

Zarządzenie Nr 292/2012

Wójta Gminy w Ozorkowie z dnia 15 czerwca 2012

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

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 (tekst jednolity : Dz. U. z 2001 r. Nr 142, poz.1591, z 2002 r. Nr 23,poz. 220, Nr 62, poz. 558, Nr 113, poz. 984, Nr 153, poz. 1271, Nr 214, poz. 1806, z 2003Nr 80, poz. 717, Nr 162, poz. 1568, z 2004 r. Nr 102, poz. 1055, Nr 116, poz. 1203, Nr 167, poz. 1759,z 2005 r. Nr 172, poz. 1441, Nr 175, poz. 1457, z 2006 r. Nr 17, poz. 128, Nr 181,poz. 1337, z 2007 r. Nr 48, poz. 327, Nr 138, poz. 974, Nr 173, poz. 1218, z 2008 r. Nr 180, poz. 1111, Nr 223, poz. 1458, z 2009 r. Nr 52, poz. 420, z 2010 r. Nr 28, poz. 142 i 146, Nr 40, poz. 230, Nr 106, poz. 675, z 2011 r. Nr 21, poz. 113, Nr 117, poz. 679, Nr 134, poz.777, Nr 149, poz. 887, Nr 217, poz. 1281, z 2012 r. poz. 567),

zarządzam, co następuje:

§ 1. Zatwierdzam Plan Ochrony Informacji Niejawnych w Urzędzie Gminy w Ozorkowie stanowiący załącznik do niniejszego zarządzenia.

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

§ 3. Nadzór nad wykonaniem zarządzenia powierzam Pełnomocnikowi Ochrony Informacji Niejawnych.

§ 4. Zarządzenie wchodzi w życie z dniem podpisania.

Wójt Gminy w Ozorkowie
Władysław Sobolewski -/-

Zatwierdzam

Załącznik Nr 1

.....
/Kierownik Jednostki/

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

OPRACOWAŁ:

*Pełnomocnik Ochrony
Informacji Niejawnych*

Akty prawne związane z ochroną informacji niejawnych

- I. Definicje w rozumieniu Planu Ochrony Informacji Niejawnych**
- II. Ocena zagrożeń zewnętrznych i wewnętrznych**
- III. Przedmiot ochrony**
- IV. Ewidencja informacji niejawnych podlegających ochronie**
- V. Zabezpieczenie informacji niejawnych**
- VI. Dostęp do informacji niejawnych**
- VII. Kancelaria materiałów niejawnych**
- VIII. Zakres udostępniania informacji niejawnych**
- IX. Zasady wykonywania dokumentów niejawnych**
- X. Wykonywanie dokumentów niejawnych z wykorzystaniem sprzętu komputerowego**
- XI. Gromadzenie dokumentów zawierających informacje niejawne**
- XII. Oznaczanie, nadawanie, zmiana i znoszenie klauzuli niejawności materiałom niejawnym**
- XIII. Zasady dostępu do informacji niejawnych**
- XIV. Nadzór w zakresie ochrony informacji niejawnych**
- XV. Odpowiedzialność karna , dyscyplinarna i służbowa za naruszenie przepisów o ochronie informacji niejawnych**
- XVII. Archiwizowanie, gromadzenie i niszczenie materiałów niejawnych**
- XVIII. Przechowywanie kluczy i pieczęci.**

ZAŁĄCZNIKI DO PLANU

1. Sposób oznaczania dokumentów niejawnych oraz umieszczania klauzul na tych dokumentach.
2. Wzory pism i uprawnień.
3. Protokół oceny dokumentacji niearchiwalnej.
4. Spis dokumentacji niearchiwalnej przeznaczonej na makulaturę lub zniszczenie.
5. Protokół komisyjnego zniszczenia dokumentów niearchiwalnych.
6. Wymagania w zakresie ochrony informacji niejawnych stanowiących tajemnice służbową oznaczonych klauzulą „zastrzeżone”.
7. Instrukcja alarmowa w przypadku zgłoszenia o podłożeniu lub znalezieniu ładunku wybuchowego w urzędzie.
8. Instrukcja postępowania w przypadku otrzymania przesyłki niewiadomego pochodzenia.
9. Wzór protokołu otwarcia szafy, sejfu.

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 w sprawie wzorów poświadczeń bezpieczeństwa,

DZIENNIK USTAW Nr 258 z 2010 r., poz. 1751

Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 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 171 z 2005 r., poz. 1433

Rozporządzenie Prezesa Rady Ministrów z dnia 25 sierpnia w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego.

DZIENNIK USTAW Nr 174 z 2005 r., poz., 1447

Rozporządzenie Prezesa Rady Ministrów z dnia 29 sierpnia w sprawie wysokości i trybu pobierania przez służbę ochrony państwa , opłat za przeprowadzenie postępowania bezpieczeństwa przemysłowego, sprawdzeń oraz postępowań sprawdzających.

DZIENNIK USTAW Nr 200 z 2005 r., poz. 1650

Rozporządzenie Prezesa Rady Ministrów z dnia 29 września w sprawie trybu i sposobu przyjmowania , przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne.

DZIENNIK USTAW Nr 159 z 2010 r., poz.1069

Rozporządzenie Prezesa Rady Ministrów z dnia 13 sierpnia w sprawie sposobu oznaczania materiałów, umieszczania na nich klauzul tajności, a także zmiany nadanej klauzuli tajności.

I. DEFINICJE W ROZUMIENIU PLANU OCHRONY INFORMACJI NIEJAWNYCH:

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

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

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.

- 1) rękojmnia zachowania tajemnicy** – jest to zdolność osoby do spełnienia ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem, stwierdzona w wyniku przeprowadzenia postępowania sprawdzającego;
- 2) dokumentem** - jest każda utrwalona informacja niejawna;
- 3) materiałem** - jest dokument lub przedmiot chroniony jako informacja niejawna, przedmiot lub dowolna jego część.
- 4) jednostka organizacyjna** - jest podmiot wymieniony w art. 1 ust. 2 ustawy o ochronie informacji niejawnych;
- 5) 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.);
- 6) sieć teleinformatyczna** - jest organizacyjne i techniczne połączenie systemów teleinformatycznych

7) akredytacja bezpieczeństwa teleinformatycznego - jest dopuszczenie systemu lub sieci teleinformatycznej do wytwarzania, przetwarzania, przechowywania lub przekazywania informacji niejawnych, na zasadach określonych w ustawie;

8) dokumentacja bezpieczeństwa systemu lub sieci informatycznej - są Szczególne Wymagania Bezpieczeństwa oraz Procedury Bezpiecznej Eksploatacji danego systemu lub sieci teleinformatycznej, sporządzone zgodnie z zasadami określonymi w ustawie.

9) ryzykiem – jest kombinacja prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji;

10) szacowaniem ryzyka – jest całościowy proces analizy i oceny ryzyka;

11) zarządzaniem ryzyka – są skoordynowane działania w zakresie zarządzania bezpieczeństwem informacji, z uwzględnieniem ryzyka,

12) kancelaria materiałów niejawnych – wydzielone, wyodrębnione pomieszczenie przeznaczone do ewidencjonowania, opracowywania, przechowywania dokumentów niejawnych oznaczonych klauzulą „poufne”

13) pracownik kancelarii materiałów niejawnych – osoba wyznaczona przez kierownika jednostki do prowadzenia kancelarii materiałów niejawnych.

II. OCENA ZAGROŹEŃ ZEWNĘTRZNYCH I WEWNĘTRZNYCH.

1.1. OCENA ZAGROŹEŃ ZEWNĘTRZNYCH

Zagrożeniami zewnętrznymi dla Urzędu Gminy w Ozorkowie :

- możliwość napadu przez zorganizowane grupy przestępcze i terrorystyczne, działające w sposób profesjonalny, przemyślany i zorganizowany,
- możliwość napadu przez pojedynczych przestępców, możliwość napadu przez przypadkowe osoby wykorzystujące nadarzającą się okazję z powodu nieprawidłowości i ochronie mienia urzędu.

