ZARZĄDZENIE NR 90 /2012
WÓJTA GMINY BOROWIE

z dnia 27 grudnia 2012 r.

w sprawie ochrony informacji niejawnych w Urzędzie Gminy Borowie.

Na podstawie art. 43 ust.3,4 i 5 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. Nr182, poz.1228) zarządzam, co następuje:

§ 1. W Urzędzie Gminy na czas „ P ” nie istnieje Kancelaria Tajna.

§ 2. Za ewidencjonowanie, wytwarzanie i przechowywanie dokumentacji niejawnej w Urzędzie Gminy czynię odpowiedzialną osobę zatrudnioną na stanowisku Inspektora ds. obronnych, OC i zarządzania kryzysowego.

§ 3. W celu zapewnienia ochrony informacji niejawnych oraz dostosowania przepisów o ochronie informacji niejawnych zatwierdzam:

1. Dokumentację określającą poziom zagrożeń związanych z nieuprawnionym dostępem do informacji niejawnych lub ich utratą, stanowiącą załącznik. nr 1 do niniejszego zarządzenia.

2. Instrukcję dotyczącą sposobu i trybu przetwarzania informacji niejawnych o klauzuli „zastrzeżone” w podległych komórkach organizacyjnych oraz zakres i warunki stosowania środków bezpieczeństwa fizycznego w celu ich ochrony, stanowiącą załącznik nr 2 do niniejszego zarządzenia.

3. Instrukcję dotyczącą sposobu i trybu przetwarzania informacji niejawnych o klauzuli „poufne” w podległych komórkach organizacyjnych, stanowiącą załącznik nr 3 do niniejszego zarządzenia.

4. Instrukcję zarządzania systemem informatycznym przy przetwarzaniu informacji niejawnych o klauzuli „ ZASTRZEŻONE ” stanowiącą załącznik nr 4 do niniejszego zarządzenia

§ 4. Przetwarzanie materiałów o klauzuli "poufne" i "zastrzeżone" odbywa się w pomieszczeniu Nr 7 Urzędu Gminy.

§ 5. Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT GMINY
Wójt Gminy
mgr inż. Wiesław Gąska
Wiesław Gąska

Załącznik Nr 1 do Zarządzenia Nr /2012
Wójta Gminy Borowie
z dnia grudnia 2012 r.

Dokumentacja określająca poziom zagrożeń związanych z nieuprawnionym dostępem do informacji niejawnych lub ich utratą.

I. Wymagania bezpieczeństwa fizycznego.

A. Środki bezpieczeństwa fizycznego:

1. Szafy – kategoria K1 – K1S1 x K1S2

Lp.	Środek bezpieczeństwa	Poziom zagrożenia (liczba punktów)			Ocena jednostki
		Niski	Średni	Wysoki	
1	**2**	**3**	**4**	**5**	**6**
1.	Konstrukcja szafy K1S1	2	3	4	**2**
2.	Zamek do szafy K1S2	2	3	4	**2**
3.	**Kategoria K1**	4	9	16	**4**

2. Pomieszczenie – kategoria K2 - K2S1 x K2S2

Lp.	Środek bezpieczeństwa	Poziom zagrożenia (liczba punktów)			Ocena jednostki
		Niski	Średni	Wysoki	
1	**2**	**3**	**4**	**5**	**6**
1.	Konstrukcja pomieszczenia K2S1	2	3	4	**2**
2.	Zamek do drzwi pomieszczenia K1S2	2	3	4	**2**
3.	**Kategoria K2**	4	9	16	**4**

3. Budynki – kategoria K3

Lp.	Środek bezpieczeństwa	Poziom zagrożenia (liczba punktów)			Ocena jednostki
		Niski	Średni	Wysoki	
1	**2**	**3**	**4**	**5**	**6**
3.	**Kategoria K3**	2	3	5	**2**

4. **Kontrola dostępu – kategoria K4 – K4S1 + K4S2**

Lp.	Środek bezpieczeństwa	Poziom zagrożenia (liczba punktów)			Ocena jednostki
		Niski	Średni	Wysoki	
1	**2**	**3**	**4**	**5**	**6**
1.	System kontroli dostępu K4S1	2	3	4	**2**
2.	Kontrola interesantów K4S2	1	1	3	**1**
3.	**Kategoria K4**	3	4	7	**3**

5. **Personel bezpieczeństwa, systemy sygnalizacji napadu i włamania – kategoria K5 – K5S1 + K5S2**

Lp.	Środek bezpieczeństwa	Poziom zagrożenia (liczba punktów)			Ocena jednostki
		Niski	Średni	Wysoki	
1	**2**	**3**	**4**	**5**	**6**
1.	Personel bezpieczeństwa K5S1	2	3	5	**1**
2.	System sygn. Nap. I włamania K5S2	2	3	4	**3**
3.	**Kategoria K2**	4	6	9	**4**

6. **Granice – kategoria K6 – K6S1 + K6S2 + K6S3 + K6S4 + K6S5 + K6S6**

Lp.	Środek bezpieczeństwa	Poziom zagrożenia (liczba punktów)			Ocena jednostki
		Niski	Średni	Wysoki	
1	**2**	**3**	**4**	**5**	**6**
1.	Ogrodzenie K6S1	2	3	4	**3**
2.	Kontrola w punkt. dostępu K6S2	0	0	1	**0**
3.	System kontr. Osób i przedm. przy wejściu /wyjściu K6S3	0	0	1	**1**
4.	System wykrywania naruszeń ogrodzenia K6S4	0	0	1	**1**
5.	Oświetlenie chronionego obszaru K6S5	0	0	1	**0**
6.	System dozoru wizyjnego granic	0	0	1	**0**
7.	**Kategoria K2**	2	3	9	**5**

