Zarządzenie Nr 72/2011

Wójta Gminy w Kijach

z dnia 15 listopada 2011 roku

w sprawie zatwierdzenia „Planu Ochrony Informacji Niejawnych w Urzędzie Gminy w Kijach".

Na podstawie art.15 ust. 1 pkt 5 oraz art. 43 ust.5 ustawy z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych(Dz.U. Nr 182 poz. 1228) oraz art. 33 ust.3 ustawy z dnia 8 marca 1990 roku o samorządzie gminnym(Dz. U. z 2001r. Nr 142, poz. 1591 ze zm.)zarządzam, co następuje:

§1

Zatwierdzam Plan Ochrony Informacji Niejawnych w Urzędzie Gminy w Kijach 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 podjęcia.

W Ó J T

mgr Krzysztof Słonina

Załącznik
do Zarządzenia Nr 72/2011
Wójta Gminy
Kije z dnia 15.11.2011r.

ZATWIERDZAM:

WÓJT
mgr Krzysztof Słonina

PLAN OCHRONY INFORMACJI NIEJAWNYCH W GMINIE KIJE

OPRACOWAŁA:
Anna Janas
Pełnomocnik ds. Ochrony Informacji Niejawnych

Spis treści

PLAN OCHRONY INFORMACJI NIEJAWNYCH W URZĘDZIE GMINY KIJE

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

1. Podstawy prawne ochrony informacji niejawnych

USTAWA z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych Dz.U. Nr 182, poz. 1228

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.2010.258.1752

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

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

ROZPORZĄDZENIE Prezesa Rady Ministrów z dnia 13 sierpnia 2010 roku w sprawie sposobu oznaczania materiałów, umieszczania na nich klauzul tajności, a także zmiany nadanej klauzuli tajności Dz.U.2010.159.1069

ROZPORZĄDZENIE Rady Ministrów z dnia 01 czerwca 2010 roku w sprawie organizacji i funkcjonowania kancelarii tajnych Dz.U.2010.114.765

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

2. Definicje używane w Planie ochrony informacji niejawnych

W rozumieniu planu ochrony informacji niejawnych:

* **ustawą** -jest ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228),

* **służbą ochrony państwa** -jest Agencja Bezpieczeństwa Wewnętrznego

* **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;

* **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;

* **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 póź. zm.);

* **Urzędem** -jest Urząd Gminy w Kijach,

* **Wójtem** -jest Wójt Gminy Kije

* **pełnomocnikiem ochrony** -jest Pełnomocnik ds. Ochrony Informacji Niejawnych w Urzędzie Gminy w Kijach,

3. Przedmiot ochrony

Przedmiotem ochrony w Urzędzie są :

a) informacje niejawne oznaczone:
- klauzulą „poufne",
- klauzulą „zastrzeżone",

b) pomieszczenia, w których są przechowywane i opracowane materiały niejawne.

4. Klasyfikacja informacji niejawnych

Informacjom niejawnym nadaje się następujące klauzule:

- **"poufne",** jeżeli nieuprawnione ujawnienie informacji spowoduje szkodę Rzeczypospolitej Polskiej w obszarze polityki międzynarodowej, obronności, porządku publicznego lub bezpieczeństwa obywateli, utrudniłoby wykonywanie ustawowych zadań przez organy, służby lub instytucje odpowiedzialne za ochronę bezpieczeństwa, osłabiłoby system finansowy Polski lub naraziłoby na szkodę interesy ekonomiczne lub funkcjonowanie gospodarki narodowej.

Ujawnienie takie:

a) utrudni prowadzenie bieżącej polityki zagranicznej Rzeczypospolitej Polskiej;

b) utrudni realizację przedsięwzięć obronnych lub negatywnie wpłynie na zdolność bojową Sił Zbrojnych Rzeczypospolitej Polskiej;

c) zakłóci porządek publiczny lub zagrozi bezpieczeństwu obywateli;

d) utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę bezpieczeństwa lub podstawowych interesów Rzeczypospolitej Polskiej;

e) utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę porządku publicznego, bezpieczeństwa obywateli lub ściganie sprawców przestępstw i przestępstw skarbowych oraz organom wymiaru sprawiedliwości;

f) zagrozi stabilności systemu finansowego Rzeczypospolitej Polskiej;

g) wpłynie niekorzystnie na funkcjonowanie gospodarki narodowej.

