Zarządzenie Nr 37/09
Wójta Gminy Banie Mazurskie
z dnia 08 października 2009 r.

w sprawie zmiany Regulaminu Organizacyjnego Urzędu Gminy Banie Mazurskie.

Na podstawie art. 33 ust. 2 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (tekst jednolity Dz. U. z 2001r. Nr 142, poz. 1591 z późn. zm.) **zarządza się**, co następuje:

§ 1

W Regulaminie określającym organizację i zasady funkcjonowania Urzędu Gminy Banie Mazurskie stanowiącym załącznik do Zarządzenia nr 2/2003 Wójta Gminy Banie Mazurskie z dnia 27 stycznia 2003r., z późniejszymi zmianami, wprowadza się następujące zmiany:

a) w Rozdziale III Struktura Organizacyjna Urzędu Gminy w Części I – referaty i samodzielne stanowiska pracy dodaje się punkt 15 w brzmieniu:
„ 15. Pion ochrony".

b) w Rozdziale IV „Zakresy zadań referatów i samodzielnych stanowisk pracy" § 7 otrzymuje brzmienie:

„ § 7. Zakres zadań i odpowiedzialności **Skarbnika** obejmuje:
1) opracowywanie projektu budżetu gminy,
2) nadzór i koordynację działań podejmowanych w zakresie prawidłowej realizacji budżetu gminy i przestrzegania dyscypliny finansów publicznych,
3) przygotowywanie okresowych analiz i sprawozdań z wykonania budżetu dla Rady Gminy i Wójta Gminy,
4) nadzór i koordynację działań w zakresie:
   a) prowadzenia rachunkowości w Urzędzie zgodnie z przepisami prawa,
   b) wykonywania przepisów ustaw: o finansach publicznych, dochodach jednostek samorządu terytorialnego, o podatkach i opłatach lokalnych oraz o opłacie skarbowej,
   c) gospodarowania środkami budżetowymi przez jednostki organizacyjne Urzędu i gminne jednostki organizacyjne, ze szczególnym uwzględnieniem prawidłowości zawierania umów pod względem finansowym,
5) wykonywanie zadań informatyka Urzędu , **za**kres spraw obejmuje :
   a) wdrażanie i eksploatację systemów komputerowych w Urzędzie, a w szczególności:
      - zakup sprzętu komputerowego i oprogramowania oraz zabezpieczenie dla niego serwisu gwarancyjnego i pogwarancyjnego,
   b) ustalenie dla poszczególnych stanowisk warunków, jakie musi spełniać program komputerowy, by usprawnił pracę tego stanowiska i ułatwił niezbędny obieg informacji między poszczególnymi stanowiskami pracy,
   c) wybieranie, przy współudziale merytorycznych pracowników, programów spełniających ustalone warunki na podstawie informacji uzyskanych w firmach informatycznych i sprawdzenia funkcjonowania tych programów w praktyce,

d) nadzór nad instalacją sprzętu i programów w komputerach,
e) ustalanie sposobów zabezpieczania danych, kodowania informacji bazy danych, listy i wartości parametrów niezbędnych do uruchomienia i obsługi stanowisk, sposobu i częstości archiwizacji i rekonstrukcji danych,
f) wprowadzanie zmian (nie naruszających praw autorskich) w programach i wydrukach na podstawie uwag użytkowników programów,
g) okresowe przeglądy sprzętu, nośników pamięci oraz warunków pracy na stanowiskach komputerowych,
h) konserwacja sprzętu i usuwanie usterek, zgłaszanie awarii sprzętu i programów firmom zobowiązanym do dokonywania napraw w ramach zawartych umów,
i) projekty urządzania dalszych stanowisk w ramach ogólnego programu komputeryzacji gminy,
j) konsultacje i wymiana informacji o programach wykorzystywanych w innych urzędach, propozycje usprawnienia wymiany tych informacji,
k) administrowanie siecią informatyczną w Urzędzie,