Łącznie środki bezpieczeństwa fizycznego : 4 + 4 + 2 + 3 + 4 + 5 = 22

B. Podstawowe wymagania bezpieczeństwa fizycznego :

Lp.	Najwyższa klauzula tajności inf. przetw. w jedn. organizac	Poziom zagrożenia (liczba punktów)			Ocena jednostki
		Niski	Średni	Wysoki	
1	2	3	4	5	6
	POUFNE				
1.	Obowiązkowe K1 + K2 + K3	10	21	37	10
2.	Obowiązkowe K4 + K5	7	10	16	7
3.	Dodatkowe K6	2	3	9	5
4.	Łącznie suma punktów	19	34	62	22
5.	Poziom zagrożenia		X		

Lp.	Najwyższa klauzula tajności inf. przetw. w jedn. organizac	Poziom zagrożenia (liczba punktów)			Ocena jednostki
		Niski	Średni	Wysoki	
1	2	3	4	5	6
	ZASTRZEŻONE				
1.	Obowiązkowe K1 + K2 + K3	10	21	37	10
2.	Dodatkowe K4 , K5 lub K6	3	6	9	2
4.	Łącznie suma punktów	13	27	46	12
5.	Poziom zagrożenia	X			

II. Określenie poziomu zagrożenia jednostki organizacyjnej

1. *LOKALIZACJA*

	WARIANTY	PUNKTACJA	OCENA JEDNOSTKI
A	Budynek wolnostojący i ogrodzony	0	**2 pkt**
B	Budynek wolnostojący nie ogrodzony	2	
C	Budynek w zabudowie zwartej	4	
D	Budynek użytkowany wspólnie z innymi podmiotami	8	

Budynek, w którego najbliższym sąsiedztwie nie ma innych obiektów. Ogrodzenie budynku stanowi barierę chroniącą przed bezpośrednim wejściem do środka. Budynek częściowo ogrodzony, ale w taki sposób, że wejście jest możliwe tylko po wcześniejszym pokonaniu ogrodzenia.

Budynek bez ogrodzenia. Budynek częściowo ogrodzony, ale wejście do budynku nie wymaga pokonania ogrodzenia.

Budynek, którego ściany przylegają do budynku innej jednostki organizacyjnej.

Budynek użytkowany przez więcej niż jedną jednostkę organizacyjną, ze wspólnym wejściem.

2. *OCHRONA FIZYCZNA*

	WARIANTY	PUNKTACJA	OCENA JEDNOSTKI
A	Całodobowa ochrona osobowa z wykorzystaniem systemów elektronicznych	0	**4 pkt**
B	Całodobowa ochrona osobowa	2	
C	Całodobowa ochrona przy zastosowaniu systemów elektronicznych	4	
D	Ochrona sprawowana tylko po godzinach pracy	6	
E	Brak ochrony	8	

Budynek jest chroniony całodobowo przez przedsiębiorcę wykonującego zadania w zakresie ochrony osób i mienia lub wewnętrzną służbę ochrony i jednocześnie wykorzystuje się elektroniczne systemy wspomagające (system nadzoru wizyjnego, system sygnalizacji włamania i napadu).

Budynek jest chroniony całodobowo przez przedsiębiorcę wykonującego zadania w zakresie ochrony osób i mienia lub wewnętrzną służbę ochrony bez wykorzystania elektronicznych systemów wspomagających.

Budynek jest chroniony przez całą dobę tylko systemami elektronicznymi (systemem sygnalizacji włamania i napadu lub systemem nadzoru wizyjnego). Działanie systemów musi powodować reakcję osób w sytuacjach alarmowych.

Ochrona budynku sprawowana jest tylko po godzinach pracy przez osoby lub systemy elektroniczne.

Brak ochrony.

3. *LICZBA OSÓB MAJĄCYCH DOSTĘP DO INFORMACJI NIEJAWNYCH OZNACZONYCH KLAUZULĄ „ŚCIŚLE TAJNE", „TAJNE" I „POUFNE" (ŁĄCZNIE)*

	WARIANTY	PUNKTACJA	OCENA JEDNOSTKI
A	do 20 % ogólnej liczby pracowników	2	**2 pkt**
B	od 21% do 30%	4	
C	od 31% do 50%	6	
D	powyżej 51%	10	

*Przy określeniu liczby osób mających dostęp do informacji niejawnych należy uwzględnić wszystkich pracowników jednostki organizacyjnej uprawnionych do dostępu do informacji **od klauzuli „poufne" wzwyż**, na podstawie przepisów ustawy o ochronie informacji niejawnych lub na podstawie innych przepisów (o ustroju sądów powszechnych, ustroju sądów wojskowych oraz o prokuraturze).*
W przypadku nowo organizowanej jednostki organizacyjnej należy przyjąć wartości szacunkowe.

4. *ILOŚĆ INFORMACJI NIEJAWNYCH PRZETWARZANYCH W JEDNOSTCE ORGANIZACYJNEJ OZNACZONYCH KLAUZULĄ „ŚCIŚLE TAJNE", „TAJNE" I „POUFNE" (ŁĄCZNIE)*

	WARIANTY	PUNKTACJA	OCENA JEDNOSTKI
A	do 100 dokumentów niejawnych	2	**2 pkt**
B	101 – 200 dokumentów niejawnych	3	
C	201 – 500 dokumentów niejawnych	6	
D	501 – 1000 dokumentów niejawnych	8	
E	powyżej 1000 dokumentów niejawnych	10	

*Przy określeniu ilości dokumentów przetwarzanych w jednostce organizacyjnej należy brać pod uwagę **wszystkie dokumenty niejawne od klauzuli „poufne" wzwyż**, zarejestrowane w urządzeniach ewidencyjnych w minionym roku kalendarzowym oraz pozostające w faktycznej dyspozycji jednostki, zarejestrowane w latach poprzednich (suma dokumentów będzie opowiadała wskazanemu wyżej wariantowi).*

W przypadku nowo organizowanej jednostki organizacyjnej należy przyjąć wartości szacunkowe.

