

**ZARZĄDZENIE NR 15/23
WÓJTA GMINY NOWINKA**

z dnia 1 lutego 2023 r.

w sprawie wyznaczenia Administratora Systemu Informatycznego

Na podstawie art. 24 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 osobowych), art. 33 ust. 1 i 3 ustawy z dnia 8 marca 1990 r. ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2023 r. poz. 40) oraz § 20 Obwieszczenia Prezesa Rady Ministrów z dnia 9 listopada 2017 roku w sprawie ogłoszenia jednolitego tekstu rozporządzenia Rady Ministrów 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), zarządzam co następuje:

§ 1. 1. Wyznaczam Pana Leszka Surazyńskiego na Administratora Systemu Informatycznego z dniem 1 lutego 2023 r.

2. Traci moc zarządzenie Nr 97/19 Wójta Gminy Nowinka.

3. Zakres działania ASI stanowi załącznik do niniejszego zarządzenia.

§ 2. Zarządzenie wchodzi w życie z dniem podpisania.

Wójt Gminy Nowinka

Teresa Strękowska

Zakres zadań i uprawnień Administratora Systemów Informatycznych

1. Administrator Systemów Informatycznych, zwany dalej ASI, wykonuje zadania w zakresie niniejszego Zarządzenia oraz upoważnień i pełnomocnictw nadanych przez Administratora Danych Osobowych.
2. Celem działania ASI jest nadzorowanie i realizowanie zasad bezpieczeństwa przetwarzania i ochrony danych osobowych w systemach informatycznych Urzędu Gminy Nowinka.
3. ASI, realizując swoje zadania współpracuje z IOD w Urzędzie Gminy Nowinka.
4. Do zakresu zadań ASI należy w szczególności:
 - a) monitorowanie:
 - zbierania, przechowywania, przekazywania i udostępniania danych osobowych przetwarzanych w systemach informatycznych,
 - b) zabezpieczeń systemów informatycznych w zakresie stosowania:
 - Firewall/VPN oraz programów antywirusowych,
 - szyfrowania dysków i środków ochrony kryptograficznej,
 - mechanizmów autoryzacji i kontroli dostępu do danych (uwierzytelnianie użytkowników, hasła),
 - zabezpieczenia przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do baz danych osobowych;
 - c) nadzorowanie:
 - zakładania, blokowania, zawieszania i uaktywniania kont w systemie informatycznym,
 - logicznych i informatycznych zabezpieczeń systemów w zakresie:
 - przepływu informacji pomiędzy systemami informatycznymi a siecią publiczną,
 - działań inicjowanych z sieci i z systemów informatycznych,
 - umów i procedur przekazywania podmiotowi zewnętrznemu dostępu do systemów informatycznych oraz elektronicznych nośników informacji zawierających dane osobowe,
 - tworzenia kopii zapasowych zbiorów danych osobowych,
 - zasad ochrony, przekazywania i niszczenia kopii zapasowych zbiorów danych osobowych oraz programów zastosowanych do ich przetwarzania,
 - d) realizowanie przedsięwzięć w zakresie:
 - wyjaśniania i dokumentowania, wspólnie z IOD, przypadków naruszenia zasad bezpieczeństwa systemów informatycznych,
 - dokonywania oceny zgodności programów z przepisami bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych, kontrolowania, wspólnie z IOD, pracowników w zakresie przestrzegania zasad bezpieczeństwa i ochrony danych osobowych poprzez prowadzone sprawdzenia (kontrole lub audyty).