

Zarządzenie Nr 59 /2018
Wójta Gminy Jedwabno
z dnia 22 czerwca 2018 roku

w sprawie zatwierdzenia „Planu Ochrony Informacji Niejawnych w Urzędzie Gminy
w Jedwabnie”

Na podstawie art.15 ust.1 pkt.5 ustawy z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych (Dz.U. z 2018r,poz. 412) oraz art.33 ust.3 ustawy z dnia 8 marca 1990 roku o samorządzie gminnym (Dz.U. z 2018 r, poz. 449 ze zm.) **z a r z ą d z a m**, co następuje :

§ 1.

Zatwierdzam plan ochrony informacji niejawnych w Urzędzie Gminy w Jedwabnie, 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.

Traci moc plan ochrony informacji niejawnych w Urzędzie Gminy w Jedwabnie zatwierdzony zarządzeniem Nr 47/2011 Wójta Gminy Jedwabno z dnia 14 czerwca 2011 roku.

§ 5.

Zarządzenie wchodzi w życie z dniem podpisania.


Wójt

(Sławomir Ambroziak)

Wójt
Sławomir Ambroziak

Zatwierdzam:

Załącznik
do Zarządzenia Nr 59/2018
Wójta Gminy Jedwabno
z dnia 22 czerwca 2018 r.

**PLAN OCHRONY
INFORMACJI NIEJAWNYCH
W URZĘDZIE GMINY W JEDWABNIE**

Jedwabno, dnia 22 czerwca 2018 r.

SPIS TREŚCI

1. Podstawy prawne ochrony informacji niejawnych.....	3
2. Definicje używane w Planie ochrony informacji niejawnych.....	3
3. Przedmiot ochrony.....	4
4. Klasyfikacja informacji niejawnych.....	4
5. Dostęp do informacji niejawnych.....	5
5.1 Uprawnienia do dostępu do informacji niejawnych.....	5
5.2 Udostępnianie informacji niejawnych.....	5
6. Zasady wykonywania i przetwarzania dokumentów niejawnych.....	5
7. Wykonywanie dokumentów zawierających informacje niejawne za pomocą komputera.....	5
8. Ochrona fizyczna.....	6
9. Ocena zagrożeń zewnętrznych i wewnętrznych.....	7
9.1 Zagrożenia zewnętrzne.....	7
9.1.1 Rodzaje zagrożeń.....	7
9.1.2 Symptomy mogące świadczyć o przygotowaniu napadu lub włamania do budynku Urzędu.....	7
9.1.3 Wnioski.....	8
9.2 Zagrożenia wewnętrzne.....	8
9.2.1 Rodzaje zagrożeń.....	8
9.2.2 Wnioski.....	8
10. Postępowanie w przypadku naruszenia ustawy o ochronie informacji niejawnych i przepisów wykonawczych do ustawy.....	9
11. Instrukcja postępowania w przypadku otrzymania przesyłki niewiadomego pochodzenia.....	9
12. Instrukcja alarmowa w przypadku zgłoszenia o podłożeniu lub znalezieniu ładunku wybuchowego w budynku Urzędu.....	10
12.1 Alarmowanie.....	10
12.2 Akcja poszukiwawcza ładunku wybuchowego po uzyskaniu informacji o jego podłożeniu.....	10
12.3 Postanowienia końcowe dotyczące działań w przypadku zgłoszenia o podłożeniu ładunku wybuchowego.....	11

1. Podstawy prawne ochrony informacji niejawnych

Plan Ochrony Informacji niejawnych w Urzędzie Gminy w Jedwabnie określa zasady i tryb postępowania z informacjami niejawnymi oraz zapewnia jednolity sposób postępowania z tymi informacjami w Urzędzie Gminy w Jedwabnie.

USTAWA z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2018r, poz. 412)

ROZPORZĄDZENIE Prezesa Rady Ministrów z dnia 28 grudnia 2010 roku w sprawie wzoru decyzji o cofnięciu poświadczenia bezpieczeństwa (Dz.U.2010.258.1754)

ROZPORZĄDZENIE Prezesa Rady Ministrów z dnia 28 grudnia 2010 roku w sprawie wzoru decyzji o odmowie wydania poświadczenia bezpieczeństwa (Dz.U.2010.258.1753)

ROZPORZĄDZENIE Prezesa Rady Ministrów z dnia 28 grudnia 2010 roku w sprawie wzorów poświadczeń bezpieczeństwa (Dz.U.z 2015,poz. 220)

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.z 2015 r, poz.205)

ROZPORZĄDZENIE Prezesa Rady Ministrów z dnia 22 grudnia 2011 roku w sprawie sposobu oznaczania materiałów, umieszczania na nich klauzul tajności.(Dz.U.2011r, 1692)

USTAWA z dnia 14 lipca 1983r o narodowym zasobie archiwalnym i archiwach (Dz.U.z 2011r, Nr 123, poz. 698 z późn.zm.)