6) wykonywanie zadań Administratora Bezpieczeństwa Systemu Informatycznego zakres spraw obejmuje:

a) nadzór nad zabezpieczeniem pomieszczeń, w których przetwarzane są dane osobowe oraz kontrola przebywających w nich osób,
b) zapewnienie awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania,
c) zabezpieczenie komputerów, w których przetwarzane są dane osobowe w hasła dostępu przed nieautoryzowanym uruchomieniem oraz brakiem dostępu osób nieupoważnionych do przetwarzania danych osobowych,
d) nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych na których zapisane są dane osobowe,
e) 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 uwzględnienie wymogów bezpieczeństwa informacji (§ 11 ust. 2 pkt 1 rozporządzenia),
f) nadzór nad czynnościami związanymi ze sprawdzaniem systemu pod kątem obecności wirusów komputerowych, częstotliwości ich sprawdzania oraz nadzorowanie wykonywania procedur uaktualniania systemów antywirusowych i ich konfiguracji,
g) nadzór nad wykonywaniem kopii awaryjnych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu,
h) nadzór nad przeglądami, konserwacjami oraz uaktualnieniami systemów służących do przetwarzania danych osobowych oraz wszystkimi innymi czynnościami wykonywanymi na bazach danych osobowych,
i) nadzór nad systemem komunikacji w sieci komputerowej oraz przesyłaniem danych za pośrednictwem urządzeń teletransmisji,
j) nadzór nad obiegiem oraz przechowywaniem dokumentów i wydawnictw zawierających dane osobowe generowane przez system informatyczny,

k) 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),
- nadzór nad tym, aby hasła użytkowników były zmieniane co najmniej raz na miesiąc,
- kontrola dostępu do danych osobowych przetwarzanych w systemie, aby był możliwy wyłącznie po podaniu identyfikatora i właściwego hasła,
- nadzór nad hasłami użytkowników (również po upływie terminu ich ważności),
- kontrolowanie, wyrejestrowania identyfikatorów i unieważnienia haseł osób, które utraciły uprawnienia do przetwarzania danych osobowych .

l) kontrolowanie , - jeżeli istnieją odpowiednie możliwości techniczne – ekranów monitorów stanowisk komputerowych, na których przetwarzane są dane osobowe, automatycznie wyłączały się po upływie ustalonego czasu nieaktywności użytkownika,

ł) 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,

m) 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,

n) 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 (§11 ust. 1 rozporządzenia),

7) odpowiedzialność za:
   a) wykonanie określonych w niniejszym regulaminie zadań,
   b) organizację i funkcjonowanie systemu nadzoru i kontroli finansowej wszystkich jednostek organizacyjnych Urzędu Gminy oraz w ramach pełnomocnictw przyznanych przez Wójta Gminy - gminnych jednostek organizacyjnych. „

c) w Rozdziale V część I – Zakresy zadań referatów i samodzielnych stanowisk pracy dodaje się § 20 e. w brzmieniu:

„ § 20 e. Ochrona informacji niejawnych (IN) - Pion Ochrony, (Symbol PO).

1. Za ochronę informacji niejawnych w Urzędzie Gminy odpowiada Wójt Gminy.
2. Wójtowi podlega bezpośrednio pełnomocnik do spraw ochrony informacji niejawnych, zwany dalej "Pełnomocnikiem ochrony".

3. Pełnomocnik ochrony kieruje wyodrębnioną komórką organizacyjną do spraw ochrony informacji niejawnych (IN), zwaną dalej "pionem ochrony", do zadań którego należy:

a) zapewnienie ochrony informacji niejawnych w tym ich ochrony fizycznej,
b) zapewnienie ochrony systemów i sieci teleinformatycznych w których są wytwarzane, przetwarzane, przechowywane lub przekazywane informacje niejawne.
c) kontrola ochrony informacji niejawnych oraz przestrzegania przepisów o ochronie tych informacji,
d) okresowa kontrola ewidencji, materiałów i obiegu dokumentów,
e) opracowywanie planu ochrony informacji niejawnych i nadzorowanie jego realizacji,
f) szkolenie pracowników w zakresie ochrony informacji niejawnych według zasad określonych w przepisach w/w ustawy.
g) informowanie właściwej służby Agencji Bezpieczeństwa Wewnętrznego o fakcie wydania lub odmowy wydania poświadczenia bezpieczeństwa do poziomu „poufne" i „zastrzeżone".
h) prowadzenie i przechowywanie akt zakończonych zwykłych postępowań sprawdzających.
i) prowadzenie wykazu stanowisk i prac zleconych osób dopuszczonych do pracy na stanowiskach z dostępem do informacji niejawnych".

§ 2

Zarządzenie wchodzi w życie z dniem podpisania.

Wójt Gminy Banie Mazurskie

Jan Sobuta