5. ZAGROŻENIE POŻAREM

	WARIANTY	PUNKTACJA	OCENA JEDNOSTKI
A	Automatyczne systemy gaszenia	0	**2 pkt**
B	Wyposażenie budynku w stałe instalacje gaśnicze	1	
C	Wyposażenie budynku w podręczne środki gaśnicze	2	
D	Brak ochrony przeciwpożarowej	4	

Zabezpieczenie budynku będą stanowić systemy sygnalizacji pożarowej wraz z samoczynnymi systemami gaszenia.

Budynek wyposażony w instalacje gaśnicze, umożliwiające samoczynne gaszenie pożaru (p. zraszacze, hydranty).

W budynku znajdują się jedynie podręczne środki gaśnicze (p. gaśnice, koce).

6. KONSTRUKCJA BUDYNKU

	WARIANTY	PUNKTACJA	OCENA JEDNOSTKI
A	Budynek o konstrukcji zapewniającej wysoki stopień odporności na włamanie	0	**4 pkt**
B	Budynek o konstrukcji odpornej na siłowe wtargnięcie	4	
C	Budynek o konstrukcji szkieletowej	8	

Konstrukcja budynku wykonana z betonu lub porównywalnego materiału z drzwiami antywłamaniowymi i oknami zabezpieczonymi przed włamaniem.

Budynek wykonany z cegieł lub materiałów o podobnych właściwościach, z oknami i drzwiami zabezpieczonymi przed wtargnięciem.

Szkieletowa konstrukcja budynku z wypełnieniem wykonanym z materiałów o niskiej odporności na włamanie (np. pojedynczej cegły, pustaka, aluminium, drewna lub elementów szklanych).

7. INNE CZYNNIKI

	Czynniki mogące wpływać na poziom bezpieczeństwa informacji niejawnych	Punktacja 1 - 10	Ocena jednostki	Uzasadnienie
A	brak		*0*	
B	brak		*0*	
C				
D				
SUMA			***0***	

Analiza zagrożeń powinna uwzględniać inne czynniki wynikające ze specyfiki jednostki organizacyjnej, nie uwzględnione w tabelach powyżej, a mogące mieć wpływ na ochronę informacji niejawnych np.:

A. Najbliższe sąsiedztwo:

- obiekty przedstawicielstw i podmiotów zagranicznych,
- obiekty sportowe i hale widowiskowe,
- ogólnodostępne parkingi i garaże,
- zakłady przemysłowe i instalacje stanowiące zagrożenie dla życia i zdrowia.

B. Lokalizacja jednostki organizacyjnej na obszarach zagrożonych powodzią, szkodami górniczymi itp.

W przypadku uwzględnienia dodatkowego czynnika należy go ocenić według zaproponowanej skali i uzasadnić ocenę. Punkty należy podsumować.

WYNIK		
Czynnik		**Punktacja**
I	Lokalizacja	2
II	Ochrona fizyczna	4
III	Liczba osób mających dostęp do informacji niejawnych	2
IV	Ilość informacji niejawnych przetwarzanych w jednostce organizacyjnej	2
V	Zagrożenie pożarem	2
VI	Konstrukcja budynku	4
VII	Inne	0
SUMA		**16**

POZIOM ZAGROŻENIA		
NISKI	***ŚREDNI***	***WYSOKI***
1 pkt - 15 pkt	16 pkt - 28 pkt	powyżej 28 pkt
[ ]*	[X]*	[ ]*

**) wstawić „X" przy odpowiednim poziomie*

ZATWIERDZAM
WÓJT GMINY
Wójt Gminy
mgr inż. Wiesław Gąska
Wiesław Gąska

Załącznik Nr 2 do Zarządzenia Nr /2012
Wójta Gminy Borowie
z dnia grudnia 2012 r.

Instrukcja dotycząca sposobu i trybu przetwarzania informacji niejawnych oznaczonych klauzulą "zastrzeżone"

§ 1. Instrukcja dotycząca sposobu i trybu przetwarzania informacji niejawnych oznaczonych klauzulą **„zastrzeżone"** oraz zakresu i warunków stosowania środków bezpieczeństwa fizycznego w celu ich ochrony, zwana dalej instrukcją, stanowi wewnętrzne uregulowanie w Urzędzie Gminy Borowie dotyczące całokształtu zagadnień związanych z ochroną informacji niejawnych oznaczonych klauzulą „zastrzeżone", zwanych dalej informacjami zastrzeżonymi i określa:

1) warunki dostępu do informacji zastrzeżonych,
2) zasady udostępniania informacji zastrzeżonych,
3) zasady ewidencjonowania dokumentów zastrzeżonych,
4) zasady przechowywania i zabezpieczania dokumentów zastrzeżonych,
5) zasady opracowania dokumentów zastrzeżonych,
6) zasady wysyłania przesyłek zawierających informacje zastrzeżone,
7) zasady gromadzenia dokumentów zastrzeżonych,
8) zasady nadzoru w zakresie przestrzegania warunków ochrony informacji zastrzeżonych.

§ 2. 1. Informacjami niejawnymi o klauzuli „zastrzeżone" są informacje, którym nie nadano wyższej klauzuli tajności, a ich nieuprawnione ujawnienie może mieć szkodliwy wpływ na wykonywanie przez organy władzy publicznej lub inne jednostki organizacyjne zadań z zakresu obrony narodowej, polityki zagranicznej, bezpieczeństwa publicznego, przestrzegania praw i wolności obywateli, wymiaru sprawiedliwości albo interesów ekonomicznych Rzeczypospolitej Polskiej.

