Zarządzenie Nr 40/2021
Wójta Gminy Banie Mazurskie
z dnia 30 kwietnia 2021 roku

zmieniające zarządzenie w sprawie nadania Regulaminu Organizacyjnego Urzędu Gminy w Baniach Mazurskich.

Na podstawie art. 33 ust. 2 ustawy z dnia 8 marca 1990r. o samorządzie gminnym (t.j. Dz. U. z 2020r. poz. 713 z późn. zm.) zarządzam, co następuje:

§ 1. W zarządzeniu Nr 10/2021 Wójta Gminy Banie Mazurskie z dnia 29 stycznia 2021r. w sprawie nadania Regulaminu Organizacyjnego Urzędu Gminy w Baniach Mazurskich w Regulaminie Organizacyjnym Urzędu Gminy w Baniach Mazurskich stanowiącym załącznik do Zarządzenia wprowadza się następujące zmiany:

1) § 19 otrzymuje brzmienie:
„§ 19 Pion Ochrony.

1. Pion ochrony tworzą:
   1) Pełnomocnik ds. Ochrony Informacji Niejawnych, (POIN)
   2) Pracownik Kancelarii Materiałów Niejawnych,
   3) Inspektor Bezpieczeństwa Teleinformatycznego (IBTI)

2. Za ochronę informacji niejawnych w Urzędzie Gminy odpowiada Wójt.
3. Wójtowi podlega bezpośrednio Pełnomocnik ds. Ochrony Informacji Niejawnych, zwany dalej "Pełnomocnikiem Ochrony".
4. **Pełnomocnik ds. Ochrony Informacji Niejawnych**, do jego zadań należy:
   1) zapewnienie ochrony informacji niejawnych w tym ich ochrony fizycznej,
   2) zapewnienie ochrony systemów i sieci teleinformatycznych, w których są wytwarzane, przetwarzane, przechowywane lub przekazywane informacje niejawne.
   3) kontrola ochrony informacji niejawnych oraz przestrzegania przepisów o ochronie tych informacji,
   4) okresowa kontrola ewidencji, materiałów i obiegu dokumentów,
   5) opracowywanie planu ochrony informacji niejawnych i nadzorowanie jego realizacji,
   6) szkolenie pracowników w zakresie ochrony informacji niejawnych według zasad określonych w przepisach w/w ustawy,
   7) informowanie właściwej służby Agencji Bezpieczeństwa Wewnętrznego o fakcie wydania lub odmowy wydania poświadczenia bezpieczeństwa do poziomu „poufne" i „zastrzeżone".
   8) prowadzenie i przechowywanie akt zakończonych zwykłych postępowań sprawdzających,
   9) prowadzenie wykazu stanowisk i prac zleconych osób dopuszczonych do pracy na stanowiskach z dostępem do informacji niejawnych.
   10) klasyfikowanie, w imieniu Wójta informacji niejawnych,
   11) określanie w imieniu Wójta - szczegółowych wymagań w zakresie ochrony informacji niejawnych na poszczególnych stanowiskach pracy w Urzędzie,
   12) określanie w imieniu Wójta - odrębnie dla każdej klauzuli tajności stanowisk oraz rodzajów prac, z którymi może łączyć się dostęp do informacji niejawnych,
   13) wyrażanie w imieniu Wójta - zgody na udostępnianie informacji niejawnych stanowiących tajemnicę służbową,
   14) szkolenie pracowników Urzędu Gminy w zakresie ochrony informacji niejawnych,
   15) zapewnienie środków ochrony fizycznej informacji niejawnych wytwarzanych, przetwarzanych, przekazywanych i przechowywanych w Urzędzie Gminy.

