**ZARZĄDZENIE Nr 27**
**WÓJTA GMINY BOJADŁA**
**z dnia 29 maja 2012 r.**

**w sprawie zatwierdzenia „Planu ochrony informacji niejawnych, w tym w razie wprowadzenia stanu nadzwyczajnego w Urzędzie Gminy Bojadła"**

Na podstawie art. 15 ust. 1 pkt 5 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. Nr 182, poz. 1228),

zarządzam, co następuje:

**§ 1.** Zatwierdzam i wprowadzam do użytku „Plan ochrony informacji niejawnych, w tym w razie wprowadzenia stanu nadzwyczajnego w Urzędzie Gminy Bojadła" stanowiący załącznik do niniejszego zarządzenia.

**§ 2.** Zobowiązuję pracowników do wprowadzenia i stosowania ustaleń zawartych w Planie, o którym mowa w § 1.

**§ 3.** Nadzór nad wykonaniem zarządzenia powierzam Pełnomocnikowi Ochrony Informacji Niejawnych.

**§ 4.** Zarządzenie wchodzi w życie z dniem podpisania.

GMINY BOJADŁA

Wójt Gminy Bojadła
mgr inż. Grzegorz Doszel
.....

*Załącznik*
*do Zarządzenia Nr 41*
*Wójta Gminy Bojadła*
*z dnia 29 05.2012 r.*

***Nie podlega archiwizacji***
***do czasu deaktualizacji***

**ZATWIERDZAM:**
**WÓJT GMINY**

Wójt Gminy Bojadła
mgr inż. Grzegorz Doszel
.....

# PLAN
# OCHRONY INFORMACJI NIEJAWNYCH, W TYM W RAZIE WPROWADZENIA STANU NADZWYCZAJNEGO W URZĘDZIE GMINY BOJADŁA

**OPRACOWAŁ:**
**PEŁNOMOCNIK**
**OCHRONY INFORMACJI NIEJAWNYCH**

**Franciszek WAŁECKI**

**BOJADŁA, 2012 R.**

## Spis treści

# PLAN OCHRONY
## informacji niejawnych w Urzędzie Gminy Bojadła

opracowany na podstawie postanowień art. 15 ust. 1 pkt. 5 ***ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych*** (Dz. U. Nr 182, poz. 1228).

Pion ochrony informacji niejawnych tworzy pion ochrony w składzie: pełnomocnik ochrony, oraz kierownik kancelarii materiałów niejawnych.

Współpraca urzędu gminy z podmiotami zewnętrznymi, polegająca na zawieraniu umów wymagających dostępu tychże podmiotów do informacji niejawnych, wymaga w tym zakresie konsultacji z pełnomocnikiem ochrony.

### 1. PODSTAWY PRAWNE OCHRONY INFORMACJI NIEJAWNYCH

Plan ochrony informacji niejawnych w Urzędzie Gminy Bojadła określa zasady i tryb postępowania z informacjami niejawnymi oraz zapewnia jednolity sposób postępowania z tymi informacjami w Urzędzie Gminy Bojadła.

1. Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228).
2. Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. Nr 159, poz. 948).
3. Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 roku w sprawie wzoru decyzji o cofnięciu poświadczenia bezpieczeństwa (Dz.U.2010.258.1754).
3. Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 roku w sprawie wzoru decyzji o odmowie wydania poświadczenia bezpieczeństwa (Dz.U.2010.258.1753).
4. Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 roku w sprawie wzorów poświadczeń bezpieczeństwa (Dz.U.2010.258.1752).
5. Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 roku w sprawie wzorów zaświadczeń stwierdzających odbycie szkolenia w zakresie ochrony informacji niejawnych oraz sposobu rozliczania kosztów przeprowadzenia szkolenia przez Agencję Bezpieczeństwa Wewnętrznego lub Służbę Kontrwywiadu Wojskowego (Dz.U.2010.258.1751).
6. Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 roku w sprawie przekazywania informacji, udostępniania dokumentów oraz udzielania pomocy służbom i instytucjom uprawnionym do prowadzenia poszerzonych postępowań sprawdzających, kontrolnych postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego (Dz.U.2010.258.1750).
7. Rozporządzenie Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności (Dz. U. Nr 288.1692).
8. Rozporządzenie Rady Ministrów z dnia 7 grudnia 2011 roku w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych (Dz. U. Nr 276, poz. 1631).
9. Rozporządzenie Prezesa Rady Ministrów z dnia 26 lutego 2010 roku w sprawie postępowania z dokumentacją w komórkach organizacyjnych wykonujących zadania w zakresie obronności i bezpieczeństwa państwa (Dz.U.2010.34.181).
10. Rozporządzenie Prezesa Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne (Dz. U. Nr 271, poz.1603).