1.2. SYMPTOMY MOGĄCE ŚWIADCZYĆ O PRZYGOTOWANIU NAPADU LUB WŁAMANIA DO BUDYNKU

- wzmożone zainteresowanie osób postronnych obiektem, pomieszczeniem urzędu objawiające się między innymi: podejmowaniem prób uzyskania informacji o danym obiekcie, pomieszczeniu 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 przejawianie zainteresowaniem tym, co się po latach zmieniło,
- interesowaniem się osobami funkcyjnymi, w tym także ich przywarami oraz sposobem wykonywania obowiązków służbowych,
- obserwacja sposobu działania systemu ochronnego, sekretariatu, sprzątaczkę itp.,
- rozpoznawanie systemu technicznych zabezpieczeń, w tym stosowanych urządzeń alarmowych,
- celowe uszkodzanie urządzeń alarmowych, linii telefonicznych, oświetlenia itp.,
- próby pozyskania do grup przestępczych , pracowników urzędu (dotyczy głównie osób mających problemy finansowe, towarzyskie, a także służbowe).

1.3. WNIOSKI:

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

1. systematyczna , skrupulatna i wnikliwa kontrola systemu ochrony przez osoby odpowiedzialne za jego organizację,
2. pracownicy pionu ochrony w czasie dnia pracy powinny zwracać szczególną uwagę na możliwość zaistnienia ewentualnych zagrożeń,
3. stosować zasadę niedopuszczania osób niepowołanych do penetracji strefy bezpieczeństwa,
4. wykonywanie prac porządkowych, remontowych itp. w strefie bezpieczeństwa wyłącznie pod nadzorem osób odpowiedzialnych.

2.1. 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 Gminy celem łatwiejszej pracy grup przestępczych na terenie urzędu,
- próby wglądu w dokumenty niejawne przez osoby nieuprawnione.

2.2. WNIOSKI

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

1. zwracanie szczególnej uwagi na osoby , które mogą być zainteresowane zaborem dokumentu,
2. prowadzić szczególny nadzór , by nie dokonywano prób kserowania, kopiowania bez zgody przełożonego,
3. uwrażliwianie pracowników w trakcie prowadzonych szkoleń na możliwość prób kontaktu grup przestępczych z pracownikami, którzy mają dostęp do dokumentów szczególnie ważnych,
4. zastosowanie zasady, 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. 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 zasadach określonych przez kierownika jednostki , opisanych w Planie Ochrony Informacji Niejawnych,
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 ewidencjonuje 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 załączniku do Planu Ochrony Informacji Niejawnych,
9. Prowadzi się równie Rejestr Dzienników służący do ewidencjonowania ksiąg i dzienników ewidencyjnych ,rejestrów.
10. Pracownik kancelarii materiałów niejawnych przyjmuje przesyłki za pokwitowaniem i odciska na nich pieczęć oraz datę wpływu do jednostki organizacyjnej.

Przyjmując przesyłkę, sprawdza się:

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

11. W przypadku stwierdzenia uszkodzenia przesyłki lub śladów jej otwierania osoba kwitująca odbiór przesyłki sporządza wraz z doręczającym, protokół uszkodzenia.

Jeden egzemplarz protokołu przekazuje się nadawcy, drugi – pełnomocnikowi ochrony w jednostce organizacyjnej odbiorcy, a w przypadku gdy w obiegu przesyłek pośredniczył przewoźnik - kolejny egzemplarz protokołu przekazuje się także jemu.

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 w wyniku czynności, o których mowa w pkt.12, pracownik kancelarii materiałów niejawnych sporządza w dwóch egzemplarzach protokół z otwarcia przesyłki zawierający opis nieprawidłowości, jeden egzemplarz przekazując do kancelarii nadawcy.

14. Pracownik kancelarii materiałów niejawnych odnotowuje fakt sporządzenia protokołu, o którym mowa w pkt. 11 i 13, w odpowiednim dzienniku lub rejestrze w rubryce "Informacje uzupełniające/Uwagi".

V. ZABEZPIECZENIE INFORMACJI NIEJAWNYCH

1. Informacje niejawne oznaczone klauzulą „**poufne**” należy przechowywać w kancelarii materiałów niejawnych, zabezpieczonych zgodnie z przepisami ustawy o ochronie informacji niejawnych, w szafie klasy A;

Szafa stalowa klasy A

1/ Korpus szafy, drzwi, skrytki i inne elementy konstrukcyjne muszą być wykonane z blachy ze stali konstrukcyjnej, o grubości co najmniej 1 mm, zabezpieczonej przed korozją. Połączenia korpusu szafy powinny zapewnić mu dostateczną sztywność.

2/ Szafa może być wyposażona w zamykane skrytki.

3/ Drzwi szafy mogą być jednoskrzydłowe lub dwuskrzydłowe, zabezpieczone rygłem co najmniej na trzech krawędziach.

4/ Szafa musi być wyposażona w zamek mechaniczny kluczowy, co najmniej klasy A wg Polskiej Normy PN-EN 1300, zabezpieczony przed działaniem destrukcyjnym, w tym przed przewierceniem.

5/ Szafy jednoskrzydłowe powinny być wyposażone w mechanizm ryglowy blokujący je na co najmniej trzech krawędziach (rygle w średnicy min. 12 mm lub przekroju min. 112 mm² rozstaw rygli max. 450 mm).

6/ Szafy dwuskrzydłowe powinny być wyposażone w mechanizm dźwigowy, umieszczony na skrzydle aktywnym, blokujący je na co najmniej 3 krawędziach (rygle w średnicy min. 12 mm lub przekroju min. 112 mm², rozstaw rygli max. 450 mm); skrzydło aktywne musi blokować skrzydło bierne na całej ich wysokości. W przypadku niezależnego zamykania obu skrzydeł każde z nich powinno być wyposażone w oddzielny mechanizm ryglujący.

7/ Podstawa szafy musi posiadać te same rozmiary co wierzch. W szafie może znajdować się zaślepiony otwór umożliwiający jej zakotwienie.

8/ Szafa musi posiadać certyfikat wydany przez jednostkę certyfikującą akredytowaną w krajowym systemie akredytacji, potwierdzający zgodność wyrobu z wymaganiami klasy A.

9/ Szafa musi posiadać tabliczkę, wydana przez jednostkę certyfikującą akredytowaną w krajowym systemie akredytacji, zamontowana na wewnętrznej, górnej stronie drzwi, zawierająca następujące dane:

- 1) nazwę wyrobu;
- 2) nazwę i kod identyfikacyjny producenta, typ i numer modelu;
- 3) numer fabryczny, rok produkcji, klasę wyrobu, numer certyfikatu;
- 4) masę.

2. W uzasadnionych przypadkach podyktowanych względami dłuższego okresu czasu, niezbędnego do wykonania zadań związanych z dostępem do informacji niejawnych, dokumenty o klauzuli „poufne” mogą być wydawane poza wydzielone pomieszczenie , lecz pod warunkiem ,że odbiorca dokumentu zapewni warunki ochrony tych dokumentów spełniając wymogi określone w pkt.2 , przechowując je w szafach metalowych klasy „A” z odpowiednim zamknięciem;

3. Dokumenty lub materiały oznaczone klauzulą „poufne” mogą być przechowywane poza szafami stalowymi w pomieszczeniach kancelarii odpowiadające jednak co najmniej klasie O odporności na włamanie wg Polskiej Normy PN-EN 1143-1,

4. Szafy metalowe , w których przechowuje się dokumenty o klauzuli „poufne” po zakończeniu pracy należy zamknąć i sprawdzić sposób ich zabezpieczenia;

5. Informacje niejawne oznaczone klauzulą „zastrzeżone” można przechowywać w pomieszczeniu kancelarii tajnej lub na stanowiskach pracy , w meblach biurowych zamykanych na klucz.

VI. DOSTĘP DO INFORMACJI NIEJAWNYCH OZNACZONYCH KLAUZULĄ „POUFNE” LUB „ZASTRZEŻONE”

1. Informacje niejawne oznaczone klauzulą „poufne” lub „zastrzeżone” mogą być udostępniane wyłącznie osobie uprawnionej do dostępu do informacji niejawnych o określonej klauzuli niejawności.

2. Uzyskanie uprawnień do dostępu do informacji niejawnych o klauzuli „poufne” może nastąpić: po uzyskaniu przez pracownika poświadczenia bezpieczeństwa po przeprowadzonym przez Pełnomocnika ochrony zwykłym postępowaniu sprawdzającym, po przeszkoleniu danej osoby

w zakresie ochrony informacji niejawnych i uzyskaniu odpowiedniego zaświadczenia o przeszkoleniu.