- **"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

1) 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

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 „poufne" lub „zastrzeżone" poprzedzony jest skrótem literowym, odpowiednio, „Pf" lub „Z".

8) Dokumenty niejawne wytworzone w Urzędzie powinny być oznaczone w sposób określony w rozporządzeniu Prezesa Rady Ministrów z dnia 13 sierpnia 2010 r. w sprawie sposobu oznaczania materiałów, umieszczania na nich klauzul tajności, a także zmiany nadanej klauzuli tajności (Dz. U. Nr 159, poz. 1069).

7. 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".

8.Ochrona fizyczna systemu lub sieci teleinformatycznej.

Ochrona fizyczna systemu lub sieci teleinformatycznej polega na :

1) umieszczeniu urządzeń systemu lub sieci teleinformatycznej w strefie kontrolowanego dostępu
2) zastosowaniu środków zapewniających ochronę fizyczną, w szczególności przed:
   a) nieuprawnionym dostępem,
   b) podglądem,
   c) podsłuchem.

9. Ochrona elektromagnetyczna systemu lub sieci teleinformatycznej.

Ochrona elektromagnetyczna systemu lub sieci teleinformatycznej polega na :

1) 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.

2) system lub sieć teleinformatyczną wyposaża się w mechanizmy kontroli dostępu odpowiednie do klauzuli tajności informacji niejawnych w nich przetwarzanych.

10.Ochrona fizyczna budynku i pomieszczeń.

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 (w najbliższym czasie będzie założony).
2) Kody do instalacji alarmowej do budynku Urzędu mogą posiadać: Wójt, Sekretarz Gminy, Kierownik USC 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 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 „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.

11.Ocena zagrożeń zewnętrznych i wewnętrznych

Zagrożenia zewnętrzne

1) Zagrożeniami zewnętrznymi dla Urzędu są:
   a) możliwość napadu przez zorganizowane grupy przestępcze i terrorystyczne, działające w sposób profesjonalny, przemyślany i zorganizowany,
   b) możliwość napadu przez pojedynczych przestępców, możliwość napadu przez przypadkowe osoby wykorzystujące nadarzającą się okazję z powodu nieprawidłowości w ochronie mienia Urzędu.

2) Symptomy mogące świadczyć o przygotowaniu napadu lub włamania do budynku Urzędu :
   a) 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,

b) nawiązanie rozmów przez osoby postronne z pracownikami,
c) podszywanie się pod byłych pracowników Urzędu i przejawianie zainteresowaniem tym, co się po latach zmieniło,
d) interesowanie się osobami funkcyjnymi, w tym także ich przywarami oraz sposobem wykonywania obowiązków służbowych,
e) obserwacja sposobu działania systemu ochronnego, sekretariatu, sprzątaczki itp.,
f) rozpoznawanie systemu technicznych zabezpieczeń, w tym stosowanych urządzeń alarmowych,
g) celowe uszkadzanie urządzeń alarmowych, linii telefonicznych, oświetlenia itp.,
h) próby pozyskania do grup przestępczych pracowników Urzędu (dotyczy głównie osób mających problemy finansowe, towarzyskie, a także służbowe)

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

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

Zagrożenia wewnętrzne

1) Rodzaje zagrożeń:
a) próby zaboru dokumentów lub mienia przez pracowników Urzędu,
b) próby powielania, kserowania dokumentów służbowych dla celów prywatnych,
c) byli pracownicy urzędu zwolnieni dyscyplinarnie,
d) rozpoznanie organizacji pracy Urzędu celem łatwiejszej pracy grup przestępczych na terenie urzędu,
e) próby wglądu w dokumenty niejawne przez osoby nieuprawnione,
f) spożywanie alkoholu – przesłanka do wykroczeń dyscyplinarnych i przestępstw.

2) W związku z przedstawionymi kierunkami zagrożeń należy wykonywać następujący czynności uprzedzające ewentualne możliwości zaistnienia zagrożeń:

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

12. 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:
a) sprawowanie nadzoru nad realizacją zadań i przestrzeganiem przepisów określonych w Planie ochrony,
b) 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 właściwe Służby Ochrony Państwa.

