronicznych (w tym w nagraniach),*
- Rejestr czynności przetwarzania danych osobowych[14],
- Rejestr umów powierzenia *przetwarzania danych osobowych,*
- Analiza ryzyka dla ochrony danych osobowych. *Szacowanie ryzyka,*
- Ocena skutków dla ochrony danych osobowych,
- DPIA praca zdalna[15],
- DPIA monitoring wizyjny,
- Instrukcja postępowania z kluczami *oraz zabezpieczenia pomieszczeń i budynków w Urzędzie[16],*

---

12 Zarządzenie nr 55/20 Burmistrza Szydłowca z dnia 10 kwietnia 2020 r.

13 Zarządzenie nr 89/2022 Burmistrza Szydłowca z dnia 21 czerwca 2022 r.

14 Zarządzenie nr 184/18 Burmistrza Szydłowca z dnia 14 września 2018 r.

15 DPIA ang. Data Protection Impact Assessment. Ocena dla skutków ochrony danych wymagana przez art. 35 RODO.

16 Zarządzenie nr 40/20 Burmistrza Szydłowca z dnia 16 marca 2020 r.

- Audyt zgodności przetwarzania danych osobowych z przepisami z zakresu ochrony danych osobowych,
- Audyt wewnętrzny „obiektywna i niezależna ocena funkcjonowania Urzędu Miejskiego w Szydłowcu w zakresie systemu bezpieczeństwa przetwarzania informacji oraz ochrony danych osobowych z uwzględnieniem przepisów powszechnie obowiązujących oraz regulaminów i norm wewnętrznych",
- Klauzule informacyjne,
- Polityka czystego biurka/ekranu,
- Procedura retencji danych w ZFŚS,
- Rejestr udostępnień danych osobowych.

(akta kontroli str. 226-227, płyta cd-1 plik 11)

4. W okresie objętym kontrolą nie przeprowadzono w Urzędzie analiz ryzyka w związku z potrzebą zapewnienia ciągłości działania systemów informatycznych *(dalszy opis w sekcji Stwierdzone nieprawidłowości).*

(akta kontroli str. 4-14)

5. W Urzędzie nie ustanowiono polityki ciągłości działania. Dokumentem dotyczącym polityki ciągłości działania była jedynie procedura przywracania systemu informatycznego po awarii, będąca częścią SZBI *(dalszy opis w sekcji Stwierdzone nieprawidłowości).*

(akta kontroli str. 12-14, 221-234, płyta cd-1 plik 14)

6. W Urzędzie nie opracowano również planów ciągłości działania dotyczących poszczególnych komponentów systemu informatycznego ani planów odtworzeniowych. W konsekwencji nie przeprowadzano testów w tym zakresie *(dalszy opis w sekcji Stwierdzone nieprawidłowości).*

(akta kontroli str. 226-231)

7. Dokumentacja SZBI została wdrożona w Urzędzie w 2022 r., a w 2023 r dokonano jej przeglądu, z którego sporządzono Raport[17].

(akta kontroli str. 17, 231, 440 )

Pani Burmistrz wyjaśniła*, że: Dokumentacja nie została zaktualizowana z uwagi na brak zmian w otoczeniu. Rekomendacje i zalecenia wynikające z okresowego przeglądu dokumentacji zostaną uwzględnione w aktualizacji w roku 2024. ( ...) W związku z przeprowadzonym audytem przegląd dokumentacji SZBI jest planowany na IV kwartał 2024 r.*

(akta kontroli str. 226-234, 440*)*

8. W Urzędzie w okresie objętym kontrolą został wyznaczony pracownik odpowiedzialny za bezpieczeństwo informacji oraz zapewnienie ciągłości działania, któremu wprost nie zostały przypisane obowiązki w tym zakresie[18]. Jak wyjaśniła Zastępca Burmistrza Pani Aneta Furmańska*: Zadania te nie zostały wprost wpisane do zakresu obowiązków, jednak wynikają one z innych obowiązków m.in.: administrowanie siecią komputerową czy stały nadzór nad systemem informatycznym.*

   W trakcie kontroli został uzupełniony zakres obowiązków pracownika Urzędu w przedmiotowym zakresie.

(akta kontroli str. 226-232, 240)

---

[17] Raport z przeglądu dokumentacji z dnia 26 kwietnia 2023 r.

[18] Zakres obowiązków z dnia 1 czerwca 2007 r. obowiązujący do dnia 3.06.2024 r., zakres obowiązków z dnia 4 czerwca 2024 r. oraz zakres działania Administratora Systemu Informatycznego (ASI), stanowiący załącznik do zarządzenia nr 152/2018 Burmistrza Szydłowca z dnia 26 lipca 2018 r.

Pracownik odpowiedzialny w Urzędzie za te zadania miał ukończone kierunkowe studia wyższe oraz długoletnią praktykę zawodową na stanowisku informatyka. Brał również udział w szkoleniach organizowanych przez Ministerstwo Cyfryzacji w ramach Krajowego Systemu Cyberbezpieczeństwa. Zakres działania Administratora Systemu Informatycznego został mu określony w zarządzeniu Burmistrza Szydłowca[19].

