

Z a r z ą d z e n i e nr 14/2011

**Starosty Grudziądzkiego
z dnia 14 listopada 2011 r.**

**w sprawie rejestrowania, przechowywania, obiegu i wydawania
materiałów niejawnych o klauzuli „poufne” i „zastrzeżone”.**

Na podstawie art. 43 ust.2 ustawy z dnia 05 sierpnia 2010 roku o ochronie informacji
niejawnych (Dz. U. nr 182, poz. 1228)

zarządzam, co następuje:

§ 1

Dla dokumentów zawierających informacje niejawne oznaczone klauzulą „poufne” lub „zastrzeżone” tworzy się kancelarię zwaną dalej „Kancelarią dokumentów niejawnych” w pomieszczeniu Nr 29 Starostwa Powiatowego.

§ 2

Na kierownika kancelarii wyznaczam inspektora Wydziału Organizacyjnego, Panią Agnieszkę Zawadka, która w zakresie wykonywania obowiązków podlegać będzie bezpośrednio pełnomocnikowi ds. ochrony informacji niejawnych.

§ 3

Kierownik kancelarii odpowiada za właściwe rejestrowanie, przechowywanie, obieg i wydawanie dokumentów uprawnionym do tego pracownikom.

§ 4

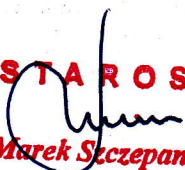
Sposób i tryb przetwarzania informacji niejawnych o klauzuli „poufne” określa „Instrukcja w zakresie sposobu i trybu przetwarzania informacji niejawnych o klauzuli poufne”, stanowiąca załącznik nr 1 do zarządzenia.

§ 5

Sposób i tryb przetwarzania informacji niejawnych o klauzuli „zastrzeżone” określa „Instrukcja w zakresie sposobu i trybu przetwarzania informacji niejawnych o klauzuli zastrzeżone”, stanowiąca załącznik nr 2 do zarządzenia.

§ 6

Zarządzenie wchodzi w życie z dniem podpisania.

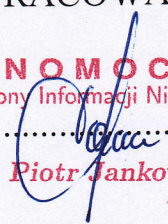
STAROSTA

Marek Szczepanowski

STAROSTWO POWIATOWE W GRUDZIĄDZU

STAROSTA
Marek Szczepanowski**ZATWIERDZAM**

**INSTRUKCJA
W ZAKRESIE SPOSOBU I TRYBU PRZETWARZANIA
INFORMACJI NIEJAWNYCH O KALUZULI
„POUFNE”**

OPRACOWAŁ:

PEŁNOMOCNIK
ds. Ochrony Informacji Niejawnych.....

mgr Piotr Jankowski-----
GRUDZIĄDZ 2011 R.

1. Podstawy prawne, informacje ogólne.

1. Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182 poz. 1228).
2. Pozostałe, wybrane akty prawne regulujące ochronę informacji niejawnych (obowiązują do czasu wydania nowych w 2011 r.):

- Rozporządzenie Rady Ministrów z dnia 1 czerwca 2010 r. w sprawie organizacji i funkcjonowania kancelarii tajnych (Dz. U. Nr 114, poz. 765);
- 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. Nr 159, poz. 1069);
- Rozporządzenie Prezesa Rady Ministrów z dnia 29 września 2005 r. w sprawie trybu i sposobu przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne (Dz. U. Nr 200 poz. 1650); **Zmiany:** rozporządzenie Prezesa RM z 15.12.2008 r. (Dz. U. Nr 25 poz. 1491);
- Rozporządzenie Prezesa Rady Ministrów z dnia 25 sierpnia 2005 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. Nr 171 poz. 1433);

3. Zakres rzeczowy informacji poufnych określa art.5.3 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych:

Informacjom niejawnym nadaje się klauzulę „poufne”, jeżeli ich nieuprawnione ujawnienie spowoduje szkodę dla Rzeczypospolitej Polskiej przez to, że:

- utrudni prowadzenie bieżącej polityki zagranicznej Rzeczypospolitej Polskiej;
- utrudni realizację przedsięwzięć obronnych lub negatywnie wpłynie na zdolność bojową Sił Zbrojnych Rzeczypospolitej Polskiej;
- zakłóci porządek publiczny lub zagrazi bezpieczeństwu obywateli;
- utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę bezpieczeństwa lub podstawowych interesów Rzeczypospolitej Polskiej;
- utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę porządku publicznego, bezpieczeństwa obywateli lub ściganie sprawców przestępstw i przestępstw skarbowych oraz organom wymiaru sprawiedliwości;
- zagrazi stabilności systemu finansowego Rzeczypospolitej Polskiej;
- wpłynie niekorzystnie na funkcjonowanie gospodarki narodowej.