13. Instrukcja postępowania w przypadku otrzymania przesyłki niewiadomego pochodzenia

1) 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:

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

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

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

Należy:

a) Nie naruszyć zawartości -nie rozsypywać, nie przenosić, nie dotykać, nie wąchać, nie powodować ruchu powietrza w pomieszczeniu (wyłączyć systemy wentylacyjne, zamknąć okna).
b) Całą zawartość umieścić w worku plastikowym, zamknąć go i zakleić taśmą lub plastrem.
c) Dokładnie umyć ręce
d) Zaklejony worek umieścić w drugim worku, zamknąć go i zakleić.
e) Ponownie umyć ręce.
f) Powiadomić:
   -Komendę Powiatową Policji tel. 997;
   -Komendę Powiatową Państwowej Straży Pożarnej tel. 998;
   -Powiatową Stację Sanitarno-Epidemiologiczną.
   -Pogotowie Ratunkowe tel. 999;

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

14. Instrukcja alarmowa 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:
   - Wójta,
   - Komendanta Powiatowego Policji

2) Zawiadamiając Policję należy podać treść rozmowy ze zgłaszającym o podłożeniu ładunku wybuchowego, którą należy prowadzić wg poniższych wskazówek:

   a) miejsce i opis zlokalizowanego przedmiotu, który może być ładunkiem wybuchowym,
   b) numer telefonu, z którego prowadzona jest rozmowa i swoje stanowisko,
   c) 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-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, piwnice, 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 .

15. Odpowiedzialność karna, dyscyplinarna i służbowa za naruszenie przepisów o ochronie informacji niejawnych.

Zakres odpowiedzialności karnej osób, które dopuściły się przestępstwa lub czynu zabronionego przeciwko ochronie informacji niejawnych został określony przepisami Kodeksu Karnego w art. 266 (ustawa z dnia 06 czerwca 1997 r. Kodeks Karny, Dz.U.Nr 88, poz. 553 ze zmianami.) i brzmi :"*funkcjonariusz publiczny, który ujawnia osobie nieuprawnionej informację niejawną o klauzuli „zastrzeżone" lub „poufne" lub informację, którą uzyskał w związku z wykonywaniem czynności służbowych, a której ujawnienie może narazić na szkodę prawnie chroniony interes, podlega karze pozbawienia wolności do lat 3".*

16. Okresy ochronne dla dokumentów niejawnych

1) Informacje niejawne podlegają ochronie do czasu zniesienia lub zmiany klauzuli tajności.
2) Zniesienie lub zmiana klauzuli tajności są możliwe wyłącznie po wyrażeniu pisemnej zgody przez osobę która nadała klauzulę tajności i jest uprawniona do podpisania dokumentu lub oznaczenia innego niż dokument materiału, albo jej przełożonego w przypadku ustania lub zmiany ustawowych przesłanek ochrony.

17. Ustalenia końcowe.

1. Wójt, Zastępca Wójta, Sekretarz - Pełnomocnik Ochrony, Skarbnik :
   1) zapoznają podległych pracowników z ustaleniami Planu Ochrony Informacji Niejawnych ,
   2) zapewnią bieżące przestrzeganie postanowień Planu Ochrony w zakresie ochrony informacji niejawnych, mogących występować na poszczególnych stanowiskach pracy.
2. Osoby wymienione w pkt 1, wprowadzą jako obowiązującą zasadę, zapoznawania z Planem Ochrony wszystkie osoby, które podejmują pracę w komórkach organizacyjnych.
3. W przypadku wystąpienia wątpliwości, a także potrzeby przybliżenia zasad dotyczących realizacji zadań związanych z ochroną informacji niejawnych, sporządzania i wykonania dokumentów zawierających informacje niejawne, pracownicy Urzędu mogą w każdym czasie zwracać się o wyjaśnienia czy też instruktaż do:
   1) Wójta Gminy
   2) Sekretarz Urzędu Gminy- Pełnomocnika Ochrony,
4. Integralną część Planu ochrony stanowią załączniki w ilości 9, wy specyfikowane w dołączonym do Planu ochrony Zestawieniu załączników.

ZESTAWIENIE ZAŁĄCZNIKÓW DO PLANU OCHRONY INFORMACJI NIEJAWNYCH W URZĘDZIE GMINY W KIJACH

STR.