(akta kontroli str. 8-14, 226-232)

9. W Urzędzie wyznaczono Inspektora Ochrony Danych (dalej: IOD)[20]. W dniu 30 kwietnia 2018 r. została zawarta umowa z podmiotem zewnętrznym o powierzenie obowiązków Administratora Bezpieczeństwa Informacji (ABI) oraz bieżącą obsługę w zakresie zagadnień dotyczących ochrony danych osobowych[21]. Umowa określała zakres obowiązków ABI/IOD[22]. Burmistrz Szydłowca dokonał zgłoszenia oraz aktualizacji zgłoszenia wyznaczenia IOD w Urzędzie do Prezesa Urzędu Ochrony Danych Osobowych. Regulamin wykonywania zadań przez IOD został wprowadzony zarządzeniem Burmistrza z dnia 30 grudnia 2019 r.[23]. Wyznaczony w Urzędzie IOD posiadał kwalifikacje do pełnienia tej funkcji.

(akta kontroli str. 221-232, płyta cd-2 plik 20)

10. IOD wykonywał swoje obowiązki w Urzędzie w sposób niezależny, gdyż podlegał bezpośrednio Burmistrzowi, co było zgodne z art. 38 ust. 3 RODO.

(akta kontroli str. 233-234)

11. Zgodnie z art. 21 ust. 1 ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa[24] (dalej: ustawa ksc) w Urzędzie wyznaczono oraz zgłoszono do CSIRT NASK osobę do utrzymywania kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa[25]. Ponadto, na podstawie art. 21 ust. 2 ustawy ksc w dniu 4 czerwca 2024 r. zostało podpisane zarządzenie Burmistrza Szydłowca o wyznaczeniu osoby do utrzymywania kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, w zakresie zadań publicznych zależnych od systemów informacyjnych, realizowanych przez jednostki podległe.

(akta kontroli str. 8-14, płyta cd-1 plik 18-19)

12. W Polityce Bezpieczeństwa Informacji (PBI) wskazano jakie dokumenty powinny być sporządzone w ramach zapewnienia bezpieczeństwa informacji. Dokumentami takimi były m.in. polityki i procedury, określające szczegółowe zasady wdrożenia zabezpieczeń technicznych tj. procedura sporządzania kopii zapasowych oraz procedura zarządzania uprawnieniami do pracy w systemach teleinformatycznych.

    W Urzędzie nie opracowano natomiast:
    1) Regulaminu korzystania z zasobów informatycznych.
    2) Procedury zarządzania sprzętem i oprogramowaniem.

---

19 Zarządzenie Burmistrza Szydłowca nr 153/18 z dnia 26 lipca 2018 r.

20 Zarządzenie nr 81/18 Burmistrza Szydłowca z dnia 17 maja 2018 r.

21 Zgodnie z art. 158 ust. 1 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781), osoba pełniąca w dniu 24 maja 2018 r. funkcję administratora bezpieczeństwa informacji (…), staje się inspektorem ochrony danych osobowych.

22 Obowiązki IOD wynikają z przepisu prawa tj. art. 39 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 RODO).

23 Zarządzenie nr 174/2019 Burmistrza Szydłowca z dnia 30 grudnia 2019 r.

24 Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz. U. z 2024 r. poz. 1077.

25 Zarządzenie nr 75/21 Burmistrza Szydłowca z dnia 12 maja 2021 r. sprawie wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa oraz zarządzenie Burmistrza Szydłowca Nr 71/24 z dnia 5 czerwca 2024 r.

3) Procedury zarządzania konfiguracją.
4) Procedury bezpiecznej utylizacji sprzętu elektronicznego.
5) Procedury zarządzania zmianami i wykonywaniem testów.
6) Polityka fizycznego dostępu do pomieszczeń (w tym serwerowni).
7) Polityki dostępu do infrastruktury informatycznej zewnętrznych podmiotów w związku z realizacją procedur serwisowych.
8) Procedury zarządzania pojemnością przestrzenią dyskową.

(*dalszy opis w sekcji Stwierdzone nieprawidłowości*).

(akta kontroli str. 238-240)

13. Zgodnie z § 19 ust. 2 pkt 2 rozporządzenia KRI w Urzędzie zasoby informatyczne były na bieżąco inwentaryzowane. Dane gromadzone były w specjalnie do tego przeznaczonej aplikacji, która pozwalała na częściową automatyzację tego procesu. Gromadzona była również kopia konfiguracji urządzeń sieciowych. Na podstawie oględzin w zakresie inwentaryzacji sprzętu informatycznego będącego w użytkowaniu UM w Szydłowcu ustalono, że w oprogramowaniu inwentaryzującym znajdowały się informacje o urządzeniach, które zostały wybrane do badania. Urząd posiadał aktualne informacje o danym zasobie informatycznym oraz o jego konfiguracji. Zasoby te były przypisane do osób, które opowiadały za dany sprzęt.

(akta kontroli str. 221-234, 246-252, płyta cd-2 plik 23)

14. Urząd przystąpił do rządowego programu „Cyberbezpieczny Samorząd”[26]. Umowa została zawarta w dniu 7 lipca 2024 . Czas realizacji umowy, zgodnie z Regulaminem Konkursu Grantowego, wynosi 24 miesiące od wejścia w życie umowy o powierzeniu grantu, jednak nie dłużej niż do 30 czerwca 2026 r. Pomiar poprawy cyberbezpieczeństwa przewidziany jest poprzez sporządzenie Ankiety Dojrzałości Cyberbezpieczeństwa w Urzędzie.

