NAJWYŻSZA IZBA KONTROLI
Delegatura w Katowicach

LKA.410.14.1.2024

Bernard Wilczek
Burmistrz Sośnicowic
ul. Rynek 19
44-153 Sośnicowice

WYSTĄPIENIE POKONTROLNE

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

NAJWYŻSZA IZBA KONTROLI
Delegatura w Katowicach
ul. Powstańców 29, 40-039 Katowice
T +48 32 784 42 00, F +48 32 784 42 30
lka@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana	Urząd Miejski w Sośnicowicach, ul. Rynek 19 (44-153) Sośnicowice[1].
Kierownik jednostki kontrolowanej	Bernard Wilczek, Burmistrz Sośnicowic, od 6 maja 2024 r. do nadal[2]. W okresie objętym kontrolą funkcję kierownika jednostki poprzednio pełnił Leszek Kołodziej, Burmistrz Sośnicowic, od 19 listopada 2018 r.
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 kontroli w 2024 r.[3] (także okresy wcześniejsze w zakresie uczestnictwa w programie Cyfrowa Gmina/Cyfrowy Powiat).
Podstawa prawna podjęcia kontroli	Art. 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[4]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Katowicach
Kontrolerzy	1. Wiesław Pietrzyk, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LKA/131/2024 z 17 czerwca 2024 r. 2. Szymon Gruca, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LKA/132/2024 z 17 czerwca 2024 r. (akta kontroli str.1-8)

[1] Zwany dalej: *„Urzędem”.*
[2] Zwany dalej: *„Burmistrzem”.*
[3] Data zakończenia kontroli w Urzędzie 30 sierpnia 2024 r.
[4] Dz. U. z 2022 r. poz. 623, dalej: ustawa o NIK.

II. Ocena ogólna[5] kontrolowanej działalności

OCENA OGÓLNA

W Urzędzie nie funkcjonował System Zarządzania Bezpieczeństwem Informacji, nie podjęto żadnych działań regulacyjnych mających na celu zapewnienie ciągłości działania Urzędu, nie prowadzono również okresowych analiz ryzyka utraty integralności, poufności lub dostępności informacji, a wykorzystywanym przez Urząd zbiorom danych podlegającym zabezpieczeniu nie przypisano odpowiedniego poziomu ochrony. Opracowano natomiast i wprowadzono do stosowania Politykę Bezpieczeństwa Informacji jednak ww. dokument nie był na bieżąco aktualizowany.

Urząd wdrożył rozwiązania organizacyjne i techniczne w zakresie bezpieczeństwa informacji obejmujące m.in. zapobieganie utracie informacji lub nieuprawnionemu do nich dostępowi, stosowanie zabezpieczeń przed szkodliwym oprogramowaniem, ustanowienie zasad (procedur) bezpiecznej pracy zdalnej, w tym przy przetwarzaniu mobilnym i pracy na odległość, regularne tworzenie kopii zapasowych systemów informatycznych i ich właściwe przechowywanie.

W Urzędzie przeprowadzono audyt wewnętrzny z zakresu bezpieczeństwa informacji. Powołano inspektora ochrony danych posiadającego odpowiednie kwalifikacje do pełnienia tej funkcji oraz sporządzono dokumentację w zakresie ochrony danych osobowych, a także zapewniono szkolenia osób zaangażowanych w proces przetwarzania informacji.

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[6] kontrolowanej działalności

OBSZAR

1. Organizacja bezpieczeństwa informacji i zapewnienia ciągłości działania systemów informatycznych

Opis stanu faktycznego

1.1. Urząd nie dysponował aktualnymi zidentyfikowanymi zgodnie z klasyfikacją określoną w Polskiej normie, zbiorami danych osobowych podlegających zabezpieczeniu.

Do kontroli Urząd przedłożył 11 zbiorów danych zgłoszonych do rejestracji Generalnemu Inspektorowi Ochrony Danych w dniu 16 października 1999 r. i jak wyjaśnił Burmistrz *(…) Od tego czasu nie były aktualizowane".*

Do kontroli przedłożono również dwuczęściowy dokument (nie zawierał daty sporządzenia) pn. *„Zbiór danych osobowych przetwarzanych w sposób tradycyjny"* [18 zbiorów danych] i *„Zbiór danych przetwarzanych w systemie informatycznym"* [38 zbiorów danych]. Zgodnie z treścią adnotacji zawartej na tym dokumencie był on „(…) w trakcie konsultacji i miał być załącznikiem do nowej Polityki bezpieczeństwa informacji i ochrony danych osobowych w Urzędzie[7] a planowane wprowadzenie tego dokumentu określono na przełom trzeciego i czwartego kwartału 2024 r". W trzech kolumnach tego dokumentu zawarto informacje dotyczące nazwy zbioru, zawartości pól informatycznych i użytkowników przetwarzających dany zbiór lub część zbioru (w tej kolumnie wskazano jedynie, że dostęp posiadali jedynie uprawnieni pracownicy Urzędu, lub referatu). Do danych zawartych w ww. zbiorach nie przypisano odpowiedniego

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

[6] Oceny cząstkowe to oceny działalności w poszczególnych obszarach badań kontrolnych. Ocena cząstkowa może być sformułowana jako ocena pozytywna, ocena negatywna albo ocena w formie opisowej.

[7] Zwana dalej: *„PBI".*

poziomu ochrony, zgodnego z ich wagą, *co przedstawiono w obszarze pierwszym w sekcji Stwierdzone nieprawidłowości*.

(akta kontroli str. 9-16, 19-20, 337-341)

1.2. W Urzędzie nie funkcjonował System Zarządzania Bezpieczeństwem Informacji[8] o którym mowa w § 19 ust. 1 - 3 rozporządzenia Rady Ministrów z dnia 12 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[9], co przedstawiono w obszarze pierwszym w sekcji *Stwierdzone nieprawidłowości.*

W Urzędzie funkcjonowała PBI, wprowadzona zarządzeniem Burmistrza z dnia 20 maja 2019 r.[10]. W czterech działach tego dokumentu zawarto:

- Zasady i kwestie podstawowe;
- Ochronę danych osobowych w Urzędzie – zasady ogólne;
- Obsługę praw jednostki i realizację obowiązków informacyjnych;
- Bezpieczeństwo i przetwarzanie danych.

W PBI nie zawarto wszystkich elementów określonych w § 1 pkt 15 rozporządzenia KRI, takich jak procedury bezpieczeństwa wraz z ich planem wdrożenia i egzekwowania, co przedstawiono w obszarze pierwszym w sekcji *Stwierdzone nieprawidłowości.*

W zarządzeniu wprowadzającym PBI, Burmistrz zobowiązał każdą osobę przetwarzającą dane osobowe do zapoznania się z treścią PBI i zobowiązał wszystkich pracowników Urzędu do stosowania zasad w niej określonych przy przetwarzaniu danych osobowych.

Analiza dokumentacji kadrowej 15 pracowników wykazała, że złożyli oni oświadczenia, że zapoznali się z *„(…) przepisami dotyczącymi ochrony danych osobowych, w szczególności z przepisami Rozporządzenia Parlamentu Europejskiego nr 2016/679 (…)[11], Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[12] oraz wprowadzonymi i wdrożonymi do stosowania przez Administratora Danych[13] procedurami określonymi w Polityce Bezpieczeństwa oraz w Instrukcji zarządzania systemem informatycznym".*

(akta kontroli str.: 17-19a, 21-26, 48-81, 79-81, 92-94, 180-196, 284-286)

Za PBI oraz inne dokumenty służące ochronie danych jak wyjaśnił Burmistrz *„(…) odpowiadał Inspektor Danych Osobowych[14] (firma zewnętrzna), z ramienia Urzędu osobą, która zgłaszała wątpliwości, wnosiła o utworzenie dokumentów i wprowadzała je w formalny obieg (Zarządzenia Burmistrza)"* była inspektor do spraw promocji, której Burmistrz powierzył wykonywanie dodatkowych zadań

[8] Zwany dalej: *„SZBI".*

[9] Dz.U. z 2024 r. poz. 773. W okresie objętym kontrolą był to przepis § 20 ust. 1-3 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 (Dz. U. z 2017 r. poz. 2247)., zwane dalej: *„rozporządzeniem KRI'.*

[10] Nr zarządzenia 63/2019.

[11] Rozporządzenia Parlamentu Europejskiego i Rady (UE) 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). Dz. Urz. UE L 119 z 04.05.2016, str. 1, ze zm., zwane dalej: *„RODO".*

[12] Dz.U. z 2019 r. poz. 1781, zwana dalej: *„UODO".*

[13] Zwany dalej: *„ADO".*

[14] Zwany dalej: *„IOD".*

związanych z zakresu ochrony danych osobowych, natomiast za ochronę danych osobowych w kwestiach technicznych/ informatycznych odpowiadał inspektor do spraw informatyzacji.