4. Uprawnienia do dostępu do informacji poufnych posiadają osoby, które uzyskały poświadczenie bezpieczeństwa upoważniające do postępu do informacji niejawnych oznaczonych klauzulą „poufne” lub wyższą.

2. Fizyczna ochrona informacji niejawnych oznaczonych klauzulą „poufne”

1. Organizacja pracy osoby odpowiedzialnej za prowadzenie ewidencji i przechowywanie dokumentów oznaczonych klauzulą „POUFNE” winna zapewnić możliwość ustalenia w każdych warunkach i okolicznościach, gdzie znajdują się dokumenty niejawne pozostające w dyspozycji jednostki organizacyjnej oraz kto z tymi dokumentami się zapoznał.
2. Dokumenty i materiały oznaczone klauzulą „POUFNE”, można udostępniać wyłącznie osobom legitymującą się posiadaniem ważnym Poświadczeniem Bezpieczeństwa dopuszczającym do pracy z dokumentami niejawnymi o klauzuli „poufne”, lub wyższej.
3. Dokumenty i materiały oznaczone klauzulą „POUFNE” są przyjmowane, rejestrowane, udostępniane, przechowywane i wysyłane przez upoważnioną na piśmie osobę. Osoba ta winna legitymować się posiadaniem ważnym Poświadczeniem Bezpieczeństwa dopuszczającym do pracy z dokumentami niejawnymi o klauzuli „poufne”, lub wyższej.
4. Pracownik jednostki organizacyjnej upoważniony do odbioru przesyłek, po stwierdzeniu że jest ona niejawna, niezwłocznie przekazuje ją upoważnionej osobie prowadzącej specjalnie wydzieloną do tego celu kancelarię.
5. Dokumenty zawierające informacje niejawne oznaczone klauzulą „poufne”, rejestruje się, przechowuje i zabezpiecza w „Kancelarii dokumentów niejawnych” pokój nr 29, znajdującej się w strefie ochronnej, w szafie metalowej z zamkami o skomplikowanym mechanizmie, posiadającej odpowiedni certyfikat.
6. W toku postępowania z dokumentami oznaczonymi klauzulą „POUFNE” prowadzi się „Dziennik ewidencji” przeznaczony do rejestracji korespondencji oraz „Rejestr dzienników, książek ewidencyjnych i teczek.
7. W przypadkach uzasadnionych, kierownik jednostki organizacyjnej może wyrazić zgodę na przechowywanie dokumentów poza kancelarią, pod warunkiem spełnienia wymogów bezpieczeństwa odpowiednich dla dokumentów niejawnych o klauzuli „poufne”.
8. Obieg dokumentacji „poufnej” musi odbywać się w sposób zabezpieczający ją przed wglądem osób nieupoważnionych. Przenoszenie dokumentów do innych pomieszczeń w toku ich opracowywania lub zapoznawania się z nimi odbywa się w zamykanych teczkach kartonowych lub nieprzezroczystych kopertach zabezpieczających te dokumenty przed wglądem osób nieuprawnionych.
9. Wytwarzając dokumenty drukowane należy posługiwać się do tego celu wydzieloną maszyną do pisania, znajdującą się w „Kancelarii dokumentów niejawnych”, w strefie ochronnej. Zabrania się wykorzystania do tego celu techniki komputerowej.