(akta kontroli str. 504-533)

Zastępca Burmistrza Pani Aneta Furmańska wyjaśniła, że: *Środki z projektu zostaną przeznaczone na potrzeby w trzech obszarach: organizacyjnym, kompetencyjnym i technicznym.*

(akta kontroli str. 233-234)

Stwierdzone nieprawidłowości

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

1. W Urzędzie nie zidentyfikowano wszystkich posiadanych i przetwarzanych zbiorów danych (innych niż zbiory danych osobowych), co było działaniem nierzetelnym. Ponadto, zidentyfikowanych danych nie sklasyfikowano z uwzględnieniem wymagań prawnych, wartości, krytyczności i wrażliwości na nieuprawnione ujawnienie lub modyfikację o czym mowa w pkt. A.8.1.1 i A.8.2.1 załącznika A normy PN-EN ISO/IEC 27001:2017, stanowiącym, że należy zidentyfikować informacje, aktywa związane z informacjami i środkami przetwarzania informacji oraz sporządzić i utrzymywać ewidencję tych aktywów; informacje powinny być klasyfikowane z uwzględnieniem wymagań prawnych, wartości, krytyczności i wrażliwości na nieuprawnione ujawnienie lub modyfikację.

(akta kontroli str. 435-442)

Zastępca Burmistrza Pani Aneta Furmańska wyjaśniła, że: *Nie dokonano formalnej identyfikacji z powodu braku procedur w tej materii. Osobą odpowiedzialną za ten stan rzeczy jest Informatyk Urzędu Miejskiego. Urząd zamierza dokonać identyfikacji danych po opracowaniu stosownych procedur. Z uwagi na szeroki zakres prac, procedury zostaną wdrożone do końca 2024 roku. Urząd zamierza przypisać*

[26] Wartość umowy - 807.417,72 zł , w tym dofinansowanie z UE 82% a z budżetu państwa 18%.

*zbiorom odpowiedni poziom ochronnych po dokonaniu ich identyfikacji i klasyfikacji zgodnie z ISO 27001.*

(akta kontroli str. 438-439)

2. W Urzędzie nie były prowadzone analizy ryzyka w związku z potrzebą zapewnienia ciągłości działania systemów informatycznych, co było działaniem nierzetelnym.

(akta kontroli str. 4-14)

Zastępca Burmistrza Pani Aneta Furmańska wyjaśniła, że *bezpośrednią przyczyną braku dokumentacji dotyczącej ciągłości działania było pominięcie tego zagadnienia w zakresie obowiązków Informatyka Urzędy Miejskiego. Osobą odpowiedzialną za ten stan rzeczy jest Sekretarz Gminy – bezpośredni przełożony Informatyka. Działania te planowano przy aktualizacji dokumentacji SZBI.*

(akta kontroli str. 502-503)

3. W Urzędzie nie ustanowiono polityk ciągłości działania oraz nie opracowano planów zapewnienia ciągłości działania oraz planów odtworzeniowych, co było działaniem nierzetelnym.

(akta kontroli str. 12-14, 221-234, płyta cd-1 plik 14)

Zastępca Burmistrza Pani Aneta Furmańska wyjaśniła, że: *bezpośrednią przyczyną braku dokumentacji dotyczącej ciągłości działania było pominięcie tego zagadnienia w zakresie obowiązków Informatyka Urzędy Miejskiego. Osobą odpowiedzialną za ten stan rzeczy jest Sekretarz Gminy – bezpośredni przełożony Informatyka. Taka dokumentacja powstanie w ramach realizacji projektu Cyberbezpieczny Samorząd (…) Przewidujemy w obszarze organizacyjnym dokonać przeglądu i aktualizacji obecnie stosowanej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji. W tym celu przeprowadzimy audyt zgodności z wymaganiami uoKSC/KRI poprzez wykwalifikowanych audytorów, którego celem będzie dokonanie aktualizacji dokumentacji i procedur, a także opracowania nowych Polityk Bezpieczeństwa Informacji oraz określenie analizy ryzyka i obsługi incydentów wraz z procedurami określającymi ciągłość działania.*

(akta kontroli str. 502-503)

4. W Urzędzie nie opracowano i nie zawarto w SZBI polityk i procedur takich m.in. jak: regulamin korzystania z zasobów informatycznych, procedura zarządzania sprzętem i oprogramowaniem, procedura zarządzania konfiguracją, procedura bezpiecznej utylizacji sprzętu elektronicznego, procedura zarządzania zmianami i wykonywaniem testów, polityki, fizycznego dostępu do pomieszczeń (w tym serwerowni), polityka dostępu do infrastruktury informatycznej zewnętrznych podmiotów w związku z realizacją procedur serwisowych oraz procedura zarządzania pojemnością przestrzenią dyskową, co było nierzetelne.