(akta kontroli str.: 17-19a)

Ponadto w Urzędzie obowiązywał szereg odrębnych dokumentów mających wpływ na bezpieczeństwo informacji takich jak:

- Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych, wprowadzona 21 lutego 2019 r.[15];
- Procedura powierzenia danych osobowych w Urzędzie wprowadzona 21 lutego 2019 r.[16];
- Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie wprowadzona 20 maja 2019 r.[17];
- Analiza ryzyka, w tym karty ryzyka wykonane w okresie od 25 kwietnia do 16 maja 2022 r.;
- Instrukcja obsługi serwerowni, wprowadzona 19 grudnia 2022 r.[18];
- Procedura ochrony danych osobowych w ramach pracy zdalnej obowiązująca w Urzędzie, wprowadzona 15 września 2023 r.[19];
- Rejestr czynności przetwarzania prowadzony od września 2023 r.;
- Procedura audytów wewnętrznych w zakresie bezpieczeństwa informacji obowiązująca w Urzędzie, wprowadzona 25 kwietnia 2024 r.[20];
- Procedura szkolenia osób zaangażowanych w proces przetwarzania informacji obowiązująca w Urzędzie, wprowadzona 25 kwietnia 2024 r.[21];
- Procedura nadawania, zmiany i odbierania uprawnień do przetwarzania danych w systemie informatycznym w Urzędzie, wprowadzona 10 lipca 2024 r.[22];
- Instrukcja tworzenia kopii zapasowych zbiorów danych, oprogramowania oraz systemów służących do przetwarzania danych w Urzędzie, wprowadzona 10 lipca 2024 r.[23].

(akta kontroli str. 21-26, 38-47, 95-98, 118-179, 287-293, 444)

1.3 W Urzędzie sporządzono dokumentację w zakresie bezpieczeństwa danych osobowych, która stanowiła elementy składowe PBI takie jak wzór oświadczenia pracownika o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych, w tym z wdrożonymi przez ADO do stosowania zasadami określonymi w PBI oraz w Instrukcji zsi; ewidencję osób upoważnionych do przetwarzania danych osobowych; wykaz pomieszczeń stanowiących obszar przetwarzania danych osobowych Urzędu i Regulamin ochrony danych osobowych w Urzędzie.

W PBI określono m.in. zasady i metody minimalizacji, w tym zasadę zarządzania adekwatnością danych, zasadę reglamentacji i zarządzania dostępem do danych, zasadę zarządzania okresem przechowywania danych i weryfikacji

[15] Nr zarządzenia 20/2019
[16] Nr zarządzenia 21/2019.
[17] Zwana dalej: *„Instrukcją zarządzania zsi”.*
[18] Nr zarządzenia 203/2022.
[19] Nr zarządzenia 119/2023.
[20] Nr zarządzenia 69/2024.
[21] Nr zarządzenia 68/2024.
[22] Nr zarządzenia 118/2024, zwana dalej: *„Procedurą nadawania uprawnień”.*
[23] Nr zarządzenia 119/2024, zwana dalej: *„instrukcją kopii zapasowych”.*

dalszej przydatności danych oraz zawarto informację dotyczącą realizacji przez Urząd obowiązku informacyjnego w stosunku do osób, których dane były przetwarzane.

Zgodnie z postanowieniami PBI, ADO prowadził w formie pisemnej i elektronicznej Rejestr czynności przetwarzania danych osobowych, który był narzędziem rozliczania zgodności z ochroną danych w Urzędzie i był dokumentem opisującym, zgodnie z art. 30 RODO, czynności przetwarzania dokonywane przez ADO.

(akta kontroli str.48,78, 92-94, 278-283)

1.4 W zakresie prowadzonych analiz ryzyka w związku z potrzebą zachowania ciągłości działania systemów informatycznych oraz utraty integralności, poufności lub dostępności informacji oraz podejmowania dalszych działań związanych z wynikami tej analizy, zgodnie z zapisami zawartymi w dziale IV PBI, ADO stosował środki bezpieczeństwa ustalone w ramach analiz ryzyka i adekwatności środków bezpieczeństwa oraz ocen skutków dla ochrony danych osobowych.

W ramach środków bezpieczeństwa – analizy zagrożeń i ryzyk występujących przy przetwarzaniu danych osobowych określono charakterystykę możliwych zagrożeń, takich jak:

- zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu), których występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu,
- zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki przetwarzających dane, pozostawienie danych lub pomieszczeń bez nadzoru, błędy operatorów systemu, awarie sprzętowe, błędy oprogramowania), przy których może dojść do zniszczenia danych lub naruszenia ich poufności,
- zagrożenia zamierzone, świadome i celowe – najpoważniejsze zagrożenia, gdzie występują naruszenia poufności danych. Zagrożenia te można podzielić na: nieuprawniony dostęp z zewnątrz (włamanie), nieuprawniony dostęp do danych w wewnątrz (przez osoby nieuprawnione).

Stosownie do wymagań określonych w § 19 pkt 2 ppkt 3 rozporządzenia KRI w Urzędzie sporządzono analizę ryzyka bezpieczeństwa informacji, w ramach której w okresie od 25 kwietnia do 16 maja 2022 r. sporządzono 18 kart ryzyk, z których wynikało, że prawdopodobieństwo wystąpienia ryzyka utraty ciągłości, integralności, poufności lub dostępności informacji zostało zidentyfikowane i opisane.

W reakcji na ww. ryzyka zalecono zaplanowanie i ewentualne podjęcie działań mających na celu zmniejszenie ryzyka, lub zapewnienie, że ryzyko pozostanie najwyżej na tym samym poziomie. We wszystkich przypadkach przyjęto działania zapobiegawcze (mechanizmy kontrolne) w celu redukcji ryzyka, lecz nie dokonano ponownej oceny Analizy ryzyka w celu sprawdzenia skuteczności przyjętych mechanizmów kontrolnych, co przedstawiono w obszarze pierwszym w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 48-78, 135-179)

W sprawie zapoznania pracowników z ww. Analizą ryzyka, Burmistrz wyjaśnił, że została ona przekazana kierownictwu Urzędu oraz zakomunikowana pracownikom.

(akta kontroli str. 337-349)

1.5 W Urzędzie nie ustanowiono polityki ciągłości działania określającej założenia, zakres oraz podstawowe zasady zarządzania ciągłością działania, co przedstawiono w obszarze pierwszym w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str.337-342)

1.6 W Urzędzie nie opracowano i nie wdrożono Planu zapewnienia ciągłości działania ani planów odtworzeniowych, co przedstawiono w obszarze pierwszym w sekcji *Stwierdzone nieprawidłowości.*

W sprawie określenia akceptowalnego czasu na przywrócenie ciągłości działania systemów informatycznych Urzędu, Burmistrz wyjaśnił, że *„Nie posiadamy szacunków dotyczących czasu przywracania poszczególnych systemów i procesów działania".*

(akta kontroli str.35, 37, 337-342)

1.7 Biorąc pod uwagę, że w Urzędzie nie zostały ustalone polityki ciągłości działania i nie opracowano planów zapewnienia ciągłości działania dokumenty te nie podlegały testowaniu bądź treningowi.

Dopiero w Instrukcji tworzenia kopii zapasowych wprowadzonej w trakcie kontroli w pkt 1 ppkt 7 zapisano, że kopie zapasowe zbiorów danych należy okresowo sprawdzać pod kątem ich przydatności do odtworzenia w przypadku awarii systemu, co przedstawiono w obszarze pierwszym w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 15-26, 44-47, 65-72)

1.8 W okresie objętym kontrolą w PBI dokonano jednej zmiany, która dotyczyła wprowadzenia zarządzeniem Burmistrza z dnia 4 sierpnia 2022 r.[24], Procedury rejestracji i inwentaryzacji oprogramowania i sprzętu komputerowego.

Poza ww. zmianą PBI nie była aktualizowana, co przedstawiono w obszarze pierwszym w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 79-81)

1.9 W Urzędzie nie wyznaczono pracowników odpowiedzialnych za bezpieczeństwo informacji oraz zapewnienie ciągłości działania, co przedstawiono w obszarze pierwszym w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 339-341)

1.10 Zgodnie z art. 37 ust 1 lit. a rozporządzenia RODO, Burmistrz wyznaczył IOD[25].

IOD legitymował się tytułem Audytora wewnętrznego SZBI zgodnie z normą PN-EN ISO/IEC 27001:2017. Ponadto ww. ukończył studia podyplomowe w zakresie IOD, posiadał następujące certyfikaty: ukończenia kursu IOD; ukończenia warsztatów IOD i posiadania kompetencji w zakresie pełnienia funkcji IOD.

