ZARZĄDZENIE Nr 32/10
Wójta Gminy Kruklanki
z dnia 27 lipca 2010 r.

w sprawie : zmiany Regulaminu Organizacyjnego Urzędu Gminy w Kruklankch

Na podstawie art. 33 ust. 2 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (tj. Dz. U. z 2001 r. Nr 142, poz. 1591 z póź. zm.) w związku z § 102 ust. 1 Statutu Gminy Kruklanki przyjętego uchwałą Nr XII/92/08 Rady Gminy Kruklanki z dnia 18 kwietnia 2008 r., zarządzam, co następuje:

§ 1.

W Regulaminie Organizacyjnym Urzędu Gminy w Kruklankch stanowiącego załącznik do Zarządzenia Nr 21/08 Wójta Gminy Kruklanki z dnia 27 maja 2008 roku; zm. z 2009r. zarządzenie Nr 28/09 i Nr 59/09, wprowadza się następujące zmiany:

1. W rozdziale **III STRUKTURA ORGANIZACYJNA URZĘDU**

   w § 9 dodaje się pkt 5) w brzmieniu:

   „ **5) PION OCHRONY - POIN"**
   Pion Ochrony tworzą:
   1. Pełnomocnik ds.ochrony informacji niejawnych,
   2. Administrator Bezpieczeństwa Informacji,
   3. Kierownik Kancelarii Tajnej, "

2. W rozdziale IV ZAKRESY DZIAŁANIA REFERATU, SAMODZIELNYCH I WIELOOSOBOWYCH STANOWISK PRACY ORAZ RADCY PRAWNEGO

1) w § 19 skreśla się pkt 30
2) w § 23 dodaje się pkt 17) w brzmieniu:
   „ 17) wykonywanie obowiązków Administratora Bezpieczeństwa Informacji."
3) § 25 otrzymuje brzmienie:

" **PION OCHRONY INFORMACJI NIEJAWNYCH**

Pion Ochrony tworzą:

1. Pełnomocnik do spraw Ochrony Informacji Niejawnych, do którego zadań należy w szczególności:

1) Zapewnienie ochrony informacji niejawnych,
2) Zapewnienie ochrony systemów i sieci teleinformatycznych, w których są wytwarzane, przetwarzane, przechowywane lub przekazywane informacje niejawne,
3) Kontrola ochrony informacji niejawnej, oraz przestrzegania przepisów o ochronie tych informacji,
4) Okresowa kontrola ewidencji, materiałów i obiegu dokumentów,
5) Opracowywanie planu ochrony informacji niejawnych,
6) Prowadzenie wykazu stanowisk i prac zleconych oraz osób dopuszczonych do pracy na stanowiskach z którymi wiąże się dostęp do informacji niejawnych.
7) Szkolenie pracowników w zakresie ochrony informacji niejawnych,
8) Prowadzenie zwykłych postępowań sprawdzających,
9) Nadzór merytoryczny nad Kierownikiem Kancelarii Tajnej.

2. Administrator Bezpieczeństwa Informacji, do którego zadań należy w szczególności:

1) nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których przetwarzane są dane osobowe oraz kontrolą przebywających w nich osób,
2) zapewnienie awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania,
3) dopilnowanie, aby komputery przenośne, w których przetwarzane są dane osobowe zabezpieczone były hasłem dostępu przed nieautoryzowanym uruchomieniem oraz aby mikrokomputery te nie były udostępniane osobom nieupoważnionym do przetwarzania danych osobowych,
4) nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych na których zapisane są dane osobowe,
5) zarządzanie hasłami użytkowników i nadzór nad przestrzeganiem procedur określających częstotliwość ich zmiany zgodnie z wytycznymi, które powinny być zawarte w instrukcji określającej sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji,
6) nadzór nad czynnościami związanymi ze sprawdzaniem systemu pod kątem obecności wirusów komputerowych, częstości ich sprawdzania oraz nadzorowanie wykonywania procedur uaktualniania systemów antywirusowych i ich konfiguracji,
7) nadzór nad wykonywaniem kopii awaryjnych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu,
8) nadzór nad przeglądami, konserwacjami oraz uaktualnieniami systemów służących do przetwarzania danych osobowych oraz wszystkimi innymi czynnościami wykonywanymi na bazach danych osobowych,
9) nadzór nad systemem komunikacji w sieci komputerowej oraz przesyłaniem danych za pośrednictwem urządzeń teletransmisji,
10) nadzór nad obiegiem oraz przechowywaniem dokumentów i wydawnictw zawierających dane osobowe generowane przez system informatyczny,
11) nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane osobowe oraz kontrolą dostępu do danych osobowych. Nadzorowanie, o którym mowa wyżej powinno obejmować:

- ustalenie identyfikatorów użytkowników i ich haseł (identyfikatory użytkowników należy wpisać do ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych - art. 39 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych),
- dopilnowanie, aby hasła użytkowników były zmieniane co najmniej raz na miesiąc,
- dopilnowanie aby dostęp do danych osobowych przetwarzanych w systemie był możliwy wyłącznie po podaniu identyfikatora i właściwego hasła,
- dopilnowanie, aby hasła użytkowników były trzymane w tajemnicy (również po upływie terminu ich ważności),
- dopilnowanie, aby identyfikatory osób, które utraciły uprawnienia do przetwarzania danych osobowych zastały natychmiast wyrejestrowane, a ich hasła unieważnione.

12) dopilnowanie, aby - jeżeli istnieją odpowiednie możliwości techniczne – ekrany monitorów stanowisk komputerowych, na których przetwarzane są dane osobowe, automatycznie wyłączały się po upływie ustalonego czasu nieaktywności użytkownika,
13) dopilnowanie, aby w pomieszczeniach, gdzie przebywają osoby postronne, monitory stanowisk dostępu do danych osobowych były ustawione w taki sposób, aby uniemożliwić tym osobom wgląd w dane,
14) podjęcie natychmiastowych działań zabezpieczających stan systemu informatycznego w przypadku otrzymania informacji o naruszeniu zabezpieczeń systemu informatycznego lub informacji o zmianach w sposobie działania programu lub urządzeń wskazujących na naruszenie bezpieczeństwa danych,
15) analiza sytuacji, okoliczności i przyczyn, które doprowadziły do naruszenia bezpieczeństwa danych (jeśli takie wystąpiło) i przygotowanie oraz przedstawienie administratorowi danych

odpowiednich zmian do instrukcji zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych,
16) śledzenie osiągnięć w dziedzinie zabezpieczania systemów informatycznych w ogóle i wdrażanie takich narzędzi, metod pracy oraz sposobów zarządzania systemem informatycznym, które bezpieczeństwo to wzmocnią,
17) przestrzeganie zasad i wymagań bezpieczeństwa systemu,
18) bieżąca kontrola zgodności funkcjonowania systemu teleinformatycznego ze szczególnymi wymaganiami bezpieczeństwa,
19) kontrola przestrzegania procesu bezpiecznej eksploatacji,
20) właściwe funkcjonowanie systemu teleinformatycznego,
21) zapewnienie obsługi informatycznej Urzędu, w tym tworzenie i administrowanie siecią oraz zarządzanie programami informatycznymi,
22) utrzymanie należytego stanu technicznego sprzętu komputerowego, egzekwowanie gwarancji, serwisowania oraz legalności oprogramowania,
23) planowanie rozwoju narzędzi informatycznych oraz organizowanie i wdrażanie zabezpieczeń systemów informatycznych,
24) analiza kosztów rzeczowych funkcjonowania narzędzi informatycznych Urzędu oraz dbanie o terminowe uiszczanie opłat z tym związanych,
25) zapewnianie łączności telekomunikacyjnej i informatycznej oraz dbałość o racjonalną gospodarkę w tym zakresie,
26) realizacja programu budowy społeczeństwa informacyjnego.

3. Kierownik Kancelarii Tajnej, do którego zadań należy:
Prowadzenie Kancelarii Tajnej, w tym w szczególności:
a) bezpośredni nadzór nad obiegiem dokumentów niejawnych w Urzędzie,
b) prowadzenie wymaganych rejestrów dokumentów,
c) udostępnianie lub wydawanie dokumentów zawierających informacje niejawne oznaczone klauzulami „poufne" lub „zastrzeżone", osobom posiadającym stosowne poświadczenie bezpieczeństwa,
d) egzekwowanie zwrotu dokumentów zawierających informacje niejawne,
e) kontrola przestrzegania właściwego oznaczania i rejestrowanie dokumentów w Kancelarii Tajnej w Urzędzie,
f) współpraca z pełnomocnikiem do spraw ochrony informacji niejawnych,
g) prowadzenie bieżącej kontroli postępowania z dokumentami zawierającymi informacje niejawne, które zostały udostępnione pracownikom.

§ 2

Zarządzenie wchodzi w życie z dniem podpisania.

Wójt Gminy
Władysław Gładkowski