ZARZĄDZENIE NR 1/2018
WÓJTA GMINY TUROŚL

z dnia 12 listopada 2018 r.

w sprawie w sprawie wyznaczenia Administratora systemów Informatycznych w Urzędzie Gminy Turośl

Na podstawie § 3 ust. 1 Polityki Bezpieczeństwa Danych Osobowych w Urzędzie Gminy Turośl stanowiącej załącznik do Zarządzenia Nr 6/2018 Wójta Gminy Turośl z dnia 30 sierpnia 2018 roku w sprawie wprowadzenia Polityki Bezpieczeństwa Danych Osobowych w Urzędzie Gminy Turośl oraz art. 24 ust. 1 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 swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólnego rozporządzenie o ochronie danych osobowych /Dz. U. UE, L 119, 4.5.2016/) zarządzam, co następuje:

§ 1. W celu realizacji postanowień wynikających z uregulowań zawartych w Polityce Bezpieczeństwa Danych Osobowych w Urzędzie Gminy Turośl oraz obowiązków wynikających z wyżej wymienionego rozporządzenia, wyznaczam Pana Adama Lewandowskiego na Administratora Systemów Informatycznych (ASI) w Urzędzie Gminy Turośl.

§ 2. Zakres czynności dla Administratora Systemów Informatycznych stanowi załącznik do niniejszego zarządzenia.

§ 3. Zarządzenie wchodzi w życie z dniem podjęcia.

Wójt Gminy

Piotr Niedbała

Załącznik do zarządzenia Nr 1/2018
Wójta Gminy Turośl
z dnia 12 listopada 2018 r.

Zakres czynności Administratora Systemów Informatycznych w Urzędzie Gminy Turośl

1) prowadzenie monitoringu przetwarzania danych;
2) administrowanie systemem informatycznym;
3) zapewnienie optymalnej ciągłości działania systemu informatycznego;
4) nadzór nad naprawami, konserwacją oraz likwidacja urządzeń komputerowych, na których zapisane są dane osobowe;
5) nadawanie, zmiana i blokowanie uprawnień do systemów informatycznych;
6) właściwa konfiguracja systemu informatycznego zapewniająca jego bezpieczeństwo i ograniczenie dostępu do danych osobowych przez osoby nieupoważnione;
7) monitorowanie funkcjonowania zabezpieczeń wdrożonych w celu ochrony danych osobowych;
8) zarządzanie hasłami użytkowników i nadzór nad przestrzeganiem procedur określających częstotliwość ich zmiany;
9) monitorowanie funkcjonowania zabezpieczeń nadzór nad czynnościami związanymi z prowadzeniem systemu sprawdzania oraz nadzorowanie wykonywanych procedur uaktualniania systemów antywirusowych i ich konfiguracji;
10) podejmowanie działań w przypadku wykrycia naruszeń bezpieczeństwa w systemie zabezpieczeń lub podejrzenia naruszeń;
11) nadzór nad wykorzystywanym oprogramowaniem oraz jego legalnością;
12) nadzór nad wykonywaniem i przechowywaniem kopii zapasowych.
13) nadzór nad przeglądami, konserwacjami oraz uaktualnieniami systemów służących do przetwarzania danych osobowych;
14) prowadzenie ewidencji sprzętu informatycznego oraz oprogramowania;
15) informowanie na bieżąco ADO i IOD o przypadkach awarii programów wynikających z posługiwania się przez użytkowników nieautoryzowanym oprogramowaniem oraz niewłaściwego wykorzystywania sprzętu komputerowego;
16) pomoc IOD w przeprowadzeniu analizy ryzyka.