W okresie objętym kontrolą Urząd zawarł dwie umowy[26] z podmiotem zewnętrznym na świadczenie przez Wykonawcę na rzecz ADO usług związanych z realizacją zadań ochrony danych osobowych oraz zadań przypisanych IOD, zgodnie z przepisami ustawy UODO, RODO i innymi obowiązującymi przepisami prawa.

W obydwu zawartych umowach w § 1 pkt 3, Wykonawcy przypisano realizację takich zadań jak nadzorowanie systemu ochrony danych osobowych w Urzędzie, w tym:

[24] Zarządzenie nr 118/2022, zwana dalej: *„Procedurą inwentaryzacyjną".*
[25] Dz.U. z 2018 r. poz. 1000.
[26] Umowa nr UM/272/4/2023 zawarta w dniu 2 stycznia 2023 r. i umowa nr UM/272/48/2024 zawarta w dniu 12 stycznia 2024 r. Zgodnie z zawartymi umowami Zleceniobiorca wykonywał usługi odpowiednio w okresie od 1 stycznia do 31 grudnia 2023 r. i od dnia zawarcia umowy do 31 grudnia 2024 r.

1) informowanie ADO, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzania im w tej sprawie,
2) monitorowanie przestrzegania RODO, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk ADO lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty,
3) udzielanie na żądanie ADO zaleceń, co do oceny skutków dla ochrony danych osobowych oraz monitorowanie ich wykonania zgodnie z RODO,
4) pomoc w prowadzeniu rejestru czynności przetwarzania danych osobowych,
5) współpraca z organem nadzorczym,
6) zgłoszenie naruszenia bezpieczeństwa do organu nadzoru oraz osób, których dane dotyczą,
7) pomoc w prowadzenia rejestru naruszeń ochrony danych osobowych,
8) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w RODO (art. 36) oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach,
9) pełnienie funkcji punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz wykonywaniem praw przysługujących im na mocy RODO oraz innych przepisów,
10) pełnienie funkcji inspektora ochrony danych osobowych.

Przy świadczeniu usług objętych treścią ww. umów na Wykonawcę w § 3 nałożono obowiązek zachowania najwyższej staranności wymaganej ze względu na zawodowy charakter prowadzonej działalności, w tym przestrzegania obowiązujących przepisów prawa oraz przepisów wewnętrznych obowiązujących ADO.

Zgodnie z § 8 pkt 1 w obydwu umowach w zakresie poufności zapisano, że w czasie obowiązywania umów, jak i po ich wygaśnięciu lub rozwiązaniu lub w przypadku odstąpienia od umów, Wykonawca zobowiązany będzie do zachowania poufności wszelkich informacji dotyczących ADO, uzyskanych w trakcie realizacji usług, w szczególności tych prawnie chronionych. Wykonawca będzie chronić informacje i dokumenty, dane osobowe, w tym także w formie elektronicznej, wytworzone dla celów realizacji niniejszych umów, przed zniszczeniem, uszkodzeniem lub nieupoważnionym dostępem i rozpowszechnianiem.

Ww. zapisy były zgodne w wymogami określonymi w art. 37 ust. 1 lit. a i ust. 5 oraz w art. 39 ust. 1 i ust. 2 RODO.

(akta kontroli str. 291-317)

1.11 W okresie objętym kontrolą IOD, świadczył na rzecz ADO usługi związane z realizacją zadań ochrony danych osobowych oraz zadań przypisanych IOD w latach 2023-2024, na podstawie dwóch umów zawartych z podmiotem zewnętrznym, odpowiednio 2 stycznia 2023 r. i 12 stycznia 2024 r.

W umowach zapisano, że ADO zapewnia organizacyjną odrębność IOD, w celu niezależnego wykonywania przez niego zadań. Ustalono, że wystąpił konflikt interesów, bowiem IOD brał udział w opracowaniu raportu z Audytu

bezpieczeństwa informacji (KRI) w Urzędzie, co przedstawiono w obszarze pierwszym w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 99, 304-317, 342-344)

1.12 W sprawie wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, Burmistrz wyjaśnił, że zgłoszono osobę do kontaktu z Zespołem Reagowania na Incydenty Bezpieczeństwa Komputerowego[27] *„(…) na podstawie polecenia ustnego ówczesnego Burmistrza (…). Zgłoszenie nastąpiło 14 marca 2022 r., gdyż w trakcie rutynowego przeglądu dokumentacji nie stwierdzono obecności dokumentu potwierdzającego wcześniejsze zgłoszenie osoby do kontaktu z CSIRT GOV".*

Ustalono, że formularz zgłoszenia osoby wyznaczonej do kontaktów z CSIRT GOV został zgodnie z instrukcją przesłany w formie załącznika do wiadomości e-mailem w dniu 14 marca 2022 r.

Stosownie do art. 22 ust. 1 pkt 5 ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa[28], zgłoszenie obejmowało dane osoby wyznaczonej do kontaktu (imię i nazwisko), numer telefonu oraz adres poczty elektronicznej (określono dostępność w przedziale czasowym). Z uwagi na brak dokumentu potwierdzającego wyznaczenie ww. osoby, nie było możliwości sprawdzenia czy Urząd dochował wymaganego 14 dniowego terminu na zgłoszenie, od chwili wyznaczenia tej osoby.

W zakresie wyznaczenia osoby do utrzymywania ww. kontaktów dotyczących zadań publicznych zależnych od systemów informacyjnych, realizowanych przez jednostki organizacyjne Urzędu oraz przez jednostki jemu podległe lub przez niego nadzorowane Burmistrz wyjaśnił, że *„Urząd Miejski nie posiada jednostek podległych"* oraz że *„Urząd nie posiada informacji czy jednostki organizacyjne wyznaczyły osoby do utrzymywania kontaktów z CSIRT GOV"*.

(akta kontroli str.318-322)

1.13 W PBI nie zawarto katalogu dokumentów (polityki, procedury, instrukcje), które powinny być sporządzone w zakresie zapewnienia bezpieczeństwa informacji. Taka dokumentacja została sporządzona w formie odrębnych procedur i instrukcji, co szczegółowo opisano powyżej w pkt 1.2.

(akta kontroli str. 21-26, 38-47, 95-98, 118-179, 287-293)

1.14 Oględziny w zakresie inwentaryzacji sprzętu informatycznego obejmujące badanie dziesięciu komputerów, jednego serwera, dwóch laptopów, jednego routera i jednej drukarki wykazały, że Urząd posiadał aktualne informacje o posiadanych zasobach informatycznych, w tym informacje o ich rodzaju, konfiguracji, lokalizacji oraz osobach odpowiedzialnych za sprzęt. Urząd inwentaryzował sprzęt w formie elektronicznej wykorzystując do tego celu specjalistyczny program (System bezpieczeństwa i administracji).

Ustalono, że w inwentaryzacji nie ujęto jednego routera. W zakresie inwentaryzacji pozostałego sprzętu ustaleń dokonano na podstawie adresów MAC (serwer i komputery) nazwy i modelu (drukarka), bowiem tylko jednemu komputerowi nadano numer inwentarzowy, co zostało opisane w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str.79-81, 326-336)

[27] Zwany dalej.: *„CSIRT GOV".*
[28] Dz. U. z 2024 r. poz. 1077, zwana dalej: *„ustawą o ksc".*

1.15 W dniu 14 grudnia 2023 r. Urząd[29] w ramach wzmocnienia krajowego systemu cyberbezpieczeństwa złożył wniosek w konkursie grantowym do Projektu „Cyberbezpieczny Samorząd”[30]. W dniu 29 sierpnia 2024 r. beneficjent zawarł z Centrum Projektów Polska Cyfrowa umowę na powierzenie grantu[31].

Wartość umowy zgodnie ze złożonym wnioskiem o przyznanie grantu będzie wynosić 580 600,0 zł, w tym kwota dofinansowania wyniesie 528 346,24 zł, a wkład własny Gminy będzie wynosił 52 253,76 zł.

W ramach realizacji tej umowy zaplanowano wydatkowanie środków finansowych w ramach realizacji dwóch zadań, tj.:

- Zadanie pierwsze obejmujące zakup sprzętu i oprogramowania wraz ze szkoleniem z dostarczonej technologii, w tym:
  - wdrożenie wysokodostępnej platformy serwerowej;
  - wdrożenie systemu backupu z biblioteką taśmową i wdrożenie systemu backupu HDD;
  - wdrożenie oprogramowania do tworzenia i zarządzania kopiami zapasowymi;
  - wdrożenie technologii Active Directory w celu sprawniejszego zarządzania zasobami danych użytkowników – usługa wraz z dostawą 50 szt. Licencji dostępowych;
  - wdrożenie systemu EDR dla 50 stanowisk – licencja na 24 miesiące;
  - wdrożenie zasilania awaryjnego z agregatu prądotwórczego z automatycznym rozruchem zaniku zasilania sieciowego;
  - zakup dwóch UPS dla infrastruktury sieciowej i zakup jednego UPS dla infrastruktury serwerowej.
- Zadanie drugie obejmujące zakup usługi aktualizacji i szkolenia pracowników w zakresie SZBI, w tym:
  - ankieta dojrzałości;
  - aktualizacja SZBI;
  - szkolenia dla 50 pracowników w zakresie cyberbezpieczeństwa.

