Zarządzenie Nr 0050/12/18
Wójta Gminy Krupski Młyn
z 29 stycznia 2018 roku

w sprawie: zmiany Regulaminu Organizacyjnego Urzędu Gminy Krupski Młyn.

Na podstawie art. 33 ust. 2 ustawy z dnia 8 marca 1990 roku o samorządzie gminnym (t.j. Dz. U. z 2017 r. poz. 1875 z późn. zm.)

z a r z ą d z a m , c o n a s t ę p u j e

§ 1

Dokonać zmiany w Regulaminie Organizacyjnym Urzędu Gminy Krupski Młyn nadanego Zarządzeniem Nr 0152/73/2003 Wójta Gminy Krupski Młyn z dnia 30 grudnia 2003 roku (t.j. Zarządzenie nr 0050/8/2018 Wójta Gminy Krupski Młyn z dnia 16 stycznia 2018 r.) w sposób następujący:

1. W rozdziale III Kierowanie Urzędem:
   a) w § 8 ust. 4 skreśla się słowa „Pełnomocnikiem ds. Ochrony Informacji Niejawnych oraz”,
   b) dodaje się ust. 5 o treści:
   „5. Pracownik ds. ewidencji ludności jest jednocześnie Pełnomocnikiem ds. Ochrony Informacji Niejawnych”.
2. W § 19 „Samodzielne stanowisko ds. informatyki” dotychczasową treść skreśla się i wprowadza nową w brzmieniu:
   „§ 19 Samodzielne stanowisko ds. informatyki”.

Do zakresu działania samodzielnego stanowiska ds. informatyki należy przede wszystkim:

1. Administrowanie gminną siecią informatyczną obsługującą Urząd Gminy Krupski Młyn i Gminny Zespół Oświatowy.
2. Zapewnienie poprawnego działania i bieżące utrzymanie sieci, przełączników, routerów, firewalli i towarzyszących im systemów informatycznych, instalacja i konfiguracja urządzeń sieci LAN i WAN.
3. Administrowanie serwerami, dokonywanie bieżących przeglądów i konserwacji.
4. Administrowanie bazami danych.
5. Administrowanie systemem antywirusowym, prowadzenie profilaktyki antywirusowej, szkolenia dla pracowników.
6. Zarządzanie systemami informatycznymi w celu zapewnienia sprawnego i efektywnego dostępu do zasobów oraz zabezpieczeniem prawidłowości działania sprzętu informatycznego.
7. Wykonywanie czynności związanych z diagnostyką, naprawą, modernizacją, usuwaniem awarii sprzętu komputerowego.