3. Przyznawanie uprawnień do dostępu do informacji niejawnych oznaczonych klauzulą „POUFNE”

1. Informacje niejawne, którym nadano określoną klauzulę tajności:
 - mogą być udostępnione wyłącznie osobie uprawnionej, zgodnie z przepisami ustawy dotyczącymi dostępu do określonej klauzuli tajności;
 - muszą być przetwarzane w warunkach uniemożliwiających ich nieuprawnione ujawnienie;
 - muszą być chronione, odpowiednio do nadanej klauzuli tajności.
2. Informacje niejawne mogą być udostępnione wyłącznie osobie dającej rękojmię zachowania tajemnicy i tylko w zakresie niezbędnym do wykonywania przez nią pracy lub pełnienia służby na zajmowanym stanowisku albo wykonywania czynności zleconych.
3. Dopuszczenie do pracy z dostępem danej osoby do informacji niejawnych o klauzuli „Poufne” może nastąpić po:
 - uzyskaniu poświadczenia bezpieczeństwa;
 - odbyciu szkolenia w zakresie ochrony informacji niejawnych.
4. Poświadczenie bezpieczeństwa wydaje pracownikowi Pełnomocnik Ochrony Informacji Niejawnych po przeprowadzeniu zwykłego postępowania sprawdzającego prowadzonego na pisemny wniosek kierownika jednostki organizacyjnej.
 - upływu ważności dotychczas posiadanego poświadczenia bezpieczeństwa.
5. Pisemne upoważnienie, o którym mowa wyżej, wydawane jest po odbyciu obowiązkowego szkolenia w zakresie ochrony informacji niejawnych. Szkolenie przeprowadza Pełnomocnik a ds. Ochrony Informacji Niejawnych w Starostwie Powiatowym.
6. Poświadczenie bezpieczeństwa w przypadku dostępu do informacji niejawnych o klauzuli „poufne” wydaje się na okres 10 lat. Uprawnia ono do dostępu do informacji niejawnych o niższej klasie czyli do informacji niejawnych o klauzuli „zastrzeżone”
7. Szkolenie w zakresie ochrony informacji niejawnych przeprowadza się w celu zapoznania z:
 - przepisami dotyczącymi ochrony informacji niejawnych oraz odpowiedzialności karnej, dyscyplinarnej i służbowej za ich naruszenie, w szczególności za nieuprawnione ujawnienie informacji niejawnych,
 - niezbędnym do wykonywania pracy lub pełnienia służby, z uwzględnieniem zasad zarządzania ryzykiem bezpieczeństwa informacji niejawnych, w szczególności szacowania ryzyka,
 - sposobami ochrony informacji niejawnych oraz postępowania w sytuacjach zagrożenia dla takich informacji lub w przypadku ich ujawnienia.
8. Szkolenie, o którym mowa wyżej, kończy się wydaniem zaświadczenia. Odbierając zaświadczenie, osoba przeszkolona składa pisemne oświadczenie o zapoznaniu się z przepisami o ochronie informacji niejawnych. Szkolenie przeprowadza się nie rzadziej niż raz na 5 lat.

4. Zasady sporządzania i wysyłania dokumentów niejawnych.

A. Sporządzanie dokumentów „poufnych”

Nazwa jednostki organizacji

Kolejny numer z dziennika ewidencji

OR.- Pf- / 2011

Skrót klauzuli tajności

Grudziądz, dnia 27.04.2011 r.
POUFNE
Egz. nr....//Egz. pojedynczy

„Jawne po odłączeniu załączników” – na każdej stronie
„.....(nazwa klauzuli tajności) po odłączeniu załączników „ na każdej stronie

„udzielenie informacji tylko za pisemną zgodą nadawcy”
„kopiowanie tylko za pisemną zgodą nadawcy”
„odpis tylko za pisemną zgodą nadawcy”
„kopiowanie od...do... tylko za pisemną zgodą nadawcy”
„odpis od...do... tylko za pisemną zgodą nadawcy”
„wypis (wyciąg) od...do... tylko za pisemną zgodą nadawcy”
„podlega ochronie do...” (jeżeli został określony krótszy okres ochrony niż ten wynikający z klauzuli tajności)

lub „adresaci według rozdzielnika”

**Dyrektor
WBZK
Bydgoszcz**

TREŚĆ PISMA

Liczba stron lub innych jednostek miary wszystkich załączników

Kolejny numer z dziennika ewidencji

„tylko adresat” – w przypadku gdy adresatowi wysła się inną liczbę załączników, niż pozostawia w aktach „do zwrotu” – jeżeli w załączniku mają zostać zwrócone osobie **uprawnionej do jego podpisania**

Załączników:.....str.

Zał. nr.....- klauzula tajności:...../11.....str.....

Skrót klauzuli tajności Pf

Liczba stron załącznika lub informacji określająca rodzaj załączonego materiału i jego odpowiednią jednostkę miary

**Starosta
Marek Szczepanowski**

Wykonano w.....egz. /Egz. pojedynczy

Egz. nr.1 – adresat

Egz. nr.2 – a/a

Sporządził:.....