Okres realizacji umowy ustalono na 24 miesiące liczone od dnia wejścia w życie umowy, ale nie dłużej niż do 30 czerwca 2026 r.

W § 7 pkt 1 Umowy, beneficjent został zobowiązany do pomiaru wartości osiągniętych w wyniku realizacji Projektu, zamieszczonych we wniosku o przyznanie grantu, tj. poprawy bezpieczeństwa w obszarze organizacyjnym, technicznym i kompetencyjnym. Natomiast w pkt 2 beneficjent został zobowiązany do przekazania informacji o postępie rzeczowym realizacji Projektu w formie wskazanej przez Operatora w terminie 30 dni następujących po upływie 12 miesięcy od podpisania umowy przy wykorzystaniu transzy pierwszej oraz w terminie 30 dni następujących po upływie 18 miesięcy od dnia podpisania umowy przy wykorzystaniu transzy drugiej.

(akta kontroli str. 17-18, 27-33, 197-228)

[29] Zwany dalej: *„beneficjentem”.*

[30] Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC); Priorytet II: Zaawansowane usługi cyfrowe; Działanie 2.2. Projekt o numerze FERC.02.02-CS.01-001/23.

[31] Umowa została przesłana do podpisania w wersji elektronicznej do Urzędu w dniu 30 lipca 2024 r., numer grantu o numerze FERC.02.02-CS.01-001/23/2413/FERC.02.02-CS.01-001/23/2024.

Stwierdzone nieprawidłowości

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

1. Sklasyfikowanym zbiorom danych przetwarzanych w Urzędzie nie przypisano odpowiedniego poziomu ochrony. Brak działań w tym zakresie należy uznać jako nierzetelne. Ponadto stanowiło to naruszenie pkt. A.8.1.1 i A.8.2.1 załącznika A normy PN-EN ISO/IEC 27001:2017, która stanowiła, 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.

   Burmistrz wyjaśnił, że zbiory nie były aktualizowane i nie dysponuje *„(...) żadnym aktualnym zestawieniem "zbioru danych i informacji będących w posiadaniu Urzędu i jednocześnie przez Urząd przetwarzanych, sklasyfikowanych z uwzględnieniem wymagań prawnych wartości, krytyczności i wrażliwości na nieuprawnione ujawnienie lub modyfikację".* Dalej ww. wyjaśnił, że przedstawione do kontroli zbiory danych są dokumentem wzorcowym przygotowanym *„(…) w celu zinwentaryzowania i sklasyfikowania przetwarzanych informacji w odpowiednich referatach przez ich pracowników. W ślad za nim zostanie przekazana pracownikom ankieta, w której pracownicy określą zbiory danych przez nich przetwarzane. Ankiety zostaną zweryfikowane i utworzone zostaną bazy danych" „(…) Wskazane (…) Zbiory danych stworzone były na potrzeby kontroli i obowiązują do dziś. W ramach projektu „Cyberbezpieczny samorząd" zostaną zaktualizowane zbiory danych".*

   NIK zwraca uwagę, że w toku kontroli nie przedstawiono żadnego dokumentu na potwierdzenie, że przedstawione bazy danych zostały formalnie wprowadzone do stosowania.

   (akta kontroli str. 9-16, 19-20, 337-341)

2. W Urzędzie nie funkcjonował SZBI, co stanowiło naruszenie § 19 ust. 1 rozporządzenia KRI, który stanowił, 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, w związku z ust. 3 tego rozporządzenia, który stanowił, że wymagania określone w ust. 1 i 2 uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą, w tym: 1) PN-ISO/IEC 27002 - w odniesieniu do ustanawiania zabezpieczeń; 2) PN-ISO/IEC 27005 - w odniesieniu do zarządzania ryzykiem.

   Burmistrz wyjaśnił, że *„Oficjalnie w Urzędzie nie funkcjonuje SZBI. Funkcjonuje jednak PBI oraz odrębne procedury"*. Dalej ww. wyjaśnił, że *„(…) SZBI, który ma zostać wprowadzony w IV kwartale roku, i Zbiór Danych Osobowych będzie jedną z jego składowych. (…) SZBI jest w trakcie tworzenia, a tymczasem jego składowe funkcjonują w Urzędzie w ramach PBI i poszczególnych procedur."*

NIK wskazuje, że przywołane w wyjaśnieniach odrębne procedury nie tworzą spójnego, usystematyzowanego systemu, co nie pozwala na zrealizowanie wymogów określonych w § 19 ust. 1 ww. rozporządzenia.

(akta kontroli str. 17-19a, 21-26, 48-81, 79-81, 92-94, 180-196, 284-286, 337-341)

3. W PBI nie zawarto wszystkich elementów określonych w § 2 pkt 15 rozporządzenia KRI, który stanowił, że użyte w rozporządzeniu określenia oznaczają: polityka bezpieczeństwa informacji - zestaw efektywnych, udokumentowanych zasad i procedur bezpieczeństwa wraz z ich planem wdrożenia i egzekwowania. PBI nie była aktualizowana, co stanowiło naruszenie § 19 ust 2 pkt 1, który stanowił, o zapewnieniu aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia. Natomiast w zakresie aktualizacji ww. dokumentu, stosownie do załącznika A PN-ISO/IEC 27001:2017, punkt A.5.1.2., PBI należy poddawać przeglądom w zaplanowanych odstępach czasu lub wtedy, gdy wystąpią istotne zmiany, aby zapewnić, że nadal są właściwe, adekwatne i skuteczne.

   Biorąc pod uwagę, że od ostatniej aktualizacji PBI w 2022 r. w Urzędzie wprowadzono odrębnie cztery procedury oraz dwie instrukcje, brak działań w celu zaktualizowania PBI w ww. zakresie należy ocenić jako nierzetelność[32].

   Burmistrz wyjaśnił w tej sprawie, że *„Funkcjonująca w UM Sośnicowice Polityka Bezpieczeństwa została stworzona przez zewnętrzną firmę obsługującą UM w zakresie ochrony danych i pełnienia funkcji IOD w latach jej tworzenia. Obecna firma pełniąca ww. usługi jest w trakcie modyfikacji i dostosowania do obowiązujących przepisów prawa"*

   (akta kontroli str. 48-78, 337-341)

4. Niedokonanie ponownej oceny 18 kart ryzyka zawartych w Analizie ryzyka, w których przyjęto do realizacji od czterech do 13 działań zapobiegawczych (mechanizmów kontrolnych) w celu redukcji ryzyk oraz zalecono podjęcie działań w zakresie zmniejszenia ryzyk lub co najmniej, utrzymania ich na tym samym poziomie. Pomimo takich zapisów od 2022 roku nie dokonano ponownej oceny w celu sprawdzenia adekwatności i skuteczności przyjętych mechanizmów kontrolnych. Brak działań w tym zakresie należy uznać jako nierzetelność.

   W tej sprawie Burmistrz wyjaśnił, że *„Karty analizy ryzyka nie były aktualizowane od 2022 r. ze względu na znikome zmiany sprzętowe oraz organizacyjne urzędu. Analiza ryzyka zostanie przeprowadzona po wdrożeniu rozwiązań przewidzianych w projekcie grantowym „Cyberbezpieczny Samorząd".*

   (akta kontroli str. 48-78, 135-179, 320-342)

5. Nieustanowienie Polityki ciągłości działania określającej założenia, zakres oraz podstawowe zasady zarządzania ciągłością działania i w rezultacie: nieopracowanie Planu zapewnienia ciągłości działania ani planów odtworzeniowych i nie określenie akceptowalnego czasu na przywrócenie ciągłości działania systemów informatycznych; nietestowanie i niepoddanie

[32] Sprawy dotyczące nadawania uprawnień i tworzenia kopii zapasowych zostały w niewielkim stopniu opisane w PBI w części II, w § 1 i w § 4.

treningowi Polityki ciągłości działania; niewyznaczenie pracowników odpowiedzialnych za bezpieczeństwo informacji oraz zapewnienie ciągłości działania. Niepodjęcie działań ww. zakresie należy uznać jako nierzetelność.

Celem Polityki ciągłości działania jest określenie założeń, zakresu oraz podstawowych zasad zarządzania ciągłością działania oraz zdefiniowanie, w jaki sposób Urząd zapewni, że spełnione będą wszystkie warunki umożliwiające odtworzenie działalności po katastrofie lub innym incydencie zakłócającym działanie. Celem zarządzania ciągłością działania jest identyfikacja potencjalnych zagrożeń dla urzędu, określenie wpływu, jaki zagrożenia te mogą wywrzeć na działalności jednostki oraz zapewnienie odpowiedniego przygotowania urzędu na sytuacje awaryjne, dające możliwość efektywnego reagowania na sytuacje awaryjne i zapewnienie dalszego ciągłego działania Urzędu. Dokument ten stanowi podstawę opracowania Planu zapewnienia ciągłości działania oraz planów odtworzeniowych.