3. Uzyskanie uprawnień dostępu do informacji niejawnych o klauzuli „zastrzeżone” może nastąpić:

- po uzyskaniu przez pracownika upoważnienia dostępu do informacji niejawnych oznaczonych klauzulą „zastrzeżone” wydanego przez kierownika jednostki,
- po przeszkoleniu danej osoby w zakresie przepisów ustawy o ochronie informacji niejawnych i uzyskaniu odpowiedniego zaświadczenia.

4. **Zwyczajne postępowanie sprawdzające** wobec pracowników jednostki w związku z dostępem do informacji niejawnych oznaczonych klauzulą „poufne” na pisemne polecenie kierownika jednostki przeprowadza Pełnomocnik ds. Ochrony Informacji Niejawnych.

5. Osoba podlegająca procedurze postępowania sprawdzającego zobowiązana jest do:

- wypełnienia określonej przepisami ustawy ankiety bezpieczeństwa osobowego,
- wypełnienia ankiety w sposób dokładny i zgodny z prawdą.

6. Odmowa poddania się postępowaniu sprawdzającemu ze strony osoby, która jest lub będzie zatrudniona na stanowisku związanym z dostępem do informacji niejawnych o klauzuli „poufne”, a w związku z tym nie uzyskanie poświadczenia bezpieczeństwa warunkującego dostęp do informacji oznaczonych klauzulą „poufne” może skutkować:

- przeniesieniem danej osoby na stanowisko nie związane z informacjami niejawnymi o klauzuli „poufne”,
- rozwiązaniem umowy o pracę w przypadku niemożności zmiany stanowiska,
- niemożnością zatrudnienia na danym stanowisku, w przypadku ubiegania się o zatrudnienie w Urzędzie.

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 udostępnienia lub wydania materiału osobie

nieuprawnionej.

W celu uniemożliwienia osobom nieuprawnionym dostępu do informacji niejawnych o klauzuli „poufne” należy w szczególności:

- 1) zorganizować strefy ochronne;
- 2) wprowadzić system kontroli wejść i wyjść ze stref ochronnych;
- 3) określić uprawnienia do przebywania w strefach ochronnych;
- 4) stosować wyposażenie i urządzenia służące ochronie informacji niejawnych, którym przyznano certyfikaty.

1. Kancelarie materiałów niejawnych tworzy kierownik jednostki organizacyjnej.

2. Kancelaria kieruje pracownik kancelarii, wyznaczany przez kierownika jednostki organizacyjnej na wniosek pełnomocnika ochrony.

3. Do podstawowych zadań pracownika kancelarii należy:

- 1) bezpośredni nadzór nad obiegiem dokumentów;
- 2) udostępnianie lub wydawanie dokumentów osobom do tego uprawnionym;
- 3) egzekwowanie zwrotu dokumentów;
- 4) kontrola przestrzegania właściwego oznaczania i rejestrowania dokumentów w kancelarii oraz jednostce organizacyjnej;
- 5) prowadzenie bieżącej kontroli postępowania z dokumentami;
- 6) wykonywanie poleceń pełnomocnika ochrony;

4. W przypadku zmiany na stanowisku pracownika kancelarii materiałów niejawnych sporządza się protokół zdawczo-odbiorczy.

5. Protokół, o którym mowa w ust. 4, sporządza się w obecności pracownika zdającego obowiązki, osoby przejmującej obowiązki oraz pełnomocnika ochrony. Protokół sporządza się w dwóch egzemplarzach; pierwszy egzemplarz przechowywany jest w kancelarii materiałów niejawnych, drugi – u pełnomocnika ochrony.

6. W przypadku czasowej nieobecności pracownika kancelarii jego obowiązki przejmuje upoważniony pracownik pionu ochrony. W razie ich braku kancelarie przejmuje protokolarnie inny pracownik wyznaczony przez kierownika jednostki na wniosek pełnomocnika ochrony.

7. W pomieszczeniach kancelarii można wydzielić miejsce, w którym osoby upoważnione mogą zapoznawać się z dokumentami – czytelnie.

- 1) czytelnia powinna być zorganizowana w sposób umożliwiający stały nadzór ze strony pracownika kancelarii.

2) w czytelni zabrania się instalowania systemu nadzoru wizyjnego.

8. Dokumenty i materiały oznaczone różnymi klauzulami tajności są przechowywane w odrębnych szafach lub pomieszczeniach, chyba że wchodzi one w skład zbioru dokumentów.

9. Po zakończeniu pracy kierownik kancelarii lub upoważniony pracownik kancelarii jest obowiązany sprawdzić prawidłowość zamknięcia szaf i pomieszczeń kancelarii.

10. Zasady i sposób zdawania, przechowywania i wydawania kluczy oraz ich duplikatów do pomieszczeń oraz szaf kancelarii, a także zasady ustalania, zmiany i deponowania haseł lub szyfrów, w przypadku stosowania zamków szyfrowych, określa plan ochrony informacji niejawnych.

11. Wszelkie nieprawidłowości związane z naruszeniem zasad, określonych powyżej należy niezwłocznie zgłaszać pełnomocnikowi ochrony.

12. Zasady określone obowiązują odpowiednio w stosunku do innych pomieszczeń, w których są przechowywane dokumenty lub materiały, oraz osób za te pomieszczenia odpowiedzialnych.

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

- 1) rejestr dzienników, książek ewidencyjnych i teczek,
- 2) dziennik ewidencji,
- 3) książkę doręczeń przesyłek miejscowych,

14. W przypadkach uzasadnionych organizacja ochrony informacji niejawnych kancelaria może prowadzić także inne rejestry ni wymienione wyżej wymienione, w tym odrębne rejestry dla dokumentów oznaczonych różnymi klauzulami tajności – np. kartę zapoznania się z dokumentem niejawnym oznaczonym klauzula „poufne”,

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

POSTĘPOWANIE Z PRZESYŁKAMI

1. Pracownik kancelarii przyjmuje przesyłki lub dokumenty za pokwitowaniem i odciska na nich pieczęć oraz datę wpływu do jednostki organizacyjnej.

2. Przyjmując przesyłkę, sprawdza się:

- 1) prawidłowość adresu;
- 2) całość pieczęci i opakowania;

- 3) zgodność odcisku pieczęci na opakowaniu z nazwą jednostki nadawcy;
 - 4) zgodność numeru na przesyłce z numerem tej przesyłki w wykazie lub w książce doręczeń.
3. W przypadku stwierdzenia uszkodzenia przesyłki lub śladów jej otwierania pracownik kancelarii kwitujący odbiór przesyłki sporządza, wraz z doręczającym, protokół uszkodzenia. Jeden egzemplarz protokołu przekazuje się nadawcy, drugi pełnomocnikowi ochrony w jednostce organizacyjnej odbiorcy, a w przypadku gdy w obiegu przesyłek pośredniczył przewoźnik – kolejny egzemplarz protokołu przekazuje się także jemu.
4. Po otwarciu przesyłki pracownik kancelarii:
- 1) sprawdza, czy zawartość przesyłki odpowiada wyszczególnionym na niej numerom ewidencyjnym;
 - 2) ustala, czy liczba załączników i stron jest zgodna z liczbą oznaczona na poszczególnych dokumentach.
5. W przypadku stwierdzenia nieprawidłowości pracownik kancelarii sporządza w dwóch egzemplarzach protokół z otwarcia przesyłki zawierający opis nieprawidłowości, jeden egzemplarz przekazując do kancelarii nadawcy,
6. Pracownik kancelarii odnotowuje fakt sporządzenia protokołu, w odpowiednim dzienniku lub rejestrze w rubryce „Informacje uzupełniające/Uwagi”.
7. W kancelarii materiałów niejawnych nie otwiera się przesyłek oznaczonych „do rąk własnych”. W odpowiednim dzienniku lub rejestrze wpisuje się nadawcę, numer i datę wpływu dokumentu; w rubryce „Informacje uzupełniające/Uwagi” odnotowuje się, że przesyłka była oznaczona „do rąk własnych”,
8. Na opakowaniu przesyłek, wpisuje się datę wpływu, pozycję i numer, pod którym zarejestrowano przesyłkę. Przesyłkę przekazuje się – za pokwitowaniem – bezpośrednio adresatowi, a w razie jego nieobecności – osobie przez niego upoważnionej do odbioru,
9. Zatrzymanie przez adresata dokumentu, adresowanego „do rąk własnych”, odnotowuje się w rubryce „Informacje uzupełniające/Uwagi”.
10. W przypadku zwrotu do kancelarii przesyłki adresowanej „do rąk własnych”, pracownik kancelarii uzupełnia dane dotyczące przesyłki w odpowiednim dzienniku lub rejestrze.
11. Jeżeli adresat podjął decyzję o przechowywaniu przesyłki „do rąk własnych” w kancelarii w stanie zamkniętym, pracownik kancelarii dokonuje czynności, o których mowa w ust. 10, przy udziale adresata. Przesyłka jest w takim przypadku przechowywana

w formie zapieczętowanego pakietu, a fakt ten odnotowuje się w rubryce „Informacje uzupełniające/Uwagi”.