(akta kontroli str. 238-240)

Zastępca Burmistrza Pani Aneta Furmańska wyjaśniła, że *dotychczasowa dokumentacja SZBI została opracowana przez Informatyka UM i zawiera tylko wymienione w KRI elementy. Brakujące regulaminy i procedury zostaną opracowane w najbliższym czasie. Burmistrz Szydłowca powołał w tym celu zespół ds. uzupełnienia dokumentacji SZBI. Zarządzenie nr 80/24 z dnia 26 czerwca 2024 r.*

(akta kontroli str. 240-241)

**OCENA CZĄSTKOWA**

W Urzędzie nie zidentyfikowano zbiorów danych (oprócz rejestrów danych osobowych) wymagających ochrony, nie ustanowiono polityki ciągłości działania ani planów ciągłości działania i planów odtworzeniowych, nie przeprowadzono analizy ryzyka w zakresie zapewnienia ciągłości działania oraz nie przeprowadzano testów w tym zakresie, a także nie opracowano i nie zawarto w SZBI polityk i procedur takich

m. in. jak: regulamin korzystania z zasobów informatycznych, procedura zarządzania sprzętem i oprogramowaniem.

W Urzędzie natomiast prawidłowo realizowano zadania dotyczące m.in. ustanowienia i wdrożenia Polityki Bezpieczeństwa Informacji, opracowania dokumentacji z zakresu ochrony danych osobowych oraz gromadzenia aktualnych informacji o zasobach informatycznych obejmujących ich rodzaj i konfigurację.

OBSZAR

## 2. Wdrożone i wykorzystywane rozwiązania organizacyjne i techniczne zapewniające bezpieczeństwo informacji oraz ciągłość działania

Opis stanu faktycznego

1. Urząd zapobiegał możliwości zainstalowania nieautoryzowanego oprogramowania użytkownikom systemów informatycznych niebędących pracownikami służb informatycznych w Urzędzie. W trakcie oględzin podjęto próby zainstalowania nieautoryzowanego oprogramowania na dziesięciu komputerach stacjonarnych. Użytkownicy tych komputerów posiadali stosowne uprawnienia do logowania się do systemu. Na przedmiotowych komputerach zalogowali się pracownicy Urzędu będący ich użytkownikami. Podczas oględzin Informatyk Urzędu wyświetlił opcję wskazującą kto jest zalogowany. Próby te wykazały, że użytkownicy nie mieli możliwości zainstalowania nieautoryzowanego oprogramowania.

   (akta kontroli str. 246-264)

2. W Urzędzie realizowany był obowiązek dotyczący zapewnienia w procesie przetwarzania informacji posiadania stosownych uprawnień do realizowanych zadań. Pracownicy Urzędu uczestniczyli w tym procesie w stopniu adekwatnym do realizowanych przez nich zadań oraz obowiązków. Na losowo wybranej próbie obejmującej 15 pracowników Urzędu, wykonujących zadania w systemach informatycznych ustalono, że pracownicy ci posiadali stosowne uprawnienia oraz, że uprawnienia te były zgodne z realizowanymi czynnościami zapisanymi w zakresach obowiązków[27]. Nadawanie/modyfikowanie/odbieranie uprawnień było realizowane w Urzędzie w oparciu o przyjętą procedurę będącą elementem PBI. Procedura ta opisywała m.in. obowiązki kierownictwa jednostki. Kierownicy poszczególnych komórek organizacyjnych decydowali o uprawnieniach pracowników, a w przypadku zmian zadań realizowanych przez pracownika bezzwłocznie, pisemnie występowali o zmianę uprawnień w systemie IT. Informatyk poinformował, że po otrzymaniu takiego wniosku bezzwłocznie dokonuje stosownych zmian w systemie.

   (akta kontroli str. 246-264, 405-410)

3. Pracownikom, którzy zakończyli zatrudnienie w Urzędzie blokowano dostęp do systemów informatycznych. W badanym okresie sześciu pracowników zakończyło pracę w UM, w tym dwóch, którzy ze względu na charakter wykonywanej pracy nie mieli dostępu do systemów informatycznych Urzędu. Weryfikacją objęto przypadki dotyczące czterech byłych pracowników. Sporządzone zostały formalne wnioski o zamknięcie kont/odebranie uprawnień byłym pracownikom przez przełożonego lub pracownika Wieloosobowego Stanowiska ds. Kadrowych. Trzy wnioski zostały sporządzone bezzwłocznie, a w jednym przypadku po 60 dniach (*dalszy opis w sekcji Stwierdzone nieprawidłowości*).

   (akta kontroli str. 246-264, 405-410)

4. W wyniku oględzin trzech systemów informatycznych zarządzanych przez Urząd stwierdzono, że wprowadzono w nich zabezpieczenia techniczne w celu zapewnienia ochrony przetwarzanych informacji przed nieuprawnionym dostępem. W tym celu w systemach informatycznych Urzędu wykorzystywano identyfikatory użytkowników

[27] W ramach próby znaleźli się także pracownicy na dwóch stanowiskach kierowniczych (naczelnicy).

oraz hasła dostępu o odpowiedniej złożoności. Złożoność hasła polegała na ustanowieniu wymogu wprowadzenia przez użytkownika systemu informatycznego ciągu znaków o określonej długości i złożoności. Oględziny trzech systemów informatycznych zarządzanych przez Urząd pod kątem wymagań dla haseł dostępu do tych systemów wykazały, że wymogi w zakresie złożoności (siły) haseł oraz okresów po jakim hasło powinno być zmienione zostały zachowane. Zweryfikowane w toku oględzin systemy informatyczne wykorzystywane w Urzędzie umożliwiały realizację tych wymogów. W Urzędzie komputery z systemem operacyjnym Windows były zarządzane centralnie w oparciu o mechanizm *Microsoft Active Directory*.