5. Pracownik kancelarii materiałów niejawnych.

1) Kierowanie pracą kancelarii materiałów niejawnych w celu zapewnienia sprawnej i zgodnej z obowiązującymi przepisami prawa realizacji zadań, w szczególności:
   a) bezpośredni nadzór nad obiegiem materiałów niejawnych w Urzędzie Gminy;
   b) Zapewnienie możliwości ustalenia w każdych okolicznościach, gdzie znajduje się materiał niejawny pozostający w dyspozycji Urzędu Gminy, oraz kto z tym materiałem się zapoznał na podstawie ewidencji kancelaryjnej.
   c) udostępnianie materiałów niejawnych osobom do tego uprawnionym;
   d) wydawanie materiałów osobom do tego uprawnionym, które zapewniają odpowiednie warunki do ich przechowywania;
   e) egzekwowanie zwrotu materiałów niejawnych;
   f) kontrola przestrzegania właściwego oznaczania i rejestrowania materiałów w kancelarii oraz jednostce organizacyjnej;
   g) przygotowanie i uczestniczenie w kontroli stanu ewidencyjnego oraz obiegu materiałów niejawnych zgodnie z opracowanym harmonogramem;
   h) ustalenie w każdych okolicznościach, gdzie znajduje się materiał niejawny pozostający w dyspozycji Urzędu Gminy;
   i) prowadzenie bieżącej kontroli sposobu wytwarzania, obiegu, ochrony oraz przechowywania materiałów niejawnych;
   j) Prowadzenie (w elektronicznej lub wydruku) wykazu osób upoważnionych do dostępu informacji niejawnych na podstawie danych otrzymanych od pełnomocnika ds. ochrony informacji niejawnych zawierającym:
      - imię i nazwisko;
      - datę wydania, klauzula tajności, okres ważności posiadanych przez te osoby poświadczeń bezpieczeństwa lub upoważnienia;
      - numer zaświadczenia o odbyciu szkolenia w zakresie ochrony informacji niejawnych.

6. Inspektor Bezpieczeństwa Teleinformatycznego.

1) udział w procesie zarządzania ryzykiem w systemie teleinformatycznym oraz tworzeniu dokumentacji bezpieczeństwa systemu;

2) bieżąca kontrola zgodności funkcjonowania systemu teleinformatycznego ze szczególnymi wymaganiami bezpieczeństwa oraz przestrzegania procedur bezpiecznej eksploatacji, w ramach, której sprawdza:

   a) poprawność realizacji zadań Administratora systemu lub zastępcy administratora systemu, w szczególności właściwe zarządzanie konfiguracją oraz uprawnieniami przydzielanymi użytkownikom;

   b) znajomość i przestrzeganie przez użytkowników zasad ochrony informacji niejawnych oraz procedur bezpiecznej eksploatacji w systemie teleinformatycznym, a w szczególności w zakresie wykorzystania urządzeń i narzędzi służących do ochrony informacji niejawnych w systemie teleinformatycznym;

   c) stan zabezpieczeń systemu teleinformatycznego, w szczególności analizując rejestry zdarzeń systemu teleinformatycznego;

3) organizowanie i prowadzenie szkoleń;

4) monitorowanie zmian (np. w funkcjonowaniu mechanizmów zabezpieczeń, aktualizacji oprogramowania itp.);

5) reagowanie na sygnały o incydentach w zakresie bezpieczeństwa, wyjaśnianie ich przyczyn, raz na kwartał przeglądanie i dokumentowanie logów systemowych;

6) przeprowadzanie okresowej analizy zagrożeń;

7) tworzenie planów awaryjnych i organizowanie treningów w ich realizacji;

8) informowanie Pełnomocnika Ochrony o wszelkich zdarzeniach związanych lub mogących mieć związek z bezpieczeństwem systemu teleinformatycznego;

9) Prowadzenie dziennika Inspektora bezpieczeństwa teleinformatycznego;

10) Prowadzenie okresowych szkoleń dla użytkowników systemu teleinformatycznego w zakresie bezpieczeństwa ochrony informacji niejawnych;

11) Prowadzenie razem z Administratorem systemu lub zastępca administratora systemu okresowych testów bezpieczeństwa systemu teleinformatycznego;

12) Informowanie Pełnomocnika Ochrony o wszelkich zdarzeniach związanych lub mogących mieć wpływ na bezpieczeństwo systemu teleinformatycznego".

2) Po § 19 dodaje się § 19 a. w brzmieniu:

„§ 19 a. 1. Administrator Systemu.

1) Udział w procesie zarządzania ryzykiem w systemie teleinformatycznym oraz tworzenie dokumentacji bezpieczeństwa systemu;

2) Utrzymanie zgodności dokumentacji bezpieczeństwa z konfiguracją systemu teleinformatycznego;

3) Tworzenie, usuwanie i blokowanie kont użytkowników, wdrażanie uprawnień w systemie wynikających z przydzielonych praw dostępu, przydzielanie pierwszych haseł;

4) Szkolenie użytkowników;

5) Konfigurowanie urządzeń i oprogramowania;

6) Monitorowanie zmian (np. w funkcjonowaniu mechanizmów zabezpieczeń, itp.);