2. Informacjami niejawnymi o klauzuli „zastrzeżone" w Urzędzie Gminy są informacje dotyczące m.in.:

1) „Planu operacyjnego funkcjonowania Gminy Borowie w warunkach zewnętrznego zagrożenia bezpieczeństwa państwa i w czasie wojny" , Karty realizacji zadań operacyjnych,
2) Dokumentacja Akcji Kurierskiej,
3) Inne wg decyzji osób uprawnionych do podpisania dokumentów zastrzeżonych.

§ 3. Uprawnienia do dostępu do określonych informacji zastrzeżonych mogą posiadać osoby, które spełniają następujące warunki:

1) posiadają poświadczenie bezpieczeństwa upoważniające do dostępu do informacji niejawnych o klauzuli „zastrzeżone" lub upoważnienie Wójta zgodnie z art. 21 ust. 4 ustawy o ochronie informacji niejawnych,
2) odbyli przeszkolenie w zakresie ochrony informacji niejawnych i posiadają zaświadczenie stwierdzające odbycie tego szkolenia ;

§ 4. 1. O dostępie do dokumentów zastrzeżonych decyduje Wójt w formie dekretacji dokonanej w sposób trwały na dokumencie, która kieruje ten dokument do konkretnego kierownika komórki organizacyjnej odpowiedzialnej za załatwienie sprawy.
2. Po dekretacji Wójta i zarejestrowaniu we właściwym „ Dzienniku ewidencji dokumentów niejawnych " , osoba uprawniona do jego ewidencji - powiadamia właściwego kierownika jednostki organizacyjnej / komórki organizacyjnej ,o dokumencie.

3. Kierownik komórki organizacyjnej urzędu po zapoznaniu się z dokumentem w pomieszczeniu Nr 7, może zadekretować go wskazując pracownika, który będzie odpowiedzialny za załatwienie sprawy.

4. Osoba uprawniona do ewidencji dokumentów niejawnych przekazuje dokument zastrzeżony wskazanemu w dekretacji uprawnionemu pracownikowi, po uzyskaniu potwierdzenia przyjęcia dokumentu.

5. Dekretacja Wójta może dotyczyć osoby kierującej zespołem funkcjonalnym powołanym zarządzeniem Wójta do realizacji określonego zadania, wówczas osoba kierująca odpowiada za udostępnianie informacji zastrzeżonych w związku ze szkoleniem i przygotowaniem zespołu do realizacji zadania. Fakt zapoznania się z informacjami zastrzeżonymi jest potwierdzany.

6. W przypadku potrzeby związanej z załatwieniem sprawy i zapoznaniem się z treścią dokumentu zastrzeżonego przez innego pracownika jednostki organizacyjnej konieczne jest rozszerzenie dekretacji przez kierownika tej jednostki na tym dokumencie.

7. W przypadku potrzeby związanej z załatwieniem sprawy i zapoznaniem się z treścią dokumentu zastrzeżonego przez pracownika innej jednostki organizacyjnej konieczne jest rozszerzenie dekretacji na kierownika innej jednostki organizacyjnej przez Wójta na tym dokumencie.

8. W przypadku konieczności przekazania dokumentu innemu pracownikowi należy zwrócić go do osoby uprawnionej do ewidencji dokumentów niejawnych, który przekaże go zgodnie z dekretacją na dokumencie po dokonaniu właściwych zapisów w „ Dzienniku ewidencji " dokumentów.

9. Każdy pracownik, który zapoznał się z treścią dokumentu zastrzeżonego, dokonuje stosownej adnotacji stwierdzającej ten fakt bezpośrednio na dokumencie lub w karcie zapoznania się z dokumentem, która może być założona przez osobę uprawnioną do ewidencji dokumentów niejawnych w przypadku dokumentu, z którym będzie zapoznana większa liczba pracowników. Karta zapoznania się z dokumentem zastrzeżonym jest przekazywana razem z dokumentem.
Fakt jej założenia odnotowywany jest na dokumencie przez osobę uprawnioną do ewidencji dokumentów niejawnych. Karta podlega rozliczeniu się podobnie jak i dokument zastrzeżony.

10. Informacje zastrzeżone mogą być udostępniane pracownikom uprawnionym w zakresie niezbędnym do załatwienia sprawy.

11. Za właściwe zabezpieczenie dokumentu zastrzeżonego przed nieuprawnionym dostępem odpowiada osoba, która pobrała go od osoby uprawnionej do ewidencji dokumentów niejawnych. Nadzór nad prawidłowym zabezpieczeniem dokumentów zastrzeżonych prowadzą przełożeni tej osoby.

§ 5. 1. Dokumenty zawierające informacje zastrzeżone podlegają obowiązkowi ewidencjonowania.

2. Ewidencją objęte są dokumenty zastrzeżone zarówno otrzymane jak i wytworzone w Urzędzie Gminy .

3. Dokumenty otrzymane jak i wykonane w Urzędzie Gminy ewidencjonowane są we właściwym „ Dzienniku ewidencji " dokumentów lub „ Rejestrze wydanych przedmiotów ", zgodnych ze wzorem zawartym w załączniku nr 3 do Rozporządzenia Rady Ministrów z dnia 1 czerwca 2010 r., prowadzonych przez osobę uprawnioną do ewidencji dokumentów niejawnych.