Wykonał:.....

lub „adresaci według rozdzielnika”

imię i nazwisko lub inne dane identyfikujące sporządzającego i wykonawcę

OR.- Pf-/ 2011

Kolejny numer z
dziennika ewidencji

Skrót klauzuli tajności

Załącznik nr.....do pisma nr.....z dnia.....

POUFNE

Egz. nr..../ Egz. pojedynczy

TREŚĆ DOKUMENTU

Starosta

Marek Szczepanowski

Wykonano w.....egz. /Egz. pojedynczy

Egz. nr.1 – adresat

lub „adresaci według rozdzielnika”

Egz. nr.2 – a/a

Sporządził:.....

Wykonał:.....

imię i nazwisko lub inne dane identyfikujące
sporządzającego i wykonawcę

KLAUZULA TAJNOŚCI

numer strony/liczba stron całego pisma

B. Wysyłanie dokumentów niejawnych.

Do momentu wydani nowego rozporządzenia w sprawie trybu i sposobu przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne stosuje się zapisy dotychczasowego rozporządzenia.

Materiały zawierające informacje niejawne powinny być opakowane w dwie nieprzezroczyste i mocne koperty, przy czym na kopertach muszą być umieszczone:

- 1) na wewnętrznej:
 - a) klauzula tajności i ewentualne dodatkowe oznaczenia,
 - b) imienne określenie adresata,
 - c) imię, nazwisko i podpis osoby pakującej,
 - d) numer, pod którym dokument został zarejestrowany w dzienniku rejestracji dokumentów,
- 2) na zewnętrznej:
 - a) nazwa jednostki organizacyjnej adresata,
 - b) adres siedziby adresata,
 - c) numer wykazu i pozycji w wykazie przesyłek nadanych,
 - d) nazwa jednostki organizacyjnej nadawcy.

Miejsca sklejenia każdej koperty zabezpiecza się przez odcisnięcie pieczęci „do pakietów” i za pomocą przezroczystej taśmy samoprzylepnej, przy czym na kopercie zewnętrznej, zamiast tej taśmy, może być stosowana pieczęć odcisnięta w substancji zapewniającej jej trwały odcisk.

Przesyłki wysyłane za pośrednictwem „Poczty Polskiej” oraz innych podmiotów prowadzących działalność w zakresie usług pocztowych, przekazuje się je jako przesyłki polecone lub z zadeklarowaną wartością.

Wzór wewnętrznego oznaczenia opakowania przesyłki niejawnej

.....
(numer, pod którym dokument
został zarejestrowany w
odpowiednim dzienniku oraz
kod, miejscowość i nazwa nadawcy)

.....
(klauzula tajności)

Dyrektor Wydziału
Bezpieczeństwa i Zarządzania Kryzysowego
Bydgoszcz

Pakował

.....
Jan Kowalski

5.Odpowiedzialność karna i dyscyplinarna

51

Ustawa o ochronie informacji niejawnych nie zawiera przepisów dotyczących odpowiedzialności z tytułu nieuprawnionego przekazania komuś informacji niejawnych. Uznano, iż tę kwestię, a w szczególności prawno - karne skutki nieuprawnionego ujawnienia informacji niejawnych reguluje w sposób dostateczny kodeks karny (ustawa z dnia 06.06.1997 r., Dz. U. Nr 88, poz. 553, z późn. zm.) w Rozdziale XXXIII „przestępstwa przeciwko ochronie informacji niejawnych”.

Art 265

§ 1. Kto ujawnia lub wbrew przepisom ustawy wykorzystuje informacje niejawne o klauzuli „tajne” lub „ściśle tajne”, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 2. Jeżeli informację określoną w § 1 ujawniono osobie działającej w imieniu lub na rzecz podmiotu zagranicznego, sprawca podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

§ 3. Kto nieumyślnie ujawnia informację określoną w § 1, z którą zapoznał się w związku z pełnieniem funkcji publicznej lub otrzymanym upoważnieniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

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.

§ 3. Ściganie przestępstwa określonego w § 1 następuje na wniosek pokrzywdzonego.

Art 267

§ 1. Kto bez uprawnienia uzyskuje informację dla niego nie przeznaczoną, otwierając zamknięte pismo, podłączając się do przewodu służącego do przekazywania informacji lub przełamując elektroniczne, magnetyczne albo inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem specjalnym.

§ 3. Tej samej karze podlega, kto informację uzyskaną w sposób określony w § 1 lub 2 ujawnia innej osobie.