7) Przeglądanie plików zawierających informacje o wybranych zdarzeniach w systemie – logów systemowych;

8) Reagowanie na sygnały o incydentach w zakresie bezpieczeństwa i usuwanie ich skutków;

9) Informowanie przełożonych i Inspektora bezpieczeństwa teleinformatycznego o wszelkich zdarzeniach związanych lub mogących mieć związek z bezpieczeństwem systemu TI;

10) Prowadzenie dziennika administratora systemu;;

11) Prowadzenie razem z Inspektorem bezpieczeństwa teleinformatycznego okresowych testów bezpieczeństwa systemu teleinformatycznego;

12) Reagowanie wspólnie z Inspektorem bezpieczeństwa teleinformatycznego na incydenty bezpieczeństwa występujące w systemie teleinformatycznym;

13) Zgłaszanie do Pełnomocnika Ochrony potrzeb w zakresie serwisowania i certyfikacji środków ochrony elektromagnetycznej;

14) Prowadzenie wykazu osób mających dostęp do systemu teleinformatycznego zawierający, co najmniej: imię i nazwisko, posiadane poświadczenie bezpieczeństwa (jego numer, klauzulę i datę ważności) oraz przydzielanie użytkownikom konta, zgodnie z uprawnieniami nadanymi przez kierownika jednostki organizacyjnej.

2. Inspektor Ochrony Danych (IOD).

1) sprawowanie nadzoru nad przestrzeganiem przepisów o ochronie danych osobowych i informowanie Administratora oraz wszystkich osób przetwarzających dane o obowiązkach na nich spoczywających,
2) prowadzenie szkoleń z zakresu ochrony danych osobowych,
3) aktualizowanie i sprawowanie nadzoru nad dokumentacją z zakresu ochrony danych osobowych, w tym Polityką ochrony danych,
4) współpraca z Administratorem w zakresie oceny adekwatności i aktualności wdrożonego w jednostce rejestru czynności przetwarzania danych osobowych, a w razie potrzeby wspólnie z Administratorem dokonywanie jego bieżącej aktualizacji,
5) współpraca z Administratorem w zakresie oceny skutków planowanych operacji przetwarzania danych,
6) pełnienie funkcji punktu kontaktowego dla Prezesa Urzędu Ochrony Danych Osobowych w kwestiach związanych z przetwarzaniem danych osobowych,
7) sprawowanie nadzoru nad naruszeniami ochrony danych osobowych,
8) opiniowanie wpływających wniosków pod kątem ochrony danych osobowych,
9) Sprawowanie nadzoru nad procesem wydawania upoważnień i uprawnień do przetwarzania danych osobowych oraz systemów informatycznych,
10) prowadzenie spraw w zakresie udostępniania kopii przetwarzanych danych osobowych, udzielanie odpowiedzi na wniosek o cel, zakres, ujawnienie oraz okres przechowywania danych,
11) realizowanie procedury dotyczącej: sprostowania/uzupełniania, usuwania, danych osobowych, przenoszenia oraz sprzeciwu w zakresie przetwarzania danych osobowych,
12) opiniowanie umowy powierzenia przetwarzania danych osobowych.

3. Administrator Systemów Informatycznych (ASI).

1) Prowadzi nadzór i realizację zasad bezpieczeństwa przetwarzania i ochrony danych osobowych w systemach informatycznych Urzędu Gminy.

2) Pełni nadzór i kontrolę realizacji przedsięwzięć określonych w art. 36 ust. 1 i w art. 38 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. oraz w rozporządzeniu MSWiA z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

3) ASI, realizując swoje zadania współpracuje z Inspektorem Ochrony Danych w Urzędzie Gminy Banie Mazurskie.
4) **Zakres spraw ASI w szczególności 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,

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,

5) 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:
a) 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),
b) nadzór nad tym, aby hasła użytkowników były zmieniane, co najmniej raz na miesiąc,
c) kontrola dostępu do danych osobowych przetwarzanych w systemie, aby był możliwy wyłącznie po podaniu identyfikatora i właściwego hasła,
d) nadzór nad hasłami użytkowników (również po upływie terminu ich ważności),
e) kontrolowanie, wyrejestrowania identyfikatorów i unieważnienia haseł osób, które utraciły uprawnienia do przetwarzania danych osobowych.
f) kontrolowanie, - jeżeli istnieją odpowiednie możliwości techniczne – ekranów monitorów stanowisk komputerowych, na których przetwarzane są dane osobowe, tak, aby automatycznie wyłączały się po upływie ustalonego czasu nieaktywności użytkownika,
g) 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,
h) 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,
i) 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. 1rozporządzenia),

