ZARZĄDZENIE NR 170/2026
BURMISTRZA MIEROSZOWA

z dnia 1 czerwca 2026 r.

w sprawie wyznaczenia Administratora Systemów Informatycznych Urzędzie Miejskim w Mieroszowie

Na podstawie art. 31 oraz art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz.U. z 2026 r. poz. 662), w związku z Rozporządzeniem 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, Dz. U. UE.L.2016.119. l ze zm.), zarządzam co następuje:

§ 1. Wyznaczam Administratora Systemów Informatycznych (ASI) w Urzędzie Miejskim w Mieroszowie. Imienne wskazanie osoby pełniącej funkcję ASI następuje w dokumentacji wewnętrznej Urzędu. Dane osobowe osoby pełniącej funkcję ASI nie są przeznaczone do podania do publicznej wiadomości. Do publicznej wiadomości jako dane kontaktowe ASI podaje się adres poczty elektronicznej: informatyk@mieroszow.pl oraz numer telefonu głównego do Urzędu: 74 303 01 88.

§ 2. Administrator Systemów Informatycznych (ASI) jest odpowiedzialny za nadzorowanie prawidłowego funkcjonowania sprzętu i oprogramowania, koordynowanie techniczno-organizacyjnej obsługi systemów informatycznych, w szczególności systemów służących do przetwarzania danych osobowych, oraz realizację zadań określonych w załączniku do niniejszego zarządzenia.

§ 3. Zarządzenie wchodzi w życie z dniem podpisania.

Burmistrz Mieroszowa

Andrzej Lipiński

Załącznik do zarządzenia nr 170/2026

Burmistrza Mieroszowa

z dnia 1 czerwca 2026 r.

Zakres działania Administratora Systemu Informatycznego (ASI)

Administrator Systemów Informatycznych, zwany dalej ASI, w zakresie zadań wykonywanych na rzecz zapewnienia bezpieczeństwa systemów informatycznych oraz informacji w nich przetwarzanych, działa zgodnie z Polityką Bezpieczeństwa Informacji oraz procedurami obowiązującymi u Administratora. W zakresie ochrony danych osobowych ASI współpracuje z Inspektorem Ochrony Danych (IOD). Do zadań ASI należy:

1. Wdrażanie, utrzymywanie i monitorowanie technicznych oraz organizacyjnych zabezpieczeń systemów informatycznych, zgodnie z Polityką Bezpieczeństwa Informacji i obowiązującymi procedurami.

2. Współpraca z Inspektorem Ochrony Danych w zakresie bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych.

3. Prowadzenie lub aktualizowanie inwentaryzacji sprzętu, oprogramowania, systemów informatycznych, kont uprzywilejowanych, nośników danych oraz innych zasobów IT służących do przetwarzania informacji.

4. Współudział w określaniu zasad nadawania, modyfikowania i odbierania uprawnień w systemach informatycznych, w uzgodnieniu z Administratorem, właścicielami procesów lub osobami upoważnionymi oraz, w zakresie ochrony danych osobowych, z IOD.

5. Realizacja decyzji Administratora lub osób upoważnionych w zakresie nadawania, zmiany, zawieszania i odbierania uprawnień dostępu do systemów informatycznych oraz wybranych funkcji narzędzi służących do przetwarzania danych.

6. Tworzenie, modyfikowanie, blokowanie i usuwanie kont użytkowników w systemach informatycznych, zgodnie z obowiązującą procedurą zarządzania dostępem.

7. Nadawanie haseł tymczasowych, resetowanie haseł oraz stosowanie polityk haseł i innych mechanizmów uwierzytelniania zgodnie z obowiązującymi procedurami bezpieczeństwa.

8. Weryfikowanie, czy konta i uprawnienia użytkowników są aktualne, w szczególności w przypadku zmiany stanowiska, zakończenia zatrudnienia lub ustania podstawy dostępu do systemu.

9. Planowanie, wykonywanie, nadzorowanie oraz dokumentowanie kopii zapasowych systemów i danych, zgodnie z przyjętymi zasadami tworzenia i odtwarzania kopii bezpieczeństwa.

10. Okresowe testowanie możliwości odtworzenia danych i systemów z kopii zapasowych oraz dokumentowanie wyników tych testów.