12. Przesyłki pilne, telegramy i szyfrogramy doręcza się adresatom bezzwłocznie.

Przy kwitowaniu odbioru tych przesyłek odnotowuje się godzinę doręczenia.

13. Otrzymaną i wysłaną przesyłkę bądź wytworzony dokument rejestruje się odpowiednio w kolejności wytworzenia lub otrzymania.

14. Wszelkich adnotacji, w dziennikach ewidencyjnych, dokonuje się atramentem lub tuszem. Zmian dokonuje się kolorem czerwonym, umieszczając datę i czytelny podpis dokonującego zmiany.

15. Zabrania się wycierania i zamazywania adnotacji, .

16. Dokumenty, materiały oraz zbiory dokumentów dotyczące spraw ostatecznie zakończonych przechowuje się w kancelarii do czasu zniesienia okresu ochronnego. Po upływie tego okresu przekazuje się je do archiwum zakładowego lub składnicy akt.

OBOWIĄZKI PRACOWNIKA KANCELARII MATERIAŁÓW NIEJAWNYCH

- Przed otwarciem drzwi sprawdzić stan zamków i zabezpieczenie drzwi,
- Sprawdzić stan zabezpieczeń szaf, sprzętu biurowego.
- Przestrzegać zasad zakazu wstępu osobom nieuprawnionym do kancelarii materiałów niejawnych ,

VIII. ZAKRES UDOSTĘPNIANIA INFORMACJI NIEJAWNYCH

1. Udostępnianie pracownikowi informacji niejawnych oznaczonych klauzula „poufne” uwarunkowane jest posiadaniem właściwego i ważnego poświadczenia osobowego .
2. Udostępnianie informacji niejawnych oznaczonych klauzula „zastrzeżone” określonej osobie może nastąpić w oparciu o ważne Poświadczenie Bezpieczeństwa lub pisemne upoważnienie kierownika jednostki – wzór upoważnienia stanowi załącznik do Planu Ochrony Informacji Niejawnych.

IX. ZASADY WYKONYWANIA DOKUMENTÓW NIEJAWNYCH

1. Propozycje przyznania klauzuli niejawności na wykonywanym dokumencie przedstawia osoba sporządzająca dokument,
2. Klauzule niejawności na danym dokumencie przyznaje osoba która jest upoważniona do odpisania dokumentu,

3. Rękopisy sporządzanych dokumentów niejawnych powinny być opracowywane w brulionach (zeszytach pracy) uprzednio zarejestrowanych kancelarii materiałów niejawnych.
4. Dokumenty niejawne powinny być opisane i oznaczone zgodnie Rozporządzeniem 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 z 2010 roku , poz.1069) Wzór sposobu opisanie dokumentu stanowi załącznik do Planu OIN.

X. WYKONYWANIE DOKUMENTÓW NIEJAWNYCH Z WYKORZYSTANIEM SPRZĘTU KOMPUTEROWEGO

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 kierownik jednostki organizacyjnej, który w szczególności:
 - 1) zapewnia opracowanie dokumentacji bezpieczeństwa teleinformatycznego;
 - 2) realizuje ochronę fizyczną, elektromagnetyczną systemu lub sieci.
 - 3) zapewnia niezawodność transmisji oraz kontrole dostępu do urządzeń systemu lub sieci teleinformatycznej;
 - 4) dokonuje analizy stanu bezpieczeństwa teleinformatycznego oraz zapewnia usunięcie stwierdzonych nieprawidłowości;
 - 5) zapewnia przeszkolenie z zakresu bezpieczeństwa teleinformatycznego dla osób uprawnionych do pracy w systemie lub sieci teleinformatycznej;
 - 6) zawiadamia właściwą służbę ochrony państwa o zaistniałym incydencie bezpieczeństwa teleinformatycznego dotyczącym informacji niejawnych oznaczonych co najmniej klauzulą „poufne”.

4. Ochrona fizyczna systemu lub sieci teleinformatycznej polega na:

- 1) umieszczeniu urządzeń systemu lub sieci teleinformatycznej w strefie ochronnej, zwanej również „strefą kontrolowanego dostępu” w zależności od:
 - a) klauzuli tajności,

- b) ilości,
- c) zagrożeń dla poufności, integralności lub dostępności- informacji niejawnych;

2) zastosowaniu środków zapewniających ochronę fizyczną, w szczególności przed:

- a) nieuprawnionym dostępem,
- b) podglądem,
- c) podsłuchem.

5.Ochrona elektromagnetyczna systemu lub sieci teleinformatycznej polega na:

^ niedopuszczeniu do utraty poufności i dostępności informacji niejawnych przetwarzanych w urządzeniach teleinformatycznych.

· Utrata poufności następuje w szczególności na skutek wykorzystania elektromagnetycznej emisji ujawniającej pochodzącej z tych urządzeń.

· Utrata dostępności następuje w szczególności na skutek zakłócania pracy urządzeń teleinformatycznych za pomocą impulsów elektromagnetycznych o dużej mocy.

6. 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.

7. W celu zapewnienia kontroli dostępu do systemu lub sieci teleinformatycznej

- 1) kierownik jednostki organizacyjnej lub osoba przez niego upoważniona ustala warunki i sposób przydzielania uprawnień osobom uprawnionym do pracy w systemie lub sieci teleinformatycznej;
- 2) administrator systemów określa warunki oraz sposób przydzielania tym osobom kont oraz mechanizmów kontroli dostępu, a także zapewnia ich właściwe wykorzystanie.

8. System lub sieć teleinformatyczna wyposaża się w mechanizmy kontroli dostępu odpowiednie do klauzuli tajności informacji niejawnych w nich przetwarzanych.

9. Systemy i sieci teleinformatyczne, w których mają być wytwarzane, przetwarzane, przechowywane lub przekazywane informacje niejawne, podlegają akredytacji

bezpieczeństwa teleinformatycznego przez służby ochrony państwa.

10. Akredytacji udziela się na czas określony , nie dłuższy niż 5 lat.

11. Akredytacja, o której mowa następuje na podstawie dokumentów szczególnych wymagań bezpieczeństwa i procedur bezpiecznej eksploatacji.

12. ABW udziela akredytacji bezpieczeństwa teleinformatycznego dla systemu teleinformatycznego przeznaczonego do przetwarzania informacji niejawnych o klauzuli „poufne” lub wyższej.

13. ABW udziela albo odmawia udzielenia akredytacji, o której mowa w pkt.12 , w terminie 6 miesięcy od otrzymania kompletnej dokumentacji bezpieczeństwa systemu teleinformatycznego. W uzasadnionych przypadkach, w szczególności wynikających z rozległości systemu i stopnia jego skomplikowania, termin ten może być przedłużony o kolejne 6 miesięcy. Od odmowy udzielenia akredytacji nie służy odwołanie.

14. Potwierdzeniem udzielenia przez ABW akredytacji, o której mowa w pkt. 13, jest świadectwo akredytacji bezpieczeństwa systemu teleinformatycznego.

15. Świadectwo, o którym mowa w pkt. 14, wydaje się na podstawie:

1) zatwierdzonej przez ABW dokumentacji bezpieczeństwa systemu teleinformatycznego;

2) wyników audytu bezpieczeństwa systemu teleinformatycznego przeprowadzonego przez ABW .

16. ABW może odstąpić od przeprowadzenia audytu bezpieczeństwa systemu teleinformatycznego, o którym mowa w pkt.15 pkt 2, jeżeli system jest przeznaczony do przetwarzania informacji niejawnych o klauzuli „poufne”.

17. Kierownik jednostki organizacyjnej udziela akredytacji bezpieczeństwa teleinformatycznego dla systemu teleinformatycznego przeznaczonego do przetwarzania informacji niejawnych o klauzuli „zastrzeżone” przez zatwierdzenie dokumentacji bezpieczeństwa systemu teleinformatycznego.

18. W ciągu 30 dni od udzielenia akredytacji bezpieczeństwa teleinformatycznego, o której mowa w pkt. 17, kierownik jednostki organizacyjnej przekazuje ABW dokumentację bezpieczeństwa systemu teleinformatycznego.