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. z 2018r, poz. 412)
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. z 2017r, poz. 1219);

8. **Urzędem** - jest Urząd Gminy w Jedwabnie,
9. **Wójtem** - jest Wójt Gminy Jedwabno
10. **Pełnomocnikiem ochrony** - jest Pełnomocnik ds. Ochrony Informacji Niejawnych w Urzędzie Gminy w Jedwabnie,

3. Przedmiot ochrony

Przedmiotem ochrony w Urzędzie są

1. Informacje niejawne oznaczone:
 - klauzulą „zastrzeżone”,
2. Pomieszczenia, w których są przechowywane i opracowane materiały niejawne.

4. Klasyfikacja informacji niejawnych

Informacjom niejawnym nadaje się następujące klauzule:

1. "zastrzeżone", jeżeli nie nadano informacjom wyższej klauzuli tajności, a ich nieuprawnione ujawnienie może mieć szkodliwy wpływ na wykonywanie przez organy władzy publicznej lub inne jednostki organizacyjne zadań w zakresie obrony narodowej, polityki zagranicznej, bezpieczeństwa publicznego, przestrzegania praw i wolności obywateli, wymiaru sprawiedliwości albo interesów ekonomicznych Rzeczypospolitej Polskiej.

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 „ściśle tajne”, „tajne” oraz „poufne” lub otrzymały pisemne upoważnienie kierownika jednostki – jeżeli nie posiadają poświadczenia bezpieczeństwa.
- 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. Zasady wykonywania i przetwarzania dokumentów niejawnych

1. Klauzulę tajności nadaje osoba, która jest uprawniona do podpisania dokumentu lub oznaczenia innego niż dokument materiału.
2. Uprawnienie do przyznania, obniżenia i znoszenia klauzuli tajności przysługuje wyłącznie w zakresie posiadanego prawa dostępu do informacji niejawnych.
3. Zawyżanie lub zaniżanie klauzuli tajności jest niedopuszczalne.
4. Dokumenty niejawne wpływające do Urzędu podlegają ewidencjonowaniu w dzienniku ewidencji.
5. Dokumenty niejawne wytworzone w Urzędzie rejestruje się w dzienniku ewidencji.
6. Każdy dokument niejawny przychodzący lub wychodzący z Urzędu ewidencjonuje się w odrębnej pozycji właściwego dziennika ewidencyjnego.
7. Numer ewidencyjny każdego dokumentu niejawnego stanowiącego tajemnicę o klauzuli „zastrzeżone” poprzedzony jest skrótem literowym, odpowiednio „Z”.
8. Dokumenty niejawne wytworzone w Urzędzie powinny być oznaczone w sposób określony w rozporządzeniu Prezesa Rady Ministrów z dnia 20 grudnia 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności (Dz. U. z 2011r, 288, poz. 1692)

7. Wykonywanie dokumentów zawierających informacje niejawne za pomocą komputera

Pracownicy, którzy do opracowywania i wykonywania dokumentów zawierających informacje oznaczone klauzulą „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 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 teleinformatycznym.
3. Za właściwą organizację bezpieczeństwa teleinformatycznego odpowiada Wójt, który w szczególności:
 - 1) zapewnia opracowanie dokumentacji bezpieczeństwa teleinformatycznego,
 - 2) realizuje ochronę fizyczną systemu teleinformatycznego,
 - 3) zapewnia niezawodność transmisji oraz kontrolę dostępu do urządzeń systemu teleinformatycznego,
 - 4) dokonuje analizy stanu bezpieczeństwa teleinformatycznego oraz zapewnia usunięcie stwierdzonych nieprawidłowości,
 - 5) zapewnia przeszkolenie z zakresu bezpieczeństwa teleinformatycznego dla osób uprawnionych do pracy w systemie teleinformatycznym,
4. Pełnomocnik zawiadamia kierownika jednostki-Wójta o zaistniałym incydencie bezpieczeństwa teleinformatycznego dotyczącym informacji niejawnych oznaczonych klauzulą „zastrzeżone”.
5. Ochrona fizyczna systemu teleinformatycznego polega na:

- 1) umieszczeniu urządzeń systemu teleinformatycznego w strefie kontrolowanego dostępu
- 2) zastosowaniu środków zapewniających ochronę fizyczną, w szczególności przed:
 - a) nieuprawnionym dostępem,
 - b) podglądem,
 - c) podsłuchem.
6. System teleinformatyczny wyposaża się w mechanizmy kontroli dostępu odpowiednie do klauzuli tajności informacji niejawnych w nich przetwarzanych.

8. 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 alarmowania zgodnie z umową o usługę ochrony w formie monitorowania i ochrony obiektu w systemie dyskretnego ostrzegania zawartą ze specjalistyczną firmą monitorującą. W/w firma zapewnia monitorowanie sygnałów lokalnego systemu alarmowego przez stałe prowadzenie obserwacji sygnałów i przekazywanie ich grupie interwencyjnej. Monitorowanie sygnałów lokalnego systemu alarmowego odbywa się całodobowo.