§ 4. Ściganie przestępstwa określonego w § 1-3 następuje na wniosek pokrzywdzonego.

Art. 268

§ 1. Kto nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Jeżeli czyn określony § 1 dotyczy zapisu na komputerowym nośniku informacji, sprawca podlega karze pozbawienia wolności do lat 3.

§ 3. Kto dopuszczając się czynu określonego w § 1 lub 2, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 4. Ściganie przestępstwa określonego w § 1-3 następuje na wniosek pokrzywdzonego.

Art. 268a

§ 1. Kto nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności do lat 3.

§ 2. Kto, dopuszczając się czynu określonego w § 1, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 3. Ściganie przestępstwa określonego w § 1 lub 2 następuje na wniosek pokrzywdzonego.

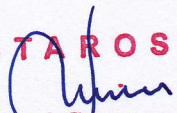
Art. 269

§ 1. Kto, niszczy, uszkadza, usuwa lub zmienia dane informatyczne o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego albo zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

§ 2. Tej samej karze podlega, kto dopuszcza się czynu określonego w § 1, niszcząc albo wymieniając nośnik informacji lub niszcząc albo uszkadzając urządzenie służące automatycznemu przetwarzaniu, gromadzeniu lub przekazywaniu danych informatycznych.

STAROSTWO POWIATOWE W GRUDZIĄDZU

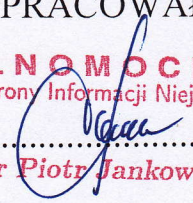
ZATWIERDZAM

STAROSTA

Marek Szczepanowski

INSTRUKCJA
W ZAKRESIE SPOSOBU I TRYBU PRZETWARZANIA
INFORMACJI NIEJAWNYCH O KALUZULI
„ZASTRZEŻONE”

OPRACOWAŁ:

PEŁNOMOCNIK
ds. Ochrony Informacji Niejawnych


mgr Piotr Jankowski

1. Podstawy prawne, informacje ogólne.

1. Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182 poz. 1228).
2. Pozostałe, wybrane akty prawne regulujące ochronę informacji niejawnych (obowiązują do czasu wydania nowych w 2011 r.):
 - Rozporządzenie Rady Ministrów z dnia 1 czerwca 2010 r. w sprawie organizacji i funkcjonowania kancelarii tajnych (Dz. U. Nr 114, poz. 765);
 - 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. Nr 159, poz. 1069);
 - Rozporządzenie Prezesa Rady Ministrów z dnia 29 września 2005 r. w sprawie trybu i sposobu przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne (Dz. U. Nr 200 poz. 1650); **Zmiany:** rozporządzenie Prezesa RM z 15.12.2008 r. (Dz. U. Nr 25 poz. 1491);
 - Rozporządzenie Prezesa Rady Ministrów z dnia 25 sierpnia 2005 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. Nr 171 poz. 1433);

3. Zakres rzeczowy informacji zastrzeżonych określa art. 5.4 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych:

„Informacjom niejawnym nadaje się klauzulę „zastrzeżone”, jeżeli nie nadano im wyższej klauzuli, 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”

4. Uprawnienia do dostępu do informacji zastrzeżonych posiadają osoby, które uzyskały poświadczenie bezpieczeństwa upoważniające do postępu do informacji niejawnych oznaczonych klauzulą „zastrzeżone” lub wyższą.

2. Fizyczna ochrona informacji niejawnych oznaczonych klauzulą „zastrzeżone”

1. Organizacja pracy osoby odpowiedzialnej za prowadzenie ewidencji i przechowywanie dokumentów oznaczonych klauzulą „ZASTRZEŻONE” winna zapewnić możliwość ustalenia w każdych warunkach i okolicznościach, gdzie znajdują się dokumenty niejawne pozostające w dyspozycji jednostki organizacyjnej oraz kto z tymi dokumentami się zapoznał.
2. Dokumenty i materiały oznaczone klauzulą „zastrzeżone” rejestruje się, przechowuje i zabezpiecza w „Kancelarii dokumentów niejawnych” pokój nr 29 przez wyznaczoną osobę zwaną kierownikiem kancelarii. Osoba ta winna legitymować się posiadaniem ważnym Poświadczeniem bezpieczeństwa lub pisemnym upoważnieniem do dostępu do informacji niejawnych oznaczonych klauzulą „zastrzeżone”.
3. W toku postępowania z dokumentami oznaczonymi klauzulą „zastrzeżone” prowadzi się „Dziennik ewidencji” przeznaczony do rejestracji korespondencji oraz „Rejestr dzienników, książek ewidencyjnych i teczek”.