Na podstawie listy identyfikatorów użytkowników ww. trzech badanych systemów pod kątem loginów ustalono, że nazwa pozwala na bezpośrednie powiązanie ich z daną osobą[28]. W trakcie oględzin nie stwierdzono, żeby na dane konto mogło zalogować się kilka osób.

(akta kontroli str. 246-264)

5. W wyniku oględzin dwóch stanowisk pracy w Wydziale Spraw Obywatelskich UM, gdzie załatwiane są sprawy z zakresu wydawania dowodów osobistych stwierdzono, że usytuowanie monitorów komputerowych w miejscach obsługi obywateli uniemożliwiało wgląd do danych wyświetlanych na tych monitorach. Było to zgodne z § 19 ust. 2 pkt 7 rozporządzenia KRI.

   (akta kontroli str. 246-264)

6. Zasady wykonywania pracy zdalnej w Urzędzie zostały opisane w załączniku nr 9 do SZBI, w którym określono mechanizmy gwarantujące bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość.

   (akta kontroli str. 62-65)

   W Urzędzie wprowadzono rozwiązania informatyczne zapewniające bezpieczną pracę użytkowników w formie pracy zdalnej[29]. Pracownicy przeszli szkolenie stanowiskowe. Dane zgromadzone na laptopach zostały zabezpieczenie w sposób uniemożliwiający dostęp do nich osobom nieuprawnionym. Powszechną praktyką pozwalającą na zachowanie poufności informacji w przypadku utraty (zagubienia, kradzieży) urządzenia mobilnego (komputera przenośnego) było szyfrowanie danych zgromadzonych na dysku twardym. W trakcie oględzin losowo wybranych dwóch laptopów potwierdzono, że w Urzędzie stosuje się rozwiązanie polegające na wykorzystywaniu oprogramowania odpowiedzialnego za szyfrowanie danych zgromadzonych na dyskach twardych komputerów przenośnych. Było to zgodne z § 19 ust. 2 pkt 9 i 11 rozporządzenia KRI.

   (akta kontroli str. 246-264)

7. W serwerowni Urzędu zastosowano zabezpieczenia fizyczne w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie. Serwery wykorzystywane przez Urząd były zlokalizowane w wyodrębnionym pomieszczeniu, do którego dostęp posiadał wyłącznie informatyk Urzędu. Nie stwierdzono przypadków aby serwery umieszczono w pokojach pracowników. W trakcie oględzin w serwerowni Urzędu stwierdzono, że pomieszczenie to pełniło funkcję magazynu zużytego sprzętu informatycznego. W serwerowni na regałach znajdowały się m.in. nie związane z przeznaczeniem tego pomieszczenia klawiatury komputerowe. W trakcie kontroli zlikwidowano w serwerowni magazyn zużytego sprzętu informatycznego.

---

[28] Login powstał od połączenia pierwszych liter imienia i nazwiska użytkownika.

[29] W PBI szczegółowo opisano procedurę bezpiecznej pracy zdalnej. Szczegółowo został określony sposób zabezpieczenia i konfiguracji sprzętu IT wykorzystywanego przez Pracowników w trakcie pracy zdalnej. Pracownicy, według oświadczenia Informatyka przeszli szkolenie stanowiskowe.

(akta kontroli str. 246-264)

8. Analiza czterech umów serwisowych zawartych przez Urząd z podmiotami zewnętrznymi w okresie objętym kontrolą wykazała, że zamieszczone w nich zapisy gwarantowały zachowanie bezpieczeństwa informacji w związku z realizacją umowy. Było to zgodne z § 20 ust. 2 pkt 10 starego rozporządzenia KRI, a obecnie § 19 ust. 2 pkt 10 rozporządzenia KRI.

(akta kontroli str. 364-404 )

9. Sprzęt informatyczny Urzędu w okresie objętym kontrolą nie był przekazywany poza Urząd (do serwisu lub poprzez jego zbycie). Jak oświadczył Informatyk, w Urzędzie formalnie nie określono zasad dostępu serwisu do zasobów informatycznych Urzędu. Serwis odbywa się bowiem w siedzibie Urzędu. Stary sprzęt naprawiany był przez informatyka Urzędu a sprzęt objęty gwarancją producenta naprawiany był pod nadzorem informatyka. Wyeksploatowany sprzęt IT Urzędu nie był zbywany, a zużyty był utylizowany.

(akta kontroli str. 246-264)

10. W Urzędzie ustalone zostały procedury w zakresie tworzenia i przechowywania kopii zapasowych. Kopie przechowywano w pokoju Informatyka Urzędu w kasie pancernej. W wyniku oględzin sposobu sporządzania kopii zapasowych i ich przechowywania stwierdzono, że w Urzędzie stale prowadzone są działania w zakresie bieżącego sporządzania kopii zapasowych w środowisku wirtualnym oraz jednego serwera fizycznego. Dla każdej kopii zapasowej została przewidziana retencja danych wypełniając wymogi przechowywania kopii zapasowych określone w zakresie zarządzania danymi osobowymi. W zakresie środowiska wirtualnego sporządzane są kopie dzienne, pełne oraz kopia tygodniowa pełna. Serwer fizyczny ma określone sporządzanie kopii w trybie dziennym (kopia różnicowa) oraz tygodniowym (kopia pełna). Było to zgodne z zapisami zawartymi w Załączniku nr 11 do PBI.

