ZARZĄDZENIE Nr 50/26
WÓJTA GMINY KIWITY
z dnia 15 czerwca 2026 r.

w sprawie wyznaczenia Administratora Systemów Informatycznych w Urzędzie Gminy Kiwity

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz. U. z 2026r. poz. 662) oraz wprowadzonej Polityki Bezpieczeństwa Informacji oraz w oparciu o art. 24 ust. 1 i ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku 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), zarządzam, co następuje:

§ 1. Powołuję Pana Michała Pasynka – inspektora ds. obsługi informatycznej na Administratora Systemów Informatycznych (ASI) w Urzędzie Gminy Kiwity.

§ 2. Do zadań Administratora Systemów Informatycznych należy:

a) zarządza systemami informatycznymi organizacji w sposób gwarantujący utrzymanie poufności, dostępności i integralności gromadzonych w nich danych na poziomie pozwalającym zachować zgodność z wymogami prawnymi i organizacyjnymi;
b) sprawuje nadzór nad wdrożeniem stosownych środków administracyjnych, technicznych i fizycznych w celu zapewnienia bezpieczeństwa danych w obszarze teleinformatycznym;
c) sprawuje nadzór nad funkcjonowaniem zabezpieczeń systemów informatycznych – dba o odporność organizacji przed zagrożeniami w obszarze cyberbezpieczeństwa;
d) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia bezpieczeństwa powierzonego mu systemu informatycznego, zgodnie z procedurami nadzoru nad incydentami bezpieczeństwa oraz utrzymania ciągłości działania;
e) zarządza uprawnieniami w zakresie uprawnień i dostępów do systemów informatycznych w ramach procedury zarządzania uprawnieniami i dostępami;
f) przydziela każdemu użytkownikowi SI indywidualne konta w systemie informatycznym organizacji, stosowne do wyznaczonego zakresu obowiązków, wprowadza modyfikacje uprawnień użytkowników, a także ich wyrejestrowuje na polecenie Administratora Danych, blokując jednocześnie dostęp do konta i zasobów informatycznych;
g) wprowadza zmiany uprawnień w systemach informacyjnych na czas nieobecności pracownika zgodnie z wytycznymi kierownika jednostki/kierowników komórek organizacyjnych oraz planem zastępstw;
h) dba o aktualizację Deklaracji stosowania zabezpieczeń w zakresie technicznych środków bezpieczeństwa wdrożonych w organizacji;

i) sprawuje nadzór nad inwentaryzacją i jej aktualnością w odniesieniu do produktów, usług i procesów ICT służących do przetwarzania informacji;

j) tworzy, aktualizuje i doskonali elementy składające się na plany ciągłości działania w Urzędzie w tym sprawuje nadzór nad kopiami zapasowymi;

k) na bieżąco przesyła Inspektorowi Ochrony Danych informacje dotyczące zdarzeń wpływających na bezpieczeństwo systemów informatycznych, w tym m.in. wykrytego oprogramowania złośliwego lub szpiegującego, oprogramowania nielegalnego lub zainstalowanego bez upoważnienia, awarii systemu informatycznego lub jego nieprawidłowego działania, stwierdzenia faktu korzystania z systemu informatycznego przez osobę niepowołaną, awarii zasilania, co może mieć wpływ na bezpieczeństwa przetwarzania danych osobowych;

l) zbiera informacje o zagrożeniach cyberbezpieczeństwa i podatnościach na incydenty systemu informacyjnego;

m) monitoruje infrastrukturę teleinformatyczną pod kątem podatności mogących mieć wpływ na jej bezpieczeństwo, rejestruje je, dokonuje analizy ryzyka dla zidentyfikowanych podatności oraz adekwatnie do wyników analizy podejmuje działania w celu ich wyeliminowania i/lub zabezpieczenia infrastruktury i systemów przed ich negatywnym wpływem na bezpieczeństwo

n) podjęcie natychmiastowych działań zabezpieczających stan systemu informatycznego w przypadku otrzymania informacji o naruszeniu zabezpieczeń systemu informatycznego lub informacji o zmianach w sposobie działania programu lub urządzeń wskazujących na naruszenie bezpieczeństwa danych,

o) analiza sytuacji, okoliczności i przyczyn, które doprowadziły do naruszenia bezpieczeństwa danych (jeśli takie wystąpiło).

§ 3. Wyżej wymienione zadania ASI wskazują jedynie w sposób ogólny zagadnienia dotyczące bezpieczeństwa danych w systemach, gdzie przetwarzane są dane osobowe. Niezależnie od wymienionych tam czynności, zadaniem ASI jest śledzenie osiągnięć w dziedzinie zabezpieczania systemów informatycznych w ogóle i wdrażanie takich narzędzi, metod pracy oraz sposobów zarządzania systemem informatycznym, które bezpieczeństwo to wzmocnią. Działania szczegółowe, jakie ASI powinien podejmować w celu realizacji określonych wyżej zadań uzależnione powinny być od:

- architektury systemu informatycznego, w którym dane są przetwarzane,
- zastosowanych narzędzi w ramach oprogramowania systemowego,
- użytych narzędzi do zarządzania bazą danych oraz przyjętych rozwiązań w stosowanych aplikacjach użytkowych.

§ 4. Niniejsze wyznaczenie wygasa z chwilą ustania zatrudnienia (bez względu na podstawę prawną

zatrudnienia) lub odwołania Administratora z pełnienia ww. funkcji.

§ 5. Administrator Systemów Informatycznych zobowiązany jest do zachowania w tajemnicy informacji w zakresie danych osobowych i sposobów ich zabezpieczania, również po odwołaniu z pełnienia ww. funkcji, a także po ustaniu zatrudnienia lub współpracy.

§ 6. Traci moc zarządzenie Nr 41/16 Wójta Gminy Kiwity z dnia 30 września 2016 r. w sprawie powołania Administratora Systemu Informatycznego.

§ 7. Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT
Jacek Pawlik

RADCA PRAWNY
Bogusława Dworzańska