### 2. DEFINICJE UŻYWANE W PLANIE OCHRONY INFORMACJI NIEJAWNYCH

W rozumieniu planu ochrony informacji niejawnych:

1. **ustawą** - jest ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228),
2. **służbą ochrony państwa** - jest Agencja Bezpieczeństwa Wewnętrznego,
3. **rękojmią zachowania tajemnicy** — jest zdolność osoby do spełnienia ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem, stwierdzona w wyniku przeprowadzenia postępowania sprawdzającego,
4. **dokumentem** — jest każda utrwalona informacja niejawna,

5. **materiałem** — jest dokument lub przedmiot albo dowolna ich część, chronione jako informacja niejawna, a zwłaszcza urządzenie, wyposażenie lub broń wyprodukowane albo będące w trakcie produkcji, a także składnik użyty do ich wytworzenia,
6. **przetwarzaniem informacji niejawnych** — są wszelkie operacje wykonywane w odniesieniu do informacji niejawnych i na tych informacjach, w szczególności ich wytwarzanie, modyfikowanie, kopiowanie, klasyfikowanie, gromadzenie, przechowywanie, przekazywanie lub udostępnianie,
7. **systemem teleinformatycznym** — jest system teleinformatyczny w rozumieniu art. 2 pkt 3 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. Nr 144, poz. 1204, z późn. zm.),
8. **urzędem** - jest Urząd Gminy Bojadła,
9. **wójtem** - jest Wójt Gminy Bojadła,
10. **pełnomocnikiem ochrony** - jest Pełnomocnik ds. Ochrony Informacji Niejawnych w Urzędzie Gminy Bojadła.

## 3. ZAŁOŻENIA I POSTANOWIENIA OGÓLNE PLANU

**1.** Przedmiotem ochrony w Urzędzie Gminy Bojadła są informacje niejawne stanowiące tajemnicę służbową oznaczone klauzulą „poufne" i klauzulą „zastrzeżone" występujące i mogące wystąpić w zakresie ich działania oraz pomieszczenia, w których są przechowywane i opracowywane materiały niejawne.

**2.** Plan ochrony informacji niejawnych w Urzędzie Gminy Bojadła jest dokumentem określającym sposoby zapewnienia fizycznego bezpieczeństwa informacji, który:

a) określa środki bezpieczeństwa zapewniające ochronę informacji niejawnych, występujących lub mogących występować w Urzędzie, przed ich nieuprawnionym ujawnieniem, a także szczegółowe zadania w tym zakresie dla odpowiednich pracowników Urzędu i innych osób,

b) określa procedury oraz sposoby postępowania w ramach środków, o których mowa w pkt. a oraz sposoby postępowania w przypadku naruszenia zasad ochrony fizycznej wynikających z tych środków,

c) dostosowuje środki bezpieczeństwa oraz procedury, o których mowa w pkt. a i b do zakresu, klauzuli tajności oraz liczby informacji niejawnych wytwarzanych i przechowywanych w Urzędzie, uwzględniając liczbę oraz poziom dostępu do informacji niejawnych pracowników urzędu.

## 4. CHARAKTERYSTYKA OBIEKTU

### 4.1 Położenie obiektu

Pomieszczenie biurowe, w którym wykonywane i przechowywane są materiały niejawne o klauzuli poufne i zastrzeżone usytuowane jest na I piętrze budynku zlokalizowanego przy ul. Sulechowskiej 35 w Bojadłach.

### 4.2 Dostępność komunikacyjna

Budynek położony jest przy drodze łączącej Sulechów ze Wschową. W pobliżu budynku znajduje się przystanek autobusowy komunikacji PKS.

### 4.3 Otoczenie budynku

W pobliżu budynku znajdują się zabudowania mieszkalne i gospodarcze..

### 4.4 Podmioty na terenie obiektu

Właścicielem budynku jest gmina. Jest to obiekt wolno stojący, zlokalizowany przy ul. Sulechowskiej 35. Pomieszczenia w obiekcie zajmowane są wyłącznie przez Urząd Gminy.

### 4.5 Charakterystyka budynku

Jest to budynek o konstrukcji murowanej. Pomieszczenia biurowe posiadają ściany z cegły palonej. Konstrukcja dachu jest drewniana, jedna klatka schodowa murowana i jedna drewniana. Budynek posiada dwa wejścia od ul. Sulechowskiej i jedno od zaplecza. Okna na parterze zabezpieczone są kratami.

W budynku zainstalowana jest instalacja alarmowa, do której dostęp posiadają Wójt i wyznaczone przez niego osoby.

## 5. DOSTĘP DO INFORMACJI NIEJAWNYCH

### 5.1 Uprawnienia do dostępu do informacji niejawnych.

Uprawnienia do dostępu do informacji niejawnych posiadają osoby które:

a) uzyskały poświadczenie bezpieczeństwa upoważniające do dostępu do informacji niejawnych oznaczonych klauzulą co najmniej „poufne" lub otrzymały pisemne upoważnienie Wójta Gminy do dostępu do informacji niejawnych o klauzuli „zastrzeżone",

b) odbyły przeszkolenie w zakresie ochrony informacji niejawnych.

### 5.2 Udostępnianie informacji niejawnych:

a) informacje niejawne mogą być udostępniane wyłącznie osobie dającej rękojmię zachowania tajemnicy tylko w takim zakresie, jaki jest niezbędny do załatwienia konkretnej sprawy a wynikającym z zakresu czynności,

b) informacje niejawne mogą być udostępnione tylko osobom uprawnionym do dostępu do informacji określonych tą klauzulą i z uwzględnieniem ograniczenia określonego w pkt a.