4. Po odebraniu dokumentu zastrzeżonego od osoby uprawnionej do ewidencji dokumentów niejawnych przez uprawnionego pracownika, co jest potwierdzane przez pracownika w rubryce nr 14 „ Dziennika ewidencji ", dokument jest rejestrowany przez pobierającego w odpowiedniej teczce spraw z zastrzeżeniem ust **5.**

5. Teczka spraw, w której przechowywane są dokumenty zastrzeżone oznaczona jest klauzulą „zastrzeżone" oraz symbolami według rzeczowego wykazu akt i podlega ochronie określonej w instrukcji.

6. Fakt wysłania wykonanego dokumentu w Urzędzie Gminy odnotowywany jest odpowiednio w „Dzienniku ewidencji " lub „ Rejestrze wydanych przedmiotów " przez osobę uprawnioną do ewidencji dokumentów niejawnych..

§ 6. 1. Dokumenty zastrzeżone podlegają obowiązkowej ochronie przed nieuprawnionym ujawnieniem.

2. Dokumenty zastrzeżone przechowuje się zamknięte w meblach biurowych, szafach metalowych lub sejfach.

3. Pomieszczenia, w których przechowywane są dokumenty zastrzeżone muszą być zamknięte na zamek patentowy jeśli nie przebywa w nich żaden pracownik.

4. Teczki spraw zawierające dokumenty zastrzeżone mogą być przechowywane z dokumentami jawnymi na wydzielonych i oznakowanych półkach.

5. Dokumenty zastrzeżone w postaci cyfrowej mogą być przechowywane w systemach i sieciach teleinformatycznych posiadających akredytację służby ochrony państwa zgodnie z zapisami ustawy o ochronie informacji niejawnych.

6. W przypadku braku możliwości przechowywania dokumentów zastrzeżonych w komórkach organizacyjnych urzędu, dokumenty te są przechowywane przez osobę uprawnioną do ewidencji dokumentów niejawnych w pomieszczeniu Nr 7.

7. W przypadku powstania zagrożenia np. pożarem w miarę możliwości, biorąc pod uwagę zapewnienie przede wszystkim bezpieczeństwa dla życia i zdrowia, należy dokumenty zastrzeżone ewakuować w pierwszej kolejności.

8. Nadzór nad prawidłowym przechowywaniem dokumentów zastrzeżonych sprawują kierownicy jednostek (komórek)organizacyjnych urzędu.

§ 7. 1. Dokumenty o klauzuli „zastrzeżone" są sporządzane i wykonywane przez pracownika merytorycznie odpowiedzialnego za jego opracowanie.

2. Praca z dokumentem zastrzeżonym, w tym sporządzanie i wykonanie może odbywać się w jednostce organizacyjnej urzędu, jeśli warunki pracy umożliwiają zapewnienie warunków ochrony przed jego nieuprawnionym ujawnieniem i nieuprawnionym do niego dostępem i zapoznaniem się przez osoby do tego nieuprawnionych.

3. Jeżeli w jednostce organizacyjnej urzędu nie ma wymaganych warunków wówczas dokument zastrzeżony musi być sporządzony i wykonany w pomieszczeniu Nr 7 Urzędu Gminy.

4. Jeżeli dokument zastrzeżony w danej chwili nie jest wykorzystywany do realizacji zadania przez uprawnionego pracownika musi być on zabezpieczony zgodnie z **§6** instrukcji.

5. Dokumenty zastrzeżone mogą być przetwarzane w systemach i sieciach teleinformatycznych posiadających akredytację służby ochrony państwa zgodnie z zapisami ustawy o ochronie informacji niejawnych.

6. Wykonany dokument jest rejestrowany w odpowiedniej ewidencji dokumentów przez osobę uprawnioną do ewidencji dokumentów niejawnych, a następnie zostaje podpisany przez uprawnioną do tego osobę.

§ 8. Dokumenty zastrzeżone, które mają być wysłane poza Urząd są przygotowane do wysłania przez osobę uprawnioną do ewidencji dokumentów niejawnych poprzez właściwe zapakowanie i opisanie przesyłki. Następnie są przekazane do kancelarii ogólnej co odnotowane jest w ewidencji dokumentów.

§ 9. 1. Dokumenty zastrzeżone są gromadzone przez pracowników upoważnionych do dostępu do tych informacji w teczkach akt z klauzulą „zastrzeżone".

2. Informacje zastrzeżone podlegają ochronie do czasu zniesienia klauzuli tajności.

3. W przypadku spraw ostatecznie zakończonych, gdy dokument jest nadal chroniony, teczki akt o klauzuli „zastrzeżone" mogą być przekazane do pomieszczenia Nr 7, w której będą one przechowywane do chwili zniesienia klauzuli niejawności (jeżeli pomieszczenie to posiada możliwości lokalowe i stosowne zabezpieczenia do przechowywania takich dokumentów).

4. W przypadku zniesienia klauzuli tajności, jednostka (komórka) organizacyjna lub osoba uprawniona do ewidencji dokumentów niejawnych podejmuje decyzję co do dalszych losów dokumentów zgodnie z obowiązującymi przepisami dotyczącymi dokumentów jawnych (np. przekazuje teczki akt do archiwum zakładowego).

§ 10. 1. Pracownik samorządowy jest zobowiązany do dochowania tajemnicy ustawowo chronionej zgodnie z ustawą o pracownikach samorządowych oraz Regulaminem Organizacyjnym Urzędu Gminy.

2. Odpowiedzialność karną za przestępstwa przeciwko ochronie informacji w tym informacji zastrzeżonych określa ustawa kodeks karny.

3. W przypadku nieuprawnionego ujawnienia informacji niejawnych o klauzuli "zastrzeżone" należy powiadomić Pełnomocnika ds. ochrony informacji niejawnych.

4. Kierownicy komórek organizacyjnych urzędu zapewniają i nadzorują stosowanie ustaleń zawartych w niniejszej instrukcji.