4. Dokumenty o klauzuli „zastrzeżone” przechowywane są w „Kancelarii dokumentów niejawnych” lub w komórce merytorycznej posiadającej odpowiednie warunki przechowywania.
5. Czasowe udostępnianie dokumentacji zastrzeżonej osobom upoważnionym, w ramach komórki organizacyjnej i między komórkami organizacyjnymi odbywa się bezpośrednio, za pokwitowaniem osobie, która nimi dysponuje.
6. Obieg dokumentacji zastrzeżonej musi odbywać się w sposób zabezpieczający ją przed wglądem osób nieupoważnionych.
7. Przenoszenie dokumentów o klauzuli „zastrzeżone” do innych pomieszczeń w toku ich opracowywania lub zapoznawania się z nimi odbywa się w zamykanych teczkach kartonowych lub nieprzezroczystych kopertach zabezpieczających te dokumenty przed wglądem osób nieuprawnionych.
8. Dokumentację zastrzeżoną po zakończeniu pracy przechowuje się w sposób zabezpieczający ją przed wglądem osób nieupoważnionych, tj. w zamykanych na klucz meblach biurowych.

Zaleca się, aby dokumenty oznaczone klauzulą „zastrzeżone” nie były przechowywane luzem, lecz wpinane do odpowiednio opisanego segregatora lub skoroszytu.

3. Przyznawanie uprawnień do dostępu do informacji niejawnych oznaczonych klauzulą „zastrzeżone”

1. Informacje niejawne, którym nadano określoną klauzulę tajności:

- mogą być udostępnione wyłącznie osobie uprawnionej, zgodnie z przepisami ustawy dotyczącymi dostępu do określonej klauzuli tajności;
- muszą być przetwarzane w warunkach uniemożliwiających ich nieuprawnione ujawnienie;
- muszą być chronione, odpowiednio do nadanej klauzuli tajności.

2. Informacje niejawne mogą być udostępnione wyłącznie osobie dającej rękojmię zachowania tajemnicy i tylko w zakresie niezbędnym do wykonywania przez nią pracy lub pełnienia służby na zajmowanym stanowisku albo wykonywania czynności zleconych.

3. Dopuszczenie do pracy lub zlecenie prac związanych z dostępem danej osoby do informacji niejawnych o klauzuli „zastrzeżone” może nastąpić po:

- pisemnym upoważnieniu wydanym przez Starostę, jeżeli osoba ta nie posiada ważnego poświadczenia bezpieczeństwa;
- odbyciu szkolenia w zakresie ochrony informacji niejawnych.

4. Starosta udziela pisemnego upoważnienia do dostępu do informacji niejawnych oznaczonych klauzulą „zastrzeżone” na wniosek osoby zainteresowanej w przypadku:

- wykonywania na podstawie przepisów prawa zadań związanych z dostępem do informacji niejawnych,
- wpływu ważności dotychczas posiadanego poświadczenia bezpieczeństwa.

5. Pisemne upoważnienie, o którym mowa wyżej, wydawane jest po odbyciu obowiązkowego szkolenia w zakresie ochrony informacji niejawnych. Szkolenie przeprowadza Pełnomocnik ds. Ochrony Informacji Niejawnych w Starostwie Powiatowym.

6. Szkolenie w zakresie ochrony informacji niejawnych przeprowadza się w celu zapoznania z:

- przepisami dotyczącymi ochrony informacji niejawnych oraz odpowiedzialności karnej, dyscyplinarnej i służbowej za ich naruszenie, w szczególności za nieuprawnione ujawnienie informacji niejawnych,
- niezbędnym do wykonywania pracy lub pełnienia służby, z uwzględnieniem zasad zarządzania ryzykiem bezpieczeństwa informacji niejawnych, w szczególności szacowania ryzyka,
- sposobami ochrony informacji niejawnych oraz postępowania w sytuacjach zagrożenia dla takich informacji lub w przypadku ich ujawnienia.

7. Szkolenie, o którym mowa wyżej, kończy się wydaniem zaświadczenia. Odbierając zaświadczenie, osoba przeszkolona składa pisemne oświadczenie o zapoznaniu się z przepisami o ochronie informacji niejawnych.