## 6. STREFA OCHRONNA

### 6.1. Opis strefy

Strefę ochronną stanowi pomieszczenie stanowiska spraw obronnych. W pomieszczeniu tym przechowywane są również w metalowej szafie dokumenty niejawne o klauzuli poufne. Dostęp do pomieszczenia ma inspektor ds. obronnych, pełnomocnik ochrony informacji, pracownik sekretariatu prowadzący ewidencję materiałów niejawnych – zwany dalej pracownikiem sekretariatu oraz Wójt Gminy. Prawo przebywania w pomieszczeniu mają również osoby posiadające poświadczenie bezpieczeństwa do informacji niejawnych o klauzuli co najmniej poufne.

W uzasadnionych pełnieniem obowiązków służbowych okolicznościach, w strefie ochronnej mogą przebywać osoby (tzw. goście) posiadający stosowne upoważnienia oraz poświadczenie ubezpieczeństwa i zaświadczenie o szkoleniu na temat ochrony informacji niejawnych.
Osoby te mogą przebywać w pomieszczeniu tylko pod nadzorem pracownika odpowiedzialnego za sprawy obronne, pełnomocnika ochrony lub pracownika sekretariatu.

Drzwi do strefy oraz szafa metalowa przeznaczona do przechowywania dokumentów poufnych powinny spełniać wymogi określone w odrębnych przepisach. Okna pomieszczenia powinny być okratowane i zabezpieczone dodatkowo siatką.

Drzwi do strefy są stale zamknięte. Otwarte mogą być wyłącznie przez pracownika ds. obronnych, pełnomocnika ochrony, pracownika sekretariatu lub Wójta Gminy po uprzednim pobraniu kluczy, (pobranie kluczy jest każdorazowo ewidencjonowane).

Klucze od strefy ochronnej przechowywane są przez Sekretarza Gminy w plombowanym referentką pojemniku i zamykane w jego oplombowanym sejfie.

Sekretarz Gminy prowadzi ewidencję zdawania i pobierania plombowanego pojemnika z kluczami – odnotowując dokładną godzinę oraz datę pobrania i zwrotu pojemnika.
Nad prawidłowością prowadzenia ewidencji czuwa pełnomocnik ochrony jako osoba zobowiązana do kontroli środków ochrony fizycznej.

Sprzątanie pomieszczenia strefy ochronnej może odbywać się tylko i wyłącznie pod nadzorem pracownika ds. obronnych, pełnomocnika ochrony lub pracownika sekretariatu.

Po zakończeniu pracy drzwi pomieszczenia strefy ochronnej są zamykane i plombowane referentką pracownika ds. obronnych, pełnomocnika ochrony lub pracownika sekretariatu.

Ewidencję referentek prowadzi pracownik sekretariatu według ustaleń Sekretarza Gminy.

### 6.2 Sposób reagowania na nieuprawnione naruszenie strefy

Za naruszenie strefy przyjmuje się wtargnięcie i przebywanie w strefie osób nieuprawnionych, bez wiedzy oraz nadzoru pracownika ds. obronnych, pełnomocnika ochrony, pracownika sekretariatu lub Wójta Gminy.

## 7. OCHRONA FIZYCZNA

1. Budynek i znajdujące się w nim pomieszczenia stanowiące siedzibę Urzędu podlegają ochronie. Ochrona fizyczna polega na stałym monitoringu budynku i znajdujących się w nim pomieszczeń poprzez system alarmowy.

2. Kody do instalacji alarmowej do budynku Urzędu mogą posiadać: Wójt, Sekretarz Gminy, oraz upoważnieni pracownicy odpowiedzialni za otworzenie i zamknięcie budynku Urzędu.
3. Pomieszczenia, w których znajdują się informacje niejawne z klauzulą „poufne" i „ zastrzeżone " po godzinach pracy powinny być zamykane, a klucze zdawane do depozytu.
4. Sprzątanie pomieszczenia w którym są przechowywane informacje niejawne powinno odbywać się w obecności upoważnionego pracownika przed zakończeniem pracy.
5. Informacje niejawne oznaczone klauzulą „poufne" należy przechowywać w szafach metalowych z zamkami o skomplikowanym mechanizmie.
6. W uzasadnionych przypadkach podyktowanych względami dłuższego okresu czasu, niezbędnego do wykonania zadań związanych z dostępem do informacji niejawnych, dokumenty o klauzuli „poufne" mogą być wydawane poza pomieszczenie służące do przechowywania lecz pod warunkiem, że odbiorca dokumentu zapewni warunki ochrony tych dokumentów przechowując je w szafach metalowych z odpowiednim zamknięciem.
7. Szafy metalowe, w których przechowuje się dokumenty o klauzuli „poufne" po zakończeniu pracy należy zamknąć i zaplombować pieczęcią do plasteliny.
8. Informacje niejawne oznaczone klauzulą „zastrzeżone" można przechowywać na stanowiskach pracy, w meblach biurowych zamykanych na klucz.

## 8. ODPOWIEDZIALNOŚĆ ZA OCHRONĘ INFORMACJI NIEJAWNYCH

Osobą odpowiedzialną za zasób dokumentów niejawnych przechowywanych w pomieszczeniu biurowym, w którym przechowywane są materiały niejawne jest pracownik sekretariatu. Osoba ta jest odpowiedzialna za:

- dokumenty niejawne, które wpłynęły lub zostały wytworzone w jednostce,
- dokumenty *zastrzeżone* i *poufne*, zwrócone przez pracowników po załatwieniu sprawy.