Załącznik nr 1 do Planu ochrony

WYKAZ STANOWISK I FUNKCJI ORAZ RODZAJÓW PRAC ZLECONYCH, Z KTÓRYMI MOŻE ŁĄCZYĆ SIĘ DOSTĘP DO INFORMACJI NIEJAWNYCH STANOWIĄCYCH TAJEMNICĘ SŁUŻBOWĄ

OZNACZONYCH KLAUZULĄ „POUFNE"

LP	STANOWISKO - FUNKCJA	UWAGI
1	**Wójt Gminy**	
2	**Sekretarz Gminy - Pełnomocnik do spraw Ochrony Informacji Niejawnych**	
3	**Inspektor ds. bezpieczeństwa teleinformatycznego**	
4	**Administrator Bezpieczeństwa**	
5	**Pracownik d/s Wojskowych i Obrony Cywilnej**	

OZNACZONYCH KLAUZULĄ „ZASTRZEŻONE"

LP	STANOWISKO - FUNKCJA	UWAGI
1.	**Wójt Gminy**	
2.	**Sekretarz Gminy -** **Pełnomocnik do spraw Ochrony Informacji Niejawnych**	
3.	**Administrator Bezpieczeństwa**	
4.	**Inspektor do spraw bezpieczeństwa teleinformatycznego**	
5.	**Pracownik d/s Wojskowych i Obrony Cywilnej**	
6.	**Kierownik USC**	

RODZAJE PRAC ZLECONYCH, Z KTÓRYCH WYKONYWANIEM MOŻE ŁĄCZYĆ SIĘ DOSTĘP DO INFORMACJI NIEJAWNYCH STANOWIĄCYCH TAJEMNICĘ SŁUŻBOWĄ

RODZAJE PRAC ZLECONYCH	UWAGI
Prace polegające na wykonywaniu ekspertyz, analiz, opinii, tłumaczeń, archiwizacji, szkoleń oraz udzielaniu konsultacji, jeżeli do ich wykonania potrzebny jest dostęp do informacji niejawnych stanowiących tajemnicę służbową oznaczonych klauzulą „poufne", „zastrzeżone" lub w wyniku których powstałyby takie informacje.	

WYKAZ
INFORMACJI NIEJAWNYCH MOGĄCYCH WYSTĘPOWAĆ W ZAKRESIE DZIAŁANIA URZĘDU GMINY W KIJACH

OZNACZONYCH KLAUZULĄ „POUFNE"

LP	RODZAJ INFORMACJI	UWAGI

OZNACZONYCH KLAUZULĄ „ZASTRZEŻONE"

LP	RODZAJ INFORMACJI	UWAGI
1	**Plan Akcji Kurierskiej dla Gminy Kije**	
2	**Sprawozdania roczne z akcji kurierskiej**	
3	**Dokumentacja dotycząca stałego dyżuru**	
4	**Wnioski o nadanie medali "za długoletnie pożycie małżeńskie"**	
5	**Plan Ochrony Zabytków**	
6	**Ankieta bezpieczeństwa osobowego**	
7	**Wnioski do ABW w sprawie postępowań sprawdzających**	
8	**Korespondencja z ABW w sprawie postępowań sprawdzających**	
9	**Plany Ochrony Obiektów Urzędu Gminy Kije**	
10	**Plan Operacyjny Funkcjonowania Gminy Kije w warunkach zewnętrznego zagrożenia bezpieczeństwa państwowego w czasie wojny**	

Załącznik Nr 3 do Planu ochrony

SPOSÓB OZNACZANIA DOKUMENTÓW NIEJAWNYCH ORAZ UMIESZCZANIA KLAUZUL NA TYCH DOKUMENTACH

STRONA PIERWSZA DOKUMENTU

.....
Miejscowość, data sporządzenia dokumentu

KLAUZULA TAJNOŚCI
Egz. Nr .....

.....
Nazwa jednostki organizacyjnej

- sygnatura literowo-cyfrowa
- numer z dziennika korespondencji
  łamany przez rok lub dwie ostatnie cyfry roku

ADRESAT

/treść dokumentu/

KLAUZULA TAJNOŚCI
Nr strony / ilość stron dokumentu

STRONA DRUGA I KOLEJNE STRONY DOKUMENTU

KLAUZULA TAJNOŚCI
Egz. Nr .....

- sygnatura literowo-cyfrowa
- numer z dziennika korespondencji
  łamany przez rok lub dwie ostatnie cyfry roku

/ciąg dalszy treści dokumentu/

KLAUZULA TAJNOŚCI
Nr strony / ilość stron całego dokumentu

STRONA OSTATNIA DOKUMENTU

KLAUZULA TAJNOŚCI
Egz. Nr .....