Stosownie do ustalonej normy określonej w załączniku A PN-ISO/IEC 27001:2017, pkt A.17.1.1. pkt A.17.1.2 i pkt 17.1.3., przy planowaniu ciągłości bezpieczeństwa informacji Urząd powinien określić wymagania dotyczące bezpieczeństwa informacji i ciągłości zarządzania bezpieczeństwem informacji w niekorzystnych sytuacjach np. w czasie kryzysu lub katastrofy, przy wdrażaniu ciągłości bezpieczeństwa Urząd powinien ustanowić, udokumentować, wdrożyć i utrzymywać procesy, procedury i zabezpieczenia dla zapewnienia w niekorzystnej sytuacji wymaganego poziomu ciągłości bezpieczeństwa informacji oraz przy weryfikowaniu, przeglądzie i ocenie ciągłości bezpieczeństwa informacji Urząd powinien weryfikować ustanowione i wdrożone zabezpieczenia ciągłości bezpieczeństwa informacji w regularnych odstępach czasu celem zapewnienia ich aktualności i skuteczności w niekorzystnych sytuacjach.

W złożonych wyjaśnieniach Burmistrz potwierdził fakt, że działania w ww. zakresie nie zostały podjęte, jednak nie wskazał przyczyn tych zaniechań.

NIK wskazuje, że w dziale czwartym PBI w pkt 4 lit. d) Analizy ryzyka i adekwatności środków bezpieczeństwa zapisano w zakresie ciągłości działania, że ADO może ustalić przydatność i stosować takie środki i podejście jak środki zapewnienia ciągłości działania i zapobiegania skutkom katastrof, czyli zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.

(akta kontroli str. 62, 339-341)

6. Niezinwentaryzowanie jednego routera oraz nienadanie w aplikacji inwetaryzacyjnej numerów inwentarzowych dla 14 zbadanych sprzętów stanowiło naruszenie postanowień pkt 8 ppkt 2, pkt 9 ppkt 2, pkt 10 ppkt 2, pkt 11, Procedury inwentaryzacyjnej.

   Burmistrz wyjaśnił w tej sprawie, że *„Nie nadano numerów inwentaryzacyjnych sprzętowi przez niedopatrzenie pracownika i zostanie niezwłocznie uzupełnione. Routery również zostaną zinwentaryzowane w oprogramowaniu IT Manager”.*

   (akta kontroli str.79-81, 326-336, 342-345)

7. W latach 2023-2024 IOD, któremu powierzono świadczenie na rzecz ADO usługi związanej z realizacją zadań ochrony danych osobowych, zadań przypisanych IOD, na podstawie zarządzenia Burmistrza z 2020 r. oraz powierzenia tych obowiązków w § 4 pkt 2 zawartych dwóch kolejnych umów, był jednym z dwóch autorów raportu z Audytu bezpieczeństwa informacji (KRI) w Urzędzie, co stanowiło naruszenie art. 38 ust 6 RODO, który stanowił, że IDO może wykonywać inne zadania i obowiązki. Administrator lub podmiot przetwarzający zapewniają, by takie zadania i obowiązki nie powodowały konfliktu interesów. W tym przypadku zaangażowania IOD do roli wewnętrznego audytora w zakresie bezpieczeństwa informacji KRI powoduje konflikt interesów, bowiem audytor powołany do sprawdzania przestrzegania zgodności działań Urzędu (jego pracowników) z przepisami prawa (w tym z przepisami RODO) decyduje o stosowaniu tych przepisów w Urzędzie.

   Burmistrz wyjaśnił w tej sprawie, że IOD *„(…) brał udział w opracowaniu raportu KRI, gdyż część dotycząca RODO jest niewielka i nie dostrzeżono przeciwwskazań, by Inspektor był członkiem zespołu. Także w uprzednich latach p. (…) był częścią zespołu i kontrola z Urzędu Marszałkowskiego raport KRI przyjęła bez zastrzeżeń".*

   NIK nie podziela tych wyjaśnień, bowiem - jak wyjaśnił Burmistrz - Audyt zawierał część dotyczącą RODO a ww. przepis określał, że ADO zapewnia, by zadania i obowiązki nie powodowały konfliktu interesów, w szczególności, aby inne przydzielone IOD zadania lub obowiązki nie kolidowały z jego podstawową funkcją jaką jest ochrona danych osobowych u konkretnego administratora danych.

   (akta kontroli str. 99, 304-317, 342-344)

OCENA CZĄSTKOWA

Zbiorom danych przetwarzanych w Urzędzie, podlegających zabezpieczeniu nie przypisano odpowiedniego poziomu ochrony, w tym nie uwzględniono określonych w Polskiej Normie wymagań prawnych, wartości, krytyczności i wrażliwości na nieuprawnione ujawnienie lub modyfikację. W Urzędzie nie funkcjonował SZBI, nie aktualizowano kart ryzyka w Analizie ryzyka w celu oceny adekwatności i skuteczności zastosowanych działań minimalizujących ryzyka, nie podjęto działań regulacyjnych dotyczących zapewnienia ciągłości działania Urzędu oraz nie podjęto działań w celu wyeliminowania konfliktu interesów przy sporządzeniu Audytu bezpieczeństwa informacji przez IOD.

W Urzędzie wprowadzono natomiast Politykę Bezpieczeństwa Informacji z uwagą, że dokument ten nie był aktualizowany od 2022 r., powołano IOD posiadającego odpowiednie kwalifikacje do pełnienia tej funkcji oraz sporządzono dokumentację w zakresie ochrony danych osobowych.

OBSZAR

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

Opis stanu faktycznego

2.1. Oględziny 10 komputerów pracowników Urzędu[33] wykazały brak możliwości zainstalowania nieautoryzowanego oprogramowania. Po ustaleniu faktycznie zalogowanego użytkownika danego komputera i próbie zainstalowania oprogramowania testowego system na wszystkich objętych próbą komputerach wyświetlał się monit o podanie hasła administratora, a więc wymagane było podniesienie poziomu dostępu do uprawnień administratora lokalnego.

W sprawie zabezpieczenia telefonów służbowych, Inspektor do spraw informatyzacji wyjaśnił, że jest używany jeden telefon szyfrowany mechanizmami systemu Apple iOS.

Ww. zabezpieczenia były zgodne z wymogami § 19 ust. 2 pkt 7 lit. c rozporządzenia KRI**,** które stanowiło, że Burmistrz, zapewnił środki uniemożliwiające nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji.

(akta kontroli str. 274, 229-231)

2.2. W okresie objętym kontrolą w Urzędzie obowiązywała wprowadzona 10 lipca 2024 r., Procedura nadawania uprawnień, która została opracowana na skutek realizacji wniosku po przeprowadzonym audycie. Wcześniej ww. zakres był określony w dziale drugim w § 1 Instrukcji zarządzania SI oraz w PBI w dziale IV w części nadawania dostępu do informacji podlegających ochronie. W załączniku nr 1 PBI określono wzór upoważnienia do przetwarzana danych osobowych.

(akta kontroli str.22, 38-43, 67)

Analiza zakresów czynności 15 pracowników Urzędu wykonujących zadania w systemach informatycznych wykazała, że 14 pracowników posiadało pisemne upoważnienia do przetwarzania danych osobowych zgodne z powierzonymi obowiązkami zapisanymi w ich zakresach czynności służbowych. W przypadku jednej pracownicy, nieprzypisanie obowiązków prowadzenia spraw z zakresu ochrony danych osobowych w zakresie czynności, przedstawiono w obszarze drugim w sekcji *Stwierdzone nieprawidłowości.*

Nie stwierdzono przypadków nieuzasadnionego rozszerzenia uprawnień pracownika.

Ustalono, że upoważnienia nie były na bieżąco aktualizowane, co przedstawiono w obszarze drugim w sekcji *Stwierdzone nieprawidłowości*

(akta kontroli str.22, 38-43, 68-70, 342-344, 350-365, 366-398, 399-424)

[33] Pięć komputerów stacjonarnych i pięć laptopów.

2.3 W okresie objętym kontrolą w Urzędzie rozwiązano stosunek pracy z czterema pracownikami. Odbieranie dostępu do systemów informatycznych w przypadku tych pracowników zostało zweryfikowane na podstawie oględzin, które wykazały, że według stanu na dzień 12 lipca 2024 r. konta ww. pracowników były nieaktywne.

Ustalono, że ostatnia aktywność w systemie informatycznym ww. pracowników miała miejsce przed dniem ustaniem stosunku pracy[34].