8. Usuwanie nieprawidłowości i zakłóceń w funkcjonowaniu oprogramowania komputerowego.
9. Nadzorowanie i konfigurowanie urządzeń peryferyjnych.
10. Nadzorowanie prawidłowości funkcjonowania i wykorzystywania sprzętu komputerowego.
11. Zapewnienie możliwie najwyższego poziomu bezpieczeństwa, ochrony haseł i dostępu do sieci.
12. Wykonywanie i weryfikowanie kopii bezpieczeństwa systemów i konfiguracji urządzeń.
13. Planowanie oraz wdrażanie i rozbudowa infrastruktury technicznej oraz systemów informatycznych.
14. Koordynowanie działań w zakresie informatyzacji oraz wdrażanie postępu technicznego w informatyzacji.
15. Dbanie o prawidłowe wydatkowanie środków publicznych na funkcjonowanie systemu informatycznego.
16. Przygotowywanie umów na usługi informatyczne i rozliczanie ich realizacji.
17. Zarządzanie pocztą elektroniczną, usługami hostingowymi (serwis BIP, Orange, Gronet).
18. Zarządzanie treścią Biuletynu Informacji Publicznej, konfiguracja dostępu, zakładanie kont użytkowników.
19. Administrowanie systemem elektronicznej komunikacji z Głównym Urzędem Statystycznym, instalowanie programów do sprawozdań, przesyłanie danych do GUS.
20. Prowadzenie szkoleń pracowników w zakresie obsługi sprzętu informatycznego, oprogramowania, ochrony i bezpieczeństwa danych.
21. Wsparcie techniczne dla użytkowników w zakresie problemów związanych ze środowiskiem informatycznym.
22. Zabezpieczenie dokumentacji dotyczącej licencji oprogramowania.
23. Analizowanie problemów związanych z legalnością stosowanego oprogramowania komputerowego.
24. Wykonywanie napraw sprzętu komputerowego, wymiana uszkodzonych części i podzespołów oraz koordynowanie spraw w zakresie wykonywania większych remontów i usuwania awarii.
25. Wykonywanie instalacji i aktualizacji systemów oraz oprogramowania na stanowiskach roboczych.
26. Realizowanie obowiązków wynikających z przepisów ustawy o ochronie danych osobowych w zakresie informatyki.
27. Współpracowanie z inspektorem ds. ochrony danych osobowych i podinspektorem ds. promocji, sportu , bip, monitoringu wizyjnego i sieci szerokopasmowej.
28. Współpracowanie z pracownikami i kierownictwem urzędu w zakresie nadawania uprawnień dla użytkowników oraz opracowywania projektów i wdrażania regulaminów zabezpieczenia danych komputerowych, sprzętu i ochrony sieci informatycznych, instrukcji zarządzania systemem informatycznym oraz wspomaganie rejestracji zbiorów danych osobowych do GIODO.
29. Identyfikowanie i analiza zagrożeń oraz ryzyk, na które narażone może być przetwarzanie danych osobowych w systemach informatycznych.
30. Monitorowanie zabezpieczeń wdrożonych w celu ochrony danych osobowych w systemach informatycznych oraz ich przetwarzania.
31. Zgłaszanie i obsługa awarii oprogramowania komputerowego we współpracy z zewnętrznymi dostawcami, wnioskowanie o wprowadzenie zmian w oprogramowaniu po zgłoszeniu przez użytkownika systemu.

32. Kontrolowanie i zabezpieczanie prawidłowości przebiegu czynności serwisowych w zainstalowanych systemach informatycznych.
33. Utrzymywanie kontaktów z dostawcami telekomunikacyjnymi w zakresie dostarczania usług Internetu.
34. Pełnienie funkcji Lokalnego Administratora Systemu w zakresie Systemów Rejestrów Państwowych (ŹRODŁO), zgłaszanie spraw na portalu ATMOSFERA.
35. Planowanie i realizowanie wydatków budżetowych związanych z zakupami nowych urządzeń i programów oraz eksploatacją sprzętu komputerowego.
36. Wdrażanie oprogramowania, koordynowanie, nadzorowanie i dokonywanie odbioru prac wdrożeniowych.
37. Stosowanie środków technicznych mających na celu zabezpieczenie danych osobowych przed ujawnieniem.
38. Okresowe sprawdzanie kopii zapasowych pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu.
39. Przygotowywanie urządzeń, dysków lub innych informatycznych nośników zawierających dane osobowe do likwidacji i ich likwidacja.
40. Organizowanie i prowadzenie szkoleń informatycznych.
41. Zarządzanie działaniem elektronicznej skrzynki podawczej na platformie EPUAP. Konfiguracja, zakładanie kont, profilu zaufanego, użytkowników, pomoc w tworzeniu usług zgłoszonych do realizacji przez pracownika.
42. Określanie potrzeb w zakresie zabezpieczenia systemów informatycznych, w których przetwarzane są dane osobowe.
43. Prowadzenie spraw z zakresu kwalifikowanego podpisu elektronicznego pracowników, instalacja, konfiguracja i aktualizacja oprogramowania do podpisu elektronicznego.
44. Nadzorowanie nad zachowaniem spójności oprogramowania wdrażanego i eksploatowanego.
45. Wykonywanie czynności wspomagających zamknięcie roku w systemach księgowych (RADIX).
46. Zarzadzanie użytkownikami i administracja systemem Lex.
47. Poprawna konfiguracja certyfikatów pozwalających na przesyłanie danych do ZUS w programie Płatnik.
48. Nadzorowanie poprawnej pracy i administracja systemu PFRON.
49. Konfigurowanie i aktualizacja tokenów dla użytkowników bankowości elektronicznej.
50. Wdrażanie systemu Ferro.
51. Administrowanie usługą Office 365 i przyłączanie użytkowników.
52. Przyjmowanie paczek komunikacyjnych, otwieranie okresów sprawozdawczych oraz instalacja aktualizacji w systemie Bestia.
53. Wspomaganie systemów do zarządzania bazą OC, SHRIMP.
54. Opiniowanie inwestycji informatycznych i udział merytoryczny w inwestycjach informatycznych.
55. Udział merytoryczny w pozyskiwaniu środków unijnych związanych z zadaniami informatycznymi.