- sygnatura literowo- cyfrowa
- numer z dziennika ewidencji
  łamany przez rok lub dwie ostatnie cyfry roku

/ciąg dalszy treści dokumentu/

Pod treścią - informacja o załącznikach jeśli występują

- Liczba załączników
- Klauzule tajności załączników wraz z nr ewidencyjnym z DEWD
- Liczba stron lub kart każdego załącznika
- W przypadku gdy adresatowi wysyła się inna liczbę załączników niż pozostawia w aktach, dodatkowo napis „tylko adresat"
- W przypadku gdy załączniki należy zwrócić napis „do zwrotu"

.....
stanowisko oraz imię i nazwisko
osoby podpisującej dokument

- **Liczba wykonanych egzemplarzy**
- **Adresaci poszczególnych egzemplarzy**
- **Nazwisko osoby, która sporządziła dokument**
- **Nazwisko osoby, która wykonała dokument**

KLAUZULA TAJNOŚCI
Nr strony / ilość stron dokumentu

Załącznik Nr 4 do Planu Ochrony

WZÓR

POŚWIADCZENIE BEZPIECZEŃSTWA NR .....

Na podstawie art. 28 pkt. 1 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U.Nr 182, poz. 1228) po przeprowadzeniu na wniosek /polecenie *

_____

(nazwa wnioskodawcy albo stanowisko osoby, która poleciła przeprowadzenie postępowania*)

przez _____

(nazwa i adres siedziby organu, który przeprowadził postępowanie)

zwykłego/poszerzonego * postępowania sprawdzającego, stwierdza się , że Pan /Pani

_____

(imię i nazwisko, data urodzenia)

daje rękojmię zachowania tajemnicy

w zakresie dostępu do informacji niejawnych oznaczonych klauzulą

_____ - na okres do : _____

(nazwa klauzuli tajności) (termin ważności)

_____ - na okres do :* _____

(nazwa klauzuli tajności) (termin ważności)

_____ - na okres do :* _____

(nazwa klauzuli tajności) (termin ważności)

_____ _____

(miejscowość i data) mp. (podpis i imienna pieczątka osoby upoważnionej)

* niepotrzebne skreślić

Z A Ś W I A D C Z E N I E NR .....

stwierdzając odbycie szkolenia
w zakresie ochrony informacji niejawnych

Stwierdza się, że Pani (Pan):

- imię i nazwisko _____
- nr PESEL _____

odbyła (odbył) szkolenie w zakresie ochrony informacji niejawnych na podstawie przepisów ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. Nr 182, poz. 1228), zorganizowane przez Pełnomocnika do spraw ochrony informacji niejawnych w Urzędzie Gminy w Kijach

.....
(miejscowość i data)

.....
(podpis i imienna pieczątka pełnomocnika lub jego zastępcy)

Załącznik Nr 6 do Planu Ochrony

Upoważnienie do dostępu do informacji niejawnych o klauzuli „zastrzeżone"

Pan/Pani

.....

Nr pisma .....

.....
(miejscowość , data)

Zgodnie z art. 21 ust. 4 ustawy z dnia 5 sierpnia 2010r. (Dz.U. Nr 182, poz. 1228), o ochronie informacji niejawnych,

u p o w a ż n i a m

Pana/Panią ..... do dostępu do informacji niejawnych oznaczonych klauzulą „ zastrzeżone" zatrudnionego / zatrudnioną w Urzędzie Gminy w Kijach na stanowisku .....

.....
(podpis kierownika jednostki)

Upoważnienie ważne jest na czas zatrudnienia w Urzędzie Gminy w Kijach lub do odwołania,
Dostęp do informacji niejawnych o klauzuli „zastrzeżone" może nastąpić po odbyciu szkolenia w zakresie przepisów ustawy o ochronie informacji niejawnych.

Załącznik nr 7 do Planu ochrony

PROTOKÓŁ OTWARCIA SEJFU (SZAFY METALOWEJ)*

W dniu ..... r.

Komisja w składzie:

1. .....
2. .....
3. .....

(nazwisko i imię, stanowisko służbowe)

dokonała otwarcia sejfu/szafy metalowej* znajdującej się w pomieszczeniu nr .....
której użytkownikiem jest .....

