

**Zarządzenie Nr 36 /2011
Wójta Gminy Somonino
z dnia 24 czerwca 2011 r.**

w sprawie zatwierdzenia "Planu Ochrony Informacji Niejawnych" w Urzędzie Gminy w Somoninie.

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) oraz art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2001 r., nr 142 poz. 1591 z późn. zm.), zarządzam, co następuje:

§ 1.

Zatwierdzam Plan Ochrony Informacji Niejawnych w Urzędzie Gminy w Somoninie 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.

WÓJT

mgr Marian Kryszewski

ZATWIERDZAM

WÓJT
Kryszewski
mgr Marian Kryszewski

SOMONINO, dnia

**PLAN OCHRONY INFORMACJI NIEJAWNYCH
OZNACZONYCH KLAUZULĄ "ZASTRZEŻONE"
W KOMÓRKACH ORGANIZACYJNYCH
URZĘDU GMINY SOMONINO**



Sporządził:

PEŁNOMOCNIK
ds. Ochrony Informacji Niejawnych
Jarosław Wydrowski
Jarosław Wydrowski

SPIS TREŚCI

STRONA

I. Podstawa prawna opracowania planu -----	3
II. Przedmiot ochrony-----	3
III. Definicje-----	3 - 4
IV. Położenie – charakterystyka urzędu -----	4
V. Telefony kontaktowe -----	4
VI. Ocena zagrożeń zewnętrznych i wewnętrznych-----	5
VII. Osoby odpowiedzialne za ochronę informacji niejawnych w urzędzie -----	6
VIII. Ewidencja informacji niejawnych podlegających ochronie-----	6
IX. Zabezpieczenie informacji niejawnych -----	6-7
X. Zasady dostępu do informacji niejawnych stanowiących tajemnicę o klauzuli zastrzeżone- 7	
XI. Postępowanie w przypadku naruszenia ustawy o ochronie informacji niejawnych i przepisów wykonawczych do ustawy.-----	7
XII. Instrukcja postępowania w przypadku otrzymania przesyłki niewiadomego pochodzenia-----	8
XIII. Instrukcja alarmowa w przypadku zgłoszenia o podłożeniu lub znalezieniu ładunku wybuchowego w budynku Urzędu-----	8-9
XIV. Ochrona informacji niejawnych w urzędzie w razie wprowadzenia stanu nadzwyczajnego-----	10

I. Podstawa prawna opracowania planu;

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

II. Przedmiot ochrony

Przedmiotem ochrony w Urzędzie Gminy Somonino, są:

1. Informacje niejawne stanowiące tajemnicę służbową oznaczone:
 - klauzulą „zastrzeżone”,
2. Pomieszczenia, w których są wytwarzane, przetwarzane i przechowywane informacje niejawne.

III. Definicje

1. W rozumieniu ustawy:

- **rękojmia zachowania tajemnicy**- jest zdolność osoby do spełnienia ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem, stwierdzona w wyniku przeprowadzenia postępowania sprawdzającego,
- **dokumentem** – jest każda utrwalona informacja niejawna,
- **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,
- **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,
- **system teleinformatyczny** – jest system teleinformatyczny w rozumieniu art. 2 pkt 3 ustawy z dnia 18 lipca 2002r. o świadczeniu usług drogą elektroniczną (Dz. U. Nr 144, poz. 1204, z późn. zm),
- **dokumentem szczególnych wymagań bezpieczeństwa** – jest systematyczny opis sposobu zarządzania bezpieczeństwem systemu teleinformatycznego,
- **dokumentem procedur bezpiecznej eksploatacji systemu teleinformatycznego** – jest opis sposobu i trybu postępowania w sprawach związanych z bezpieczeństwem informacji niejawnych przetwarzanych w systemie teleinformatycznym oraz zakres odpowiedzialności użytkowników systemu teleinformatycznego i pracowników mających do niego dostęp,
- **dokumentacją bezpieczeństwa systemu teleinformatycznego** – jest dokument szczególnych wymagań bezpieczeństwa oraz dokument procedur bezpiecznej eksploatacji systemu teleinformatycznego, opracowane zgodnie z zasadami określonymi w ustawie,
- **akredytacją bezpieczeństwa teleinformatycznego** – jest dopuszczenie systemu teleinformatycznego do przetwarzania informacji niejawnych,
- **certyfikacją** – jest proces potwierdzania zdolności urządzenia, narzędzia lub innego środka do ochrony informacji niejawnych,
- **ryzykiem** – jest kombinacja prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji,
- **szacowanie ryzyka** – jest całościowy proces analizy i oceny ryzyka,
- **zarządzaniem ryzykiem** – są skoordynowane działania w zakresie zarządzania bezpieczeństwem informacji, z uwzględnieniem ryzyka,
- **zatrudnieniem** – jest również odpowiednio powołanie, mianowanie lub wyznaczenie.