(akta kontroli str. 246-264)

11. W Urzędzie przeprowadzane było regularne kopiowanie danych, które pozwalało na odtworzenie danych/aplikacji. W trakcie oględzin ustalono, że:
    - wszystkie istotne dane posiadane przez Urząd w postaci cyfrowej miały swoje odzwierciedlenie w kopiach zapasowych,
    - procedurę wykonywania kopii zapasowych zawierał Załącznik nr 11 do PBI - *Procedura wykonywanie kopii zapasowych*,
    - kopie zapasowe danych były tworzone zgodnie z zapisami PBI,
    - kopie zapasowe (nośniki z kopiami) były umieszczane w zamkniętych szafach pancernych.

    W toku oględzin wybranego przez kontrolera w sposób celowy systemu informatycznego przeprowadzono z wynikiem pozytywnym test na odzyskiwanie danych z kopii zapasowej przez upoważnionego pracownika. Odtwarzana kopia systemu pochodziła z czerwca 2024 r.

    (akta kontroli str. 246-264)

    W Urzędzie kopie zapasowe były przechowywane w miejscu ich wytwarzania, co w przypadku awarii (zalania, pożaru) stwarzało ryzyko zniszczenia zarówno danych źródłowych, jak i ich kopii *(dalszy opis w sekcji Stwierdzone nieprawidłowości*).

    (akta kontroli str. 246-264)

12. W wyniku oględzin stopnia zajętości przestrzeni dyskowej w trzech serwerach wykorzystywanych przez Urząd stwierdzono, że monitorowana była pojemność pamięci masowych (dysków twardych) wykorzystywanych w serwerach oraz przewidywane przyszłe potrzeby w tym zakresie dla systemów Urzędu. Bieżące

monitorowanie zajętości powierzchni dyskowej serwerów przypisane było do obowiązków Informatyka UM i miało na celu uniknięcie sytuacji zapełnienia dysku twardego danymi, a w konsekwencji znaczącego obniżenia wydajności pracy systemu lub też zaprzestania jego działalności. Monitorowanie zajętości było prowadzone w ramach rutynowych działań administracyjnych.

(akta kontroli str. 246-264)

13. Dla zapewnienia ciągłości działania Urzędu zidentyfikowane zostały w PBI kluczowe elementy infrastruktury i usługi IT oraz ich zabezpieczenie pod kątem wpływu czynników zewnętrznych. W procedurach Urzędu nie wskazano jednak ile czasu zajmie przywrócenie poszczególnych systemów oraz procesów do działania *(dalszy opis w sekcji Stwierdzone nieprawidłowości).*

(akta kontroli str. 246-264)

Stwierdzone nieprawidłowości

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

1. W wyniku weryfikacji dokumentacji dotyczącej czterech byłych pracowników Urzędu ustalono, że w jednym przypadku dopiero po 60 dniach nastąpiło zamknięcie kont/odebranie uprawnień. Było to niezgodne z § 20 ust. 2 pkt 5 rozporządzenia KRI.

(akta kontroli str. 246-264)

Zastępca Burmistrza Pani Aneta Furmańska wyjaśniła, że *Przyczyną zwłoki w przekazaniu danych było niedopatrzenie pracownika Wieloosobowego Stanowiska ds. Kadrowych, spowodowane natłokiem bieżącej pracy w wyniku zmniejszonej obsady, w związku z długotrwałą nieobecnością jednego z pracowników. Pracownicy Wieloosobowego Stanowiska ds. Kadrowych zostali pouczeniu o konieczności niezwłocznego przekazywania informacji dotyczących zmian kadrowych do informatyka UM.*

(akta kontroli str. 405-410)

2. Kopie zapasowe były przechowywane w miejscu ich wytwarzania, co powodowało, że w przypadku awarii (np. zalania, pożaru) zniszczeniu mogą ulec zarówno dane źródłowe, jak i ich kopie. Było to niezgodne z § 19 ust. 2 pkt 7 rozporządzenia KRI.

(akta kontroli str. 246-264)

Zastępca Burmistrza Pani Aneta Furmańska wyjaśniła, że: *Przyczyną tego stanu było założenie w procedurze wykonywania kopii zapasowych, iż replikacja danych do innej lokalizacji spełnia to wymaganie. Osobą odpowiedzialną jest autor procedury – Informatyk UM. Urząd, w przeciągu miesiąca, zakupi dodatkowy sejf do przechowywania nośników, który zostanie zlokalizowanych w innym budynku niż lokalizacja serwerowni.*

(akta kontroli str. 408-410)

3. W procedurach Urzędu nie wskazano ile czasu zajmie przywrócenie poszczególnych systemów oraz procesów do działania. Było to działanie nierzetelne.