6) Realizowanie przedsięwzięć w zakresie:

a) prowadzenia analizy bezpieczeństwa systemów informatycznych w celu określania zabezpieczeń technicznych, zapewniających skuteczną ochronę danych osobowych przetwarzanych w systemach informatycznych,

b) wyjaśniania i dokumentowania przypadków naruszania zasad bezpieczeństwa systemów informatycznych przed Administratorem Bezpieczeństwa Informacji,

c) prowadzenia opisów struktur zbiorów danych osobowych oraz schematów przepływu danych pomiędzy systemami informatycznymi,

d) dokonywania oceny zgodności aplikacji z przepisami bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych,

e) parafowania umów związanych z konserwacją, wdrażaniem oprogramowania, aplikacji, urządzeń i systemów informatycznych w zakresie stosowania zapisów bezpieczeństwa przetwarzania i ochrony danych osobowych w Urzędzie Gminy".

3) Załącznik do Regulaminu otrzymuje brzmienie:

Załącznik
do Regulaminu Organizacyjnego
Urzędu Gminy w Baniach Mazurskich

SZCZEGÓŁOWA STRUKTUR ORGANIZACYJNA URZĘDU GMINY W BANIACH MAZURSKICH

Lp.	Referat (symbol)	Stanowiska kierownicze	Stanowiska pracy	Ilość etatów
1.	WG	Wójt Gminy		1
2.	SG	Sekretarz Gminy		1
3.	Referat Finansowy (Fn)	Skarbnik Gminy Kierownik Referatu		1
			ds. księgowości budżetowej i podatku VAT	1
			ds. księgowości podatkowej	1
			ds. wymiaru podatków	1
			ds. rozliczeń finansowych płac i ewidencji majątku komunalnego	1
			ds. rozliczeń finansowych i działalności gospodarczej	1
			pomoc administracyjna	1
4.	Referat Organizacyjny (Or)	Kierownik Referatu		1
			ds. kadr i oświaty	
			ds. ewidencji ludności	1/2
			ds. współpracy z organizacjami pozarządowymi i spraw obronnych	1
			ds. obsługi biura Rady Gminy, współpracy z sołectwami i promocji gminy	1
			ds. obsługi informatycznej urzędu	1
			sekretarka	1

5.	Referat Gospodarki Komunalnej, Inwestycji i Ochrony Środowiska (GKIŚ)	Kierownik Referatu	ds. zamówień publicznych	1
		Zastępca Kierownika Referatu GKIŚ	ds. pozyskiwania funduszy zewnętrznych i ochrony środowiska	1
			ds. mienia komunalnego i gospodarki mieszkaniowej	1
			ds. gospodarki przestrzennej, inwestycji i funduszu sołeckiego	1
			ds. cmentarzy i transportu zbiorowego	1
			pomoc administracyjna	1
			robotnik gospodarczy	1
			kierowca — robotnik gospodarczy	1
			kierowca - operator równiarki	1
			robotnik gospodarczy - opiekun	1
			sprzątaczka	1
6.	Urząd Stanu Cywilnego (USC)	Kierownik USC		0
		Zastępca Kierownika USC		1/2
7.	Radca Prawny (RP)			1/2
8.	Pion Ochrony Informacji Niejawnych (IN)		Pełnomocnik ds. Ochrony Informacji Niejawnych	0
			Pracownik kancelarii materiałów niejawnych	0
			Inspektor Bezpieczeństwa Teleinformatycznego	0
9.	Koordynator ds. dostępności (KD)		Koordynator ds. dostępności	0
10.	Inspektor Ochrony Danych (IOD)		Inspektor Ochrony Danych	0

11.	Administrator Systemów Informatycznych (ASI)		Administrator Systemów Informatycznych	0
12.	Administrator Systemu (AS)		Administrator Systemu	0

§ 2. Dopuszcza się możliwość okresowego zwiększenia zatrudnienia w celu wykonania określonych prac po uprzednim zawarciu stosownych umów na organizację tych prac z Powiatowym Urzędem Pracy.

§ 3. Zarządzenie wchodzi w życie z dniem podjęcia.

WÓJT GMINY
Łukasz Kuliś

Barbara Woźniak
RADCA PRAWNY
BŁ-S-169