ZATWIERDZAM

WÓJT GMINY

Wójt Gminy

mgr inż. Wiesław Gąska

Wiesław Gąska

Załącznik Nr 3 do Zarządzenia Nr /2012
Wójta Gminy Borowie
z dnia grudnia 2012 r.

Instrukcja dotycząca sposobu i trybu przetwarzania informacji niejawnych oznaczonych klauzulą "poufne"

§ 1. Instrukcja dotycząca sposobu i trybu przetwarzania informacji niejawnych oznaczonych klauzulą **„poufne"** stanowi wewnętrzne uregulowanie w Urzędzie Gminy Borowie i określa:

1) warunki dostępu do informacji poufnych,
2) zasady udostępniania informacji poufnych,
3) zasady ewidencjonowania dokumentów poufnych,
4) zasady przechowywania i zabezpieczania dokumentów poufnych,
5) zasady opracowania dokumentów poufnych,
6) zasady wysyłania przesyłek zawierających informacje poufne,
7) zasady gromadzenia dokumentów poufnych,
8) zasady nadzoru w zakresie przestrzegania warunków ochrony informacji poufnych.

§ 2. 1. Informacjom niejawnym nadaje się klauzulę „poufne", jeżeli ich nieuprawnione ujawnienie spowoduje szkodę dla Rzeczypospolitej Polskiej przez to, że:

1) utrudni prowadzenie bieżącej polityki zagranicznej Rzeczypospolitej Polskiej,
2) utrudni realizację przedsięwzięć obronnych lub negatywnie wpłynie na zdolność bojową Sił Zbrojnych Rzeczypospolitej Polskiej,
3) zakłóci porządek publiczny lub zagrozi bezpieczeństwu obywateli,
4) utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę bezpieczeństwa lub podstawowych interesów Rzeczypospolitej Polskiej,
5) utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę porządku publicznego, bezpieczeństwa obywateli lub ściganie sprawców przestępstw i przestępstw skarbowych oraz organom wymiaru sprawiedliwości,
6) zagrozi stabilności systemu finansowego Rzeczypospolitej Polskiej,
7) wpłynie niekorzystnie na funkcjonowanie gospodarki narodowej.

2. Informacjami niejawnymi o klauzuli „poufne" w Urzędzie Gminy są miedzy innymi.:

1) ankieta bezpieczeństwa osobowego – sprzed 2012 r.
2) dzienniki ewidencji, korespondencji oraz rejestry teczek i dokumentów niejawnych,
3) inne wg decyzji osób uprawnionych do podpisania dokumentów poufnych.

§ 3. Uprawnienia do dostępu do określonych informacji poufnych posiadają osoby, które spełniają następujące warunki :
1) posiadają poświadczenie bezpieczeństwa upoważniające do dostępu do informacji niejawnych o klauzuli „poufne" lub wyższej lub zgodę na udostępnienie zgodnie z art.34 ust.9 ustawy,
2) odbyli przeszkolenie w zakresie ochrony informacji niejawnych i posiadają zaświadczenie stwierdzające odbycie tego szkolenia.

§ 4. 1. Zasady dostępu do informacji oznaczonych klauzula „poufne":

1) o dostępie do dokumentów poufnych decyduje Wójt w formie dekretacji dokonanej w sposób trwały na dokumencie do konkretnego kierownika komórki organizacyjnej

odpowiedzialnego za załatwienie sprawy, a następnie kieruje ten dokument do osoby uprawnionej do ewidencji dokumentów niejawnych,
2) po dekretacji Wójta i zarejestrowaniu we właściwej książce ewidencji dokumentów niejawnych, osoba uprawniona do ewidencji dokumentów niejawnych powiadamia właściwego kierownika jednostki organizacyjnej o dokumencie,
3) kierownik jednostki organizacyjnej urzędu po zapoznaniu się z dokumentem w pomieszczeniu Nr 7, może zadekretować go wskazując pracownika uprawnionego do dostępu do informacji poufnych, który będzie odpowiedzialny za załatwienie sprawy,
4) osoba uprawniona do ewidencji dokumentów niejawnych umożliwia zapoznanie się z dokumentem poufnym wskazanemu w dekretacji pracownikowi,
5) dekretacja Wójta może dotyczyć osoby kierującej zespołem funkcjonalnym powołanym zarządzeniem Wójta do realizacji określonego zadania, wówczas osoba kierująca odpowiada za udostępnianie informacji poufnych w związku ze szkoleniem, przygotowaniem i realizacją zadania przez zespół,
6) w przypadku potrzeby związanej z załatwieniem sprawy i zapoznaniem się z treścią dokumentu poufnego przez innego pracownika jednostki organizacyjnej konieczne jest rozszerzenie dekretacji przez kierownika tej jednostki na tym dokumencie,
7) w przypadku potrzeby związanej z załatwieniem sprawy i zapoznaniem się z treścią dokumentu poufnego przez pracownika innej jednostki organizacyjnej konieczne jest rozszerzenie dekretacji na kierownika innej jednostki organizacyjnej przez Wójta na tym dokumencie,
8) każdy pracownik, który zapoznał się z treścią dokumentu poufnego, dokonuje stosownej adnotacji stwierdzającej ten fakt bezpośrednio na dokumencie lub w karcie zapoznania się z dokumentem, która może być założona przez osobę uprawnioną do ewidencji dokumentów niejawnych w przypadku dokumentu, z którym będzie zapoznana większa liczba pracowników. Fakt jej założenia odnotowywany jest na dokumencie przez osobę uprawnioną do ewidencji dokumentów niejawnych. Karta podlega rozliczeniu się podobnie jak i dokument poufny,
9) informacje poufne mogą być udostępniane pracownikom uprawnionym w zakresie niezbędnym do załatwienia sprawy.
2. Dokumenty poufne mogą być wydawane poza pomieszczenie Nr 7 za odpowiednim pokwitowaniem, ale muszą być zwrócone i przechowywane każdorazowo po zakończeniu dnia pracy w tym pomieszczeniu.