### 8.1 Odpowiedzialność osoby pobierającej dokument

Odpowiedzialność osoby za dokument zawierający informacje niejawne rozpoczyna się w chwili pokwitowania odbioru dokumentu, a kończy w momencie oddania go kierownikowi kancelarii materiałów niejawnych. Odpowiedzialność za dokument ponosi każda osoba, której dokument ten został przekazany lub udostępniony.

### 8.2 Nadzór w zakresie ochrony informacji niejawnych

Nadzór nad realizacją zadań i przestrzeganiem przepisów określonych w niniejszym planie sprawuje pełnomocnik ochrony.

***Wójt Gminy przed rozwiązaniem stosunku pracy z pracownikiem posiadającym poświadczenie bezpieczeństwa do dostępu do informacji niejawnych o klauzuli poufne przyjmuje od niego protokolarnie całość materiałów posiadających klauzulę poufne i wyznacza pisemnie pracownika, który ma dalej prowadzić przejętą dokumentację. Protokół sporządza się w 2 egzemplarzach – dla odchodzącego pracownika oraz dla Wójta. Egzemplarz Wójta przekazywany jest do dokumentacji kadrowej.***

***O powyższym fakcie należy powiadomić pełnomocnika ochrony.***

***Przejęcie dokumentów przez nowego pracownika odbywa się na zasadach wskazanych w odrębnej instrukcji – z pominięciem wymogu dekretowania pojedynczych dokumentów. Podstawą przekazania przejętej dokumentacji jest pisemne polecenie Wójta lub dekretacja sporządzona na protokole zdawczo-odbiorczym.***

### 8.3 Odpowiedzialność za naruszenie przepisów

W stosunku do pracowników, którzy nie przestrzegając wymagań związanych z ochroną informacji niejawnych, nierzetelnie wykonują swoje obowiązki lub dopuszczają się uchybień w zakresie zabezpieczenia dokumentów i informacji podlegających ochronie, stwarzając tym samym warunki do ujawnienia tajemnicy osobom nieuprawnionym, mogą być zastosowane przewidziane prawem sankcje służbowe, dyscyplinarne lub karne, łącznie z kontrolnym postępowaniem sprawdzającym, mogącym zakończyć się decyzją o cofnięciu poświadczenia bezpieczeństwa.

## 9. UDOSTĘPNIANIE ZBIORÓW

Udostępnianie zasobów materiałów niejawnych odbywa się na zasadach określonych w ustawie, tj. osobom posiadającym odpowiednie poświadczenie bezpieczeństwa lub upoważnienie, zaświadczenie o przeszkoleniu oraz dekretację przełożonego.

## 10. PRZECHOWYWANIE KLUCZY OD POMIESZCZEŃ CHRONIONYCH I SZAF

Urządzenia (szafy i pomieszczenia), w których przechowywane są dokumenty zawierające informacje niejawne, podlegają codziennie po zakończeniu pracy zamykaniu.

Klucze od pomieszczenia i szaf, w których są przechowywane materiały niejawne przechowywane są w plombowanym referentką pracownika ds. obronnych, pełnomocnika ochrony lub pracownika sekretariatu pojemniku. Pojemnik ten przechowuje w zamykanym i plombowanym sejfie w pomieszczeniu biurowym zajmowanym przez Sekretarza Gminy. Klucz do sejfu Sekretarz Gminy przechowuje osobiście i całodobowo. Drugi, zapasowy komplet kluczy od pomieszczenia i szaf przechowywany jest w plombowanym referentką Wójta Gminy pojemniku w zamykanej szafie jego pomieszczenia biurowego.

Sekretarz Gminy prowadzi dziennik ewidencyjny zdawania i pobierania plombowanego pojemnika z kluczami – odnotowując dokładną godzinę oraz datę pobrania i zwrotu pojemnika. Nad prawidłowością prowadzenia ewidencji czuwa pełnomocnik ochrony jako osoba upoważniona do kontroli środków ochrony fizycznej.

Zabronione jest wynoszenie poza urząd gminy kluczy do pomieszczeń biurowych oraz szaf, w których są przechowywane materiały niejawne.

## 11. POSTĘPOWANIE Z INFORMACJAMI NIEJAWNYMI W RAZIE WPROWADZENIA STANU NADZWYCZAJNEGO

Szczególny obowiązek zabezpieczenia materiałów zawierających informacje niejawne powstaje w przypadku wprowadzenia stanu nadzwyczajnego.