19. W ciągu 30 dni od otrzymania dokumentacji bezpieczeństwa systemu teleinformatycznego ABW może przedstawić kierownikowi jednostki organizacyjnej, który udzielił akredytacji bezpieczeństwa teleinformatycznego, zalecenia dotyczące konieczności

przeprowadzenia dodatkowych czynności związanych z bezpieczeństwem informacji niejawnych. Kierownik jednostki organizacyjnej w terminie 30 dni od otrzymania zalecenia informuje ABW o realizacji zaleceń. W szczególnie uzasadnionych przypadkach ABW może nakazać wstrzymanie przetwarzania informacji niejawnych w systemie teleinformatycznym posiadającym akredytację bezpieczeństwa teleinformatycznego.

XI . DOKUMENT SZCZEGÓLNYCH WYMAGAŃ BEZPIECZEŃSTWA SYSTEMU

teleinformatycznego powinien zawierać w szczególności wyniki procesu szacowania ryzyka dla bezpieczeństwa informacji niejawnych przetwarzanych w systemie teleinformatycznym oraz określać przyjęte w ramach zarządzania ryzykiem sposoby osiągania i utrzymywania odpowiedniego poziomu bezpieczeństwa systemu, a także opisywać aspekty jego budowy, zasady działania i eksploatacji, które mają związek z bezpieczeństwem systemu lub wpływają na jego bezpieczeństwo. Przebieg i wyniki procesu szacowania ryzyka mogą zostać przedstawione w odrębnym dokumencie niż dokument szczególnych wymagań bezpieczeństwa.

1. Dokument szczególnych wymagań bezpieczeństwa opracowuje się na etapie projektowania, w razie potrzeby konsultuje z ABW , bieżąco uzupełnia na etapie wdrażania i modyfikuje na etapie eksploatacji przed dokonaniem zmian w systemie teleinformatycznym.

DOKUMENT PROCEDUR BEZPIECZNEJ EKSPLOATACJI opracowuje się na etapie wdrażania oraz modyfikuje na etapie eksploatacji przed dokonaniem zmian w systemie teleinformatycznym.

1. Podstawa dokonywania wszelkich zmian w systemie teleinformatycznym jest przeprowadzenie procesu szacowania ryzyka dla bezpieczeństwa informacji niejawnych przetwarzanych w tym systemie.
2. Kierownik jednostki organizacyjnej akceptuje wyniki procesu szacowania ryzyka dla bezpieczeństwa informacji niejawnych oraz jest odpowiedzialny za właściwą organizację bezpieczeństwa teleinformatycznego.
3. Bez konieczności przeprowadzania badań i oceny Szef ABW może dopuścić do stosowania w systemie teleinformatycznym przeznaczonym do przetwarzania informacji niejawnych o klauzuli „zastrzeżone” urządzenia lub narzędzia kryptograficzne, jeżeli otrzymały stosowny certyfikat wydany przez krajową władzę bezpieczeństwa państwa będącego członkiem NATO lub Unii Europejskiej lub inny uprawniony organ w NATO lub

w Unii Europejskiej.

4. Kierownik jednostki organizacyjnej wyznacza:

1) pracownika lub pracowników pionu ochrony pełniących funkcje

INSPEKTORA BEZPIECZEŃSTWA TELEINFORMATYCZNEGO,

odpowiedzialnych za weryfikację i bieżącą kontrolę zgodności funkcjonowania systemu teleinformatycznego ze szczególnymi wymaganiami bezpieczeństwa oraz przestrzegania procedur bezpiecznej eksploatacji;

2) osobę lub zespół osób, nie pełniących funkcji inspektora bezpieczeństwa teleinformatycznego, odpowiedzialnych za funkcjonowanie systemu teleinformatycznego oraz za przestrzeganie zasad i wymagań bezpieczeństwa przewidzianych dla systemu teleinformatycznego, zwanych

„ADMINISTRATOREM SYSTEMU”.

4. W sytuacjach wymagających konsultacji lub uzgodnień kierownik jednostki może zwrócić się do Agencji Bezpieczeństwa Wewnętrznego o wydanie opinii lub zaleceń w zakresie bezpieczeństwa teleinformatycznego .

5. Stanowiska lub funkcje administratora systemu oraz inspektora bezpieczeństwa teleinformatycznego mogą zajmować lub 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.

6. Zaświadczenie o odbytym szkoleniu jest przechowywane w aktach osobowych oraz dokumentacji Pełnomocnika art. ochrony informacji niejawnych.

KOPIE ZAPASOWE:

1. Zaleca się wykonywanie kopii zapasowych wykonanych dokumentów niejawnych.
2. Sposób przechowywania zapasowych kopii jest identyczny jak przechowywanie dokumentów wykonanych w formie tradycyjnej (pismo), w przypadku gdy nośnikiem informacji jest materiał inny niż pismo, klauzulę tajności i sygnaturę literowo-cyfrową umieszcza się przez ostemplowanie, nadrukowanie, wpisanie odręczne, trwałe dołączenie metek, nalepek, kalkomanii lub w inny sposób, bezpośrednio, a jeżeli jest to nie możliwe - na ich obudowie lub opakowaniu.

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

1. Klauzulę tajności nadaje osoba , która jest uprawniona do podpisania dokumentu lub oznaczenia innego niż dokument materiału,
2. Informacje niejawne podlegają ochronie w sposób określony w ustawie o ochronie informacji niejawnych do czasu zniesienia lub zmiany klauzuli tajności,
3. Osoba wymieniona w pkt.1 może określić datę lub wydarzenie , po którym nastąpi zniesienie lub zmiana klauzuli tajności,
4. Zniesienie lub zmiana klauzuli tajności jest możliwa wyłącznie po wyrażeniu pisemnej zgody przez osobę , o której mowa w pkt.1, albo jej przełożonego w przypadku ustania lub zmiany ustawowych przesłanek ochrony,
5. Należy nie rzadziej niż raz na 5 lat dokonać przeglądu materiałów celem ustalenia , czy spełniają ustawowe przesłanki ochrony,
6. Po zniesieniu lub zmianie klauzuli tajności podejmuje się czynności polegające na

naniesieniu odpowiednich zmian w oznaczeniu materiału i poinformowaniu o nich odbiorców . odbiorcy materiału, którzy przekazali go kolejnym odbiorcom , są odpowiedzialni za poinformowanie ich o zniesieniu lub zmianie klauzul tajności,

7. Poszczególne części materiału mogą być oznaczone różnymi klauzulami tajności,

8. Oznaczenie materiału klauzulą tajności polega na umieszczeniu na nim klauzuli tajności.

Przyznana klauzule tajności nanosi się w sposób wyraźny i w pełnym jej brzmieniu,

9. Wprowadza się następujące oznaczenia klauzul tajności:

„**Pf**” – dla klauzuli „poufne”;

„**Z**” – dla klauzuli „zastrzeżone”.

10. Materiały zawierające informacje niejawne utrwalone na piśmie, oznacza się w następujący sposób:

1) **na każdej stronie pisma umieszcza się:**

a) **w prawym górnym rogu**, w kolejności pionowej:

— klauzulę tajności,

— numer egzemplarza pisma, a w przypadku gdy pismo wykonano w jednym egzemplarzu — napis „*Egz. pojedynczy*”,

b) **w lewym górnym rogu**

sygnaturę literowo-cyfrową, na którą składają się oddzielone myślnikami:

- literowe oznaczenie jednostki lub komórki organizacyjnej, oznaczenie

klauzuli tajności i numer, pod którym pismo zostało zarejestrowane w odpowiedniej ewidencji, łamany przez rok lub dwie ostatnie cyfry roku,

w którym pismo zostało wykonane, a także, w zależności od potrzeb, inne oznaczenia ułatwiające ustalenie miejsca jego wykonania w jednostce lub komórce organizacyjnej nadawcy lub te przynależność pisma do określonej sprawy,

c) **w prawym dolnym rogu**

klauzulę tajności oraz numer strony łamany przez liczbę stron całego pisma;

2) **na pierwszej stronie pisma umieszcza się również:**

a) **w lewym górnym rogu** nazwę jednostki lub komórki organizacyjnej,

b) **w prawym górnym rogu:**

— nazwę miejscowości i datę podpisania pisma,

— napis o treści: „*podlega ochronie do ...*”,

— w przypadku pisma, któremu nadano bieg korespondencyjny pod numerem egzemplarza w kolejności pionowej: nazwę stanowiska adresata oraz imię i nazwisko, a w przypadku wielu adresatów dopuszcza się możliwość umieszczenia jedynie adnotacji „adresaci według rozdzielnika”,
— napis „Krypto” — w przypadku materiałów kryptograficznych;