8. Upoważnienie do dostępu do informacji niejawnych oznaczanych klauzulą „zastrzeżone” oraz zaświadczenie stwierdzające odbycie szkolenia w powyższym zakresie wydawane są na okres 5 letni.

4. Zasady sporządzania i wysyłania dokumentów „zastrzeżone”

A. Sporządzanie dokumentów „zastrzeżonych”

Nazwa jednostki
organizacji

Kolejny numer z
dziennika ewidencji

OR.- Z - / 2011

Skrót klauzuli tajności

Grudziądz, dnia 27.04.2011 r.

Zastrzeżone

Egz. nr....//Egz. pojedynczy

„Jawne po odłączeniu załączników” – na każdej stronie

„.....(nazwa klauzuli tajności) po odłączeniu załączników „ na
każdej stronie

„udzielenie informacji tylko za pisemną zgodą nadawcy”

„odpis tylko za pisemną zgodą nadawcy”

„kopiowanie od...do... tylko za pisemną zgodą nadawcy”

„odpis od...do... tylko za pisemną zgodą nadawcy”

„wypis (wyciąg) od...do... tylko za pisemną zgodą nadawcy”

„podlega ochronie do...” (jeżeli został określony krótszy okres
ochrony niż ten wynikający z klauzuli tajności)

Lub „adresaci według rozdzielnika”

**Dyrektor
W B Z K
Bydgoszcz**

TREŚĆ PISMA

Liczba stron lub innych
jednostek miary
wszystkich załączników

Załączników:.....str.

Kolejny numer z dziennika
ewidencji

Zał. nr.....- klauzula tajności: Z -...../11.....str.....

Skrót klauzuli tajności Z.

„tylko adresat” – w przypadku gdy adresatowi wysyła
się inną liczbę załączników, niż pozostawia w aktach
„do zwrotu” – jeżeli w załączniku mają zostać
zwrócone osobie **uprawnionej do jego podpisania**

Liczba stron załącznika lub informacji określająca rodzaj
załączonego materiału i jego odpowiednią jednostkę miary

**Starosta
Marek Szczepanowski**

Wykonano w.....egz. /Egz. pojedynczy

Egz. nr.1 – adresat

Egz. nr.2 – a/a

lub „adresaci według rozdzielnika”

Sporządził:.....

Wykonał:....

Kolejny numer z
dziennika ewidencji

ię i nazwisko lub inne dane identyfikujące
sporządzającego i wykonawcę

pisma nr.....z dnia.....

OR. Z- / 2011

Skrót klauzuli tajności

Zastrzeżone

Egz. nr.... / Egz. pojedynczy

TREŚĆ DOKUMENTU

Starosta
Marek Szczepanowski

Wykonano w.....egz. /Egz. pojedynczy

Egz. nr.1 – adresat

lub „adresaci według rozdzielnika”

Egz. nr.2 – a/a

Sporządził:.....

Wykonał:.....

imię i nazwisko lub inne dane identyfikujące
sporządzającego i wykonawcę

B. Wysyłanie dokumentów niejawnych.

Do momentu wydania nowego rozporządzenia w sprawie trybu i sposobu przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne stosuje się zapisy dotychczasowego rozporządzenia.

Materiały zawierające informacje niejawne powinny być opakowane w dwie nieprzezroczyste i mocne koperty, przy czym na kopertach muszą być umieszczone:

- 1) na wewnętrznej:
 - a) klauzula tajności i ewentualne dodatkowe oznaczenia,
 - b) imienne określenie adresata,
 - c) imię, nazwisko i podpis osoby pakującej,
 - d) numer, pod którym dokument został zarejestrowany w dzienniku rejestracji dokumentów,
- 2) na zewnętrznej:
 - a) nazwa jednostki organizacyjnej adresata,
 - b) adres siedziby adresata,
 - c) numer wykazu i pozycji w wykazie przesyłek nadanych,
 - d) nazwa jednostki organizacyjnej nadawcy.

Miejsca sklejenia każdej koperty zabezpiecza się przez odcisnięcie pieczęci „do pakietów” i za pomocą przezroczystej taśmy samoprzylepnej, przy czym na kopercie zewnętrznej, zamiast tej taśmy, może być stosowana pieczęć odcisnięta w substancji zapewniającej jej trwały odcisk.

Przesyłki wysyłane za pośrednictwem „Poczty Polskiej” oraz innych podmiotów prowadzących działalność w zakresie usług pocztowych, przekazuje się je jako przesyłki polecone lub z zadeklarowaną wartością.

