

ZARZADZENIE
Burmistrza Toszka Nr.0050.174. 2012
z dnia 14.06.2012 r.

w sprawie: zatwierdzenia „ Planu Ochrony Informacji Niejawnych w Urzędzie Miejskim w Toszku”.

Działając 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.)

Zarządza się , co następuje:

§ 1

Zatwierdzam Plan Ochrony Informacji Niejawnych w Urzędzie Miejskim w Toszku stanowiącym załącznik do niniejszego zarządzenia.

§ 2

Traci moc Zarządzenie Nr 8/2001 Burmistrza Toszka z dnia 4.06.2001 r. w sprawie: Planu Ochrony Urzędu Miejskiego w Toszku.

§ 3

Nadzór nad wykonaniem zarządzenia powierzam Pełnomocnikowi Ochrony Informacji Niejawnych.


§ 4

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

§ 5

Zarządzenie wchodzi w życie z dniem podjęcia .


BURMISTRZ
mgr inż. Grzegorz Kupczyk

Sporządziła: Małgorzata Marcinkowska 



ZATWIERDZAM
BURMISTRZ

[Signature]
mgr.inż. Grzegorz Kupczyk...
(Kierownik Jednostki)

Załącznik Nr ¹.....do Zarządzenia
Burmistrza Toszka z dnia 14.06.2012,
Nr 0050.174.2012

**PLAN OCHRONY INFORMACJI NIEJAWNYCH
W URZĘDZIE
MIEJSKIM W TOSZKU**

OPRACOWAŁ:

Pełnomocnik Ochrony
Informacji Niejawnych
Małgorzata Marcinkowska

Spis treści:

«Podstawy prawne ochrony informacji niejawnych

- I. Definicje używane w Planie ochrony informacji niejawnych
- II. Ocena zagrożeń zewnętrznych i wewnętrznych
- III. Przedmiot ochrony
- IV. Klasyfikacja informacji niejawnych, ewidencja informacji niejawnych
- V. Zabezpieczenie informacji niejawnych
- VI. Dostęp do informacji niejawnych
- VII. Kancelaria materiałów niejawnych
- VIII. Zasady wykonywania dokumentów niejawnych
- IX. Oznaczanie, nadawanie, zmiana i znoszenie klauzuli niejawności materiałom niejawnym
- X. Wykorzystanie sprzętu komputerowego do wykonywania dokumentów niejawnych
- XI. Gromadzenie dokumentów zawierających informacje niejawne
- XII. Archiwizowanie, gromadzenie i niszczenie materiałów niejawnych
- XIII. Przechowywanie kluczy, pieczęci.
- XIV. Nadzór w zakresie informacji niejawnych
- XV. Odpowiedzialność karna, dyscyplinarna i służbowa za naruszenie przepisów o ochronie informacji niejawnych
- XVI. Wzory pism
- XVII. Instrukcje alarmowe

URZĄD MIEJSKI W TOSZKU

AKTY PRAWNE ZWIĄZANE Z OCHRONĄ INFORMACJI NIEJAWNYCH

Dziennik Ustaw Nr 182 z 2010 r.,poz.1228

Ustawa o ochronie informacji niejawnych z dnia 5 sierpnia 2010 r.

Dziennik Ustaw Nr 114 z 2010 r.,poz.765

Rozporządzenie Prezesa Rady Ministrów z dnia 01.czerwca 2010 r. w sprawie organizacji i funkcjonowania kancelarii tajnych

Dziennik Ustaw Nr 258 z 2010 r.,poz.1752

Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie wzorów poświadczeń bezpieczeństwa

Dziennik Ustaw Nr 258 z 2010 r.,poz.1751

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 lub Służbę Kontrwywiadu Wojskowego

Dziennik Ustaw Nr 258 z 2010 r.,poz.1750

Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. 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

Dziennik Ustaw Nr 34 z 2010 r.,poz.181

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

Dziennik Ustaw Nr 288 z 2011 r.,poz.1692

Rozporządzenie Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności , a także zmiany nadanej klauzuli tajności.

Dziennik Ustaw Nr 288 z 2011 r.,poz.1692

Rozporządzenie Prezesa Rady Ministrów z dnia 13 sierpnia 2011 r. w sprawie postępowania z dokumentami w komórkach organizacyjnych wykonujących zadania w zakresie obronności i bezpieczeństwa państwa

I. DEFINICJE UŻYWANE W PLANIE OCHRONY INFORMACJI NIEJAWNYCH:

- 1.ustawą**-jest ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228);
- 2.rękojmia zachowania tajemnicy**-jest zdolność osoby do do spełnienia ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem, stwierdzona w wyniku przeprowadzenia postępowania sprawdzającego;
- 3.dokumentem**-jest każda utrwalona informacja niejawna;
- 4.materiałem**-jest dokument lub przedmiot jak też chroniony jako informacja niejawna przedmiot lub dowolna jego część;
- 5.przetwarzaniem informacji niejawnych**-są wszelkie operacje wykonywane w odniesieniu do informacji niejawnych i na tych informacjach, w szczególności ich wytwarzanie, modyfikowanie, kopiowanie, gromadzenie,przechowywanie przekazywanie lub udostępnianie;
- 6.systemem teleinformatycznym**-jest system,teleinformatyczny w rozumieniu art.2 pkt 3 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. Nr 144, poz.1204, z późn. zm.);
- 7.ryzykiem**-jest kombinacja prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji;
- 8.zarządzanie ryzykiem**-są to skoordynowane działania w zakresie zarządzania bezpieczeństwem informacji, z uwzględnieniem ryzyka;
- 9.kancelaria materiałów niejawnych**-to wydzielone, wyodrębnione, zabezpieczone pomieszczenie przeznaczone do ewidencjonowania ,opracowywania, przechowywania dokumentów niejawnych oznaczonych klauzulą „ poufne”;

II. OCENA ZAGROZEŃ ZEWNĘTRZNYCH I WEWNĘTRZNYCH;

1. Ocena zagrożeń zewnętrznych:

Zagrożeniami zewnętrznymi dla Urzędu Miejskiego w Toszku 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 nadarzająca się okazje z powodu nieprawidłowości w ochronie mienia urzędu

Symptomy mogące świadczyć o przygotowaniu napadu lub włamania do budynku:

- wzmoczone zainteresowanie osób postronnych obiektem, помещением urzędu objawiające się m. in. : podejmowaniem prób uzyskania informacji o danym obiekcie, помещению od pracowników podczas luźnych rozmów po „przypadkowym” spotkaniu,
- nawiązaniem rozmów przez osoby postronne z pracownikami,
- podszywaniem się pod byłych pracowników urzędu pracujących w urzędzie i przejawianiem zainteresowania tym, co się po latach zmieniło,
- interesowaniem się osobami funkcyjnymi, w tym także ich przywarami oraz sposobem wykonywania obowiązków służbowych,
- obserwacją sposobu działania systemu ochronnego, sekretariatu, sprzętaczki itp.,
- rozpoznawaniem 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

Wnioski:

1. Należy prowadzić 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. Należy stosować zasadę niedopuszczania osób niepowołanych do penetracji strefy bezpieczeństwa,

4. Wykonywanie prac porządkowych, remontowych itp. w strefie bezpieczeństwa tylko pod nadzorem osób odpowiedzialnych.

2. Ocena zagrożeń wewnętrznych:

- próby zaboru dokumentów lub mienia przez pracowników urzędu,

- próby powielania, kserowania dokumentów służbowych dla celów prywatnych,

- byli pracownicy urzędu zwolnieni dyscyplinarnie,

- rozpoznanie organizacji pracy Urzędu celem łatwiejszej pracy grup przestępczych na terenie urzędu,

- próby wglądu w dokumenty niejawne przez osoby nieuprawnione,

Wnioski:

W związku z przedstawionymi kierunkami zagrożeń należy:

1. Zwracać szczególną uwagę na osoby, które mogą być zainteresowane zaborem dokumentu,

2. Prowadzić szczególny nadzór, by nie dokonywano prób kserowania, kopiowania bez zgody przełożonego,

3. Uwrażliwić pracowników na sytuacje występowania prób kontaktu grup przestępczych z pracownikami, którzy mają dostęp do dokumentów szczególnie ważnych,

4. Zastosować zasadę, że do informacji niejawnych mogą mieć dostęp tylko pracownicy posiadający poświadczenie bezpieczeństwa lub właściwe upoważnienie jednorazowe wydane przez kierownika jednostki.

III. PRZEDMIOT OCHRONY

1. Informacje niejawne oznaczone klauzulą:

„ poufne ”

„ zastrzeżone ”

pomieszczenia, w których są przechowywane i opracowywane materiały niejawne

IV. KLASYFIKACJA I EWIDENCJA INFORMACJI NIEJAWNYCH

Informacjom niejawnym nadaje się następujące klauzule:

1. **„ poufne ”**, jeżeli nieuprawnione ujawnienie informacji spowoduje szkodę Rzeczypospolitej Polskiej w obszarze polityki międzynarodowej, obronności, porządku publicznym lub bezpieczeństwie obywateli, utrudniłoby wykonywanie stawowych 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 RP;
- b) utrudni realizację przedsięwzięć obronnych lub negatywnie wpłynie na zdolność bojową sił zbrojnych RP;
- c) zakłóci porządek publiczny lub zagrazi bezpieczeństwu obywateli;
- d) utrudni wykonywanie zadań służbą lub instytucjom odpowiedzialnym za ochronę bezpieczeństwa lub podstawowych interesów RP ;
- e) utrudni wykonywanie zadań służbą lub instytucjom odpowiedzialnym za ochronę porządku publicznego , bezpieczeństwa obywateli lub ściganie sprawców przestępstw i przestępstw skarbowych oraz organom wymiaru sprawiedliwości;
- f) zagrazi stabilności systemu finansowego RP;
- g) wpłynie niekorzystnie na funkcjonowanie gospodarki narodowej.

2., „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 RP

Ewidencja informacji niejawnych :

1. Informacje niejawne oznaczone klauzulą „ poufne „ muszą być ewidencjonowane w wydzielonym ,wyodrębnionym pomieszczeniu spełniającym wymogi wynikające z przepisów ustawy o ochronie informacji niejawnych,
2. Dokumenty niejawne o klauzuli „ zastrzeżone „ mogą być ewidencjonowane na poszczególnych stanowiskach pracy – odpowiednio zabezpieczone,
3. Dokumenty niejawne wpływające do Urzędu ewidencjonuje się w dzienniku ewidencyjnym,
4. Dokumenty niejawne wytworzone – wychodzące z Urzędu rejestruje się w dzienniku ewidencyjnym,
5. Każdy dokument niejawny przychodzący lub wychodzący z Urzędu rejestruje się w odrębnej pozycji dziennika ewidencyjnego,
6. Numer ewidencyjny każdego dokumentu niejawnego stanowiącego o klauzuli „ poufne „ lub „zastrzeżone „ powinien być poprzedzony skrótem literowym „ Pf” lub „ Z”
7. Ewidencjonowaniu podlegają wszystkie dokumenty niejawne oznaczone klauzulą „ poufne „ lub „ zastrzeżone „

8.Sposób właściwego opisanie dokumentu niejawnego został przedstawiony w Rozporządzeniu Prezesa Rady Ministrów z dnia 22 grudnia 2011 r.(Dz. U.Nr 288 poz . 1692 z 29 grudnia 2011 r.) w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności.

9.Prowadzi się Rejestr Dzienników służący do ewidencjonowania książek i dzienników ewidencyjnych,

10.Pracownik kancelarii materiałów niejawnych przyjmuje przesyłki za pokwitowaniem , wpisując datę wpływu do jednostki organizacyjnej.

Przyjmując przesyłkę, sprawdza:

- 1.prawidłowość adresu,
- 2.całość opakowania,
- 3.zgodność odcisku pieczęci na opakowaniu z nazwą jednostki organizacyjnej nadawcy,

11.W przypadku stwierdzenia uszkodzenia przesyłki, sporządzany jest protokół, który otrzymuje : nadawca, pełnomocnik ochrony w jednostce oraz przewoźnik,który przesyłkę dostarczył.

12.Pracownik kancelarii materiałów niejawnych :

- 1.sprawdza ,czy zawartość przesyłki odpowiada wyszczególnionym na niej numerom ewidencyjnym,
- 2.ustala, czy liczba załączników i stron jest zgodna z liczbą oznaczoną na poszczególnych dokumentach.

13.W przypadku stwierdzenia nieprawidłowości, pracownik kancelarii materiałów niejawnych sporządza protokół z ich opisem , przekazując jeden egzemplarz nadawcy.

14.Fakt sporządzenia protokołu ,pracownik kancelarii materiałów niejawnych odnotowuje w odpowiednim rejestrze w rubryce „ uwagi ”.