W sprawie odbierania pracownikom zwolnionym uprawnień dostępu do systemów informatycznych inspektor do spraw informatyzacji wyjaśnił, że *„(…) nie był on oficjalnie pisemnie informowany o ustaniu stosunków pracy poszczególnych pracowników (przełożeni pracowników nie wnioskowali o zamknięcie kont/odebranie uprawnień), ww. informację otrzymywał ustnie lub telefonicznie od inspektora ds. promocji, której dodatkowo powierzono zadania z zakresu ochrony danych osobowych".*

W pkt. 1 Procedury nadawania uprawnień wprowadzonej w trakcie kontroli w 2024 r., Burmistrz uregulował to zagadnienie i na bezpośredniego przełożonego pracownika został nałożony obowiązek zgłoszenia Administratorowi Systemów Informatycznych[35] (wyznaczonemu przez ADO) w formie pisemnej lub elektronicznej, konieczności nadania użytkownikowi uprawnień do konkretnych systemów teleinformatycznych na wzorze wskazanym w załączniku nr 1 do Procedury.

(akta kontroli str. 22, 36-40, 248-267)

2.4 Oględziny trzech systemów informatycznych Urzędu w zakresie wymagań uwierzytelniania dostępu do systemów wykazały, że:

- system obsługi jednostek samorządu terytorialnego (Korelacja) nie posiadał żadnych wymagań dotyczących złożoności hasła i okresowej jego zmiany. Wszyscy użytkownicy tego systemu posiadali konta indywidualne a podczas przeprowadzonej w trakcie oględzin testowej zmiany hasła system zaakceptował hasło o długości 3 znaków;
- Dla systemu obiegu dokumentów (LTC Finn SQL) parametry dotyczące haseł były ustawione na maksymalny poziom, tj. minimalna długość hasła 8 znaków, małe i wielkie litery oraz cyfry lub znaki specjalne a wymagana była zmiana hasła co 30 dni. Wszyscy użytkownicy systemu posiadali konta indywidualne;
- Dla systemu zarządzania budżetem jednostek samorządu terytorialnego (Besti@ JST) ustawione parametry dotyczące haseł były ustawione na minimalną długość 8 znaków, w tym wielkie i małe litery oraz cyfry a wymagana zmiana hasła co 90 dni. Wszyscy użytkownicy systemu posiadali konta indywidualne.

Oględziny próby 10 komputerów użytkowników w zakresie stosowanych haseł dostępu do systemu Windows wykazały, że na wszystkich komputerach do ich odblokowania wymagane było podanie indywidualnego hasła użytkownika, które miały długość co najmniej 8 znaków.

Ww. hasła były zgodne z wymogami określonymi w § 2 lit a) i c) Instrukcji zsi, który stanowił, że hasło dostępu składało się, z co najmniej ośmiu znaków

[34] Data zwolnienia jednego pracownika 31 stycznia 2023 r. a data ostatniej aktywności w systemie 21 marca 2022 r.; data zwolnienia jednego pracownika 21 stycznia 2024 r. a data ostatniej aktywności w systemie 17 marca 2024 r.; Data zwolnienia dwóch pracowników 30 czerwca 2024 r. a data ostatniej aktywności w systemie odpowiednio 21 września 2023 r. i 20 czerwca 2024 r.

[35] Zwany dalej: *„ASI"*.

zawierających małe i duże litery oraz cyfry lub znaki specjalne a użytkownicy systemu byli zobowiązani do zmiany hasła, co każde 30 dni.

(akta kontroli str.237-240)

2.5 Oględziny ośmiu stanowisk pracy, w tym dwóch stanowisk pracy w których realizowano zadania w zakresie ewidencji ludności i wydawania dowodów osobistych, obsługi interesanta [jedno stanowisko], obsługi podatkowej [dwa stanowiska], obsługi gospodarki oświetleniowej, energii, inwestycji [dwa stanowiska] oraz Urzędy stanu cywilnego [jedno stanowisko] wykazała, że monitory były usytuowane w sposób uniemożliwiający wgląd do wyświetlanych danych przez osoby nieuprawnione, co spełniało wymogi § 19 ust. 2 pkt 7 rozporządzenia KRI.

(akta kontroli str.241-247)

2.6 W Urzędzie ustanowiono Procedurę ochrony danych osobowych w ramach pracy zdalnej w Urzędzie. W ww. dokumencie uregulowano zagadnienia dotyczące:

- Dokumentacji ochrony danych osobowych [§ 3];
- Dostępu do danych osobowych i pracy z danymi osobowymi [§ 4];
- Obowiązków podczas spotkań zdalnych, wideokonferencji [§ 5];
- Przechowywania danych osobowych i nośników [§ 6];
- Transportu sprzętu i nośników danych [§ 7];
- Szkoleń [§ 8];
- Zgłaszania incydentów [§ 9];
- Stosowania zabezpieczeń przez pracowników [§ 10].

W sprawie zapoznania pracowników z procedurą Burmistrz wyjaśnił, że w przypadku wprowadzania zmian w dokumentach / utworzenia nowych dokumentów pracownicy zostają powiadomieni ustnie lub mailowo, a dokument do zapoznania się, znajduje się w sekretariacie

(akta kontroli str.123-130, 343-345)

2.7 Jak wyjaśnił Inspektor do spraw informatyzacji, w Urzędzie stosuje się rozwiązanie mające na celu zabezpieczenie dostępu do komputerów przenośnych osobom nieuprawnionym polegające na szyfrowaniu.

(akta kontroli str. 274-277)

2.8 Oględziny wykazały, że pomieszczenie serwerowni było zlokalizowane w wyodrębnionym klimatyzowanym pomieszczeniu Urzędu i było odpowiednio zabezpieczone. Jednakże nie prowadzono rejestru wejść i wyjść oraz czasu przebywania pracowników w pomieszczeniu, nie prowadzono również ewidencji osób upoważnionych do przebywania w serwerowni. W tej sprawie Burmistrz wyjaśnił, że z uwagi na bardzo ograniczoną ilość osób posiadających dostęp do serwerowni (informatyk i osoba pełniąca za niego zastępstwo), nie jest prowadzony taki rejestr, ani ewidencja.

Oględziny wykazały również, że Inspektor ds. informatyzacji Urzędu miał zainstalowaną przez wykonawcę systemu alarmowego aplikację powiadamiającą.

(akta kontroli str. 9, 11, 131-134, 268-273)

2.9 W okresie objętym kontrolą Urząd zawarł dwie umowy z podmiotami zewnętrznymi w ramach realizacji projektu Cyfrowa Gmina dotyczące zakupu sprzętu komputerowego[36] i sieciowego oraz częściowej modernizacji sieci LAN w dwóch budynkach Urzędu[37].

W umowach nie zawarto zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji. Burmistrz wyjaśnił w tej sprawie, że *„W zakresie umowy o dostawę sprzętu nie ma potrzeby określania poziomu bezpieczeństwa informacji, ponieważ sprzęt jest fabrycznie nowy. W przypadku reklamacji lub serwisu sprzęt komputerowy pozbawiany jest nośnika danych. W przypadku umowy o częściową modernizację sieci LAN również nie dopatrzyliśmy się wpływu na bezpieczeństwo informacji (usługa wykonywana była w godzinach pracy urzędu pod nadzorem pracowników UM)".*

(akta kontroli str. 342-345, 426-437)

2.10 W Urzędzie nie opracowano procedury dotyczącej przekazywania sprzętu IT poza jednostkę. Burmistrz wyjaśnił w tej sprawie, że nie jest przekazywany sprzęt do naprawy serwisom zewnętrznym a przekazywany *„(…) do utylizacji sprzęt pozbawiony jest nośników danych, które przechowywane są w zamykanej na klucz szafie. Sprzęt pozbawiony nośników danych odbierany jest przez PSZOK prowadzony przez ZGKiM Sośnicowice".*

W trakcie kontroli, Burmistrz uregulował zarządzeniem w sprawie Instrukcji kopii zapasowych zasady likwidacji nośników informatycznych oraz zasady usuwania danych z systemu, i tak w pkt 2 Instrukcji zapisano, że:

- W przypadku likwidacji nośników informatycznych zawierających dane osobowe lub kopie zapasowe systemów informatycznych służących do przetwarzania danych osobowych należy przed ich likwidacją usunąć dane osobowe lub uszkodzić je w sposób uniemożliwiający odczyt danych osobowych.
- Usuniecie danych z systemu powinno zostać zrealizowane przy pomocy oprogramowania przeznaczonego do bezpiecznego usuwania danych z nośnika informacji.
- W przypadku nośników informacji, przez ich zniszczenie rozumie się ich trwałe i nieodwracalne zniszczenie fizyczne do stanu nie dającego możliwość, ich rekonstrukcji i odzyskania danych.
- W przypadku braku możliwości zrealizowania procedury wewnętrznego zniszczenia nośników informacji, fakt ten należy zgłosić ADO i po przekazaniu nośników zostaną one zniszczone w ramach środków technicznych Jednostki bądź poddane procedurze utylizacji nośników informacji realizowanej przez firmę zewnętrzną, zakończonej sporządzeniem odpowiedniego protokołu utylizacji/zniszczenia.