(akta kontroli str. 246-264)

Zastępca Burmistrza Pani Aneta Furmańska wyjaśniła, że: *Przyczyną tego stanu jest zbyt ogólnie opisana procedura przywracania systemu informatycznego po awarii. Osobą odpowiedzialną jest autor procedury – Informatyk UM. Procedura w tym zakresie zostanie uzupełniona, tzn. zostanie określony czas na przywrócenie poszczególnych systemów oraz procesów do działania. Procedura zostanie zaktualizowania po opracowaniu polityki ciągłości działania i planów ciągłości działania dotyczących.*

(akta kontroli str. 502-503)

**OCENA CZĄSTKOWA**

W Urzędzie, w okresie objętym kontrolą, podejmowano działania w zakresie zapewnienia bezpieczeństwa informacji m.in. poprzez nadawanie uprawnień pracownikom adekwatnych do realizowanych przez nich zadań, stosowanie w umowach serwisowych zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji, wdrożenie systemu uniemożliwiającego instalację dowolnego oprogramowania użytkownikom nie będącym administratorami systemu, wprowadzenie rozwiązań informatycznych zapewniających bezpieczną pracę użytkowników w formie pracy zdalnej, prawidłowe zabezpieczenie serwerowni, regularne kopiowanie danych i testowanie kopii zapasowych oraz stosowanie w umowach serwisowych zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.

Stwierdzone w tym obszarze nieprawidłowości dotyczyły: zwłoki w przekazaniu przez pracownika Wieloosobowego Stanowiska ds. Kadrowych do Administratora wniosku o zamknięcie uprawnień zwolnionego pracownika, przechowywania kopii zapasowych w miejscu ich wytwarzania oraz niewskazania w procedurach Urzędu czasu przywrócenia poszczególnych systemów oraz procesów do działania.

**OBSZAR**

## 3. Działania w celu zapobiegania incydentom bezpieczeństwa informacji.

Opis stanu faktycznego

1. W Urzędzie w okresie objętym kontrolą nie przeprowadzono okresowych analiz ryzyka utraty integralności, poufności lub dostępności informacji[30] (*dalszy opis w sekcji Stwierdzone nieprawidłowości)*.

(akta kontroli str. 443-446)

2. Procedura w zakresie zgłaszania incydentów naruszenia bezpieczeństwa informacji w Urzędzie była opisana w załączniku nr 14 do SZBI[31]. Sposób postępowania w przypadku wystąpienia incydentu naruszenia ochrony danych osobowych został również opisany w przyjętej w ramach Polityki ochrony danych osobowych procedury pn. *Procedura postępowania w sytuacji naruszenia ochrony danych osobowych*[32] Procedura uwzględniała postanowienia art. 33 i 34 RODO.

(akta kontroli str. 17-101, 435-442)

Zastępca Burmistrza Pani Aneta Furmańska poinformowała, że w Urzędzie w okresie objętym kontrolą nie odnotowano *ujawnienia informacji osobom nieupoważnionym; udostępnienie hasła i loginu innym użytkownikom, złamania zasad polityki bezpieczeństwa informacji, zablokowania strony internetowej urzędu, podejrzenia kradzieży danych czy też kradzieży systemów (laptop, urządzenie przenośne)*.

(akta kontroli str. 435-442)

W okresie objętym kontrolą wystąpiły dwa incydenty bezpieczeństwa informacji. Dotyczyły one systemów zewnętrznych, administrowanych przez podmioty zewnętrzne. W związku z tym w Urzędzie nie było konieczności podejmowania działań korygujących.

(akta kontroli str. 435-442)

Zastępca Burmistrza Pani Aneta Furmańska wyjaśniła, że**:** *W Urzędzie jest przyjęte, aby wszelkie zauważone problemy w działaniu systemów były zgłaszane do Administratora Systemów Informatycznych. I ASI, po analizie, podejmuje dalsze działania. Administrator jest pierwszą linia wsparcia, a gdy problem okaże się*

---

30 W załączniku nr 6 do SZBI opracowano procedurę analizy ryzyka.

31 Zgodnie z § 19 ust. 2 pkt 13 rozporządzenia KRI i art. 22 ustawy o ksc opracowano procedurę pod nazwą Procedura zarzadzania incydentem i zapewnienie obsługi.

32 Zarządzenie nr 173/2019 Burmistrza Szydłowca z dnia 30.12.2019 r. Ostatnia aktualizacja procedury, wersja nr 3 z dnia 14 czerwca 2023 r.

*poważny informowane są władze Urzędu. Formalnie jest to określone w procedurze zarządzania incydentem i zapewnienia obsługi.*

(akta kontroli str. 435-442)

3. W okresie objętym kontrolą w Urzędzie przeprowadzono szkolenia pracowników z zakresu bezpieczeństwa informacji, co było zgodne z § 20 ust. 2 pkt 6 starego rozporządzenia KRI, a obecnie z § 19 ust. 2 pkt 6 rozporządzenia KRI. Zakres tematyczny tych szkoleń obejmował m.in. cyberbezpieczeństwo i ochronę danych osobowych.