V. ZABEZPIECZENIE INFORMACJI NIEJAWNYCH

1.Informacje niejawne oznaczone klauzulą „ **poufne** „, należy przechowywać w kancelarii materiałów niejawnych, zabezpieczone zgodnie z przepisami ustawy o ochronie informacji niejawnych drzwiami metalowymi klasy „ 0 „, odporności na włamanie wg Polskiej Normy PN-EN 1143-1,

2.Informacje niejawne oznaczone klauzulą „ zastrzeżone „, można przechowywać w pomieszczeniu kancelarii materiałów niejawnych lub na stanowiskach pracy , w meblach biurowych zamykanych na klucz.

VI. DOSTĘP DO INFORMACJI NIEJAWNYCH

Uprawnienia do dostępu do informacji niejawnych posiadają osoby , które:

1. Po przeprowadzonym postępowaniu sprawdzającym, uzyskały poświadczenie bezpieczeństwa upoważniające do dostępu do informacji niejawnych o określonej klauzuli, lub uzyskały pisemne upoważnienie kierownika jednostki – jeżeli nie posiadają poświadczenia bezpieczeństwa,
2. Odbyły przeszkolenie w zakresie ochrony informacji niejawnych.

Udostępnianie informacji niejawnych:

1. Informacje niejawne mogą być udostępniane wyłącznie osobie dającej rękojmię zachowania tajemnicy i tylko w takim zakresie, jaki jest niezbędny do załatwienia konkretnej sprawy, wynikającej z zakresu czynności
2. Informacje niejawne mogą być udostępniane tylko osobom uprawnionym do dostępu do informacji określonych tą klauzulą i z uwzględnieniem ograniczenia określonego w pkt 1.

VII. KANCELARIA MATERIAŁÓW NIEJAWNYCH

W urzędzie funkcjonuje kancelaria materiałów niejawnych, która została utworzona dla potrzeb jednostki, dla właściwego przechowywania, ewidencjonowania materiałów niejawnych oznaczonych klauzulą „poufne”. W kancelarii dopuszcza się również możliwość ewidencjonowania i przechowywania materiałów niejawnych oznaczonych klauzulą „zastrzeżone”.

Organizacja pracy kancelarii materiałów niejawnych zapewnia możliwość ustalenia w każdych okolicznościach, gdzie znajduje się materiał o klauzuli „poufne” pozostający w dyspozycji jednostki organizacyjnej oraz kto z tym materiałem się zapoznał.

Kancelaria materiałów niejawnych odmawia wydania – udostępnienia materiałów osobie nieuprawnionej.

W kancelarii przyjmuje się, rejestruje, przechowuje, przekazuje i wysyła dokumenty oraz prowadzi:

- dziennik ewidencji
- rejestr dzienników

W przypadkach uzasadnionych organizacją ochrony informacji niejawnych kancelaria może prowadzić także inne rejestry niż wymienione wyżej.

Za zgodą kierownika jednostki organizacyjnej, w porozumieniu z pełnomocnikiem ochrony, w kancelarii mogą być przyjmowane, rejestrowane, przechowywane i wysyłane dokumenty i materiały oznaczone klauzulą „zastrzeżone”.

VIII. ZASADY WYKONYWANIA DOKUMENTÓW NIEJAWNYCH

1. Propozycje przyznania klauzuli niejawności na wykonywanym dokumencie przedstawia osoba sporządzająca dokument,
2. Klauzulę niejawności na danym dokumencie przyznaje osoba, która jest upoważniona do podpisania dokumentu,
3. Uprawnienie do przyznania, obniżenia i znoszenia klauzuli tajności przysługuje wyłącznie w zakresie posiadanego prawa dostępu do informacji niejawnych,

4. Rękopisy sporządzanych dokumentów niejawnych powinny być opracowywane w brulionach uprzednio zarejestrowanych w kancelarii materiałów niejawnych,
5. Dokumenty niejawne wpływające do urzędu, jak i wytworzone w urzędzie podlegają ewidencjonowaniu w dzienniku ewidencji,
6. Dokumenty niejawne powinny być opisane i oznaczone zgodnie z Rozporządzeniem Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności (Dz. U.Nr 288 z 2011 roku, poz.1692)

IX.OZNACZANIE, NADAWANIE, ZMIANA I ZNOSZENIE KLAUZULI NIEJAWNOŚCI MATERIAŁOM NIEJAWNYM

1. Materiał oznacza się klauzulą tajności w sposób wyraźny i w pełnym brzmieniu.
2. W przypadku gdy poszczególnym częściom materiału zostały nadane różne klauzule tajności bądź gdy niektóre z tych części są jawne, wyodrębnione części oddziela się oznaczeniem odpowiedniej klauzuli tajności wskazanej w pełnym brzmieniu lub określeniem „jawne”. Części materiału zawierające tekst lub obraz oddziela się przez odpowiednie ich oznaczenie przed rozpoczęciem i po zakończeniu tekstu lub obrazu.
3. Jeżeli poszczególnym częściom materiału zostały nadane różne klauzule tajności, materiał oznacza się klauzulą tajności co najmniej równą najwyższej klauzuli tajności, jaką nadano części materiału.
4. Dokument utrwalony w formie pisma oznacza się w następujący sposób:
 - a) na środku ,jako pierwszy element w nagłówku strony, klauzulę tajności,
 - b) numer egzemplarza, a w przypadku gdy dokument wykonano w jednym egzemplarzu ,napis „ egz. pojedynczy ”
 - c) sygnaturę literowo - cyfrową, na którą składają się : literowe oznaczenie jednostki lub komórki organizacyjnej, symbol oznaczenia klauzuli tajności, numer, pod którym ten dokument został zarejestrowany, i rok, w którym dokonano rejestracji, a także, w zależności od potrzeb, inne oznaczenia ułatwiające ustalenie miejsca wykonania dokumentu w jednostce lub komórce organizacyjnej lub też jego przynależność do określonej sprawy,
 - d) numer strony oraz liczbę stron dokumentu,
 - e) na środku jako ostatni element w stopce strony, klauzulę tajności;

15. Na pierwszej stronie umieszcza się również:

- a) nazwę jednostki lub komórki organizacyjnej,
- b) nazwę miejscowości i datę podpisania dokumentu,
- c) w przypadku dokumentu, któremu nadano bieg korespondencyjny, imię i nazwisko lub nazwę stanowiska adresata; w przypadku wielu adresatów dokumentu, któremu

nadano bieg korespondencyjny, dopuszcza się możliwość umieszczenia jedynie adnotacji „ adresaci według rozdzielnika ”;

6. Na ostatniej stronie pod treścią umieszcza się również:

- a) liczbę załączników,
- b) liczbę stron lub innych jednostek miary wszystkich załączników lub informację określającą rodzaj załączonego materiału i jego odpowiednią jednostkę miary,
- c) klauzule tajności załączników wraz z numerami, pod jakimi zostały zarejestrowane, oraz liczbę stron każdego załącznika lub informację określającą rodzaj załączonego materiału i jego odpowiednią jednostkę miary,
- d) w przypadku gdy adresatowi wysyła się inną liczbę załączników niż pozostawia w aktach, dodatkowo napis „ tylko adresat ” - jeżeli załączniki mają być przekazane adresatowi bez pozostawiania ich w aktach, lub napis „ do zwrotu ”- jeżeli załączniki mają być zwrócone nadawcy,
- e) stanowisko oraz imię i nazwisko lub inne oznaczenie wskazujące osobę uprawnioną do jego podpisania,
- f) liczbę wykonanych egzemplarzy,
- g) adresatów poszczególnych egzemplarzy dokumentu albo adnotację „ adresaci według rozdzielnika ”
- h) dyspozycję „ ad acta ” w przypadku egzemplarza pozostającego w aktach nadawcy,
- i) imię i nazwisko lub inne oznaczenie wskazujące wykonawcę.