2. W sytuacjach szczególnych zagrożeń, jeżeli zwykłe środki konstytucyjne są niewystarczające, może zostać wprowadzony odpowiedni stan nadzwyczajny:

- w razie zewnętrznego zagrożenia państwa, zbrojnej napaści na terytorium Rzeczypospolitej Polskiej lub gdy z umowy międzynarodowej wynika zobowiązanie do wspólnej obrony przeciwko agresji. Prezydent Rzeczypospolitej na wniosek Rady Ministrów może wprowadzić **stan wojenny** na części albo na całym terytorium państwa (art. 229 Konstytucji RP),
- w razie zagrożenia konstytucyjnego ustroju państwa, bezpieczeństwa obywateli lub porządku publicznego, Prezydent Rzeczypospolitej na wniosek Rady Ministrów może wprowadzić na czas oznaczony, nie dłuższy niż 90 dni, **stan wyjątkowy** na części albo całym terytorium państwa (art. 230 Konstytucji RP),
- w celu zapobieżenia skutkom katastrof naturalnych lub awarii technicznych noszących znamiona klęski żywiołowej oraz w celu ich usunięcia Rada Ministrów może wprowadzić na czas oznaczony, nie dłuższy niż 30 dni, **stan klęski żywiołowej** na części albo na całym terytorium państwa. Przedłużenie tego stanu może nastąpić za zgodą Sejmu (art. 232 Konstytucji RP).

IV. Położenie – charakterystyka urzędu

Urząd Gminy – budynek Urzędu Gminy Somonino usytuowany jest przy ulicy Ceynowy 21. Jest to budynek dwupiętrowy.

Ochronę fizyczną Urzędu zapewnia system alarmowy, uzbrajany po godzinach pracy.

Do budynku prowadzi główne wejście od ulicy Ceynowy, gdzie mogą wejść interesanci, klienci i goście urzędu. Obsługa interesantów odbywa się na parterze budynku.

Po godzinach służbowych pracownicy urzędu zamykają pomieszczenia służbowe.

System alarmowy urzędu uzbraja etatowy pracownik Urzędu Gminy – zastępca kierownika urzędu Stanu Cywilnego. W weekendy system jest uzbrojony cały czas. Kody do systemu posiadają dwie osoby: Wójt Gminy oraz zastępca kierownika Urzędu Stanu Cywilnego.

Budynek urzędu po godzinach pracy chroniony jest systemem alarmowym i fizycznie zgodnie z podpisaną umową z firma ochroniarską koncesjonowaną.

V. Telefony kontaktowe

- | | | |
|-----------------------------------|---|----------------------------------|
| 1. Urząd Gminy | - | 58 684-11-21
fax 58 684-11-44 |
| 2. Komisariat Policji w Somoninie | - | 58 684-11-97 |
| 3. KP Policji w Kartuzach | - | 997. 112 lub 685-22-22 |
| 4. KP PSP w Kartuzach | - | 998, 112 lub 681-13-57 lub 58 |

VI. OCENA ZAGROŻEŃ ZEWNĘTRZNYCH I WEWNĘTRZNYCH

Urząd Gminy Somonino, jako organ administracji, generalnie nie jest narażony na radykalne oddziaływanie zagrożeń zewnętrznych i wewnętrznych. Niemniej jednak należy uwzględnić następujące zagrożenia:

OCENA ZAGROŻEŃ ZEWNĘTRZNYCH

1. Zagrożeniami zewnętrznymi dla Gminy Somonino mogą być (lub są mało prawdopodobne):
 - 1) możliwość napadu przez zorganizowane grupy przestępcze i terrorystyczne, działające w sposób profesjonalny, przemysłowy i zorganizowany,
 - 2) możliwość napadu przez pojedynczych przestępców, przypadkowe osoby wykorzystujące nadarzącą się okazję z powodu nieprawidłowości w ochronie mienia z urzędu.
2. Symptomy mogące świadczyć o przygotowaniu napadu lub włamania do budynku:
 - 1) wzmożone zainteresowanie osób postronnych obiektami, pomieszczeniami gminy objawiające się m. in. podejmowaniem prób uzyskania informacji o obiektach, pomieszczeniach od pracowników podczas rozmów,
 - 2) nawiązanie rozmów przez osoby postronne z pracownikami,
 - 3) podszywanie się pod byłych pracowników urzędu i przejawianie zainteresowania tym, co się po latach zmieniło,
 - 4) interesowanie się osobami funkcyjnymi, w tym także ich przywarami oraz sposobem wykonywania obowiązków służbowych,
 - 5) obserwacja sposobu działania systemu ochronnego, sekretariatu, sprzątaczek i tp.,
 - 6) rozpoznawanie systemu technicznych zabezpieczeń, w tym stosowanych urządzeń alarmowych,
 - 7) celowe uszkodzanie urządzeń alarmowych, linii telefonicznych, oświetlenia i tp.,
 - 8) próby uzyskania do grup przestępczych pracowników gminy.
3. Wnioski
W związku z przedstawionymi kierunkami zagrożeń należy wykonywać następujące czynności uprzedzające ewentualne możliwości zaistnienia zagrożeń:
 - 1) systematyczną, skrupulatną i wnikliwą kontrolę systemu ochrony przez osoby odpowiedzialne za jego organizację,
 - 2) pracownicy pionu ochrony w czasie dnia pracy powinni zwracać szczególną uwagę na możliwość zaistnienia ewentualnych zagrożeń,
 - 3) stosować zasadę niedopuszczania osób niepowołanych do penetracji pomieszczeń urzędu,

OCENA ZAGROŻEŃ WEWNĘTRZNYCH

1. Zagrożeniami wewnętrznymi dla Gminy Somonino mogą być (lub są mało prawdopodobne):
 - 1) próby zaboru dokumentów lub mienia przez pracowników gminy
 - 2) próby powielania, kserowania dokumentów służbowych dla celów prywatnych, byli pracownicy urzędu zwolnieni dyscyplinarnie,
 - 3) rozpoznanie organizacji pracy urzędu gminy celem łatwiejszej pracy grup przestępczych na terenie starostwa,
 - 4) próby wglądu w dokumenty niejawnie przez osoby nieuprawnione,
 - 5) możliwość kradzieży sprzętu elektronicznego i teleinformatycznego
 - 6) uprawniony użytkownik może przypadkowo lub świadomie zagrozić bezpieczeństwu informacji wytwarzanych, przetwarzanych lub przechowywanych.
2. Wnioski
W związku z przedstawionymi kierunkami zagrożeń należy wykonywać następujące czynności uprzedzające ewentualne możliwości zaistnienia zagrożeń:
 - 1) zwracanie szczególnej uwagi na osoby, które mogą być zainteresowane zaborem dokumentu,

- 2) prowadzenie szczególnego nadzoru by nie dokonywano prób kserowania, kopiowania bez zgody przełożonego,
- 3) uwrażliwienie pracowników w trakcie prowadzonych szkoleń na możliwość prób kontaktu grup przestępczych z pracownikami, którzy mają dostęp do dokumentów szczególnie ważnych,
- 4) zastosowanie zasady, że do informacji niejawnych mogą mieć dostęp tylko pracownicy posiadający poświadczenie bezpieczeństwa lub właściwe upoważnienie jednorazowe wydane przez Wójta,

VII. Osoby odpowiedzialne za ochronę informacji niejawnych w urzędzie

Zgodnie z art. 14 ust. 1 i 2 ustawy o ochronie informacji niejawnych, kierownik jednostki organizacyjnej w której są przetwarzane informacje niejawne, odpowiada za ich ochronę, w szczególności za zorganizowanie i zapewnienie funkcjonowania tej ochrony.

Wójtowi **bezpośrednio** podlega zatrudniony przez niego pełnomocnik do spraw ochrony informacji niejawnych, który odpowiada za zapewnienie przestrzegania przepisów o ochronie informacji niejawnych.

Jednym z zadań pełnomocnika jest zapewnienie ochrony informacji niejawnych, w tym stosowania środków bezpieczeństwa fizycznego. Zadanie to, pełnomocnik realizuje przy pomocy podległej mu komórki organizacyjnej do spraw ochrony informacji niejawnych, zwanej „**Pionem Ochrony**”, jeżeli jest ona utworzona w jednostce organizacyjnej.