(akta kontroli str. 34-36, 46-47)

[36] Umowa nr UM/272/71/2023 z dnia 24 sierpnia 2023 r.
[37] Umowa nr UM/272/78/2023 z dnia 8 września 2023 r.

2.11 Zasady przechowywania kopi zapasowych w ramach zapewnienia ciągłości działania Urzędu zostały określone we wprowadzonej w trakcie kontroli Instrukcji kopi zapasowych, gdzie w pkt 2 dotyczącym przechowywania kopii zapasowych oraz elektronicznych nośników informacji zawierających dane osobowe, zapisano, że:

1) Okresowe kopie zapasowe wykonywane są na macierz NAS. Kopie powinny być przechowywane w innych pomieszczeniach niż te, w których przechowywane są zbiory danych osobowych wykorzystywane na bieżąco. Kopie zapasowe przechowuje się w sposób uniemożliwiający nieuprawnione przejęcie, modyfikacje, uszkodzenie lub zniszczenie.
2) Każdy z egzemplarzy kopii zapasowej powinien być przechowywany w innej lokalizacji, w bezpiecznej odległości od serwerów systemu.
3) Dostęp do nośników z kopiami zapasowymi systemu oraz kopiami danych osobowych ma ASI.
4) Kopie zapasowe muszą być opisane w sposób umożliwiający szybką identyfikację.
6) Kopie przechowywane są przez 30 dni (kopie dzienne).

(akta kontroli str.44-47)

2.12. Obowiązek regularnego tworzenia i testowania kopii zapasowych danych i oprogramowania aplikacyjnego, w którym przetwarzane były dane wynikał z Instrukcji kopii zapasowych.

Oględziny wykazały, że przyjęty model tworzenia kopi zapasowych w Urzędzie obejmował następujące trzy zadania:

- kopia zawartości baz danych użytkowanych systemów, wykonywana codziennie i zapisywana na drugim dysku tego samego serwera,
- kopia z poprzedniej kopii wykonywana codziennie i zapisywana na serwerze NAS umieszczonym w punkcie dystrybucyjnym w budynku Urzędu (dostępne kopie z 30 dni); pomieszczenie z punktem dystrybucyjnym było zabezpieczone przed dostępem osób nieuprawnionych,
- kopia zasobów sieciowych serwera wykonywana codziennie i zapisywana na serwerze NAS umieszczonym w punkcie dystrybucyjnym jak wyżej.

Z harmonogramu zadań wykonywania kopii baz danych wynikało, że kopie były tworzone codziennie poza godzinami pracy Urzędu a dziennik ostatnich zdarzeń systemu tworzenia kopii zapasowych zawierał szczegółowe informacje dotyczące utworzonych kopii zapasowych.

Kopie zapasowe nie były tworzone na zewnętrzne nośniki danych.

Inspektor do spraw Informatyzacji oświadczył, że *„(…) zakup nowego systemu tworzenia i testowania kopii zapasowych wraz z nową przestrzenią dyskową oraz biblioteką taśmową został ujęty w realizowanym obecnie projekcie Wdrożenie rozwiązań zwiększających poziom cyberbezpieczeństwa w Urzędzie (…) w ramach programu Cyberbezpieczny Samorząd, który to projekt przewiduje stworzenie nowej infrastruktury serwerowej w Urzędzie”*.

W toku oględzin w wyniku testu odzyskania przez Inspektora do spraw informatyzacji pliku z najstarszej kopii zapasowej dostępnej na serwerze NAS ustalono, że plik został odzyskany i otworzył się prawidłowo.

Ww. działania były zgodne z wymogami § 19 ust. 2 pkt 12 lit. b) i e) oraz § 19 ust. 2 pkt 7 rozporządzenia KRI oraz zgodne z § 4 Instrukcji zsi.

(akta kontroli str. 23, 38-47, 234-236)

2.13 W Urzędzie nie opracowano procedury dotyczącej monitorowania pojemności nośników pamięci.

Oględziny użytkowanych w Urzędzie dwóch serwerów fizycznych wykazały, że:

- Serwer był zajęty na dysku A w 91,05% a na dysku B był zajęty w 17,68%;
- Serwer był zajęty w 49 %.

Inspektor do spraw informatyzacji Urzędu wyjaśnił w tej sprawie, że w Urzędzie *„(…) nie wdrożono żadnych systemów monitorowania dostępnego miejsca i nie ustawiono alarmów dotyczących dostępnej przestrzeni dyskowej, nie przewiduje się rozbudowywania obecnej przestrzeni dyskowej serwerów w związku z trwającą procedurą realizacji projektu wdrożenie rozwiązań zwiększających poziom cyberbezpieczeństwa w Urzędzie (…) w ramach programu Cyberbezpieczny Samorząd, który to projekt przewiduje stworzenie nowej infrastruktury serwerowej w Urzędzie".*

(akta kontroli str. 232-233)

2.14 W ramach zapewnienia ciągłości działania Urzędu nie zidentyfikowane zostały kluczowe elementy infrastruktury i usługi IT oraz ich zabezpieczenie pod kątem wpływu czynników zewnętrznych. Burmistrz wyjaśnił w tej sprawie, że identyfikacja i zabezpieczenie tych elementów przewidziana jest *„(…) do opracowania w nowym SZBI w ramach projektu Cyberbezpieczny Samorząd".*

W zakresie wskazania czasu na przywrócenie poszczególnych systemów oraz procesów do działania, Burmistrz wyjaśnił, że: *„Nie posiadamy szacunków dotyczących czasu przywracania poszczególnych systemów i procesów do działania".*

(akta kontroli str.34-37)

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki, w przedstawionym wyżej zakresie stwierdzono następującą nieprawidłowość:

1. Badanie dokumentacji 15 pracowników związane z wydawaniem im upoważnień dostępu do informacji podlegających ochronie wykazało, że była prowadzona w sposób nierzetelny, bowiem nie była aktualizowana I tak:
   - W przypadku dwóch pracownic pomimo zmiany nazwiska upoważnienia były wystawione na poprzednie nazwisko. Burmistrz wyjaśnił, że *„Nazwiska nie zostały zmieniony przez niedopatrzenie pracownika i zostanie niezwłocznie uzupełnione*".
   - W sześciu przypadkach pomimo awansów pracowników na wyższe stanowisko[38], w upoważnieniach nadal widniały poprzednie stanowiska pracowników. Burmistrz wyjaśnił, że *„Osoba wydająca upoważnienia nie otrzymała stosownej informacji o awansie od kadrowej UM w Sośnicowicach".*
   - W przypadku osoby zatrudnionej w Referacie Organizacyjnym i Spraw Obywatelskich w upoważnieniu zapisano, że pracownica jest upoważniona do przetwarzania danych zgodnie z przydzielonym zakresem czynności, udzielonymi pełnomocnictwami oraz poleceniami Administratora danych. W zakresie czynności pracownicy nie było żadnej informacji dotyczącej wykonywania dodatkowych zadań związanych z prowadzeniem spraw z zakresu ochrony danych osobowych powierzonych ww. przez kierownika jednostki. Burmistrz wyjaśnił, że „*Pani (…) nie zmieniono zakresu czynności w związku ze zmianą nazwiska,*

[38] W jednym przypadku awans z inspektor na Główną księgową; w trzech przypadkach z inspektora na głównego specjalistę; w jednym przypadku z podinspektora na inspektora i w jednym przypadku z inspektora na specjalistę.

ponieważ sama zmiana nazwiska nie zmieniła, zakresu obowiązków tego pracownika. Natomiast odnośnie powierzenia (…) spraw związanych z zakresem ochrony danych osobowych, nie zmieniono temu pracownikowi zakresu czynności, ponieważ przyznano jej z tego tytułu dodatek specjalny za wykonywanie dodatkowych obowiązków nie przewidzianych w zakresie czynności". Ww. dodał, że *„Zakresy czynności pracowników, nie zawierają żadnych obowiązków związanych z ochroną i przetwarzaniem danych osobowych, ponieważ tak jak przypadku przepisów BHP, obowiązki te wynikają z innych dokumentów np. takich jak Polityka Bezpieczeństwa Regulamin Ochrony Danych Osobowych itd. Zakresy czynności zawierają zapisy dotyczące obowiązku w pkt 4 przestrzegania obowiązujących przepisów o tajemnicy skarbowej, ochronie informacji niejawnych oraz o ochronie danych osobowych".*

NIK nie podziela wyjaśnienia Burmistrza, bowiem oświadczenia wprost odnoszą się m.in. do zakresów czynności i wskazana w wyjaśnieniach treść pkt 4 zakresu czynności była przypisana wszystkim pracownikom. Natomiast pracownicy powierzono dodatkowe obowiązki prowadzenia spraw z zakresu ochrony danych osobowych a zakres czynności ww. obejmował jedynie czynności na stanowisku inspektora do spraw promocji.

