

ZARZĄDZENIE NR 83.2021
WÓJTA GMINY WŁOSZAKOWICE

z dnia 7 września 2021 r.

w sprawie wyznaczenia Administratora Systemów Informatycznych w Urzędzie Gminy Włoszakowice.

Na podstawie art. 33 ust. 1, ust. 3 ustawy z dnia 8 marca 1990 roku o samorządzie gminnym (Dz. U. z 2021 r. poz. 1372), w związku z art. 24 ust. 1 i 2 rozporządzenia 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 przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) **zarządza się, co następuje:**

§ 1. 1. Wyznacza się Pana Marka Wodawskiego na Administratora Systemów Informatycznych (ASI) w Urzędzie Gminy Włoszakowice.

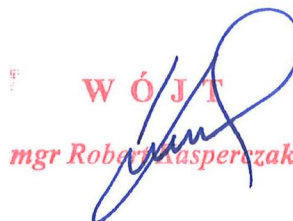
2. Administrator Systemów Informatycznych wykonuje zadania w zakresie niniejszego Zarządzenia oraz upoważnień i pełnomocnictw nadanych przez Administratora Danych Osobowych.

3. Zakres działania ASI stanowi załącznik do niniejszego zarządzenia.

§ 2. Zarządzenie podlega ogłoszeniu w Biuletynie Informacji Publicznej.

§ 3. Wykonanie zarządzenia powierza się Administratorowi Systemów Informatycznych.

§ 4. Zarządzenie wchodzi w życie z dniem podpisania.


WÓJTA
mgr Robert Kasperczak

ZAKRES DZIAŁANIA

ADMINISTRATORA SYSTEMÓW INFORMATYCZNYCH w Urzędzie Gminy Włoszakowice

Do zadań Administratora Systemów Informatycznych (ASI) należy realizowanie zadań w zakresie zarządzania i bieżącego nadzoru nad systemami informatycznymi, a w szczególności:

1. Formułowanie w uzgodnieniu z Administratorem Danych Osobowych i/lub osobami, do których administrator delegował zarządzanie uprawnieniami oraz Inspektorem Ochrony Danych (IOD) sposobu określania uprawnień w systemach informatycznych.

2. Rejestracja uprawnień użytkownika w systemach informatycznych, tj.:

- 1) tworzenie kont użytkowników w systemach informatycznych,
- 2) przypisywanie do kont, startowych haseł uwierzytelniających użytkowników tych kont,
- 3) resetowanie utraconych kont,
- 4) usuwanie kont i uprawnień dla tych kont osób, które tracą prawo dostępu do systemu.

3. Współpraca z IOD w zakresie kontroli nad przestrzeganiem zasad ochrony danych osobowych pod kątem zabezpieczeń teleinformatycznych, w tym m.in.:

- 1) współpraca przy przygotowaniu i wdrożeniu dokumentacji ochrony danych osobowych, w szczególności instrukcji zarządzania systemem informatycznym,
- 2) współpraca przy przeprowadzaniu okresowych planów sprawdzeń,
- 3) kontrola przeglądu i konserwacji systemów informatycznych służących do przetwarzania danych,
- 4) zabezpieczenie systemów służących do przetwarzania danych osobowych przed działaniem oprogramowania złośliwego.

4. Podejmowanie działań służących zapewnieniu:

- 1) ciągłości i niezawodności działania systemów, komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych osobowych w Urzędzie,
- 2) bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji,
- 3) odpowiednich działań w przypadku naruszeń w systemie zabezpieczeń,
- 4) zgodności z przepisami w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego.

5. Prowadzenie nadzoru nad:

- 1) naprawami, konserwacjami i likwidacją urządzeń komputerowych, na których zapisane są dane osobowe,
- 2) przeglądami, uaktualnieniem systemów służących do przetwarzania danych osobowych oraz podejmowanie natychmiastowych działań zabezpieczających stan systemu informatycznego w Urzędzie w przypadku otrzymania informacji o naruszeniu zabezpieczeń informatycznych. Powiadomienie o zaistnieniu tego faktu ADO oraz IOD,
- 3) przestrzeganiem zasad bezpieczeństwa w przypadku udostępnienia danych osobowych innym podmiotom drogą teletransmisji danych,
- 4) funkcjonowaniem mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych,
- 5) wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzeniem pod kątem ich dalszej przydatności do odtworzenia danych w przypadku awarii systemu,

- 6) legalnością oprogramowania wykorzystywanego na stacjach roboczych,
- 7) stanem środowiska IT, stanem sprzętu IT i wykorzystywanego oprogramowania oraz aktywności sieciowej użytkowników,
- 8) funkcjonowaniem zabezpieczeń wdrożonych w celu ochrony danych osobowych oraz bieżącego ich monitorowania,
- 9) prawidłowością archiwizacji oraz usuwania danych osobowych.