VIII. Ewidencja informacji niejawnych podlegających ochronie

1. Każdy dokument niejawny przychodzący lub wychodzący z urzędu gminy ewidencjonuje się w odrębnej pozycji właściwego dziennika ewidencyjnego.
2. Oznaczanie materiałów, umieszczanie na nich klauzul tajności a także zmiany nadanej klauzuli zgodnie z Rozporządzeniem Prezesa Rady Ministrów z dn. 13 sierpnia 2010 r.(Dz.U. Nr 159 poz. 1069)
3. Propozycję przyznania klauzuli niejawności na wykonywanym dokumencie przedstawia osoba sporządzająca dokument.
4. Klauzulę niejawności na danym dokumencie, przyznaje osoba, która jest upoważniona do podpisania dokumentu.

IX. Zabezpieczenie informacji niejawnych

1. Informacje niejawne stanowiące tajemnicę oznaczone klauzulą „zastrzeżone” przechowuje się w pomieszczeniu pełnomocnika ds. ochrony Informacji Niejawnych, można przechowywać w innych pomieszczeniach na stanowiskach pracy w meblach biurowych zamykanych na klucz.
2. wykonywanie dokumentów zawierających informacje niejawne za pomocą komputera ;

Dostęp do pomieszczenia i systemu teleinformatycznego w nim się znajdującego, posiadającego akredytację bezpieczeństwa teleinformatycznego

Akredytacja bezpieczeństwa teleinformatycznego oznacza, że system jest dopuszczony do przetwarzania informacji niejawnych, a więc zostały spełnione wszystkie wymogi – opracowana stosowna dokumentacja i zatwierdzona przez ABW.

Osobą bezpośrednio odpowiedzialną za pomieszczenie jest Pełnomocnik do spraw OIN, w posiadaniu którego znajdują się klucze do pomieszczenia. Wejście za zgodą Pełnomocnik do spraw OIN mają tylko osoby posiadające indywidualne konta dostępu do systemu teleinformatycznego, przydzielone na pisemny wniosek zainteresowanego, który jest opiniowany przez inspektora bezpieczeństwa i administratora systemu i zatwierdzany przez wójta. Osoby kontrolujące pomieszczenie wraz z systemem muszą posiadać stosowne dokumenty uprawniające do kontroli (poświadczenie – upoważnienie, legitymację, polecenie do przeprowadzenia kontroli).

Osobami odpowiedzialnymi za kontrolę dostępu do systemu są pełnomocnik do spraw OIN, będący jednocześnie Inspektorem bezpieczeństwa teleinformatycznego oraz Administrator systemu, którzy dokonują sprawdzeń działania systemu, czuwają nad jego funkcjonowaniem. Dodatkowo administrator dokonuje odpowiednich ustawień (indywidualne loginy i hasła dostępu)

dla użytkowników, ich blokowania po nieudanych próbach logowania. Odblokowanie konta możliwe jest tylko przez administratora, zaś zapisy te są okresowo kontrolowane przez inspektora bezpieczeństwa.

W razie wystąpienia zagrożenia dla systemu teleinformatycznego spowodowanego zdarzeniem losowym – pożar, zalanie wodą, użytkownik systemu powiadamia Wójta o ile to możliwe o zdarzeniu, wyłącza system TI i zabezpiecza wszystkie materiały niejawne. Wójt podejmuje decyzję o ewentualnej ewakuacji elementów systemu TI, które są deponowane w kartonach i zaplombowane. W całym procesie ewakuacji systemu TI oprócz użytkownika uczestniczą administrator systemu, inspektor bezpieczeństwa TI .

W czasie pracy w systemie teleinformatycznym, w pomieszczeniu może przebywać tylko jeden użytkownik systemu.

Zabrania się wytwarzania dokumentów niejawnych w systemach nie posiadających akredytacji bezpieczeństwa teleinformatycznego.

X. Zasady dostępu do informacji niejawnych stanowiących tajemnicę o klauzuli zastrzeżone

1. Informacje niejawne stanowiące tajemnicę służbową oznaczone klauzulą „zastrzeżone” mogą być udostępniane wyłącznie osobie uprawnionej do dostępu do informacji niejawnych
2. Uzyskanie uprawnień do dostępu do informacji niejawnych może nastąpić:
 - 1) po przeprowadzeniu zwykłego postępowania sprawdzającego i po uzyskaniu przez daną osobę poświadczenia bezpieczeństwa,
 - 2) po przeszkoleniu tej osoby, w zakresie ochrony informacji niejawnych, kończącym się wydaniem określonego przepisami zaświadczenia.
3. Dopuszczenie do pracy lub pełnienia służby na stanowiskach albo zlecenia prac, związanych z dostępem danej osoby do informacji niejawnych o klauzuli „zastrzeżone” może nastąpić po:
 - 1) pisemnym upoważnieniu przez kierownika jednostki organizacyjnej, jeżeli nie posiada ona poświadczenia bezpieczeństwa;
 - 2) odbyciu szkolenia w zakresie ochrony informacji niejawnych.