7. W przypadku dokumentu o klauzuli „ zastrzeżone ” dopuszcza się odstępianie od umieszczania w/w oznaczeń.

8. Na dokumencie w formie pisma „stanowiącym załącznik na pierwszej stronie umieszcza się dodatkowo informację „ Załącznik nr... do dokumentu nr... z dnia ... ”

9. Jeżeli wraz z dokumentem przesyła się załączniki zawierające informacje niejawne , to:

- a) dokument oznacza się klauzulą tajności nie niższą niż najwyższa klauzula tajności załączników,
- b) na dokumencie – jeżeli po trwałym odłączeniu załączników dokument jest jawny albo jego klauzula tajności jest inna niż określona zgodnie z pkt a – na każdej stronie pod numerem egzemplarza umieszcza się adnotację o jawności albo klauzuli tajności dokumentu po odłączeniu załączników,

10. Oznaczenia zniesienia klauzuli tajności na dokumencie w formie pisma dokonuje się następująco:

a) skreśla wszystkie dotychczasowe oznaczenia znoszonej klauzuli tajności,

b) nad pierwszym w kolejności skreślonym oznaczeniem klauzuli tajności umieszcza się napis „ Zniesiono klauzulę tajności ” oraz datę, podpis, imię i nazwisko lub inne oznaczenie wskazujące osobę dokonującą tych adnotacji oraz wskazuje się podstawę dokonania czynności,

11. Oznaczenia zmiany klauzuli tajności dokonuje się następująco:

a) skreśla wszystkie dotychczasowe oznaczenia znoszonej klauzuli tajności,

b) nad skreślonymi oznaczeniami klauzuli tajności umieszcza się oznaczenie nowej klauzuli tajności,

c) nad pierwszym w kolejności skreślonym oznaczeniem klauzuli tajności umieszcza się datę, podpis, imię i nazwisko lub inne oznaczenie wskazujące osobę dokonującą tych adnotacji oraz wskazuje się podstawę dokonania czynności,

12. Skreśleń i adnotacji dokonują : kierownik kancelarii materiałów niejawnych, kierownik innej niż kancelaria komórki, w której są rejestrowane materiały niejawne, albo inne osoby upoważnione przez nich lub przez kierownika jednostki organizacyjnej

13. Skreśleń i adnotacji dokonuje się kolorem czerwonym, w sposób czytelny. Wycieranie, wywabianie lub zamazywanie klauzuli tajności i dokonanych zamian jest niedozwolone.

14. Na dokumencie wytworzonym w wyniku kopiowania lub tłumaczenia umieszcza się:

a) w przypadku kopii – na pierwszej stronie sygnaturę, o której mowa w pkt 4-c,

b) w pozostałych przypadkach – odpowiednio oznaczenia o których mowa w pkt 4,

c) na wszystkich stronach:

- w przypadku kopiowania napis „ Wydruk ”, „Kopia ”, „ Odpis ”, „ Wyciąg ”, albo „ Wypis ”

d) w przypadku tłumaczenia napis „ tłumacz z języka – nazwa języka – oraz podpis, imię i nazwisko lub inne oznaczenie wskazujące osobę dokonującą tłumaczenia;

15. Na ostatniej stronie w przypadku kopiowania dodatkowo potwierdzenie zgodności z oryginałem zawierające:

a) napis „ Za zgodność „,

b) odcisk pieczęci z nazwą jednostki lub komórki organizacyjnej, w której wytworzono dokument,

c) podpis, imię i nazwisko lub inne oznaczenie wskazujące kierownika jednostki lub komórki organizacyjnej, w której dokonano kopiowania, albo osobę przez niego upoważnioną.

16. Wytworzenie dokumentu w wyniku kopiowania lub tłumaczenia odnotowuje się na ostatniej stronie dokumentu kopiowanego lub tłumaczonego przez umieszczenie informacji o:

a) nazwie jednostki lub komórki organizacyjnej, w której wytworzono dokument;

b) liczbie egzemplarzy dokumentu wytworzonego

c) dacie wytworzenia dokumentu;

d) numerze, pod jakim wytworzony dokument został zarejestrowany,

Informacje, o których mowa w pkt 15 a-c, umieszcza się przed wytworzeniem dokumentu w wyniku kopiowania lub tłumaczenia, natomiast numer, pod jakim został on zarejestrowany, umieszcza się po jego wytworzeniu.

X. WYKORZYSTANIE SPRZĘTU KOMPUTEROWEGO DO WYKONYWANIA DOKUMENTÓW NIEJAWNYCH

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 w sieci teleinformatycznej.

3. Za właściwą organizację bezpieczeństwa teleinformatycznego odpowiada kierownik jednostki organizacyjnej, który w szczególności:

- zapewnia opracowanie dokumentacji bezpieczeństwa teleinformatycznego,
- realizuje ochronę fizyczną, elektromagnetyczną systemu lub sieci,
- 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,
- zawiadamia właściwą służbę ochrony państwa o zaistniałym incydencie bezpieczeństwa teleinformatycznego dotyczącym informacji niejawnych oznaczonych co najmniej klauzulą „poufne”

4. Ochrona elektromagnetyczna systemu lub sieci teleinformatycznej polega na niedopuszczeniu do utraty poufności i dostępności informacji niejawnych przetwarzanych w urządzeniach teleinformatycznych.

5. Ochronę elektromagnetyczną systemu lub sieci teleinformatycznej zapewnia się w szczególności przez umieszczenie urządzeń teleinformatycznych, połączeń i linii w strefach kontrolowanego dostępu spełniających wymagania w zakresie tłumienności elektromagnetycznej odpowiednio do wyników szacowania ryzyka dla informacji

niejawnych, lub zastosowanie odpowiednich urządzeń teleinformatycznych, połączeń i linii o obniżonym poziomie emisji lub ich ekranowanie z jednoczesnym filtrowaniem zewnętrznych linii zasilających i sygnałowych.