1. Jako stany nadzwyczajne uważa się stany określone w art. 228 Konstytucji RP (Dz. U. z 1997 r. Nr 78, poz. 484 z późn. zm.), tj. stan wojenny, stan wyjątkowy lub stan klęski żywiołowej.
2. Stan nadzwyczajny może być wprowadzony tylko na podstawie ustawy, w drodze rozporządzenia, które podlega dodatkowemu podaniu do publicznej wiadomości.
3. Działania podjęte w wyniku wprowadzenia stanu nadzwyczajnego muszą odpowiadać stopniowi zagrożenia i powinny zmierzać do jak najszybszego przywrócenia normalnego funkcjonowania państwa.
4. W związku z wprowadzeniem stanu nadzwyczajnego działania podjęte w celu ochrony dokumentów niejawnych będących w posiadaniu Urzędu Gminy muszą odpowiadać stopniowi zagrożenia podstawowych interesów RP w zakresie obronności, bezpieczeństwa, stosunków gospodarczych i międzynarodowych państwa. Ewakuacja materiałów zawierających informacje niejawne następuje na polecenie Wójta Gminy. Koordynatorem ewakuacji jest pełnomocnik ochrony, który współpracuje w tym zakresie z pracownikami komórek organizacyjnych. Materiały niejawne przechowywane w pomieszczeniu stanowiska obronnego należy oznakować symbolami „Z" lub „E" umieszczonymi pod kategorią archiwalną w sposób trwały i widoczny. Za prawidłowe wydzielenie materiałów i właściwe ich oznaczenie symbolami „Z" i „E" odpowiedzialny pracownik sekretariatu, który dokonuje tej czynności w uzgodnieniu z wytwórcami merytorycznymi. Zabezpieczeniu poprzez ewakuację podlegają wszystkie materiały oznakowane symbolem „E". Materiały niejawne oznakowane symbolem „Z" należy zniszczyć, np. poprzez pocięcie ich w niszczarce lub spalenie.
5. Miejsce ewakuacji dla materiałów niejawnych oznaczonych symbolem „E" wyznacza każdorazowo Wójt Gminy, wskazując tym samym dokładną lokalizację.
6. Przed ewakuacją pracownik sekretariatu sporządza w miarę możliwości 2 egz. spis dokumentów przeznaczonych do ewakuacji oraz do zniszczenia, z czego jeden przekazuje Wójtowi Gminy bezpośrednio lub za pośrednictwem pełnomocnika ochrony, a drugi zabiera wraz z ewakuowaną dokumentacją.

W celu wykonania zadań związanych z ewakuacją pełnomocnik ochrony wydaje stosowne polecenie pracownikowi sekretariatu. Jeśli ewakuacja jest zarządzana w godzinach pozasłużbowych należy wezwać pracownika sekretariatu w celu sprawowania przez niego nadzoru nad zabezpieczeniem materiałów. W przypadku nieobecności pracownika sekretariatu pełnomocnik ochrony realizuje zadania związane z ewakuacją materiałów niejawnych.

W wypadku pozostawieniu w pomieszczeniu materiałów, które nie podlegają ewakuacji lub zniszczeniu pracownik sekretariatu lub pełnomocnik ochrony są zobowiązani zamknąć i zaplombować szafy oraz pomieszczenie, w którym są przechowywane materiały niejawne.

Ewakuacja akt powinna obejmować: zapakowanie materiałów do worków ewakuacyjnych lub skrzyń pakowych (będących na wyposażeniu urzędu), przemieszczenie worków na środek transportu i przewiezienie do wyznaczonego przez Wójta Gminy miejsca ewakuacji.

Nadzór i ochronę transportu do miejsca ewakuacji dokumentów zapewnia pełnomocnik ochrony.

## 12. POSTĘPOWANIE W SYTUACJACH KRYZYSOWYCH I ANALIZA RYZYKA WYSTĄPIENIA SYTUACJI KRYZYSOWYCH

### 12.1 Zagrożenia zewnętrzne

Rodzaje zagrożeń:

zagrożeniami zewnętrznymi dla Urzędu są:

- możliwość napadu przez zorganizowane grupy przestępcze i terrorystyczne, działające w sposób profesjonalny, przemyślany i zorganizowany,
- możliwość napadu przez pojedynczych przestępców, lub przypadkowe osoby wykorzystujące nadarzającą się okazję z powodu nieprawidłowości w ochronie Urzędu.

### 12.2 Symptomy mogące świadczyć o przygotowaniu napadu lub włamania do budynku Urzędu

- wzmożone zainteresowanie osób postronnych obiektem, pomieszczeniami Urzędu objawiające się między innymi: podejmowaniem prób uzyskania informacji o danym obiekcie, pomieszczeniu od pracowników podczas luźnych rozmów po „przypadkowym" spotkaniu,
- nawiązanie rozmów przez osoby postronne z pracownikami,
- podszywanie się pod byłych pracowników Urzędu i przejawianie zainteresowaniem tym, co się po latach zmieniło,
- interesowanie się osobami funkcyjnymi, w tym także ich przywarami oraz sposobem wykonywania obowiązków służbowych,
- obserwacja sposobu działania systemu ochronnego, sekretariatu, sprzątaczki itp.
- rozpoznawanie systemu technicznych zabezpieczeń, w tym stosowanych urządzeń alarmowych,
- celowe uszkadzanie urządzeń alarmowych, linii telefonicznych, oświetlenia itp.,
- próby pozyskania do grup przestępczych pracowników Urzędu (dotyczy głównie osób mających problemy finansowe, towarzyskie, a także służbowe)

### 12.3 Wnioski

W związku z przedstawionymi kierunkami zagrożeń należy wykonywać następujące czynności uprzedzające ewentualne możliwości zaistnienia zagrożeń:

- systematyczną, skrupulatną i wnikliwą kontrolę systemu ochrony przez osoby odpowiedzialne za jego organizację,
- pracownicy pionu ochrony w czasie dnia pracy powinny zwracać szczególną uwagę na możliwość zaistnienia ewentualnych zagrożeń,
- stosować zasadę niedopuszczania osób niepowołanych do penetracji strefy bezpieczeństwa,
- wykonywanie prac porządkowych, remontowych itp. w strefie bezpieczeństwa wyłącznie pod nadzorem osób odpowiedzialnych.