(akta kontroli str.22, 38-43, 67-70, 342-344, 350-365, 366-398, 399-424)

OCENA CZĄSTKOWA

W Urzędzie wdrożono skuteczne rozwiązania organizacyjne i techniczne w zakresie bezpieczeństwa informacji takie jak: zapobieganie utracie informacji lub nieuprawnionemu dostępowi w związku z realizacją procedur serwisowych; stosowanie zabezpieczeń przed szkodliwym oprogramowaniem; ustanowienie zasad (procedur) bezpiecznej pracy zdalnej, w tym przy przetwarzaniu mobilnym i pracy na odległość; regularnie tworzenie kopi zapasowych badanych systemów informatycznych; nie przechowywanie kopii zapasowych badanych systemów informatycznych w miejscu wytwarzania danych.

W Urzędzie nie aktualizowano na bieżąco dokumentacji pracowniczej w tym upoważnień dostępu do informacji podlegających ochronie.

OBSZAR

3. Działania w celu zapobiegania incydentom bezpieczeństwa informacji

Opis stanu faktycznego

3.1 Zagadnienie prowadzenia okresowych analiz ryzyka utraty integralności, poufności lub dostępności informacji, przedstawiono w obszarze pierwszym w pkt 1.4. oraz pkt 4 w sekcji *Stwierdzonych nieprawidłowości.*

(akta kontroli str.135-179, 347-349)

3.2 Obowiązki pracowników Urzędu w zakresie zgłaszania incydentów cyberbezpieczeństwa lub naruszenia bezpieczeństwa informacji (w tym osobowych) zostały uregulowane w Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych, w której zawarto:

- definicję ochrony danych osobowych [dział I];
- postępowanie w przypadku naruszenia ochrony danych osobowych [dział II];
- naruszenie ochrony danych osobowych [dział III];
- zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu [dział IV];
- zawiadomienie osoby, której dane dotyczą. o naruszeniu ochrony danych osobowych [dział V].

Integralną częścią Procedury były trzy załączniki:

- raport z naruszenia ochrony danych osobowych [nr 1];
- rejestr incydentów bezpieczeństwa, podjętych działań korygujących i zapobiegawczych;
- zgłoszenie nadzorczemu ochrony danych osobowych organowi nadzorczemu.

W Rejestrze incydentów bezpieczeństwa prowadzonym w Urzędzie nie odnotowano żadnych zadań, problemów lub incydentów w ww. zakresie.

(akta kontroli str. 82-91, 347-349)

3.3 Stosownie do zapisów działu IV w części dotyczącej nadawanie dostępu do informacji podlegającej ochronie w pkt 2 lit. c, kandydat przed przystąpieniem do pracy powinien przejść szkolenie, z zakresu zasad ochrony danych osobowych stosowanych przez ADO a realizowanych przez IOD.

Dodatkowo w trakcie kontroli w 2024 r. Burmistrz wprowadził Procedurę szkolenia osób zaangażowanych w proces przetwarzania informacji w Urzędzie, w której przewidywał raz do roku zorganizowanie szkolenia wewnętrznego lub zewnętrznego przeznaczonego dla wszystkich osób zaangażowanych w proces przetwarzania informacji. W rocznym planie szkoleń na 2024 r. w IV kwartale tego roku zaplanowano szkolenie z zakresu cyberbezpieczeństwa oraz okresowe szkolenie dotyczące ochrony danych osobowych.

Analiza dokumentacji 15 pracowników wykazała, że wszyscy oni ukończyli szkolenie z zakresu ochrony danych osobowych i bezpieczeństwa informacji. Dodatkowo inspektor do spraw informatyzacji uczestniczył w szkoleniu z zakresu podstawowych metod ochrony i analizy ruchu internetowego - poziom I.

(akta kontroli str.118-122, 358, 361-362, 365, 382-388)

3.4 Stosownie do § 19 ust. 2 pkt 14 rozporządzenia KRI, w Urzędzie przeprowadzono audyt wewnętrzny z zakresu bezpieczeństwa informacji i w sporządzonym 11 grudnia 2023 r. raporcie zostały sformułowane następujące rekomendacje:

1) Podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji oraz bezzwłoczna zmiana uprawnień, w przypadku zmiany zadań tych osób. Rekomendację zrealizowano poprzez wprowadzenie Procedury nadawania uprawnień.
2) Zapewnienie szkolenia osób zaangażowanych w proces przetwarzania informacji. Rekomendacja jest w trakcie realizacji, bowiem, w Urzędzie wprowadzono Procedurę szkolenia osób w proces przetwarzania informacji natomiast zaplanowane w czwartym kwartale 2024 r. dwa szkolenia dotyczące ochrony danych oraz cyberbezpieczeństwa nie zostały zrealizowane.
3) Zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionemu, jej ujawnienie, modyfikację, usunięcie lub zniszczenie. Rekomendacja jest w trakcie realizacji.
4) Zawieranie w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji. Zrealizowano poprzez zawarcie umów powierzenia z dostawcami oprogramowania dziedzinowego, z dostawcą usług hostingowych oraz

z podmiotem odpowiedzialnym za publikację nagrań wideo z przebiegu sesji Rady Miejskiej w Sośnicowicach. Rekomendację zrealizowano.

5) Ustalenie zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych Rekomendacja jest w trakcie realizacji, bowiem w ramach projektu „Cyberbezpieczny samorząd" zaplanowano zakupienie taśmowego urządzenia do przechowywania kopii bezpieczeństwa.

(akta kontroli str.95-117, 320-325, 438-443)

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki, w przedstawionym wyżej zakresie stwierdzono następującą nieprawidłowość:

1. Nie prowadzono okresowych analiz ryzyka utraty integralności, poufności lub dostępności informacji, co opisano w sekcji stwierdzonych nieprawidłowości w obszarze I w pkt 4.

OCENA CZĄSTKOWA

W Urzędzie w 2023 r. przeprowadzono wymagany audyt wewnętrzny z zakresu bezpieczeństwa informacji; wprowadzono Instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych; zapewniono szkolenia osób zaangażowanych w proces przetwarzania informacji, ze szczególnym uwzględnieniem określonych w rozporządzeniu zagadnień oraz zaplanowanie kolejne szkolenia.

Natomiast nie prowadzono okresowych analiz ryzyka utraty integralności, poufności lub dostępności informacji.

IV. Wnioski

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

Wnioski

1. Sklasyfikowanie przetwarzanych informacji z uwzględnieniem wymagań prawnych, wartości, krytyczności i wrażliwości na nieuprawnione ujawnienie lub modyfikację i przypisanie informacjom odpowiedniego poziomu ochrony.
2. Opracowanie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji o którym mowa w § 19 ust. 1 w związku z ust. 3 rozporządzenia KRI, uwzględniającego zalecenia normy PN-ISO/IEC 27001 i norm z nią związanych (PN-ISO/IEC 27002, PN-ISO/IEC 27005, PN-ISO/IEC 24762).
3. Zaktualizowanie Polityki Bezpieczeństwa Informacji oraz procedur w niej określonych pod kątem faktycznie stosowanych praktyk w Urzędzie, m.in. z zakresu tworzenia i przechowywania kopii zapasowych.
4. Zapewnienie przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji.
5. Ustanowienie Polityki ciągłości działania i w związku z tym opracowanie i wdrożenie Planu zapewnienia ciągłości działania oraz planów odtworzeniowych, zapewnienie ich testowania i treningu oraz wyznaczenie pracowników odpowiedzialnych za bezpieczeństwo informacji oraz zapewnienie ciągłości działania i przypisanie im czynności w tym zakresie.
6. Zinwentaryzowanie w aplikacji inwetaryzacyjnej wszystkich składników systemu informatycznego, wymaganych Procedurą inwentaryzacyjną, oraz nadanie numerów inwentarzowych elementom systemu informatycznego, które takiego numeru nie posiadają.
7. Zapewnienie prowadzenia audytów w zakresie bezpieczeństwa informacji przez różne osoby aby zapewnić ich niezależność i obiektywizm.

8. Zaktualizowanie dokumentacji pracowniczej oraz upoważnień dostępu do informacji podlegających ochronie.

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 Delegatury NIK w Katowicach. Prawo zgłaszania 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 od otrzymania wystąpienia pokontrolnego, o wykonaniu 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.

Katowice, dnia 18 września 2024 r.

Kontroler
Wiesław Pietrzyk
Gł. specjalista kontroli państwowej

.....

Najwyższa Izba Kontroli
Delegatura w Katowicach