3) na ostatniej stronie pisma umieszcza się również:

a) z lewej strony pod treścią:

— liczbę załączników oraz liczbę stron lub innych jednostek miary wszystkich załączników, jeżeli są dołączone do pisma,
— klauzulę tajności załączników wraz z numerami, pod jakimi zostały zarejestrowane w odpowiedniej ewidencji,
— liczbę stron każdego załącznika lub informacje określające 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 pozostawiania ich w aktach, napis „*do zwrotu*” — jeżeli załączniki mają zostać zwrócone osobie uprawnionej do jego podpisania,

b) z prawej strony pod treścią pisma i adnotacją o załącznikach

w kolejności pionowej: nazwa stanowiska oraz imię i nazwisko osoby uprawnionej do jego podpisania,

c) w lewym dolnym rogu w kolejności pionowej:

— liczbę wykonanych egzemplarzy,
— adresatów poszczególnych egzemplarzy pisma lub adnotacje „*adresaci według rozdzielnika*”,
— imię i nazwisko lub inne dane identyfikujące sporządzającego i wykonawcę.

2. W przypadku pisma, któremu nadano bieg korespondencyjny, na pierwszej stronie w prawym górnym rogu pod numerem egzemplarza można zamieścić dyspozycje dla adresata o treści:

- 1) „udzielanie informacji tylko za pisemną zgodą nadawcy”;
- 2) „kopiowanie tylko za pisemną zgodą nadawcy”;

- 3) „odpis tylko za pisemną zgodą nadawcy”;
- 4) „kopiowanie stron od ... do ... tylko za pisemną zgodą nadawcy”;
- 5) „odpis od ... do ... tylko za pisemną zgodą nadawcy”;
- 6) „wypis (wyciąg) od ... do ... tylko za pisemną zgodą nadawcy”.

3. W przypadkach uzasadnionych organizacja ochrony informacji niejawnych na materiałach zawierających informacje niejawne można nanosić dodatkowe oznaczenia, inne niż te, o których mowa w ust. 1 i 2.

4. Dokumenty elektroniczne przetwarzane wyłącznie w systemie teleinformatycznym, o którym mowa w art. 2 pkt. 8 ustawy, podlegające ewidencji w elektronicznym rejestrze dokumentów, oznacza się w sposób określony w ust 1.

2. W przypadku dokumentów elektronicznych, o których mowa w ust. 1, na każdej stronie w prawym górnym rogu pod klauzulą tajności zamiast oznaczenia numeru egzemplarza umieszcza się napis „*Egz. elektroniczny*”.

Materiały w postaci prezentacji multimedialnych oznacza się w następujący sposób:

- 1) na każdym slajdzie lub stronie stanowiącej integralną część prezentacji multimedialnej umieszcza się:
 - a) w prawym górnym rogu klauzulę tajności,
 - b) w prawym dolnym rogu klauzulę tajności, numer slajdu lub strony łamany przez liczbę slajdów lub stron;
- 2) na pierwszym slajdzie lub stronie stanowiącej integralną część prezentacji multimedialnej umieszcza się dodatkowo:
 - a) w lewym górnym rogu nazwę jednostki lub komórki organizacyjnej oraz sygnaturę literowo-cyfrową,
 - b) napis o treści: „*podlega ochronie do ...*”,

Na pismach stanowiących załączniki,

1. Na pierwszej stronie w prawym górnym rogu, umieszcza się dodatkowo napis: „Załącznik nr ... do pisma nr ... z dnia ...”.
2. Napis, o którym mowa w ust. 1, zamieszcza się, w miarę możliwości, na innych niż pismo materiałach.
3. Jeżeli przy piśmie przewodnim przesyła się załączniki oznaczone klauzulami tajności, to:
 - 1) klauzula pisma przewodniego lub dokumentu nie może być niższa niż klauzula

załącznika o najwyższym stopniu tajności;

Na piśmie przewodnim, jeżeli jego klauzula jest inna po odłączeniu załączników,

1. Zamieszcza się dyspozycje co do klauzuli tajności pisma po trwałym ich odłączeniu; na każdej stronie pod numerem egzemplarza zamieszcza się napis: „... (nazwa klauzuli tajności) po odłączeniu załączników” lub „Jawne po odłączeniu załączników”.
2. Przy rejestracji pisma przewodniego, o którym mowa w pkt.1, we właściwej ewidencji, w rubryce „Informacje uzupełniające/Uwagi” wpisuje się adnotacje o treści „... (nazwa klauzuli tajności) po odłączeniu załączników” lub „Jawne po odłączeniu załączników”.

Na materiałach innych niż pismo

klauzule tajności i sygnaturę literowo-cyfrową umieszcza się przez ostemplowanie, nadrukowanie, wpisanie odręczne, trwałe dołączenie metek, nalepek, kalkomanii lub w inny widoczny sposób, bezpośrednio, a jeżeli to nie jest możliwe — na ich obudowie lub opakowaniu.

Utrwalanie informacji niejawnych w formie dźwięku, obrazu lub poczty elektronicznej

powinno być poprzedzone i kończyć się informacją o nadanej klauzuli tajności, jeżeli istnieją takie możliwości techniczne.

Na trwale oprawionych zbiorach dokumentów, rejestrach, książkach, broszurach i reprodukcjach

klauzule tajności umieszcza się po prawej stronie na górze i dole zewnętrznych ścianek okładki oraz, jeżeli jest, na stronie tytułowej.

OKRESY OCHRONNE

1. Na pismach zawierających informacje niejawne, wobec których minął ustawowy okres ochrony ustanowiony przez osobę uprawnioną do nadania klauzuli :

- 1) skreśla się klauzulę tajności na każdej stronie w prawym górnym i dolnym rogu;
- 2) na pierwszej stronie nad skreśloną klauzulą tajności w prawym górnym rogu umieszcza się dodatkowo napis „Jawne” oraz datę, imię, nazwisko i podpis osoby dokonującej tych adnotacji.

2. Na pismach zawierających informacje niejawne, wobec których zniesiono lub zmieniono przyznana klauzulę tajności:

- 1) na każdej stronie w prawym górnym i dolnym rogu skreśla się dotychczasowe klauzule tajności;

- 2) nad skreślonymi klauzulami tajności umieszcza się nowe klauzule tajności;
- 3) na pierwszej stronie nad skreśloną klauzulą tajności w prawym górnym rogu umieszcza się datę, imię, nazwisko i podpis osoby dokonującej tych adnotacji oraz wskazuje się podstawy dokonanej zmiany.

3. W stosunku do pism znajdujących się w zbiorach dokumentów zawierających informacje niejawne, wobec których minął ustawowy lub ustanowiony okres ochrony, czynności, o których mowa w ust. 1—2, można dokonać najpóźniej w przypadku ich udostępniania lub przekazywania osobom spoza jednostki lub komórki organizacyjnej.

4. Na dokumentach elektronicznych nie dokonuje się skreśleń i adnotacji, o których mowa powyżej. Informacje o skreśleniach i adnotacjach umieszcza się we właściwych ewidencjach lub metadanych dokumentu elektronicznego. Skreśleń i adnotacji, dokonuje pracownik kancelarii materiałów niejawnych lub inne upoważnione osoby. Skreślenia klauzul tajności oraz adnotacji, dokonuje się kolorem czerwonym, w sposób czytelny. Wycieranie, wywabianie lub zamazywanie klauzuli tajności i dokonanych zmian jest niedozwolone.

W stosunku do pism znajdujących się w zbiorach dokumentów zawierających informacje niejawne, wobec których minął ustanowiony okres ochrony, czynności, o których mowa, można dokonać najpóźniej w przypadku ich udostępniania lub przekazywania osobom spoza jednostki lub komórki organizacyjnej.

W stosunku do materiałów innych niż pismo, na trwale oprawionych zbiorach dokumentów, rejestrach, książkach, broszurach i reprodukcjach sposoby dokonywania skreśleń i adnotacji stosuje się odpowiednio, uwzględniając sposób oznakowania tych materiałów.