3. W § 27 „Pion ochrony informacji niejawnych dotychczasową treść skreśla się i wprowadza nową w brzmieniu:

„§ 27 Pion ochrony informacji niejawnych.

Do zakresu działania Pionu ochrony informacji niejawnych należy w szczególności:

1. zapewnienie ochrony informacji niejawnych, w tym stosowanie środków bezpieczeństwa fizycznego;
2. zarządzanie ryzykiem bezpieczeństwa informacji niejawnych, w szczególności szacowanie ryzyka;
3. kontrola ochrony informacji niejawnych oraz przestrzegania przepisów o ochronie tych informacji, w szczególności okresowa (co najmniej raz na trzy lata) kontrola ewidencji, materiałów i obiegu dokumentów;
4. opracowywanie i aktualizowanie, wymagającego akceptacji kierownika jednostki organizacyjnej, planu ochrony informacji niejawnych w jednostce organizacyjnej, w tym w razie wprowadzenia stanu nadzwyczajnego, i nadzorowanie jego realizacji;
5. prowadzenie szkoleń w zakresie ochrony informacji niejawnych;
6. prowadzenie zwykłych postępowań sprawdzających oraz kontrolnych postępowań sprawdzających;
7. prowadzenie aktualnego wykazu osób zatrudnionych lub pełniących służbę w jednostce organizacyjnej albo wykonujących czynności zlecone, które posiadają uprawnienia do dostępu do informacji niejawnych, oraz osób, którym odmówiono wydania poświadczenia bezpieczeństwa lub je cofnięto;
8. przekazywanie odpowiednio ABW do ewidencji, danych z prowadzonego wykazu osób uprawnionych do dostępu do informacji niejawnych, a także osób, którym odmówiono wydania poświadczenia bezpieczeństwa lub wobec których podjęto decyzję o cofnięciu poświadczenia bezpieczeństwa;
9. zawiadamianie ABW, zgodnie z właściwością, o przypadkach naruszenia przepisów o ochronie informacji niejawnych o klauzuli „poufne" lub wyższej;
10. prowadzenie kancelarii informacji niejawnych;
11. właściwe rejestrowanie, przechowywanie, obieg i wydawanie materiałów uprawnionym osobom;
12. egzekwowanie zwrotu dokumentów zawierających informacje niejawne;
13. prowadzenie bieżącej kontroli postępowania z dokumentami zawierającymi informacje niejawne, które zostały udostępnione pracownikom.

4. W załączniku nr 1 do Regulaminu Organizacyjnego zawierającym „wykaz stanowisk pracy”, skreśla się stanowisko:”ds. ochrony danych osobowych (0,125 etatu)” i wprowadza nowy zapis: „ds. ochrony danych osobowych (0,25 etatu)”.

§ 2

Wykonanie zarządzenia powierzam Sekretarzowi Gminy.

§ 3

Zarządzenie wchodzi w życie z dniem 1 lutego 2018 roku.