### 12.4 Zagrożenia wewnętrzne

Rodzaje zagrożeń:

- próby zaboru dokumentów lub mienia przez pracowników Urzędu,
- próby powielania, kserowania dokumentów służbowych dla celów prywatnych,
- byli pracownicy urzędu zwolnieni dyscyplinarnie,

- rozpoznanie organizacji pracy Urzędu celem łatwiejszej pracy grup przestępczych na terenie urzędu,
- próby wglądu w dokumenty niejawne przez osoby nieuprawnione,
- spożywanie alkoholu – przesłanka do wykroczeń dyscyplinarnych i przestępstw.

**12.5 Wnioski**

W związku z przedstawionymi kierunkami zagrożeń należy wykonywać następujące czynności uprzedzające ewentualne możliwości zaistnienia zagrożeń:

- zwracanie szczególnej uwagi na osoby, które mogą być zainteresowane zaborem dokumentu,
- prowadzenie szczególnego nadzoru, by nie dokonywano prób kserowania, kopiowania bez zgody przełożonego,
- uwrażliwianie pracowników w trakcie prowadzonych szkoleń na możliwość prób kontaktu grup przestępczych z pracownikami, którzy mają dostęp do dokumentów szczególnie ważnych,
- zastosowanie zasady, że do informacji niejawnych mogą mieć dostęp tylko pracownicy posiadający poświadczenie bezpieczeństwa lub właściwe upoważnienie jednorazowe wydane przez Wójta.
- wprowadzenie szczególnej uwagi na osoby, których zachowanie wskazuje na nadmierne spożywanie alkoholu.

Za sytuacje kryzysowe w zakresie informacji niejawnych przyjmuje się zdarzenia:

| Lp. | Rodzaj sytuacji kryzysowej | Poziom ryzyka (skala 1 – 5) | Sposób postępowania z dokumentami |
|---|---|---|---|
| 1. | Zanik napięcia | 3 | P |
| 2. | Awaria systemu alarmowego | 4 | P |
| 3. | Pożar | 3 | E |
| 4. | Zagrożenia atmosferyczne | 2 | E |
| 5. | Zagrożenia chemiczne | 1 | E |
| 6. | Zagrożenie atakiem terroru | 2 | Z |
| 7. | Włamanie | 2 | Z |
| 8. | Napad | 1 | Z |
| 9. | Kradzież | 2 | – |
| 10. | Zniszczenie dokumentu | 4 | – |
| 11. | Wtargnięcie lub okupacja budynku | 2 | Z |
| 12. | Działanie obcych służ specjalnych | 1 | E |

W każdym z wymienionych przypadków pełnomocnik ochrony powinien podjąć działania prowadzące do wyjaśnienia przyczyn tejże sytuacji oraz usunięcia jej skutków.

Dokumenty niejawne powinny być opatrzone symbolem „Z", „P" lub „E" – zniszczyć, pozostawić lub ewakuować – symbole te pozwolą podzielić dokumenty niejawne na te, które wymagają ewakuacji oraz takie, które należy pozostawić lub zniszczyć w urzędzie.

Dokumenty wymagające ewakuacji należy przełożyć do pozostających w dyspozycji pełnomocnika ochrony worków i przewieźć jak najszybciej w bezpieczne, niezagrożone w tych okolicznościach miejsce.

## 13. POSTĘPOWANIE W PRZYPADKU NARUSZENIA USTAWY O OCHRONIE INFORMACJI NIEJAWNYCH I PRZEPISÓW WYKONAWCZYCH DO USTAWY.

1. Za ochronę informacji niejawnych w Urzędzie odpowiada Wójt. Zadania określone ustawą o ochronie informacji niejawnych w imieniu Wójta wykonuje pełnomocnik ochrony poprzez:

- sprawowanie nadzoru nad realizacją zadań i przestrzeganiem przepisów określonych w Planie ochrony,

- sprawowanie kontroli w zakresie ochrony informacji niejawnych oraz przestrzegania związanych z upoważnianiem do dostępu do tych informacji, w odniesieniu do wszystkich komórek organizacyjnych Urzędu.

2. W przypadku ujawnienia informacji niejawnych przez podległych pracowników Wójt lub upoważniony przez niego pracownik zawiadamia na piśmie pełnomocnika ochrony podając jaka informacja niejawna została ujawniona lub jakie naruszenie przepisów zostało stwierdzone.
3. Pełnomocnik ochrony przeprowadza okresowe kontrole przestrzegania ustawy o ochronie informacji niejawnych w Urzędzie. W przypadku stwierdzenia naruszenia przepisów o ochronie informacji niejawnych pełnomocnik ochrony przekłada Wójtowi pisemną informację o naruszeniu przepisów i wnioski do podjęcia decyzji.
4. W przypadku naruszenia przepisów o ochronie informacji niejawnych oznaczonych klauzulą „poufne" lub wyższą pełnomocnik ochrony powiadamia Wójta oraz właściwy oddział Agencji Bezpieczeństwa Wewnętrznego.