(nazwisko i imię, stanowisko służbowe)

Z sejfu/szafy metalowej* zostały zabrane niżej wymienione dokumenty (materiały, przedmioty):

1. .....
2. .....
3. .....

którymi obecnie dysponuje Pan/Pani .....

(nazwisko i mię, stanowisko służbowe)

Sejf/szafę metalową* zamknięto i zaplombowano (referentką do plasteliny nr .....) w obecności członków Komisji.

Podpisy członków Komisji:

1. .....
2. .....
3. .....

Upoważnienie wydane osobie, wobec której wszczęto postępowanie sprawdzające w związku z dostępem do informacji niejawnych oznaczonych klauzulą „poufne"

.....
miejscowość ,data

Pan/Pani
.....

Znak pisma : .....

Zgodnie z art. 34 ust. 9 ustawy z dnia 5 sierpnia 2010 roku (Dz.U.Nr 182,poz. 1228) o ochronie informacji niejawnych , do czasu zakończenia postępowania sprawdzającego wyrażam zgodę na udostępnienie Panu/Pani .....informacji niejawnych oznaczonych klauzulą „poufne" .

.....
podpis kierownika jednostki

Załącznik Nr 9 do Planu Ochrony

INSTRUKCJA

DOTYCZĄCA SPOSOBU I TRYBU PRZETWARZANIA INFORMACJI NIEJAWNYCH O KLAUZULI **„ZASTRZEŻONE"**

W URZĘDZIE GMINY W KIJACH

ORAZ ZAKRES I WARUNKI STOSOWANIA ŚRODKÓW BEZPIECZEŃSTWA FIZYCZNEGO W CELU ICH OCHRONY.

§ 1

Informacjom niejawnym nadaje się klauzulę „zastrzeżone", jeżeli nie nadano im 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.

§ 2.

1. Dostęp do pracy na stanowiskach związanych z dostępem danej osoby do informacji niejawnych o klauzuli „zastrzeżone" mają osoby posiadające aktualne poświadczenie bezpieczeństwa bądź pisemne upoważnienie wydane przez Wójta Gminy w Kijach oraz przeszkolenie z zakresu ochrony informacji niejawnych.
2. Ewidencję poświadczeń bezpieczeństwa oraz upoważnień, o których mowa w ust.1, prowadzi Pełnomocnik ds. Ochrony Informacji Niejawnych.
3. Pracownik, który posiada poświadczenie bezpieczeństwa wydane w innej jednostce organizacyjnej, obowiązany jest do przedłożenia oryginału Pełnomocnikowi ds. Ochrony Informacji Niejawnych tut. Urzędu.
4. Pracownicy poszczególnych referatów oraz kierownicy zobowiązani są do informowania Wójta lub Sekretarza Urzędu Gminy o konieczności wydania upoważnienia przez Wójta Gminy w Kijach dla pracowników, których zakres obowiązków będzie wymagał dostępu do dokumentów niejawnych oznaczonych klauzulą 'zastrzeżone".

§ 3

1. Dokumenty niejawne oznaczone klauzulą „zastrzeżone" wpływające do Urzędu Gminy w Kijach rejestrowane są w Dzienniku Korespondencyjnym znajdującym się w sekretariacie tut. urzędu. Rejestracja polega na spisaniu danych z koperty bez jej otwierania. Następnie dokument przekazany jest Wójtowi Gminy lub dla Sekretarza Urzędu Gminy, którzy z kolei przekazują dokument odpowiedniemu pracownikowi lub wskazanemu na kopercie adresatowi, posiadającemu upoważnienie Wójta Gminy Kije bądź aktualne poświadczenie bezpieczeństwa. Odbiorca przekazanego dokumentu niejawnego jest zobowiązany zarejestrować dokument w swoim dzienniku pism przychodzących.
2. Zadania pracowników zajmujących się wytwarzaniem i rejestracją dokumentów niejawnych oznaczonych klauzulą "zastrzeżone" dotyczące spraw związanych z ochroną informacji niejawnych w danym biurze wykonywane są na podstawie zakresu obowiązków.