Interwencja jest podejmowana w godzinach : 19,00-7,00, w czasie do 15 minut, w godzinach 7,00-19,00 w czasie do 20 minut. W przypadku stwierdzenia zagrożenia, usiłowania lub dokonania przestępstwa przeciwko życiu, zdrowiu lub mieniu w ochranianym obiekcie, firma monitorująca obiekt podejmuje czynności ochronne poprzez ujęcie sprawcy i oddanie go w ręce organów ścigania, a także zabezpieczy obiekt Urzędu Gminy w Jedwabnie ul. Warmińska 2, do czasu przybycia przedstawiciela tej instytucji, nie dłużej niż 2 godziny. Jeśli w czasie 2 godzin nie uda się powiadomić przedstawiciela Urzędu Gminy w Jedwabnie o zaistniałym zdarzeniu, firma monitorująca zabezpieczy obiekt dozorem fizycznym. Zdarzenia na obiekcie Urzędu Gminy w Jedwabnie są rejestrowane przez system komputerowy za dany miesiąc w Centrum Operacyjnym specjalistycznej firmy monitorującej. Załączanie i wyłączenie systemu alarmowego dokonywane jest przez upoważnionego przez Wójta Gminy Jedwabno użytkownika obiektu- Urzędu Gminy w Jedwabnie.

2. Kody do instalacji alarmowej do budynku Urzędu mogą posiadać: Wójt, Sekretarz, Zastępca Kierownika USC oraz upoważnieni pracownicy odpowiedzialni za otwarcie i zamknięcie budynku Urzędu.
3. Pomieszczenia, w których znajdują się informacje niejawne z klauzulą „zastrzeżone” po godzinach pracy powinny być zamykane, a klucze zabierane.
4. Sprzątanie pomieszczenia, w którym są przechowywane informacje niejawne powinno odbywać się w obecności upoważnionego pracownika przed zakończeniem pracy
5. Informacje niejawne oznaczone klauzulą „zastrzeżone” można przechowywać na stanowiskach pracy, w meblach biurowych zamykanych na klucz.
6. W uzasadnionych przypadkach podyktowanych względami dłuższego okresu czasu, niezbędnego do wykonania zadań związanych z dostępem do informacji niejawnych, dokumenty o klauzuli „zastrzeżone” mogą być wydawane poza pomieszczenie służące do przechowywania, lecz pod warunkiem, że odbiorca dokumentu zapewni warunki ochrony tych dokumentów.

9. Ocena zagrożeń zewnętrznych i wewnętrznych

9.1 Zagrożenia zewnętrzne

9.1.1 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, możliwość napadu przez przypadkowe osoby wykorzystujące nadarzającą się okazję z powodu nieprawidłowości w ochronie mienia Urzędu.

9.1.2 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 czy 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, sprzątaczkę itp.,
- rozpoznawanie systemu technicznych zabezpieczeń, w tym stosowanych urządzeń alarmowych,
- celowe uszkodzanie urządzeń alarmowych, linii telefonicznych, oświetlenia itp.,
- próby pozyskania do grup przestępczych pracowników Urzędu (dotyczy głównie osób mających problemy finansowe, towarzyskie, a także służbowe)

9.1.3 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 powinni 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.

9.2 Zagrożenia wewnętrzne

9.2.1 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 niejawnne przez osoby nieuprawnione,
- spożywanie alkoholu – przesłanka do wykroczeń dyscyplinarnych i przestępstw.

9.2.2 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 niejawnnych 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.

10. Postępowanie w przypadku naruszenia ustawy o ochronie informacji niejawnnych i przepisów wykonawczych do ustawy.

1. Za ochronę informacji niejawnnych w Urzędzie odpowiada Wójt. Zadania określone ustawą o ochronie informacji niejawnnych 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 niejawnnych oraz przestrzegania związanych z upoważnianiem do dostępu do tych informacji, w odniesieniu do wszystkich komórek organizacyjnych Urzędu.
2. W przypadku ujawnienia informacji niejawnnych przez podległych pracowników Wójta lub upoważniony przez niego pracownik zawiadamia na piśmie pełnomocnika ochrony podając jaka informacja niejawnna została ujawniona lub jakie naruszenie przepisów zostało stwierdzone.
3. Pełnomocnik ochrony przeprowadza okresowe kontrole przestrzegania ustawy o ochronie informacji niejawnnych w Urzędzie. W przypadku stwierdzenia naruszenia przepisów o ochronie informacji niejawnnych pełnomocnik ochrony przekłada Wójtowi pisemną informację o naruszeniu przepisów i wnioski do podjęcia decyzji.
4. W przypadku naruszenia przepisów o ochronie informacji niejawnnych oznaczonych klauzulą „zastrzeżone” pełnomocnik ochrony powiadamia Wójta.

11. 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;

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 (galarete, 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;
- Powiatową Stację Sanitarno-Epidemiologiczną 896248731
- Pogotowie Ratunkowe tel. 999;

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

12. 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,
 - 3) 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 Zastępca 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, świecące elementy elektroniczne itp.).
3. Pomieszczenia ogólnodostępne takie jak: korytarze, klatki schodowe, toalety, piwnica, 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