6. Systemy i sieci teleinformatyczne, w których mają być wytwarzane, przetwarzane, przechowywane lub przekazywane informacje niejawne, podlegają akredytacji bezpieczeństwa teleinformatycznego przez służby ochrony państwa.
7. Akredytacja, o której mowa następuje na podstawie dokumentów szczególnych wymagań bezpieczeństwa i procedur bezpiecznej eksploatacji.
8. Dla systemu teleinformatycznego przeznaczonego do przetwarzania informacji niejawnych o klauzuli „poufne” lub wyższej – akredytacji bezpieczeństwa udziela ABW.
9. Dla systemu teleinformatycznego przeznaczonego do przetwarzania informacji niejawnych o klauzuli „zastrzeżone”, akredytacji bezpieczeństwa udziela kierownik jednostki organizacyjnej przez zatwierdzenie dokumentacji bezpieczeństwa systemu teleinformatycznego. Dokumentacja, o której mowa jest opiniowana przez ABW.
10. Kierownik jednostki organizacyjnej wyznacza pracownika pełniącego funkcję:

-Inspektora bezpieczeństwa teleinformatycznego,

oraz pracownika pełniącego funkcję:

-Administratora systemu

Wymienione funkcje mogą pełnić osoby, posiadające poświadczenia bezpieczeństwa odpowiednie do klauzuli informacji wytwarzanych, przetwarzanych, przechowywanych lub przekazywanych w systemach lub sieciach teleinformatycznych, po odbyciu specjalistycznych szkoleń z zakresu bezpieczeństwa teleinformatycznego prowadzonych przez służby ochrony państwa.

XI. GROMADZENIE, DOKUMENTÓW ZAWIERAJĄCYCH INFORMACJE NIEJAWNE

1. Dokumenty zawierające informacje niejawne powinny być przechowywane zgodnie z rzeczowym podziałem akt,
2. Dokumenty ostatecznie załatwione wymagają wszycia w teczkę pism, po zakończeniu roku kalendarzowego, klauzule niejawności teczek określa się według dokumentu o najwyższej klauzuli tajności,
3. Dokumenty niejawne o klauzuli „poufne” muszą być przechowywane w kancelarii materiałów niejawnych. W szczególnie uzasadnionych przypadkach dokumenty te mogą być przechowywane poza kancelarią, kierownik jednostki organizacyjnej lub inna upoważniona przez niego osoba mogą wyrazić pisemną zgodę na przechowywanie dokumentów poza pomieszczeniami kancelarii, pod warunkiem spełnienia wymogów

bezpieczeństwa odpowiednich do tej klauzuli , na czas niezbędny do realizacji zadań związanych z dostępem do tych dokumentów.

4. Dokumenty niejawne o klauzuli „ zastrzeżone ” są przechowywane w kancelarii materiałów niejawnych lub na stanowiskach pracy w meblach biurowych zamykanych na klucz.

XII. ARCHIWIZOWANIE , GROMADZENIE I NISZCZENIE MATERIAŁÓW NIEJAWNYCH

1. Archiwizowanie materiałów niejawnych odbywa się z zachowaniem zasad określonych w Rozporządzeniu Ministra Kultury z dnia 16 września 2002 r. w sprawie postępowania z dokumentacją, zasad jej klasyfikowania i kwalifikowania oraz zasad i trybu przekazywania materiałów archiwalnych do archiwów państwowych (Dz. U. Nr 167, poz. 1375, z dnia 9 października 2002 r.),

2. Zasady postępowania z dokumentacją w komórkach organizacyjnych wykonujących zadania w zakresie obronności i bezpieczeństwa państwa zostały określone w rozporządzeniu Prezesa Rady Ministrów z dnia 26 lutego 2010 (Dz. U. Nr 34 poz. 181) ,

3. Dokumentacja wytwarzana i gromadzona dzieli się na:

- materiały archiwalne - wchodzące do państwowego zasobu archiwalnego;
- dokumentację niearchiwalną- inną dokumentację, nie stanowiącą materiałów archiwalnych,

4. Rzeczową klasyfikację oraz kwalifikację dokumentacji ze względu na okresy jej przechowywania , wytwarzania i gromadzenia zawierają jednolite rzeczowe wykazy akt,

5. Wykazy akt , o których mowa stanowią podstawę gromadzenia dokumentacji w akta sprawy,

6. Dokumentacja niearchiwalna , podlega brakowaniu po upływie okresu przechowywania określonego we właściwym wykazie akt,

7. Brakowanie dokumentacji niearchiwalnej następuje na podstawie zgody dyrektora miejscowo właściwego archiwum państwowego, udzielonej po rozpatrzeniu naszego wniosku.

8. Do wniosku załącza się :

- protokół oceny dokumentacji niearchiwalnej ,
- spis dokumentacji niearchiwalnej przeznaczonej do zniszczenia

9. Protokół oraz spis sporządza komisja powołana przez kierownika jednostki, w której skład wchodzi : osoba prowadząca archiwum zakładowe, przedstawiciel komórki organizacyjnej , której dokumentacja dotyczy oraz pracownik kancelarii materiałów niejawnych,

10. Urząd przechowuje w archiwum dokumenty brakowania, o których mowa wraz z dowodami przekazania nieprzydatnej dokumentacji niearchiwalnej na makulaturę bądź

protokołami jej zniszczenia,

11. Uporządkowanie materiałów archiwalnych polega na podziale rzeczowym teczek i prawidłowym ułożeniu materiałów wewnątrz teczek, ich opisaniu, nadaniu właściwego układu, sporządzeniu ewidencji oraz technicznym zabezpieczeniu,
12. Materiały archiwalne powinny być ułożone wewnątrz teczek w kolejności spraw, a w ramach sprawy – chronologicznie, poczynając od pierwszego pisma wszczynającego sprawę. Poszczególne strony akt znajdujących się w teczce powinny być opatrzone kolejną numeracją.