11. Monitorowanie stanu środowiska IT, sprzętu, oprogramowania, usług, sieci oraz zdarzeń systemowych w zakresie niezbędnym do zapewnienia bezpieczeństwa, ciągłości działania i wykrywania incydentów.

12. Monitorowanie legalności oprogramowania wykorzystywanego na stacjach roboczych, serwerach i innych urządzeniach pozostających w środowisku IT Administratora.

13. Nadzór nad ewidencją licencji oprogramowania oraz zgłaszanie potrzeb w zakresie zakupu, odnowienia lub uzupełnienia licencji.

14. Systematyczne aktualizowanie oprogramowania systemowego, aplikacyjnego i ochronnego albo nadzorowanie realizacji tych aktualizacji przez podmioty zewnętrzne.

15. Wdrażanie i utrzymywanie zabezpieczeń przed złośliwym oprogramowaniem, nieuprawnionym dostępem, utratą danych oraz innymi zagrożeniami dla systemów informatycznych.

16. Zabezpieczanie logów, zapisów zdarzeń systemowych oraz innych informacji technicznych mogących mieć znaczenie dla wyjaśniania incydentów bezpieczeństwa.

17. W przypadku stwierdzenia lub podejrzenia incydentu bezpieczeństwa podejmowanie niezwłocznych działań zabezpieczających system, dane, dowody oraz ciągłość działania systemów informatycznych.

18. Analizowanie sytuacji, okoliczności i przyczyn incydentów dotyczących bezpieczeństwa systemów informatycznych lub informacji w nich przetwarzanych oraz dokumentowanie podjętych działań.

19. Niezwłoczne informowanie Administratora o incydentach bezpieczeństwa, a jeżeli incydent dotyczy lub może dotyczyć danych osobowych - również Inspektora Ochrony Danych.

20. Udział w analizie ryzyka dotyczącej systemów informatycznych, infrastruktury IT, danych, kopii zapasowych, nośników danych i usług informatycznych.

21. Udział w opracowywaniu i aktualizowaniu procedur bezpieczeństwa dotyczących systemów informatycznych, urządzeń, sieci, kont użytkowników, kopii zapasowych, nośników danych i incydentów.

22. Opiniowanie i zgłaszanie potrzeb dotyczących inwestycji, dostaw, usług, licencji oraz opieki serwisowej niezbędnych do utrzymania i rozwoju środowiska IT Urzędu Miejskiego w Mieroszowie.

23. Współpraca z dostawcami usług informatycznych, serwisami, producentami oprogramowania i podmiotami zewnętrznymi w zakresie technicznego utrzymania systemów, usuwania awarii, aktualizacji oraz zapewnienia bezpieczeństwa środowiska IT.

24. Rozwiązywanie problemów towarzyszących eksploatacji systemów informatycznych oraz wsparcie użytkowników w zakresie bezpiecznego korzystania z tych systemów.

25. Przygotowywanie, we współpracy z IOD, instrukcji i zaleceń dla użytkowników systemów informatycznych, zgodnych z Polityką Bezpieczeństwa Informacji i obowiązującymi procedurami.

26. Prowadzenie lub współprowadzenie szkoleń i instruktaży dla użytkowników w zakresie bezpiecznego korzystania z systemów informatycznych, haseł, poczty elektronicznej, urządzeń mobilnych, nośników danych oraz reagowania na incydenty.

27. Udział w audytach, przeglądach i kontrolach dotyczących bezpieczeństwa informacji oraz przygotowywanie informacji technicznych niezbędnych do oceny bezpieczeństwa systemów informatycznych.

28. Zapewnienie bezpiecznego wycofywania z użytkowania sprzętu, nośników danych i systemów informatycznych, w szczególności poprzez usunięcie, zanonimizowanie albo zabezpieczenie danych zgodnie z obowiązującymi procedurami.

29. Dokumentowanie czynności administracyjnych, zgłoszeń, awarii, incydentów, zmian w systemach oraz innych działań mających znaczenie dla bezpieczeństwa systemów informatycznych.

30. Wykonywanie innych czynności z zakresu bezpieczeństwa systemów informatycznych, wynikających z Polityki Bezpieczeństwa Informacji, procedur wewnętrznych, decyzji Administratora lub obowiązujących przepisów prawa.