## 14. WYKONYWANIE DOKUMENTÓW ZAWIERAJĄCYCH INFORMACJE NIEJAWNE ZA POMOCĄ KOMPUTERA

Pracownicy, którzy do opracowywania i wykonywania dokumentów zawierających informacje oznaczone klauzulami „poufne" lub „zastrzeżone", wykorzystują urządzenia komputerowe, obowiązani są zabezpieczać informacje podlegające ochronie przed ich nieuprawnionym ujawnieniem, a także przed dotarciem do tych informacji przez osoby, które nie powinny zapoznać się z ich treścią.

1. Bezpieczeństwo teleinformatyczne zapewnia się, chroniąc informacje przetwarzane w systemach i sieciach teleinformatycznych przed utratą właściwości gwarantujących to bezpieczeństwo, w szczególności przed utratą poufności, dostępności i integralności.
2. Bezpieczeństwo teleinformatyczne zapewnia się przed rozpoczęciem oraz w trakcie przetwarzania informacji niejawnych w systemie lub sieci teleinformatycznej.
3. Za właściwą organizację bezpieczeństwa teleinformatycznego odpowiada Wójt, który w szczególności:
   a) zapewnia opracowanie dokumentacji bezpieczeństwa teleinformatycznego,
   b) realizuje ochronę fizyczną, elektromagnetyczną i kryptograficzną systemu lub sieci teleinformatycznej,
   c) zapewnia niezawodność transmisji oraz kontrolę dostępu do urządzeń systemu lub sieci teleinformatycznej,
   d) dokonuje analizy stanu bezpieczeństwa teleinformatycznego oraz zapewnia usunięcie stwierdzonych nieprawidłowości,
   e) zapewnia przeszkolenie z zakresu bezpieczeństwa teleinformatycznego dla osób uprawnionych do pracy w systemie lub sieci teleinformatycznej,
   f) zawiadamia właściwą służbę ochrony państwa o zaistniałym incydencie bezpieczeństwa teleinformatycznego dotyczącym informacji niejawnych oznaczonych co najmniej klauzulą „poufne".
4. Ochrona fizyczna systemu lub sieci teleinformatycznej polega na
   a) umieszczeniu urządzeń systemu lub sieci teleinformatycznej w strefie kontrolowanego dostępu
   b) zastosowaniu środków zapewniających ochronę fizyczną, w szczególności przed:
      - nieuprawnionym dostępem,
      - podglądem,
      - podsłuchem.
5. Ochrona elektromagnetyczna systemu lub sieci teleinformatycznej polega na niedopuszczeniu do utraty poufności i dostępności informacji niejawnych przetwarzanych w urządzeniach teleinformatycznych:
   a) utrata poufności następuje w szczególności na skutek wykorzystania elektromagnetycznej emisji ujawniającej pochodzącej z tych urządzeń,
   b) utrata dostępności następuje w szczególności na skutek zakłócania pracy urządzeń teleinformatycznych za pomocą impulsów elektromagnetycznych o dużej mocy.

6. System lub sieć teleinformatyczną wyposaża się w mechanizmy kontroli dostępu odpowiednie do klauzuli tajności informacji niejawnych w nich przetwarzanych.

## 15. POSTĘPOWANIE W PRZYPADKU OTRZYMANIA PRZESYŁKI NIEWIADOMEGO POCHODZENIA

W przypadku otrzymania jakiejkolwiek przesyłki niewiadomego pochodzenia lub budzącej podejrzenia z jakiegokolwiek innego powodu:

-brak nadawcy,
-brak adresu nadawcy,
-przesyłka pochodzi od nadawcy lub z miejsca, z którego nie spodziewamy się,
-inne podejrzenia.

Nie należy otwierać tej przesyłki .

**Należy:**

1. Umieścić przesyłkę w grubym worku plastikowym, szczelnie zamknąć.
2. Worek należy umieścić w drugim plastikowym worku, szczelnie zamkniętym, zakleić taśmą lub plastrem.
3. Paczki nie należy przemieszczać, należy pozostawić ją na miejscu.
4. Powiadomić:
   - Komendę Powiatową Policji tel. 997;
   - Komendę Powiatową Państwowej Straży Pożarnej tel. 998;

Służby te podejmą wszelkie niezbędne kroki w celu bezpiecznego przejęcia przesyłki.

W przypadku, gdy podejrzana przesyłka została otwarta i zawiera jakąkolwiek podejrzaną zawartość w formie stałej (galaretę, pianę, pył lub inną).

**Należy:**

1. Nie naruszyć zawartości -nie rozsypywać, nie przenosić, nie dotykać, nie wąchać, nie powodować ruchu powietrza w pomieszczeniu (wyłączyć systemy wentylacyjne, zamknąć okna).
2. Całą zawartość umieścić w worku plastikowym, zamknąć go i zakleić taśmą lub plastrem.
3. Dokładnie umyć ręce
4. Zaklejony worek umieścić w drugim worku, zamknąć go i zakleić.
5. Ponownie umyć ręce.
6. Powiadomić:
   - Komendę Powiatową Policji;
   - Komendę Powiatową Państwowej Straży Pożarnej;
   - Powiatową Stację Sanitarno-Epidemiologiczną;
   - Pogotowie Ratunkowe;

Po przybyciu właściwej służby należy bezwzględnie stosować się do jej zaleceń.

