

196/2012

Załącznik Nr 1
do Zarządzenia Nr

Burmistrza Miasta i Gminy
Murowana Goślina z dnia
10.01.2012 r.

Zatwierdzam:

.....

**PLAN OCHRONY
INFORMACJI NIEJAWNYCH
W URZĘDZIE MIASTA I GMINY MUROWANA GOŚLINA**

Opracowała: Aleksandra Pilarczyk
Pełnomocnik ds. ochrony informacji niejawnych
w Urzędzie Miasta i Gminy Murowana Goślina

Murowana Goślina, styczeń 2012

Spis treści

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

1. Podstawy prawne ochrony informacji niejawnych

Plan ochrony informacji niejawnych w Urzędzie Miasta i Gminy Murowana Goślina, zwanym dalej Urzędem, określa zasady i tryb postępowania z informacjami niejawnymi oraz zapewnia jednolity sposób postępowania z tymi informacjami w Urzędzie.

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 r. w sprawie wzoru decyzji o odmowie wydania poświadczenia bezpieczeństwa
Dz.U.2010.258.1753

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

ROZPORZĄDZENIE Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie wzorów decyzji
Dz.U.2010.258.1752

ROZPORZĄDZENIE Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie wzorów zaświadczeń stwierdzających odbycie szkolenia w zakresie ochrony informacji niejawnych oraz sposobu rozliczania kosztów przeprowadzenia szkolenia przez Agencję Bezpieczeństwa Wewnętrznego oraz Służbę Kontrwywiadu Wojskowego
Dz.U.2010.258.1751

ROZPORZĄDZENIE 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.2010.159.1069

ROZPORZĄDZENIE Rady Ministrów z dnia 1 czerwca 2010 r. w sprawie organizacji i funkcjonowania kancelarii tajnych
Dz.U. 2010.114.765

ROZPORZĄDZENIE Prezesa Rady Ministrów z dnia 26 lutego 2010 r. 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:

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 informacje 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 o świadczeniu usług drogą elektroniczną (Dz.U. Nr 144, poz. 1204 z późn. zm),
8. **Urzędem** - jest Urząd Miasta i Gminy Murowana Goślina,
9. **Burmistrzem** – jest Burmistrz Miasta i Gminy Murowana Goślina,
10. **pełnomocnikiem ochrony** – jest Pełnomocnik ds. Ochrony Informacji Niejawnych w Urzędzie Miasta i Gminy Murowana Goślina.

3. Przedmioty ochrony

1. Przedmiotem ochrony w Urzędzie są:
 - a) informacje niejawne oznaczone klauzulą „zastrzeżone”,
 - b) pomieszczenia, w których są przechowywane i opracowywane materiały niejawne.

4. Klasyfikacja informacji niejawnych w Urzędzie.

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.

5. Dostęp do informacji niejawnych.

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.

Udostępnianie informacji niejawnych:

1. 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,
2. 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 dziennika ewidencyjnego.
7. Numer ewidencyjny każdego dokumentu niejawnego stanowiącego tajemnicę o klauzuli „zastrzeżone” poprzedzony jest skrótem „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.

7. Wykonywanie dokumentów zawierających informacje niejawne za pomocą komputera.

Pracownicy, którzy do opracowywania i wykonania 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 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 Burmistrz, który w szczególności:

- zapewnia opracowanie dokumentacji bezpieczeństwa teleinformatycznego,
 - realizuje ochronę fizyczną, elektromagnetyczną systemu lub sieci teleinformatycznej,
 - zapewnia niezawodność transmisji oraz kontrolę dostępu do urządzeń systemu lub sieci teleinformatycznej,
 - dokonuje analizy stanu bezpieczeństwa teleinformatycznego oraz zapewnia usunięcie stwierdzonych nieprawidłowości,
 - zapewnia przeszkolenie z zakresu bezpieczeństwa teleinformatycznego dla osób uprawnionych do pracy w systemie lub sieci teleinformatycznej.
4. Ochrona fizyczna systemu lub sieci teleinformatycznej polega na zastosowaniu środków zapewniających ochronę fizyczną w szczególności przed:
 - nieuprawnionym dostępem,
 - podglądem,
 - podsłuchem.
 5. Ochrona elektromagnetyczna systemu lub sieci teleinformatycznej polega na niedopuszczeniu utraty poufności i dostępności informacji niejawnych przetwarzanych w urządzeniach teleinformatycznych.
 6. System lub sieć teleinformatyczną 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 budynków i znajdujących się w nim pomieszczeń poprzez system alarmowy.
2. Kody do instalacji alarmowej do budynku Urzędu mogą posiadać: Burmistrz, Z-ca Burmistrza, Sekretarz, Skarbnik, Kierownik USC, kierownicy referatów, informatyk, podinspektor ds. bezpieczeństwa oraz upoważnieni pracownicy odpowiedzialni za otwieranie i zamykanie budynków Urzędu.
3. Pomieszczenia, w których znajdują się informacje niejawne z klauzulą „zastrzeżone” po godzinach pracy są zamykane, a klucz zabierany.
4. Sprzątanie tych pomieszczeń odbywa się w obecności upoważnionego pracownika przed zakończeniem pracy.
5. Informacje niejawne oznaczone klauzulą „zastrzeżone” przechowywane są na stanowiskach pracy w meblach biurowych zamykanych na klucz.