Wzór wewnętrznego oznaczenia opakowania przesyłki niejawnej

.....
(numer, pod którym dokument
został zarejestrowany w
odpowiednim dzienniku oraz
kod, miejscowość i nazwa nadawcy)

.....
(klauzula tajności)

Dyrektor Wydziału
Bezpieczeństwa i Zarządzania Kryzysowego
Bydgoszcz

Pakował

.....
Jan Kowalski

5. Wykorzystanie systemu teleinformatycznego do przetwarzania informacji „zastrzeżonych”.

1. W przypadku wykorzystywania techniki komputerowej do wytwarzania, przetwarzania i przechowywania informacji niejawnych opracowuje się dokumentację bezpieczeństwa systemu teleinformatycznego zawierającą:
 - szczególne wymagania bezpieczeństwa systemu informatycznego,
 - procedury bezpieczeństwa informatycznego.
2. Akredytacji bezpieczeństwa teleinformatycznego dla systemu przeznaczonego do przetwarzania informacji niejawnych o klauzuli „zastrzeżone” udziela Starosta jako kierownik jednostki organizacyjnej przez zatwierdzenie dokumentacji bezpieczeństwa teleinformatycznego.
3. Sporządzanie dokumentów „zastrzeżonych” techniką komputerową dopuszczalne jest na wydzielonym w „Kancelarii dokumentów niejawnych” stanowisku komputerowym, na które została udzielona akredytacja.

6. Odpowiedzialność karna i dyscyplinarna

Ustawa o ochronie informacji niejawnych nie zawiera przepisów dotyczących odpowiedzialności z tytułu nieuprawnionego przekazania komuś informacji niejawnych. Uznano, iż tę kwestię, a w szczególności prawno - karne skutki nieuprawnionego ujawnienia informacji niejawnych reguluje w sposób dostateczny kodeks karny (ustawa z dnia 06.06.1997 r., Dz. U. Nr 88, poz. 553, z późn. zm.) w Rozdziale XXXIII „przestępstwa przeciwko ochronie informacji niejawnych”.

Art 265

§ 1. Kto ujawnia lub wbrew przepisom ustawy wykorzystuje informacje niejawne o klauzuli „tajne” lub „ściśle tajne”, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 2. Jeżeli informację określoną w § 1 ujawniono osobie działającej w imieniu lub na rzecz podmiotu zagranicznego, sprawca podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

§ 3. Kto nieumyślnie ujawnia informację określoną w § 1, z którą zapoznał się w związku z pełnieniem funkcji publicznej lub otrzymanym upoważnieniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

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

71
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.

§ 3. Ściganie przestępstwa określonego w § 1 następuje na wniosek pokrzywdzonego.

Art 267

§ 1. Kto bez uprawnienia uzyskuje informację dla niego nie przeznaczoną, otwierając zamknięte pismo, podłączając się do przewodu służącego do przekazywania informacji lub przełamując elektroniczne, magnetyczne albo inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem specjalnym.

§ 3. Tej samej karze podlega, kto informację uzyskaną w sposób określony w § 1 lub 2 ujawnia innej osobie.

§ 4. Ściganie przestępstwa określonego w § 1-3 następuje na wniosek pokrzywdzonego.

Art. 268

§ 1. Kto nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Jeżeli czyn określony § 1 dotyczy zapisu na komputerowym nośniku informacji, sprawca podlega karze pozbawienia wolności do lat 3.

§ 3. Kto dopuszczając się czynu określonego w § 1 lub 2, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 4. Ściganie przestępstwa określonego w § 1-3 następuje na wniosek pokrzywdzonego.

Art. 268a

§ 1. Kto nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności do lat 3.

§ 2. Kto, dopuszczając się czynu określonego w § 1, wyrządza znaczna szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 3. Ściganie przestępstwa określonego w § 1 lub 2 następuje na wniosek pokrzywdzonego.

Art. 269

§ 1. Kto, niszczy, uszkadza, usuwa lub zmienia dane informatyczne o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego albo zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

§ 2. Tej samej karze podlega, kto dopuszcza się czynu określonego w § 1, niszcząc albo wymieniając nośnik informacji lub niszcząc albo uszkadzając urządzenie służące automatycznemu przetwarzaniu, gromadzeniu lub przekazywaniu danych informatycznych.