XIII. PRZECHOWYWANIE KLUCZY I PIECZĘCI

Ustala się zasady gospodarki kluczami i pieczęciami:

1. Szafy metalowe kancelarii materiałów niejawnych po zamknięciu mogą być dodatkowo plombowane pieczęcią do plasteliny ,
2. Klucze do szaf metalowych kancelarii oraz pieczęcie ,po zakończeniu pracy należy złożyć w sejfie,
3. Klucze od sejfu należy zabrać i złożyć w sejfie głównym urzędu – za pokwitowaniem.
4. Klucze od drzwi wejściowych do kancelarii materiałów niejawnych po zakończeniu pracy należy umieścić w sejfie głównym urzędu- za pokwitowaniem,
5. Klucze do sejfu głównego urzędu posiadają 2 wyznaczone osoby,
6. Otworzenie i zamknięcie sejfu ,każdorazowo odbywa się za pokwitowaniem ,
7. Pieczęć do plasteliny pracownik kancelarii materiałów niejawnych zabezpiecza tak ,by osoby nieuprawnione nie mogły z niej korzystać,
8. Tworzy się zapasowy komplet kluczy do kancelarii materiałów niejawnych,
9. Zapasowy komplet kluczy należy umieścić w zamykanym pojemniku , zabezpieczonym pieczęcią .
10. Tak przygotowany komplet kluczy zapasowych ,znajduje się w jednym z sejfów urzędu,
11. Pracownik kancelarii materiałów niejawnych po przybyciu do urzędu , przed otwarciem kancelarii powinien sprawdzić , czy nie zostały naruszone pieczęcie zabezpieczające klucze oraz zabezpieczające drzwi wejściowe do kancelarii .W dalszej kolejności sprawdza się czy nie zostały naruszone pieczęcie na szafach znajdujących się w kancelarii,

XIV.NADZÓR W ZAKRESIE OCHRONY INFORMACJI NIEJAWNYCH

- 1.Za ochronę informacji niejawnych odpowiada kierownik jednostki organizacyjnej,
- 2.Zadania określone ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz.1228 z 2010 r.) w imieniu kierownika jednostki wykonuje pełnomocnik do spraw ochrony informacji niejawnych poprzez:
 - sprawowanie nadzoru nad przestrzeganiem przepisów zawartych w Planie Ochrony Informacji Niejawnych
 - sprawowanie nadzoru w zakresie ochrony informacji niejawnych oraz przestrzegania procedur związanych z upoważnieniem do dostępu do tych informacji.

XV.ODPOWIEDZIALNOŚĆ KARNA,DYSCYPLINARNA I SŁUŻBOWA ZA NARUSZENIE PRZEPISÓW O OCHRONIE INFORMACJI NIEJAWNYCH

- 1.Zakres odpowiedzialności karnej osób,które dopuściły się przestępstwa lub czynu zabronionego przeciwko ochronie informacji został określony przepisami Kodeksu Karnego (Ustawa z dnia 6 czerwca 1997 r. ,Kodeks Karny, Dz.U. z dnia 2 sierpnia 1997 r.) w art. 266.
 - § 1. Kto, wbrew przepisom ustawy lub przyjętemu na siebie zobowiązaniu, ujawnia lub wykorzystuje informację , z którą zapoznał się w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową, podlega grzywnie , karze ograniczenia wolności albo pozbawienia wolności do lat 2.
 - § 2. 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.
- 2.Wobec pracowników, którzy nie przestrzegają wymagań związanych z ochroną informacji niejawnych, dopuszczają się uchybień w zakresie niewłaściwego zabezpieczenia dokumentów, stwarzając warunki do ujawnienia tajemnicy osobom nieuprawnionym , mogą być zastosowane sankcje służbowe i dyscyplinarne.

USTAWA O OCHRONIE INFORMACJI NIEJAWNYCH

z dnia 5 sierpnia 2010 r.

(Dz.U. z 2010 r. Nr 182 poz.1228)

W Z O R Y

P I S M I U P O W A Ź N I E Ń

XVI

Spis treści

1. Zapytanie o udzielenie informacji o osobie
2. Krajowy Rejestr Karny- pismo przewodnie
3. Wniosek o sprawdzenie w kartotekach niedostępnych powszechnie
4. Polecenie wszczęcia zwykłego postępowania sprawdzającego
5. Upoważnienie do dostępu do informacji niejawnych -klauzula „, zastrzeżone „,
6. Zaświadczenie stwierdzające odbycie szkolenia w zakresie informacji niejawnych
7. Poświadczenie bezpieczeństwa
8. Wniosek o przeprowadzenie poszerzonego postępowania sprawdzającego
9. Zgoda na udostępnienie informacji niejawnych o klauzuli „, Poufne „, osobie wobec której wszczęto postępowanie sprawdzające
10. Oświadczenie
11. Sposób oznaczania pism niejawnych

Miejscowość i data.....

.....
nazwa jednostki organizacyjnej

L.dz.....

Krajowy Rejestr Karny

Biuro Informacyjne

Ul. Czerniakowska 100

00-454 Warszawa

lub

Punkt Informacyjny

Krajowego Rejestru Karnego

przy Sądzie Powszechnym

Na podstawie art. 6 ust. 1 pkt 10 ustawy z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym (Dz. U. z 2008, Nr 50, poz. 292, z późn. zm.) oraz art. 25 ust. 1 pkt 1 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2010 r., Nr 182, poz. 1228), w załączeniu przekazuję zapytanie , stanowiące załącznik nr 2 do rozporządzenia Ministra Sprawiedliwości z dnia 7 listopada 2003 r. w sprawie udzielenia informacji o osobach oraz o podmiotach zbiorowych na podstawie danych zgromadzonych w Krajowym Rejestrze Karnym (Dz. U. z 2003, Nr 198, poz. 1930 z późn. zm.) dotyczący:

15. Imię (imiona)

16. Nazwisko (w tym przybrane)

17. Nr PESEL

18. Imię ojca

Zapytanie proszę odesłać na adres:.....

.....

.....

Pieczętka i podpis pełnomocnika ochrony lub zastępcy pełnomocnika ochrony

Miejscowość i data

.....

Nazwa jednostki organizacyjnej występującej o sprawdzenie
osoby upoważnianej do dostępu do informacji niejawnych

L.dz.....

DYREKTOR

Delegatury Agencji Bezpieczeństwa Wewnętrznego

Wykaz adresów Delegatur ABW

znajduje się na stronie:

www.abw.gov.pl

WNIOSEK O SPRAWDZENIE W EWIDENCJACH I KARTOTEKACH NIEDOSTĘPNYCH POWSZECHNIE

Na podstawie art. 25 ust. 1 pkt 2 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2010 r., Nr 182, poz. 1228) wykonując nałożone zadania w związku z przeprowadzaniem zwykłym postępowaniem sprawdzającym wobec następującej osoby:

5. Nr PESEL
6. Nazwisko (w tym przybrane)
7. Imię (imiona)
8. Imię ojca
9. Imię matki
10. Nazwisko rodowe matki
11. Data urodzenia
12. Miejsce urodzenia
13. Adres zameldowania
14. Adres zamieszkania

proszę o poinformowanie, czy Agencja Bezpieczeństwa Wewnętrznego posiada informacje, które mają wpływ na wynik postępowania.