· **Na kopiach, odpisach, wypisach, wyciągach lub tłumaczeniach pism umieszcza się:**

- **na wszystkich stronach** w prawym górnym rogu odpowiednio napis:
„Kopia”, „Odpis”, „Wypis”, „Wyciąg” lub „Tłumaczenie z języka – (nazwa języka) – (imię i nazwisko tłumacza)”;
- **na pierwszej stronie dodatkowo** numer, pod jakim zostały zarejestrowane w dzienniku ewidencyjnym, numer egzemplarza wykonanej kopii, odpisu, wypisu, wyciągu lub tłumaczenia;
- **na ostatniej stronie dodatkowo** napis „Za zgodność” i odcisk tuszowej pieczęci urzędowej z nazwą jednostki lub komórki organizacyjnej (numerem jednostki wojskowej), w której sporządzono kopie, odpis, wypis, wyciąg lub tłumaczenie.

Zgodność z oryginałem kopii, odpisu, wypisu lub wyciągu potwierdza podpisem kierownik

jednostki lub komórki organizacyjnej albo inna osoba przez niego upoważniona, a tłumaczenia – osoba dokonująca tłumaczenia.

Fakt sporządzenia kopii, odpisu, wypisu, wyciągu lub tłumaczenia odnotowuje się na dokumencie, z którego sporządzono kopie, odpis, wypis, wyciąg lub tłumaczenie, przez odcisk pieczęci lub umieszczenie adnotacji informującej o:

- nazwie jednostki lub komórki organizacyjnej, w której sporządzono kopie, odpis, wypis, wyciąg lub tłumaczenie;
- liczbie egzemplarzy sporządzonych kopii, odpisów, wypisów, wyciągów lub tłumaczeń;
- dacie sporządzenia kopii, odpisu, wypisu, wyciągu lub tłumaczenia;
- numerze, pod jakim kopia, odpis, wypis, wyciąg lub tłumaczenie zostały zarejestrowane w dzienniku ewidencji wykonanych dokumentów.

Adnotacje, o których mowa, wpisuje się przed wykonaniem kopii, odpisu, wypisu, wyciągu lub tłumaczenia, natomiast numer, pod jakim zostały zarejestrowane w dzienniku ewidencyjnym, nanosi się po wykonaniu kopii, odpisu, wypisu, wyciągu lub tłumaczenia.

XIII. ZASADY DOSTĘPU DO INFORMACJI NIEJAWNYCH

1. Informacje niejawne stanowiące oznaczone klauzulą „poufne” lub „zastrzeżone” mogą być udostępniane wyłącznie osobie uprawnionej do dostępu do informacji niejawnych o określonej klauzuli niejawności,

2. Uzyskanie uprawnień do dostępu do informacji niejawnych o klauzuli „poufne” może nastąpić:

- po przeprowadzeniu zwykłego postępowania sprawdzającego wobec kandydata do dostępu do tych informacji,
- po uzyskaniu przez daną osobę poświadczenia bezpieczeństwa,
- po przeszkoleniu danej osoby w zakresie przepisów o ochronie informacji niejawnych i uzyskaniu właściwego zaświadczenia o przeszkoleniu.

3. Zwykłe postępowanie sprawdzające w związku z dostępem do informacji niejawnych o klauzuli „poufne” na pisemne polecenie kierownika jednostki organizacyjnej przeprowadza Pełnomocnik ds. Ochrony Informacji Niejawnych,

4. Osoba podlegająca postępowaniu sprawdzającemu zwykłemu zobowiązana jest do:

- wypełnienia określonej przepisami ankiety bezpieczeństwa osobowego, w sposób dokładny i zgodny z prawdą,
- odbyć szkolenie z zakresu znajomości przepisów ustawy o ochronie informacji niejawnych

prowadzone przez Pełnomocnika .

5. Odmowa poddania się postępowaniu sprawdzającemu ze strony osoby, która jest lub będzie zatrudniona na stanowisku związanym z dostępem do informacji niejawnych a w związku z tym nie uzyskanie poświadczenia bezpieczeństwa warunkującego dostęp do informacji niejawnych o klauzuli „poufne” może skutkować:

- przeniesieniem danej osoby na stanowisko nie związane z dostępem do informacji niejawnych,
- rozwiązaniem umowy o pracę w przypadku niemożności zmiany stanowiska,
- niemożnością zatrudnienia na danym stanowisku, w przypadku ubiegania się o zatrudnienie w Urzędzie.

6. Kierownik jednostki organizacyjnej może wyrazić w formie pisemnej zgodę na udostępnienie informacji niejawnych o klauzuli „poufne” osobie, która jest zatrudniona lub wykonuje prace zlecone , wobec której wszczęto zwykle postępowanie sprawdzające ,

7. Kierownik jednostki organizacyjnej uzyskuje dostęp do informacji niejawnych oznaczonych klauzulą „poufne” po uzyskaniu Poświadczenia Bezpieczeństwa oraz uzyskaniu zaświadczenia stwierdzającego odbycie szkolenia z zakresu przepisów ustawy o ochronie informacji niejawnych.

8. Postępowanie sprawdzające wobec kierownika jednostki , w przypadku potrzeby uzyskania uprawnień dostępu do informacji niejawnych oznaczonych klauzulą „poufne” przeprowadza Agencja Bezpieczeństwa Wewnętrznego,

9. Szkolenie kierownika jednostki w związku z przewidywanym dostępem do informacji niejawnych oznaczonych klauzulą „poufne” organizuje pełnomocnik ochrony wydając stosowne zaświadczenie,

10. Uzyskanie uprawnień do dostępu do informacji niejawnych o klauzuli „zastrzeżone” może nastąpić:

- po uzyskaniu przez daną osobę upoważnienia nadanego przez kierownika jednostki ,
- po przeszkoleniu danej osoby w zakresie przepisów o ochronie informacji niejawnych i uzyskaniu właściwego zaświadczenia o przeszkoleniu.

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 upoważnianiem 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 1997r.,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 informacje, 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 informacje niejawną o klauzuli „zastrzeżone” lub „poufne” lub informacje, 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 zabezpieczania dokumentów, stwarzając warunki do ujawnienia tajemnicy osobom nieuprawnionym, mogą być zastosowane sankcje służbowe i dyscyplinarne.

XVI. 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 roku (Dz.U.Nr 34 poz.181),

3. Dokumentacja wytwarzana i gromadzona dzieli się na :

- 1) materiały archiwalne - wchodzące do państwowego zasobu archiwalnego;
- 2) dokumentacje nie archiwalna - inną dokumentację, nie stanowiącą materiałów archiwalnych.

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

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

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

7. Brakowanie dokumentacji nie archiwalnej polega na ocenie jej przydatności do celów praktycznych, wydzieleniu dokumentacji nieprzydatnej i przekazaniu jej na makulaturę

8. Brakowanie dokumentacji nie archiwalnej następuje na podstawie zgody.

9. Zgodę, o której mowa wyraża dyrektor miejscowo właściwego archiwum państwowego.

10. Wniosek o wyrażenie zgody na brakowanie dokumentacji nie archiwalnej należy złożyć dyrektorowi miejscowo właściwego archiwum państwowego.

11. Do wniosku o zgodę jednorazową dołącza się:

- 1) protokół oceny dokumentacji nie archiwalnej,
- 2) spis dokumentacji nie archiwalnej przeznaczonej do przekazania na makulaturę lub zniszczenie, albo spis dokumentacji technicznej nie archiwalnej przeznaczonej na makulaturę lub zniszczenie,

12. Protokół oraz spis dokumentacji nie archiwalnej, sporządza komisja powołana przez kierownika jednostki , w której skład wchodzi:

- osoba kierująca lub prowadząca archiwum zakładowe albo składnice akt oraz przedstawiciele komórek organizacyjnych, których dokumentacja nie archiwalna podlega brakowaniu oraz kierownik kancelarii tajnej,

13. W przypadku trudności w ocenie brakowanej dokumentacji nie archiwalnej można zwrócić się do miejscowo właściwego archiwum państwowego o przeprowadzenie ekspertyzy.

14. Urząd przechowuje w archiwum zakładowym dokumenty brakowania, o których mowa wraz z dowodami przekazania nieprzydatnej dokumentacji nie archiwalnej na makulaturę bądź protokółami jej zniszczenia.

15. Uporządkowanie materiałów archiwalnych polega na podziale rzeczowym teczek

i prawidłowym ułożeniu materiałów wewnątrz teczek, ich opisaniu, nadaniu właściwego układu, sporządzeniu ewidencji oraz technicznym zabezpieczeniu.

16. 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.