XI. 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:
 - 1) sprawowanie nadzoru nad realizacją zadań i przestrzeganiem przepisów określonych w Planie Ochrony,
 - 2) sprawowanie kontroli w zakresie ochrony informacji niejawnych oraz przestrzegania związanych z upoważnieniem 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.

XII. Instrukcja postępowania w przypadku otrzymania przesyłki niewiadomego pochodzenia

W przypadku otrzymania jakiegokolwiek 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; 112
- 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 tel. 997;
- Komendę Powiatową Państwowej Straży Pożarnej tel. 998; 112
- Powiatową Stację Sanitarno-Epidemiologiczną. 58 681-07-21
- Pogotowie Ratunkowe tel. 999;

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

XIII. Instrukcja alarmowa w przypadku zgłoszenia o podłożeniu lub znalezieniu ładunku wybuchowego w budynku Urzędu

12.1 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, uzyskać od Policji potwierdzenie przyjętego zawiadomienia.

12.2 Akcja poszukiwawcza ładunku wybuchowego po uzyskaniu informacji o jego podłożeniu

1. Do czasu przybycia Policji akcją kieruje Wójt, a w czasie jego nieobecności Z- ca Wójta 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, świeące elementy elektroniczne itp.).
3. Pomieszczenia ogólnodostępne takie jak: korytarze, klatki schodowe, hale, 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.

12.3 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.

XIV. Ochrona informacji niejawnych w urzędzie w razie wprowadzenia stanu nadzwyczajnego

W rozdziale III w pkt. 2 niniejszego planu opisano stany nadzwyczajne, jakie mogą być wprowadzone na terytorium Polski. Konstytucja RP normuje kwestie kto, kiedy i na jaki okres może wprowadzić stan nadzwyczajny. Określić jego zasięg (całe terytorium Polski lub wyznaczoną jego część).

W każdym stanie nadzwyczajnym istotną sprawą jest szybki i sprawny przepływ informacji. Należy się liczyć ze zwielokrotnieniem podawanych, jak i otrzymanych informacji, których większość, szczególnie w stanie wojennym bądź stanie wyjątkowym będzie informacją niejawną. Ochrona fizyczna informacji będzie odbywać się na tych samych zasadach co w normalnym okresie funkcjonowania urzędu.

Dodatkowo osoby wchodzące w skład pionu ochrony w tym czasie będą zobligowane do większej czujności, zwracania szczególnej uwagi na osoby przejezdne, ich zachowanie. Należy zwracać szczególną uwagę na pozostawione rzeczy osobiste (paczki, teczki, samochody pozostawione przez dłuższy czas bez opieki).

O wszelkich nietypowych zachowaniach, podejrzeniach należy informować pełnomocnika ds. OIN w urzędzie, który w porozumieniu z Wójtem i na jego polecenie będzie podejmować stosowne działania wyjaśniające.

Pełnomocnik w porozumieniu z Wójtem dokonują weryfikacji wykazu osób zatrudnionych lub pełniących służbę w urzędzie albo wykonujących czynności zlecone, które posiadają uprawnienia do dostępu do informacji niejawnych i w razie potrzeby Wójt wydaje stosowne upoważnienia pracownikom nie posiadającym do chwili obecnej wymaganych poświadczeń bądź upoważnień, zaś pełnomocnik szkoli wytypowane osoby z zakresu ochrony informacji niejawnych o klauzuli „zastrzeżone”, zgodnie z art. 19 ust. 1 ustawy o ochronie informacji niejawnych, w celu ich dopuszczenia do pracy, w związku z przydzieleniem nowych zadań.

Zgodnie z art. 19 ust. 2 pkt 5a ustawy o zarządzaniu kryzysowym (Dz. U. z 2007r. Nr 131, poz. 1076 z późn. zm.), Wójt Gminy współdziała z Szefem Agencji Bezpieczeństwa Wewnętrznego w zakresie przeciwdziałania, zapobiegania i usuwania skutków zdarzeń o charakterze terrorystycznym.