.....

Pieczętka i podpis pełnomocnika ochrony lub zastępcy pełnomocnika ochrony

Miejscowość i data.....

.....
Nazwa jednostki organizacyjnej

Pełnomocnik ds. Ochrony Informacji Niejawnych

W.....

POLECENIE WSZCZĘCIA ZWYKŁEGO POSTĘPOWANIA SPRAWDZAJĄCEGO

Na podstawie art. 23 ust. 1 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2010 r., Nr 182, poz. 1228) polecam przeprowadzenie zwykłego postępowania sprawdzającego w celu wydania poświadczenia bezpieczeństwa, upoważniającego do dostępu do informacji niejawnych oznaczonych klauzulą tajności „poufne” wobec:

1. Imię (imiona)
2. Nazwisko (w tym przybrane)
3. Nr PESEL
4. Imię ojca

.....
Pieczętka i podpis kierownika jednostki organizacyjnej

Upoważnienie uprawniające dostęp do informacji niejawnych oznaczonych klauzulą
„zastrzeżone”

Nr pisma.....

.....
/miejsowość ,data/

Pan /Pani

.....

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

u p o w a ż n i a m

Pana/ą..... do dostępu do informacji
niejawnych oznaczonych klauzulą „zastrzeżone” zatrudnionego/oną
w na stanowisku

.....
/kierownik jednostki/

*Upoważnienie ważne jest na czas zatrudnienia w

*Dostęp do informacji niejawnych o klauzuli „zastrzeżone” może nastąpić po odbyciu szkolenia
w zakresie przepisów ustawy o ochronie informacji niejawnych.

ZAŚWIADCZENIE

Nr 11/2012

stwierdzające odbycie przeszkolenia w zakresie ochrony informacji niejawnych
stwierdza się, że Pan/Pani

.....
Imię i nazwisko

.....
Pesel

odbyła/a 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 Miejskim w Toszku.

Toszek,.....

.....

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 Pani(Pan)

(imię i nazwisko, data urodzenia)

daje rękojmię zachowania tajemnicy

w zakresie dostępu do informacji niejawnych oznaczonych klauzulą

_____	- na okres do:	_____
<i>(nazwa klauzuli tajności)</i>		<i>(termin ważności)</i>
_____	- na okres do:*	_____
<i>(nazwa klauzuli tajności)</i>		<i>(termin ważności)*</i>
_____	- na okres do:*	_____
<i>(nazwa klauzuli tajności)</i>		<i>(termin ważności)*</i>

(miejsowość i data)

mp.

(podpis i imienna pieczęć osoby upoważnionej)

*niepotrzebne skreślić

.....
Miejscowość i data

.....
Nazwa jednostki organizacyjnej wnioskującej o przeprowadzenie
poszerzonego postępowania sprawdzającego

L.dz.....

DYREKTOR

Delegatury Agencji Bezpieczeństwa Wewnętrznego

w.....

**WNIOSEK O PRZEPROWADZENIE
POSZERZONEGO POSTĘPOWANIA SPRAWDZAJĄCEGO**

Na podstawie art. 23 ust. 2 pkt 1 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji
niejawnych (Dz.U. z 2010 r., Nr 182, poz. 1228) wnoszę o przeprowadzenie poszerzonego
postępowania sprawdzającego w celu wydania poświadczenia bezpieczeństwa,
upoważniającego do dostępu do informacji niejawnych o klauzuli*

wobec :

27. Imię

28. Nazwisko

29. Nr PESEL

.....
Pieczętka i podpis kierownika jednostki organizacyjnej
lub osoby upoważnionej do obsady stanowiska lub zlecenia prac

Załącznik:

Załącznik – Ankieta Bezpieczeństwa Osobowego – nastr. - tylko adresat

* wpisać odpowiednią klauzulę lub klauzulę tajności

Miejscowość i data.....

.....
nazwa jednostki organizacyjnej

**ZGODA NA UDOSTĘPNIENIE INFORMACJI NIEJAWNYCH O KLAUZULI
„POUFNE” OSOBIE WOBEC KTÓREJ WSZCZĘTO POSTĘPOWANIE
SPRAWDZAJĄCE ZWYKŁE**

Postępowanie sprawdzające zostało wszczęte w dniu

Na podstawie art. 34 ust. 9 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2010 r., Nr 182, poz. 1228) wyrażam zgodę na udostępnienie informacji niejawnych oznaczonych klauzulą tajności „poufne” następującej osobie:

19. Imię (imiona)
20. Nazwisko (w tym przybrane)
21. Nr PESEL
22. Imię ojca
23. Imię matki
24. Nazwisko rodowe matki
25. Data urodzenia
26. Miejsce urodzenia

.....
Pieczątka i podpis kierownika jednostki organizacyjnej

.....
/miejsowość, data/

.....
/imię i nazwisko/

.....
/stanowisko/

O Ś W I A D C Z E N I E

Zgodnie z art. 20 ust.1 ustawy o ochronie informacji niejawnych (Dz.U.Nr 182 z 2010r. ,poz.1228) oświadczam, iż w dniuzostałem/am zapoznany/a z przepisami o ochronie informacji niejawnych.

.....
/data i czytelny podpis/

DOKUMENT NIEELEKTRONICZNY

NA KAŻDEJ STRONIE

Z A S T R Z E Ż O N E

Egz.Nr.....
Egz.pojedynczy

W lewym górnym rogu signature literowo – cyfrową , na którą składają się :

- Literowe oznaczenie jednostki lub komórki
- Symbol oznaczenia klauzuli
- Numer, pod którym dokument ten został zarejestrowany w odpowiedniej ewidencji i rok lub dwie ostatnie cyfry roku , w którym dokonano rejestracji:
- W zależności od potrzeb inne oznaczenia ułatwiające ustalenie miejsca jego wykonania w jednostce lub komórce organizacyjnej lub też przynależność dokumentu do określonej sprawy

Z A S T R Z E Ż O N E

strona/liczba stron całego dokumentu

DOKUMENT NIEELEKTRONICZNY

NA PIERWSZEJ STRONIE

nazwę jednostki lub komórki organizacyjnej,
w lewym górnym rogu , nad sygnaturą
literowo- cyfrową

nazwę miejscowości i datę
podpisania dokumentu, w prawym
górnym rogu, powyżej nr egz. lub napisu
„ egz. pojedynczy”

adresat – a w przypadku
dokumentu, któremu nadano bieg
korespondencyjny, pod nr egz.
w kolejności pionowej:
imię i nazwisko lub nazwa stanowiska
Jeśli adresatów jest wielu ,dopuszcza się
możliwość wpisu „ adresaci wg
rozdzielnika”

