

**ZARZĄDZENIE NR 69/2024**  
**BURMISTRZA SOŚNICOWIC**

z dnia 25 kwietnia 2024 r.

**w sprawie wprowadzenia Procedury audytów wewnętrznych w zakresie bezpieczeństwa informacji obowiązującej w Urzędzie Miejskim w Sośnicowicach**

Na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04. 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.U. UE. L. Nr 119, s. 1 ze zm.) zarządzam, co następuje:

**§ 1.** Procedurę audytów wewnętrznych w zakresie bezpieczeństwa informacji obowiązującą w Urzędzie Miejskim w Sośnicowicach określa Załącznik 1 do niniejszego Zarządzenia.

**§ 2.** Wykonanie zarządzenia powierza się Sekretarzowi Gminy.

**§ 3.** Zarządzenie wchodzi w życie z dniem podpisania.

Burmistrz

**Leszek Kołodziej**

**PROCEDURA AUDYTÓW WEWNĘTRZNYCH  
W ZAKRESIE BEZPIECZEŃSTWA INFORMACJI  
OBOWIĄZUJĄCA  
W URZĘDZIE MIEJSKIM W SOŚNICOWICACH**

1. Celem procedury jest zapewnienie planowego i systematycznego przeprowadzania audytów wewnętrznych Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w Urzędzie Miejskim w Sośnicowicach.
2. Audytorem wewnętrznym SZBI może zostać Pracownik Urzędu Miasta posiadający minimum roczny staż pracy w UM lub Inspektor Ochrony Danych. Osoba przeprowadzająca audyt wewnętrzny powinna posiadać ukończone szkolenie z zakresu przeprowadzania audytów wewnętrznych SZBI i/lub szkolenie „Audytor Wewnętrzny Systemu Zarządzania Bezpieczeństwem Informacji ISO 27001”.
3. Audyt wewnętrzny może być przeprowadzany przez dwóch lub więcej audytorów wewnętrznych SZBI tworzących zespół audytorów.
4. Audytor wewnętrzny, w porozumieniu z Administratorem Danych Osobowych, przygotowuje roczny plan audytów. Roczny plan audytów jest przygotowywany na dany rok kalendarzowy najpóźniej do końca stycznia roku, którego plan ma dotyczyć.
5. Roczny plan audytów określa m.in.:
  - listę obszarów oraz zagadnień, które powinny w szczególny sposób być objęte planem audytów;
  - komórki organizacyjne i procesy, które mają być audytowane;
  - orientacyjne terminy audytów.Plan audytów powinien uwzględniać status i ważność procesów i obszarów audytowanych, jak również wyniki poprzednich audytów. Burmistrz zatwierdza roczny plan audytów. Przykładowy wzór stanowi załącznik nr 1 do procedury.
6. Przeprowadzenie audytu ma na celu uzyskanie odpowiedzi na pytanie, czy działania w zakresie bezpieczeństwa informacji w danym obszarze są zgodne z przyjętym sposobem postępowania i czy są efektywne.

7. Oprócz audytów planowanych możliwe jest również przeprowadzenie audytów nieplanowanych, które mogą zostać zatwierdzone na podstawie:
- zaistniałych incydentów;
  - wyników poprzednich audytów;
  - wyników przeglądów zarządzania.
8. Audytowana komórka organizacyjna zostaje poinformowana o audycie co najmniej 7 dni przed planowanym terminem rozpoczęcia audytu.
9. Audytor dokumentuje audyt w oparciu o przygotowany harmonogram, plan audytu oraz obserwacje audytowe.
10. Realizacja audytu obejmuje następujące etapy:
- 1) spotkanie otwierające (prezentacja osobowa, przedstawienie szczegółowego planu i celu audytu oraz listy dokumentów podlegających badaniu, wyjaśnienie ewentualnych wątpliwości);
  - 2) przeprowadzenie audytu skuteczności funkcjonowania SZBI poprzez:
    - rozmowy i wywiady z personelem, analizę dokumentacji, obserwację miejsc przetwarzania informacji, oceny materiałów i sprzętu,
    - zanotowanie faktów jako wydarzeń w czasie audytu,
    - ocena faktów i określenie obiektywnych dowodów istnienia niezgodności,
    - weryfikacja wykonania działań korygujących z poprzedniego audytu,
    - rejestrowanie wszystkich ujawnionych niezgodności (w celu uwzględnienia ich w raporcie końcowym);
  - 3) spotkanie zamykające (podsumowanie audytu, omówienie stwierdzonych spostrzeżeń, niezgodności i wniosków oraz uzgodnienie terminu przedstawienia raportu z audytu);
  - 4) przedstawienie raportu z przeprowadzonego audytu zgodnie z ustalonym wcześniej terminem poprzez przesłanie sporządzonego raportu, po uprzednim zatwierdzeniu przez Sekretarza oraz Burmistrza Sośnicowic w wersji papierowej, osobom odpowiedzialnym za oceniany proces.
11. Po zakończeniu audytu, w oparciu o przedstawiony raport, opracowane zostają działań korygujące/zapobiegawcze.

.....  
(data, pieczętka i podpis Kierownika jednostki)

**Roczny plan audytów w Urzędzie Miejskim w Sońnicowicach  
na rok .....**

L.p.	Przedmiot i zakres audytu (lista obszarów oraz zagadnień objętych audytem, komórka/dział, proces)	Audyt wewn. (W) / Audyt zewn. (Z)	Osoba /podmiot audytujący	Orientacyjny termin audytu	Uwagi

.....

(data i podpis Burmistrza)