Zarządzenie Nr 0050/ 183 / 2019

Wójta Gminy Polska Cerekiew z dnia 31 grudnia 2019 roku

w sprawie powołania Administratora Systemu Informatycznego w Urzędzie Gminy w Polskiej Cerekwi

Na podstawie 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, w celu obsługi i zabezpieczenia systemu informatycznego Administratora danych

p o w o ł u j ę

z dniem 1 stycznia 2020 roku Pana Łukasza Cieplińskiego

Administratorem Systemu Informatycznego w Urzędzie Gminy w Polskiej Cerekwi

§ 1

Zakres czynności dla Administratora Systemu Informatycznego stanowi załącznik do niniejszego Zarządzenia.

§ 2

Traci moc Zarządzenie Nr 0050/23/2016 Wójta Gminy Polska Cerekiew z dnia 8 marca 2016 roku w sprawie powołania Administratora Systemu Informatycznego.

§ 3

Zarządzenie wchodzi w życie z dniem 1 stycznia 2020 roku.

Wójt Gminy

Piotr Kanzy

Załącznik do Zarządzenia Nr 0050/183/2019 Wójta Gminy Polska Cerekiew z dnia 31.12.2019 roku w sprawie powołania Administratora Systemu Informatycznego w Urzędzie Gminy w Polskiej Cerekwi

Zakres czynności dla Administratora Systemu Informatycznego w Urzędzie Gminy w Polskiej Cerekwi :

1. zarządzanie systemami i uprawnieniami użytkowników (w tym logowaniem oraz hasłami użytkowników systemów informatycznych),

2. zapewnienie sprawności i konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych przetwarzających zbiory danych osobowych,

3. realizowanie wytycznych określonych w Polityce Bezpieczeństwa Informacyjnego i dokumentach pochodnych na powierzonych systemach informatycznych i informacyjnych,

4. zgłaszanie IOD wszelkich problemów związanych z bezpieczeństwem informacji oraz bezpieczeństwem danych osobowych,

5. identyfikowanie, ocena oraz stały pomiar poziomu bezpieczeństwa w powierzonych systemach informatycznych,

6. przydzielanie uprawnienia wszystkim wskazanym przez osoby funkcyjne użytkownikom identyfikator oraz hasło do systemu informatycznego oraz dokonywanie ewentualnych modyfikacji uprawnień, a także blokowanie kont użytkowników zgodnie z zasadami określonymi w instrukcji zarządzania systemami informatycznymi służącym do przetwarzania danych osobowych,

7. podejmowanie działań w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego,

8. zarządzanie kontami użytkowników (zakłada, usuwa, edytuje, nadaje uprawnienia) we wszystkich systemach informatycznych ADO, nad którymi sprawuje nadzór w wyniku pełnionych obowiązków,

9. w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informowanie IOD o naruszeniu i współdziałanie z nim przy usuwaniu skutków naruszenia, opracowywanie szczegółowej dokumentacji naruszeń bezpieczeństwa danych osobowych,

10. wykonywanie samodzielnie lub sprawowanie nadzoru nad wykonywaniem (w przypadku ich powierzenia innej osobie) napraw, konserwacji oraz likwidacji urządzeń komputerowych, na których zapisane są dane osobowe, wykonywanie samodzielnie lub sprawowanie nadzoru nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego,

11. planowanie ciągłości działania, które dotyczy zestawu czynności w zakresie tworzenia, weryfikacji i aktualizacji planów wznawiania działania po awarii (np.: niedostępności systemów informatycznych lub uszkodzenia danych przetwarzanych w postaci elektronicznej) w umożliwiającym realizowanie przez ADO codziennych zadań,

12. wdrażanie środków technicznych umożliwiających ochronę danych osobowych, przetwarzanych w postaci elektronicznej, przed zniszczeniem, nieuprawnionym ujawnieniem, zmianą, dostępem oraz kradzieżą,

13. informowanie o dostępnych środkach, metodach oraz narzędziach ochrony danych osobowych, przetwarzanych w postaci elektronicznej, ADO oraz IOD i konsultowanie z nimi ich wdrożenia.

ASI posiada uprawnienia do:

14. sprawowania stałego nadzoru nad przetwarzaniem danych osobowych w postaci elektronicznej, w sposób bezpieczny wobec wszystkich pracowników ADO (łącznie z osobami piastującymi stanowiska kierownicze),

15. sprawowania stałego nadzoru nad przetwarzaniem danych osobowych w sposób bezpieczny wobec podmiotów zewnętrznych przetwarzających dane osobowe, dla których Podmiot sprawuje funkcję ADO,

16. zarządzanie autoryzacją użytkowników, w tym kontrola i zarządzanie hasłami do wszystkich systemów informatycznych, które ASI nadzoruje.