(akta kontroli str. 408-410)

4. W Urzędzie przeprowadzony został w roku 2023 okresowy audyt wewnętrzny z zakresu bezpieczeństwa informacji. Audytor odstąpił od wydania rekomendacji. Zastępca Burmistrza Pani Aneta Furmańska wyjaśniła, że: *Audytor wewnętrzny zatrudniony w Urzędzie Miejskim w Szydłowcu posiada kwalifikacje określone w przepisach Ustawy o finansach publicznych. Nie legitymuje się natomiast szczególnym przygotowaniem w zakresie problematyki informatycznej. (…) W celu poprawy wartości audytów bezpieczeństwa informacji, przyszłe audyty w tej materii zostaną zlecone podmiotom posiadającym odpowiednie kompetencje informatyczne. W ramach realizacji projektu w programie Cyberbezpieczny Samorząd, Urząd planuje dokonać przeglądu i aktualizacji obecnie stosowanej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji. W tym celu zostanie przeprowadzony audyt zgodności z wymaganiami uoKSC/KRI przez wykwalifikowanych audytorów.*

(akta kontroli str. 172-189, 221-234, 405-410, 438-442)

Stwierdzone nieprawidłowości

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

W Urzędzie w okresie objętym kontrolą nie przeprowadzono okresowych analiz ryzyka utraty integralności, poufności lub dostępności informacji, co było niezgodne z § 19 ust. 2 pkt 3 rozporządzenia KRI[33].

(akta kontroli str. 443-446)

Zastępca Burmistrza Pani Aneta Furmańska wyjaśniła, że: *W Urzędzie nie była przeprowadzana procedura szacowania ryzyka. Jednak zastosowane rozwiązania techniczne i wielowarstwowe zabezpieczenia skutecznie dbają o bezpieczeństwo informacji zgromadzonej w systemach informatycznych. Bezpośrednią przyczyną braku realizacji procedury analizy ryzyka było duże obciążenie Informatyka bieżącymi zadaniami. Stanowisko ds. informatyki jest stanowiskiem jednoosobowym i szeroki zakres obowiązków powoduje brak czasu na działania analityczne. Osobą odpowiedzialną za brak wykonania procedury jest Informatyk Urzędu Miejskiego. Częściową odpowiedzialność ponosi również Pełnomocnik ds. SZBI za brak nadzoru nad wykonaniem procedury.*

(akta kontroli str. 502-503)

**OCENA CZĄSTKOWA**

W Urzędzie, w okresie objętym kontrolą, podjęto działania w celu zapobiegania incydentom bezpieczeństwa informacji oraz zorganizowano szkolenia pracowników w tym zakresie. Przeprowadzono także okresowy audyt w zakresie bezpieczeństwa informacji.

Nie przeprowadzono okresowych analiz ryzyka utraty integralności, poufności lub dostępności informacji.

[33] Wcześniej w okresie objętym kontrolą obowiązywał w tym zakresie § 20 ust. 2 pkt 3 starego rozporządzenia KRI.

# IV. Wnioski

W związku ze stwierdzonymi nieprawidłowościami, Najwyższa Izba Kontroli na podstawie art. 53 ust. 1 pkt 5 ustawy o NIK przedstawia następujące wnioski:

Wnioski

1. Zidentyfikowanie wszystkich posiadanych i przetwarzanych informacji; sklasyfikowanie ich z uwzględnieniem wymagań prawnych, wartości, krytyczności i wrażliwości na nieuprawnione ujawnienie lub modyfikację; przypisanie informacjom odpowiedniego poziomu ochrony.
2. Prowadzenie analiz ryzyka w związku z potrzebą zachowania ciągłości działania systemów informatycznych Urzędu.
3. Ustanowienie polityk ciągłości działania oraz opracowanie i wdrożenie planów zapewnienia ciągłości działania i planów odtworzeniowych.
4. Opracowanie brakujących regulaminów i procedur dotyczących bezpieczeństwa systemów informatycznych Urzędu.
5. Terminowe sporządzanie i przekazywanie Administratorowi SI wniosków o zamknięcie kont/odebranie uprawnień zwalnianym pracownikom Urzędu.
6. Przechowywanie kopii zapasowych poza miejscem ich wytwarzania.
7. Wskazanie w procedurach Urzędu niezbędnego czasu koniecznego do przywrócenia poszczególnych systemów oraz procesów do działania.
8. Prowadzenie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji i podejmowanie działań minimalizujących stwierdzone ryzyko.

# V. Pozostałe informacje i pouczenia

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

Prawo zgłoszenia zastrzeżeń

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 Departamentu Administracji Publicznej Najwyższej Izby Kontroli. Prawo zgłoszenia zastrzeżeń, zgodnie z art. 61b ust. 2 ustawy o NIK, nie przysługuje do wystąpienia pokontrolnego zmienionego zgodnie z treścią uchwały w sprawie zastrzeżeń.

Obowiązek poinformowania NIK o sposobie wykonania wniosków

Zgodnie z art. 62 ustawy o NIK należy poinformować Najwyższą Izbę Kontroli, w terminie 21 dni od otrzymania wystąpienia pokontrolnego, o sposobie 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.

Warszawa, …… sierpnia 2024 r.

| Kontroler | Najwyższa Izba Kontroli<br>Departament Administracji Publicznej<br>Dyrektor |
|---|---|
| Marek Bieńkowski<br>Doradca ekonomiczny | Bogdan Skwarka |
| ..... | ..... |
| *podpis* | *podpis* |