9. Ocena zagrożeń zewnętrznych i wewnętrznych.

1. Zagrożenia zewnętrzne.
Zagrożeniami zewnętrznymi dla Urzędu są:
 - możliwość napadu przez pojedynczych przestępców,
 - możliwość napadu przez przypadkowe osoby wykorzystujące nadarżającą się okazję z powodu nieprawidłowości w ochronie mienia

Urzędu.

2. Zagrożenia wewnętrzne.

Rodzaje zagrożeń:

- próby zaboru dokumentów lub mienia przez pracowników Urzędu,
- próby powielania, kserowania dokumentów służbowych do celów prywatnych,
- niszczenie, usuwanie, zmiana zapisu istotnej informacji albo udaremnianie lub znaczne utrudnianie zapoznanie się z tą informacją,
- próby wglądu w dokumenty niejawne przez osoby nieuprawnione,
- spożywanie alkoholu – przesłanka do wykroczeń dyscyplinarnych i przestępstw,
- niszczenie, uszkodzanie, usuwanie, zmienianie lub utrudnianie dostępu do danych informatycznych albo zakłócanie lub uniemożliwienie automatycznego przetwarzania, gromadzenia lub przekazywania takich danych.

3. Wnioski

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

- systematyczna i wnikliwa kontrola systemu ochrony przez osoby odpowiedzialne za jego organizację,
- wykonywanie prac porządkowych, remontowych itp. w strefie bezpieczeństwa wyłącznie pod nadzorem osób odpowiedzialnych,
- zwracanie uwagi na osoby, które mogą być zainteresowane zaborem dokumentów,
- uwrażliwianie pracowników na możliwość prób kontaktu grup przestępczych z pracownikami mającymi dostęp do dokumentów szczególnie ważnych,
- zastosowanie zasady, że do informacji niejawnych mogą mieć dostęp tylko pracownicy posiadający poświadczenie bezpieczeństwa lub właściwe upoważnienie Burmistrza,
- zwracanie uwagi na osoby przebywające w Urzędzie, których zachowanie wskazuje na spożycie alkoholu.

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

1. Za ochronę informacji niejawnych w Urzędzie odpowiada Burmistrz. Zadania określone ustawą o ochronie informacji niejawnych w imieniu Burmistrza wykonuje pełnomocnik ochrony poprzez:
 - sprawowanie nadzoru nad realizacją zadań i przestrzeganiem przepisów określonych w Planie ochrony,
 - sprawowanie kontroli w zakresie ochrony informacji niejawnych oraz przestrzeganie warunków dostępu do tych informacji.
2. W przypadku ujawnienia informacji niejawnych przez pracowników Burmistrz 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 przedkłada Burmistrzowi pisemną informację o naruszeniu przepisów i wnioski do podjęcia decyzji.

11. Instrukcja postępowania w przypadku otrzymania przesyłki niewiadomego pochodzenia.

W przypadku otrzymania jakiegokolwiek przesyłki niewiadomego pochodzenia lub budzącej podejrzenia z jakiegokolwiek innego powodu nie należy jej otwierać.

W tym przypadku należy:

1. umieścić przesyłkę w grubym worku plastikowym, szczelnie zamknąć,
2. worek umieścić w drugim worku, zakleić taśmą lub plastrem,
3. paczki nie należy przemieszczać,
4. powiadomić Komendę Policji tel.112. Służba ta podejmie wszelkie niezbędne kroki w celu bezpiecznego przejęcia przesyłki.

W przypadku, gdy podejrzana przesyłka została otwarta i zawiera jakąkolwiek podejrzaną zawartość należy:

1. nie naruszyć zawartości – nie rozsypywać, nie przenosić, nie dotykać, nie wąchać, wyłączyć systemy wentylacyjne, zamknąć okna,
2. 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. powiadomić:
 - Komendę Policji tel. 112,
 - Wojewódzką Stację Sanitarno-Epidemiologiczną
tel. alarmowy: 609 794 670, tel. całodobowy: 509-625-016,
 - Pogotowie Ratunkowe tel. 61 296 00 65.

Po przybyciu właściwych służb należy bezwzględnie zastosować się do ich zaleceń.

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

1.1. Alarmowanie

Osoba, która przyjęła zgłoszenie o podłożeniu ładunku wybuchowego albo zauważyła w urzędzie przedmiot niewiadomego pochodzenia mogący być ładunkiem wybuchowym jest obowiązana powiadomić:

- Burmistrza,
- Komendę Policji,
- Podinspektora ds. bezpieczeństwa,
- Komendanta Straży Miejskiej.

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

1. Do czasu przybycia Policji akcją kieruje podinspektor ds. bezpieczeństwa

2. Kierujący akcją zarządza, aby użytkownicy pomieszczeń dokonali sprawdzenia, czy w nich znajdują się:
 - przedmioty, rzeczy, urządzenia, paczki itp. których wcześniej nie było i nie wnieśli ich użytkownicy pomieszczeń,
 - ślady przemieszczania wyposażenia,
 - 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, toalety, piwnice oraz najbliższe otoczenie zewnętrzne obiektu powinny być sprawdzone przez wyznaczonych do tego pracowników.
4. Zlokalizowanych przedmiotów nie wolno dotykać. O ich umiejscowieniu należy natychmiast powiadomić osoby wymienione w pkt. 12.1.
5. W takiej sytuacji kierujący akcją może wydać decyzje osób z zagrożonego obiektu przed przybyciem Policji.
6. Należy zachować spokój i opanowanie, aby nie dopuścić do przejawów paniki.