§ 5. Ewidencja dokumentów o klauzuli „poufne":

1) dokumenty zawierające informacje poufne podlegają obowiązkowi ewidencjonowania,
2) ewidencją objęte są dokumenty poufne zarówno otrzymane jak i wytworzone w Urzędzie Gminy,
3) dokumenty otrzymane jak i wykonane w Urzędzie Gminy rejestrowane są we właściwym dzienniku ewidencji, zgodnym ze wzorem zawartym w załączniku nr 3 do Rozporządzenia Rady Ministrów z dnia 1 czerwca 2010 r. w sprawie organizacji i funkcjonowania kancelarii tajnych, prowadzonym przez kancelarię niejawną,
4) fakt wysłania wykonanego dokumentu w Urzędzie Gminy odnotowywany jest w dzienniku ewidencji przez osobę uprawnioną do ewidencji dokumentów niejawnych.

§ 6. Zasady przechowywania dokumentów o klauzuli „poufne":

1) dokumenty poufne podlegają obowiązkowej ochronie przed nieuprawnionym ujawnieniem,
2) dokumenty poufne przechowywane są w pomieszczeniu Nr 7. Teczka spraw, w której przechowywane są dokumenty poufne, oznaczona jest klauzulą „poufne" oraz symbolami według rzeczowego wykazu akt,
3) dokumenty „poufne" przechowywane są osobno od dokumentów niejawnych o innej klauzuli,

4) dokumenty poufne w postaci cyfrowej mogą być przechowywane w systemach i sieciach teleinformatycznych posiadających akredytację służby ochrony państwa zgodnie z zapisami ustawy o ochronie informacji niejawnych.

§ 7. Zasady wykonywania i przetwarzania dokumentów o klauzuli „poufne":

1) dokumenty o klauzuli „poufne" są sporządzane i wykonywane przez pracownika posiadającego stosowne Poświadczenie bezpieczeństwa oraz merytorycznie odpowiedzialnego za jego opracowanie,
2) sporządzenie i wykonanie dokumentu „poufnego" odbywa się w pomieszczeniu Nr 7,
3) dokumenty poufne mogą być przetwarzane w systemach i sieciach teleinformatycznych posiadających akredytację służby ochrony państwa zgodnie z zapisami ustawy o ochronie informacji niejawnych,
4) wykonany dokument jest rejestrowany w odpowiedniej ewidencji dokumentów przez osobę uprawnioną do ewidencji dokumentów niejawnych, następnie zostaje podpisany przez uprawnioną do tego osobę.

§ 8. Dokumenty poufne, które mają być wysłane poza urząd są przygotowane do wysłania przez osobę uprawnioną do ewidencji dokumentów niejawnych, poprzez właściwe zapakowanie i opisanie przesyłki. Następnie są przekazane do kancelarii ogólnej, co odnotowane jest w ewidencji dokumentów.

§ 9. Okres ochrony dokumentów o klauzuli „poufne":

1) informacje poufne podlegają ochronie do czasu zniesienia klauzuli tajności,
2) w przypadku zniesienia klauzuli tajności, jednostka (komórka) organizacyjna lub osoba uprawniona do ewidencji dokumentów niejawnych podejmuje decyzję co do dalszych losów dokumentów zgodnie z obowiązującymi przepisami dotyczącymi dokumentów jawnych (np. przekazuje teczki akt do archiwum zakładowego).

§ 10. Zasady odpowiedzialności za ochronę dokumentów o klauzuli "poufne" :

1) pracownik samorządowy jest zobowiązany do dochowania tajemnicy ustawowo chronionej zgodnie z ustawą o pracownikach samorządowych oraz Regulaminem Organizacyjnym Urzędu Gminy,
2) odpowiedzialność karną za przestępstwa przeciwko ochronie informacji w tym informacji poufnych określa ustawa kodeks karny.

ZATWIERDZAM
WÓJT GMINY
Wiesław Gąska
Wójt Gminy
Wiesław Gąska

INSTRUKCJA
ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM PRZY PRZETWARZANIU INFORMACJI NIEJAWNYCH O KLAUZULI „ ZASTRZEŻONE ”

Administrator Danych – **WÓJT MGR INŻ. WIESŁAW GĄSKA**
w podmiocie o nazwie: **GMINA BOROWIE**

Zgodnie z **Ustawą o ochronie informacji niejawnych (Dz. U. z 2016r.,poz 1167 ze zm.)**
z dnia 5 sierpnia 2010 r.
wdraża się dokument o nazwie „Instrukcja dotycząca sposobu i trybu przetwarzania informacji niejawnych o klauzuli „ ZASTRZEŻONE ” przy wykorzystaniu systemu informatycznego” zwany dalej „instrukcją”. Zapisy tego dokumentu wchodzą w życie z dniem 27-12-2012r.

