Zarządzenie nr 29/200
Burmistrza Zaklikowa
z dnia 23.03.2020 r.

w sprawie powołania Administratora Systemu Informatycznego

Art. 24, 32 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 (ogólne rozporządzenie o ochronie danych) z dnia 27 kwietnia 2016 r. (Dz. Urz. UE. L Nr 119, str. 1) wskazuje, że Administrator powinien zapewnić odpowiednie środki techniczne oraz organizacyjne gwarantujące bezpieczeństwo przetwarzanych danych osobowych.

W związku z powyższym wyznaczam z dniem 23.03.2020 Pana Grzegorza Janik na Administratora Systemu Informatycznego w Urzędzie Miejskim z siedzibą w Zaklikowie

§ 1

Zakres czynności dla Administratora Systemu Informatycznego stanowi załącznik nr 1 do niniejszego zarządzenia.

§ 2

Upoważnienie ważne jest do odwołania.

§ 3

Zarządzenie wchodzi w życie z dniem podpisania

BURMISTRZ
Dariusz Toczyski

Załącznik nr 1 do Zarządzenia nr 29/2020
***Burmistrza** Zaklikowa*
z dnia 23.03.2020 r.

Zakres czynności Administratora Systemu Informatycznego w Urzędzie Miejskim z siedzibą w Zaklikowie :

Nadzór nad stosowaniem środków zapewniających bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych, a w szczególności przeciwdziałających dostępowi osób niepowołanych do tych systemów (administrowanie system informatycznym).

1. Wspieranie Administratora przy wdrażaniu dokumentacji z zakresu ochrony danych osobowych, w szczególności w kwestiach zarządzania systemem informatycznym.
2. Nadzorowanie działania mechanizmów uwierzytelnienia użytkowników oraz kontroli dostępu do systemu informatycznego.
3. Nadawanie haseł użytkownikom.
4. Kontrolowanie zastosowanych środków technicznych i organizacyjnych zapewniających ochronę danych osobowych przetwarzanych w systemach informatycznych w tym m.in. systemu antywirusowego, awaryjnego zasilania komputerów, konserwacja oraz uaktualnianie systemów informatycznych.
5. Podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń, identyfikacja i analiza zagrożeń oraz ocena ryzyka, na które może być narażone przetwarzanie danych osobowych w systemach informatycznych i tradycyjnych.
6. Sprawowanie nadzoru nad przechowywanymi kopiami zapasowymi.
7. Inicjowanie i nadzór nad wdrażaniem nowych narzędzi, procedur organizacyjnych oraz sposobów zarządzania systemami informatycznymi, które mają doprowadzić do wzmocnienia bezpieczeństwa przy przetwarzaniu danych osobowych.
8. Opracowanie planów awaryjnych w zakresie zapewnienia ciągłości działania i odtwarzania systemów informatycznych, między innymi przez systematyczne wykonywanie kopii zapasowych.
9. Podejmowanie działań służących zapewnieniu niezawodności zasilania urządzeń wraz z zapewnieniem awaryjnego źródła zasilania oraz zabezpieczeń przed zakłóceniami w sieci zasilającej.
10. Prowadzenie ewidencji sprzętu teleinformatycznego oraz oprogramowania.
11. Nadzorowanie napraw, konserwacji oraz likwidacji urządzeń komputerowych, na których zapisane są dane osobowe.
12. Informowanie na bieżąco Administratora o przypadkach awarii programów wynikających z posługiwania się przez użytkowników nieautoryzowanym oprogramowaniem, nie przestrzegania zasad używania programów antywirusowych, niewłaściwego wykorzystywania sprzętu komputerowego.
13. Prowadzenie dziennika zdarzeń w systemie informatycznym, w szczególności w zakresie prowadzonych prac interwencyjnych, aktualizacji, konserwacji oraz prowadzonych działań sprawdzających lub kontrolujących.

14. Poinformowanie Inspektora Ochrony Danych, w sytuacji stwierdzenia naruszenia zabezpieczeń systemu o danym naruszeniu i współpraca z Inspektorem Ochrony Danych przy usuwaniu naruszenia.
15. Dokonywanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji.
16. Przeprowadzenie co najmniej raz w roku audytu sprawdzającego stan zabezpieczenia Urzędu, pomieszczeń, programów oraz zabezpieczeń sieci informatycznej.
17. Przeprowadzanie testów penetracyjnych służących do mierzenia odporności systemu informatycznego na ataki i przesłanie raz na pół roku sprawozdania z ich przeprowadzenia do Inspektora Ochrony Danych.