

ZARZĄDZENIE Nr 88/26
WÓJTA GMINY KIWITY
z dnia 24 września 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 § 19 ust. 1 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 (Dz.U. z 2024 poz.773 z późn. zm.), art. 8, art. 14 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2026 poz. 20 z późn. zm.), art. 24 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (RODO), (Dz.U.UE.L.2016.119.1 z dnia 2016.05.04 z późn. zm.), ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2019 poz. 1781 z późn. zm.), pkt. 5.3.4 „Polityki Bezpieczeństwa Informacji” zarządzam, co następuje:

§ 1. Wyznaczam Pana Patryka Polakowskiego – inspektora ds. obsługi informatycznej na Administratora Systemów Informatycznych (ASI) w Urzędzie Gminy Kiwity.

§2. Do zadań Administratora Systemów Informatycznych należy:

- a) zarządzanie 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) sprawowanie nadzoru nad wdrożeniem stosownych środków administracyjnych, technicznych i fizycznych w celu zapewnienia bezpieczeństwa danych w obszarze teleinformatycznym;
- c) sprawowanie nadzoru nad funkcjonowaniem zabezpieczeń systemów informatycznych – dba o odporność organizacji przed zagrożeniami w obszarze cyberbezpieczeństwa;
- d) podejmowanie odpowiednich działań w przypadku naruszenia lub podejrzenia naruszenia bezpieczeństwa powierzonego mu systemu informatycznego, zgodnie z procedurami nadzoru nad incydentami bezpieczeństwa oraz utrzymania ciągłości działania;
- e) zarządzanie uprawnieniami w zakresie uprawnień iostępów do systemów informatycznych w ramach procedury zarządzania uprawnieniami i dostępami;
- f) przydzielanie 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) wprowadzanie zmiany uprawnień w systemach informacyjnych na czas nieobecności pracownika zgodnie z wytycznymi kierownika jednostki/kierowników komórek organizacyjnych oraz planem zastępstw;

- h) dbanie o aktualizację Deklaracji stosowania zabezpieczeń w zakresie technicznych środków bezpieczeństwa wdrożonych w organizacji;
- i) sprawowanie nadzoru nad inwentaryzacją i jej aktualnością w odniesieniu do produktów, usług i procesów ICT służących do przetwarzania informacji;
- j) tworzenie, aktualizowanie i doskonalenie elementów składających się na plany ciągłości działania w Urzędzie w tym sprawuje nadzór nad kopiami zapasowymi;
- k) na bieżąco przesyłanie Inspektorowi Ochrony Danych informacji dotyczących 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) zbieranie informacji o zagrożeniach cyberbezpieczeństwa i podatnościach na incydenty systemu informacyjnego;
- m) monitorowanie infrastruktury teleinformatycznej 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.

§3. ASI w momencie objęcia funkcji składa oświadczenie, którego wzór stanowi załącznik nr 1 do Zarządzenia – wzór oświadczenia ASI.

§4. Zarządzenie wchodzi w życie z dniem podpisania.

§5. Traci moc zarządzenie Nr 50/26 Wójta Gminy Kiwity z dnia 15 czerwca 2026 r. w sprawie wyznaczenia Administratora Systemów Informatycznych w Urzędzie Gminy Kiwity

Załączniki:

załącznik nr 1 do Zarządzenia – wzór oświadczenia ASI.

WÓJT
Jacek Powlik

**Załącznik nr 1 do Zarządzenia w sprawie wyznaczenia Administratora Systemów Informatycznych –
wzór oświadczenia ASI**

.....
(dane Administratora)

....., dnia

OŚWIADCZENIE ADMINISTRATORA SYSTEMÓW INFORMATYCZNYCH

Niniejszym zobowiązuję się do zachowania poufności, nieujawniania osobom nieupoważnionym i zachowania w tajemnicy wszelkich informacji prawnie chronionych i danych, z którymi mam styczność podczas wykonywania powierzonych mi zadań, a dane te nie są danymi publicznymi.

Potwierdzam, że zapoznałem/am się z dokumentacją składającą się na System Zarządzania Bezpieczeństwem Informacji wprowadzoną u administratora, w tym Polityką Bezpieczeństwa Informacji oraz wszelkimi regulacjami i procedurami z tego zakresu, wprowadzonymi przez Administratora Danych.

Wyznaczenie dotyczące pełnienia funkcji ASI wygasa z chwilą ustania Pana/Pani zatrudnienia lub współpracy (bez względu na podstawę prawną zatrudnienia lub współpracy) lub odwołania Pani/Pana przez Administratora z pełnienia ww. funkcji. Jednocześnie informuję, że zobowiązany(a) jest Pan(i) do zachowania w tajemnicy informacji w zakresie informacji prawnie chronionych, jak też danych osobowych i sposobów ich zabezpieczania, również po odwołaniu Pani/Pana z pełnienia ww. funkcji, a także po ustaniu zatrudnienia lub współpracy.

(podpis ASI)