3. Wytwarzanie i przetwarzanie dokumentów i nośników oznaczonych klauzulą „zastrzeżone" jest dopuszczalne wyłącznie na komputerach odpowiednio zabezpieczonych przed nieuprawnionym ich ujawnieniem.
4. Wójt Gminy jest odpowiedzialny za właściwą organizację bezpieczeństwa teleinformatycznego.
5. Wójt Gminy udziela akredytacji bezpieczeństwa teleinformatycznego dla systemu teleinformatycznego przeznaczonego do przetwarzania informacji niejawnych o klauzuli „zastrzeżone" przez zatwierdzenie dokumentacji bezpieczeństwa systemu teleinformatycznego.

§ 4.

1. Dokumenty niejawne oznaczone klauzulą „zastrzeżone" przechowuje się w miejscach niedostępnych powszechnie, zamykanych na co najmniej jeden zamek o skomplikowanym mechanizmie.
2. Dokumentów niejawnych oznaczonych klauzulą „zastrzeżone" nie wolno przechowywać razem z dokumentami jawnymi, chyba że stanowią integralną część dokumentacji. Wówczas teczka musi zostać wyraźnie oznaczona klauzulą „zastrzeżone".
3. Klucze do urządzeń biurowych , w którym przechowywane są dokumenty niejawne oznaczone klauzulą „zastrzeżone", po zakończanym dniu pracy muszą być zabezpieczone przez pracownika w miejscu niedostępnym i nieznanym powszechnie,
4. Klucze oraz ich duplikaty zabezpiecza pracownik, któremu w zakresie obowiązków powierzono zadania związane z ochroną informacji niejawnych.
5. Zabrania się udostępnianie kluczy do urządzeń biurowych, w których przechowywane są dokumenty niejawne oznaczone klauzulą „zastrzeżone" oraz ich duplikatów osobom nieuprawnionym.

§ 5

1. Zobowiązuje się osobę przetwarzającą dokumenty oznaczone klauzulą „zastrzeżone" do zabezpieczenia ich treści przez ujawnieniem osobie nieuprawnionej.
2. Osoba przetwarzająca dokumenty oznaczone klauzulą „zastrzeżone" ponosi odpowiedzialność za ujawnienie ich treści osobie nieuprawnionej oraz niewłaściwe ich zabezpieczenie i przechowywanie.
3. W stosunku do pracowników, którzy nie będą przestrzegać ustalonych wymagań i dopuszczą się uchybień w zakresie ochrony i zabezpieczenia informacji zastrzeżonych, zastosowane być mogą przewidziane prawem sankcje karne, dyscyplinarne i służbowe.
4. O wszelkich nieprawidłowościach związanych z przetwarzaniem i udostępnianiem dokumentów oznaczonych klauzulą „zastrzeżone" oraz o ich zagubieniu bądź zniszczeniu osoba za nie odpowiedzialna jest zobowiązana niezwłocznie powiadomić bezpośredniego przełożonego i Pełnomocnika ds. Ochrony Informacji Niejawnych.

§ 6

Dokumenty oznaczone klauzulą „zastrzeżone" należy sporządzić zgodnie z wymogami wynikającymi z treści Rozporządzenia Prezesa Rady Ministrów z dnia 13 sierpnia 2010 r. w sprawie sposobu oznaczania materiałów, umieszczania na nich klauzul tajności, a także zmiany nadanej klauzuli tajności (Dz.U. z 2010 r. Nr 159, poz. 1069).

§ 7

1. W przypadku konieczności omawiania treści dokumentów oznaczonych klauzulą „zastrzeżone", uczestnicy spotkania muszą zostać niezwłocznie poinformowani o jego niejawnym charakterze.
2. W spotkaniu , mogą uczestniczyć wyłącznie osoby :
   1) posiadające upoważnienie Wójta Gminy Kije bądź aktualne poświadczenie bezpieczeństwa co najmniej do klauzuli „zastrzeżone",
   2) których zakres obowiązków obejmuje sprawy omawiane na spotkaniu.
3. Spotkanie o charakterze niejawnym nie może być utrwalone na magnetycznych nośnikach obrazu i dźwięku. Wszelkie protokoły i notatki należy oznaczać klauzulą niejawności.

§ 8

1. Kierownictwo Urzędu zapewnia i nadzoruje stosowanie ustaleń zawartych w niniejszej instrukcji.
2. Nadzór nad całokształtem zadań związanych z ochroną informacji zastrzeżonych sprawuje Wójt Gminy i Sekretarz Urzędu Gminy.