DOKUMENT NIEELEKTRONICZNY

NA OSTATNIEJ STRONIE

- Liczba załączników
- Liczba stron lub innych jednostek miary wszystkich załączników
- Klauzule tajności załączników wraz z numerami, pod jakimi zostały zarejestrowane w odpowiedniej ewidencji oraz liczbę stron każdego załącznika lub informację określającą rodzaj załączonego materiału i jego odpowiednią jednostkę miary
- W przypadku gdy adresatowi wysyła się inną liczbę załączników niż pozostawia w aktach, dodatkowo napis „ TYLKO ADRESAT „jeżeli załączniki mają być przekazane adresatowi bez pozostawienia ich w aktach
- Napis „ DO ZWROTU „ - jeżeli załączniki mają zostać zwrócone osobie uprawnionej do jego podpisania;

Stanowisko i imie osoby uprawnionej
do podpisania dokumentu

- Liczba egzemplarzy
- Adresaci poszczególnych egzemplarzy/ lub adnotację „ adresaci wg rozdzielnika „
- Imię i nazwisko lub inne dane identyfikujące wykonawcę

INSTRUKCJE ALARMOWE

XVII

INSTRUKCJA ALARMOWA W PRZYPADKU ZGŁOSZENIA O PODŁOŻENIU LUB ZNALEZIENIU ŁADUNKU WYBUCHOWEGO W URZĘDZIE.

I. 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:
 - Kierownika obiektu lub jego zastępcę;
 - Policję.
2. Zawiadamiając Policję należy podać:
 - Treść rozmowy ze zgłaszającym o podłożeniu ładunku wybuchowego, którą należy prowadzić wg poniższych wskazówek ;
 - miejsce i opis zlokalizowanego przedmiotu, który może być ładunkiem wybuchowym;
 - numer telefonu, z którego prowadzona jest rozmowa i swoje stanowisko;
 - uzyskać od policji potwierdzenie przyjętego powyższego zawiadomienia.

II. AKCJA POSZUKIWAWCZA ŁADUNKU WYBUCHOWEGO PO UZYSKANIU INFORMACJI O JEGO PODŁOŻENIU

1. Do czasu przybycia Policji akcją kieruje administrator obiektu, a w czasie jego nieobecności osoba przez niego upoważniona ,
 2. Kierujący akcją zarządza, aby użytkownicy pomieszczeń dokonali sprawdzenia , czy w tych pomieszczeniach znajdują się :
 - przedmioty rzeczy lub urządzenia , paczki itp. , których wcześniej nie było i nie wnieśli ich użytkownicy pomieszczeń (np. interesanci);
 - ślady przemieszczania elementów wyposażenia pomieszczeń
 - 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, halle, windy, toalety, piwnice, strychy itp. Oraz najbliższe otoczenie zewnętrzne obiektu powinno być sprawdzone przez pracowników obsługi administracyjnej lub ochrony .
 4. Zlokalizowanych przedmiotów , rzeczy, urządzeń , których – w ocenie użytkowników obiektu – przedtem nie było , a zachodzi podejrzenie, iż mogą to być ładunki wybuchowe , nie wolno dotykać. O ich umiejscowieniu należy natychmiast powiadomić administratora obiektu i policję .
-

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:

- Umieścić tę przesyłkę w grubym worku plastikowym, szczelnie zamknąć,
- Worek ten należy umieścić w drugim plastikowym worku, szczelnie należy zamknąć, zawiązać supeł i zakleić taśmą klejącą,
- Paczki nie należy przemieszczać. Należy pozostawić ją na miejscu,
- Powiadomić:

policję –nr 997; tel.kom.112,

lub

straż pożarną- nr 998.

Śłużby te podejmą wszystkie niezbędne kroki w celu bezpiecznego przejęcia przesyłki.

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

Należy:

- Nie naruszać tej zawartości
Nie rozsypywać, nie przenosić, nie dotykać, nie wachać nie powodować ruchu powietrza w pomieszczeniu (wyłączyć systemy wentylacji i klimatyzacji, zamknąć okna),
- Całą zawartość umieścić w worku plastikowym, zamknąć go i zakleić taśmą lub plastrem.
- Dokładnie umyć ręce,
- Zaklejony worek umieścić w drugim worku, zamknąć go i zakleić.
- Ponownie umyć ręce.
- Powiadomić:

policję –nr 997; tel.kom.112,

lub

straż pożarną- nr 998.

**PO PRZYBYCIU WŁAŚCIWYCH SŁUŻB NALEŻY BEZWZGLĘDNI
STOSOWAĆ SIĘ DO ICH ZALECEŃ.**

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 decyzję ewakuacji osób z zagrożonego obiektu przed przybyciem policji.
6. Należy zachować spokój i opanowanie , aby nie dopuścić do przejawów paniki.

III. WSPÓLPRACA Z POLICJĄ W CZASIE AKCJI

1. Po przybyciu do obiektu policjanta lub policyjnej grupy interwencyjnej administrator obiektu powinien przekazać im wszelkie informacje dotyczące zdarzenia oraz wskazać miejsca zlokalizowanych przedmiotów, rzeczy, urządzeń obcego pochodzenia i punkty newralgiczne w obiekcie.
2. Policjant lub dowódca grupy policjantów przejmuje kierowanie akcją , a administrator obiektu winien udzielić mu wszechstronnej pomocy podczas jej prowadzenia.
3. Na wniosek policjanta, kierującego akcją, administrator obiektu podejmuje decyzje 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 administratorowi.

IV. POSTANOWIENIA KOŃCOWE DOTYCZĄCE DZIAŁAŃ W PRZYPADKU ZGŁOSZENIA O PODŁOŻENIU ŁADUNKU WYBUCHOWEGO .

1. Osobom przyjmującym zgłoszenie o podłożeniu ładunku wybuchowego oraz administratorowi obiektu nie wolno lekceważyć żadnej informacji na ten temat i każdorazowo powinni powiadamiać o tym policję, która z urzędu dokona sprawdzenia wiarygodności każdego zgłoszenia.
 2. Administrator obiektu powinien na bieżąco organizować szkolenie pracowników w zakresie sposobu zachowania w sytuacjach wymienionej w tej części planu oraz winien znać rozmieszczenie newralgicznych punktów- węzły energetyczne i wodne, które udostępnia się na żądanie policjanta kierującego akcją.
 3. Z informacjami tej części planu powinni być zapoznani wszyscy pracownicy urzędu.
-