Ilekroć w „instrukcji” jest mowa o:

1. **podmiocie** — rozumie się przez to spółkę prawa handlowego, podmiot gospodarczy nie posiadający osobowości prawnej, jednostkę budżetową;
2. **ustawie** — rozumie się przez to Ustawę o ochronie informacji niejawnych (Dz. U. z 2016r.,poz 1167 ze zm.) z dnia 5 sierpnia 2010 r.;
3. **identyfikatorze użytkownika** — rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
4. **haśle** — rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
5. **sieci telekomunikacyjnej** — rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 23 ustawy z dnia 21 lipca 2000 r. — Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852, z późn. zm.)
6. **sieci publicznej** — rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 22 ustawy z dnia 21 lipca 2000 r. — Prawo telekomunikacyjne;
7. **teletransmisji** – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej
8. **rozliczalności** — rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
9. **integralności danych** — rozumie się przez to właściwość zapewniającą, że dane „ ZASTRZEŻONE ” nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
10. **raporcie** — rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;
11. **poufności danych** — rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
12. **uwierzytelnianiu** — rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

§ 1

Za przestrzeganie w podmiocie: **GMINA BOROWIE** zapisów „instrukcji" odpowiedzialny jest Administrator danych lub zgodnie z zapisem §2 „Polityki Bezpieczeństwa" wyznaczony **Administrator Bezpieczeństwa Informacji.**

§2

W związku z tym, że w podmiocie: **GMINA BOROWIE** przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych „ Zastrzeżonych " (w pok. Nr 7), połączone jest z siecią publiczną, oraz uwzględniając kategorie przetwarzanych danych i zagrożenia, wprowadza się poziom bezpieczeństwa przetwarzania tych danych w systemie informatycznym na poziomie **wysokim,** a w związku z tym wprowadza się poniższe postanowienia:

I

Obszar, w którym są przetwarzane dane, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych „ ZASTRZEŻONYCH „ (Inspektor ds. obronnych, OC i zarządzania kryzysowego). Przebywanie osób nieuprawnionych w obszarze, w którym są przetwarzane dane, jest dopuszczalne za zgodą Administratora Danych, Administratora Bezpieczeństwa Informacji lub w obecności osoby upoważnionej do przetwarzania danych osobowych.

II

1. W systemie informatycznym służącym do przetwarzania danych „ ZASTRZEŻONYCH ", przetwarzać dane mogą wyłącznie osoby posiadające aktualne upoważnienie nadane przez Administratora Bezpieczeństwa Informacji. Użytkownik przetwarzający dane po otrzymaniu upoważnienia oraz loginu i hasła jest zobowiązany niezwłocznie dokonać zmiany hasła oraz zachować je w tajemnicy. Użytkownik jest zobowiązany do zmiany hasła nie rzadziej niż co 30 dni. Hasło nadane przez użytkownika musi składać się z co najmniej z 8 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.
2. Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się, aby:

   w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator oraz aby dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.

III

System informatyczny służący do przetwarzania danych „ ZSTRZEŻONYCH " zabezpiecza się, w szczególności przed:

1. działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego:
   - poprzez zainstalowanie programu antywirusowego o nazwie KASPERSKY ENDPOINT SECURITY,
   - poprzez zainstalowanie firewall (zapora sieciowa),
   - poprzez zabezpieczenie sieci radiowej odpowiedniej mocy uwierzytelnieniem,
2. utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej poprzez zastosowanie zasilacza awaryjnego UPS.

IV

1. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.

2. W przypadku gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni. Hasło składa się ono co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.
3. Dane „ ZASTRZEŻONE " przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych. Kopie wszystkich danych muszą być tworzone nie rzadziej niż raz na miesiąc.
4. Kopie zapasowe:
   a) przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem w pomieszczeniu zamkniętym – pokój Nr 7 (USC).
   b) usuwa się niezwłocznie po ustaniu ich użyteczności.

V

Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych „ ZASTRZEŻONYCH " w tym stosuje hasła dostępu do komputera przenośnego oraz do plików, w których przetwarzane są dane osobowe.

VI

Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane „ ZASTRZEŻONE „, przeznaczone do:

a) likwidacji — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
b) przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
c) naprawy — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

§3

1. Dla każdej osoby, której dane „ ZASTRZEŻONE „ są przetwarzane w systemie informatycznym — z wyjątkiem systemów służących do przetwarzania danych „ ZASTRZEŻONE „ ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie — system ten zapewnia odnotowanie:
   a) daty pierwszego wprowadzenia danych do systemu;
   b) identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba;
   c) źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą;
   d) informacji o odbiorcach, którym dane „ ZASTRZEŻONE „ zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych;
2. Odnotowanie informacji, o których mowa w ust. 1 pkt a i b, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.

§4

Po zakończeniu pracy w systemie informatycznym użytkownik ma obowiązek wylogować się z systemu. W przypadku braku czynności ze strony użytkownika w systemie informatycznym przez 30 min, system samoczynnie wyloguje użytkownika przetwarzającego dane osobowe.

§5

Administrator Bezpieczeństwa Informacji ma obowiązek dokonywać przeglądów technicznych sprzętu informatycznego w podmiocie oraz dbać o ich dobry stan techniczny. Zaleca się dokonywanie przeglądów okresowych co 30 dni oraz przeglądów generalnych raz na rok. W przypadku stwierdzenia usterek technicznych **Administrator Bezpieczeństwa Informacji** ma obowiązek niezwłocznie powiadomić o tym fakcie Administratora Danych.

§6

W przypadku stwierdzenia przez **Administratora Bezpieczeństwa Informacji** uchybień dotyczących przetwarzania danych w podmiocie powinien o tym fakcie niezwłocznie powiadomić Administratora Danych oraz wprowadzić takie zabezpieczenia i procedury, które w przyszłości wyeliminują takie zdarzenia.

§ 7

W sprawach nieuregulowanych w niniejszej „instrukcji" mają zastosowanie przepisy ustawy o **ochronie informacji niejawnych (Dz. U. z 2016r.,poz 1167 ze zm.)** z dnia 5 sierpnia 2010 r.

Wójt Gminy

Wiesław Gąska

WÓJT GMINY
mgr inż. Wiesław Gąska

.....

Podpis