## 16. POSTĘPOWANIE W PRZYPADKU ZGŁOSZENIA O PODŁOŻENIU LUB ZNALEZIENIU ŁADUNKU WYBUCHOWEGO W BUDYNKU URZĘDU

**Alarmowanie**

1. Osoba, która przyjęła zgłoszenie o podłożeniu ładunku wybuchowego albo zauważyła w obiekcie przedmiot niewiadomego pochodzenia mogący być ładunkiem wybuchowym jest obowiązana o tym powiadomić:
   1) Wójta,
   2) Komendanta Powiatowego Policji.
2. Zawiadamiając Policję należy podać treść rozmowy ze zgłaszającym o podłożeniu ładunku wybuchowego, którą należy prowadzić wg poniższych wskazówek:
   1) miejsce i opis zlokalizowanego przedmiotu, który może być ładunkiem wybuchowym,
   2) numer telefonu, z którego prowadzona jest rozmowa i swoje stanowisko,
   3) uzyskać od Policji potwierdzenie przyjętego zawiadomienia.

**Akcja poszukiwawcza ładunku wybuchowego po uzyskaniu informacji o jego podłożeniu.**

1. Do czasu przybycia Policji akcją kieruje Wójt, a w czasie jego nieobecności Sekretarz bądź pełnomocnik ochrony.

2. Kierujący akcją zarządza, aby użytkownicy pomieszczeń dokonali sprawdzenia, czy w tych pomieszczeniach znajdują się:

a) przedmioty, rzeczy lub urządzenia, paczki itp., których wcześniej nie było i nie wnieśli ich użytkownicy pomieszczeń,

b) ślady przemieszczania elementów wyposażenia pomieszczeń,

c) zmiany w wyglądzie zewnętrznym przedmiotów, rzeczy, urządzeń, które przedtem w pomieszczeniu były oraz emitowane z nich sygnały (np. dźwięki mechanizmów zegarowych, świecące elementy elektroniczne itp.).

3. Pomieszczenia ogólnodostępne takie jak: korytarze, klatki schodowe, hale, windy, toalety, piwnice, strychy itp. oraz najbliższe otoczenie zewnętrzne obiektu powinny być sprawdzone przez wyznaczonych do tego pracowników.

4. Zlokalizowanych przedmiotów, rzeczy, urządzeń, których w ocenie użytkowników obiektu przedtem nie było, a zachodzi podejrzenie, że mogą to być ładunki wybuchowe nie wolno dotykać. O ich umiejscowieniu należy natychmiast powiadomić Wójta i Policję.

5. W przypadku, gdy użytkownicy pomieszczeń faktycznie stwierdzą obecność przedmiotów (rzeczy, urządzeń), których wcześniej nie było lub zmiany w wyglądzie i usytuowaniu przedmiotów stale znajdujących się w tych pomieszczeniach, należy domniemywać, że pojawienie się tych przedmiotów lub zmiany w ich wyglądzie i usytuowaniu mogły nastąpić na skutek działania sprawcy podłożenia ładunku wybuchowego. W takiej sytuacji kierujący akcją może wydać decyzje ewakuacji osób z zagrożonego obiektu przed przybyciem Policji.

6. Należy zachować spokój i opanowanie, aby nie dopuścić do przejawów paniki.

**Współpraca z policją w czasie akcji**

1. Po przybyciu do obiektu policjanta bądź policyjnej grupy interwencyjnej kierujący akcją powinien przekazać im wszelkie informacje dotyczące zdarzenia oraz wskazać miejsce zlokalizowanych przedmiotów, rzeczy, urządzeń obcego pochodzenia i punkty newralgiczne w obiekcie.

2. Policjant lub dowódca grupy interwencyjnej przejmuje kierowanie akcją, a kierujący dotychczas akcją winien udzielić mu wszechstronnej pomocy.

3. Na wniosek policjanta kierującego akcją Wójt podejmuje decyzję o ewakuacji użytkowników i innych osób z obiektu, o ile wcześniej to nie nastąpiło.

4. Identyfikacją i rozpoznaniem zlokalizowanych przedmiotów, rzeczy, urządzeń obcych oraz neutralizowaniem ewentualnie podłożonych ładunków wybuchowych zajmują się uprawnione i wyspecjalizowane ogniwa organizacyjne policji, przy wykorzystaniu specjalistycznych środków technicznych.

5. Policjant kierujący akcją po zakończeniu działań przekazuje protokolarnie obiekt Wójtowi.

**Postanowienia końcowe dotyczące działań w przypadku zgłoszenia o podłożeniu ładunku wybuchowego**

1. Osobom przyjmującym zgłoszenie o podłożeniu ładunku wybuchowego oraz Wójtowi nie wolno lekceważyć żadnej informacji na ten temat. Każdorazowo osoby te winny zawiadamiać o tym Policję, która z urzędu dokona sprawdzenia wiarygodności każdego zgłoszenia.

2. Wójt powinien na bieżąco organizować szkolenie pracowników w zakresie sposobu zachowania w sytuacjach wymienionych w tej części Planu oraz winien znać rozmieszczenie newralgicznych punktów - węzły energetyczne i wodne, które udostępnia się na żądanie policjanta kierującego akcją

## 17. ZAPOZNANIE Z PLANEM

Z planem należy zapoznać wszystkich pracowników urzędu.