17. Opisanie materiałów archiwalnych polega na umieszczeniu na wierzchniej stronie każdej teczki:

- 1) nazwy jednostki organizacyjnej i komórki organizacyjnej, w której materiały powstały;
- 2) znaku akt, to jest symbolu literowego komórki organizacyjnej oraz symbolu klasyfikacyjnego według wykazu akt, obowiązującego w jednostce organizacyjnej;
- 3) tytułu teczki, to jest nazwy hasła klasyfikacyjnego według wykazu akt, obowiązującego w danej jednostce organizacyjnej, i informacji o rodzaju materiałów archiwalnych, znajdujących się w teczce;
- 4) rocznych dat krańcowych, to jest dat najwcześniejszego i najpóźniejszego materiału archiwalnego w teczce;
- 5) sygnatury teczki, to jest numeru spisu zdawczo-odbiorczego i numeru pozycji teczki w spisie zdawczo-odbiorczym;
- 6) symbolu kwalifikacyjnego materiałów archiwalnych (kategoria A);
- 7) liczby stron w teczce.

18. Czynności związane z brakowaniem materiałów nie archiwalnych, wobec których archiwum państwowe wyraziło zgodę jest dokumentowany przez sporządzenie protokołu komisyjnego zniszczenia dokumentów nie archiwalnych.

19. Protokół komisyjnego zniszczenia materiałów nie archiwalnych sporządzany jest w dwóch egzemplarzach , z czego jeden egzemplarz należy przesłać do właściwego archiwum państwowego.

XVII. PRZECHOWYWANIE KLUCZY I PIECZĘCI

Ustala się zasady gospodarki kluczami i pieczęciami :

1. Szafy metalowe kancelarii po zamknięciu mogą być dodatkowo plombowane pieczęcią do plasteliny,
2. Klucze od szaf metalowych kancelarii materiałów niejawnych oraz pieczęcie, po zakończeniu pracy należy złożyć w pomieszczeniu kancelarii w miejscu niewidocznym.
3. Po zakończeniu pracy , pracownik materiałów niejawnych zamyka i plombuje pieczęcią do

plasteliny drzwi wejściowe kancelarii,

4. Klucz od drzwi wejściowych należy umieścić w pojemniku lub woreczku , dodatkowo zabezpieczając pieczęcią do plasteliny, następnie tak przygotowany pojemnik lub woreczek należy umieścić w miejscu niewidocznym w wyznaczonym pomieszczeniu.
5. Pieczęć do plasteliny pracownik kancelarii materiałów niejawnych powinien zabezpieczać tak, by osoby nieuprawnione nie mogły z niej korzystać,
6. Tworzy się zapasowy komplet kluczy od pomieszczeń kancelarii materiałów niejawnych,
7. Zapasowy komplet kluczy należy umieścić w zamkniętym pojemniku lub woreczku na klucze, który dodatkowo powinien być zabezpieczony pieczęcią do plasteliny.
8. Tak przygotowany komplet kluczy zapasowych należy złożyć do zdeponowania w szafie metalowej w jednym z pomieszczeń Urzędu.
9. 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 czy nie zostały naruszone pieczęcie na szafach znajdujących się w kancelarii .

ZAŁĄCZNIKI
DO PLANU OCHRONY INFORMACJI
NIEJAWNYCH

ZAŁĄCZNIK Nr 1- sposób oznaczania dokumentów niejawnych oznaczonych klauzulą poufne i zastrzeżone oraz umieszczania klauzuli na tych dokumentach

<i>Pierwsza strona dokumentu zawierającego informacje niejawne</i>
--

.....
/miejscowość data sporządzenia dokumentu/

Klauzula tajności

Egz.Nr.....

.....
/nazwa jednostki lub komórki organizacyjnej/

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

/treść dokumentu/

Klauzula tajności

Nr strony /ilość stron całego dokumentu

Druga i kolejne strony dokumentu zawierającego informacje niejawne

Klauzula tajności

Egz. Nr.....

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

/treść dokumentu/

Klauzula tajności

Nr strony /ilość stron całego dokumentu

Klauzula tajności

Egz. Nr.....

- sygnatura literowo-cyfrowa
- numer z dziennika ewidencji

łamany przez rok lub dwie ostatnie cyfry roku

/treść dokumentu/

W przypadku gdy do pisma przewodniego dołączone są załączniki

- Liczba załączników,
- Klauzule tajności załączników wraz z nr dziennika ewidencyjnego,
- Liczba stron lub kart każdego załącznika,
- W przypadku, gdy adresatowi wysyła się inną liczbę załączników niż pozostawia w aktach, dodatkowo napis „tylko adresat”,
- W przypadku, gdy załączniki mają być zwrócone napis-„do zwrotu”.

.....

/stanowisko, oraz imię i nazwisko
osoby podpisującej dokument/

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

Klauzula tajności

Nr strony /ilość stron całego dokumentu/

WZORY

PISM I UPOWAŻNIEŃ

SPIS TREŚCI

1. Poświadczenie bezpieczeństwa ,
2. Zaświadczenie o przeszkoleniu ,
3. Upoważnienie do klauzuli „zastrzeżone”,
4. Kandydat na pełnomocnika- wniosek do ABW,
5. Polecenie wszczęcia zwykłego postępowania – pismo,
6. Wniosek do ABW o sprawdzenie w kartotekach ,
7. Krajowy Rejestr Karny- pismo,
8. Krajowy Rejestr Karny – zapytanie,
9. Zgoda na dostęp do informacji niejawnych o klauzuli „poufne”,
10. Wniosek do ABW o przeprowadzenie postępowania sprawdzającego,
11. Karta Informacyjna – dodatkowe informacje.

POŚWIADCZENIE BEZPIECZEŃSTWA NR

Na podstawie art 28 pkt 1 ustawy z dnia 5 sierpnia 2010r. 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:
(nazwa klauzuli tajności) (termin ważności)

..... - na okres do:*
(nazwa klauzuli tajności) (termin ważności)

..... -na okres do:*
(nazwa klauzuli tajności) (termin ważności)

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

Pouczenie

Zgodnie z art. 29 ust. 5 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U.Nr 182, poz. 1228) poświadczenie bezpieczeństwa wydane w wyniku przeprowadzenia postępowania sprawdzającego, o którym mowa w art. 23 ust.5 ustawy, zachowuje ważność wyłącznie w okresie pracy lub służby w organie, który przeprowadził postępowanie sprawdzające.

* Niepotrzebne skreślić

ZAŚWIADCZENIE NR__
stwierdzające odbycie szkolenia
w zakresie ochrony informacji niejawnych

Stwierdza się ,że Pani (Pan):

- imię i nazwisko _____
- nr PESEL _____

odbyła (odbył) szkolenie w zakresie ochrony:

- informacji niejawnych,*
- informacji niejawnych Organizacji Traktatu Północnoatlantyckiego,*
- informacji niejawnych Unii Europejskiej,*

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:

(nazwa i adres siedziby jednostki organizacyjnej)

.....
(miejscowość i data)

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

*Niepotrzebne skreślić

**Upoważnienie uprawniające dostęp do informacji niejawnych oznaczonych
klauzulą „zastrzeżone”**

Nr pisma.....

.....
/miejscowość ,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/a..... do dostępu do informacji niejawnych
oznaczonych klauzulą „zastrzeżone” zatrudnionego/ona w na
stanowisku

.....
/kierownik jednostki/

*Upoważnienie ważne jest na czas zatrudnienia wlub do odwołania,

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

Miejscowość i data

.....
Nazwa jednostki organizacyjnej

L.dz.....

DYREKTOR

**Delegatury Agencji Bezpieczeństwa
Wewnętrznego**

Wykaz adresów Delegatur ABW

znajduje się na stronie:

<http://www.abw.gov.pl/porta1/pl/73/11/Kontakt.htm>

Na podstawie art. 14 ust. 1 – 3 pkt ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2010 r., Nr 182, poz. 1228) wykonując nałożone zadania wynikające z przepisów ustawy o ochronie informacji niejawnych, w załączeniu przesyłam Ankieta Bezpieczeństwa Osobowego z wnioskiem o przeprowadzenie postępowania sprawdzającego poszerzonego wobec Pana/i....., kandydata na pełnomocnika ochrony informacji niejawnych w/nazwa jednostki/

Jednocześnie proszę o wyznaczenie miejsca i terminu szkolenia dla kandydata na pełnomocnika w/nazwa jednostki/

Załącznik: Ankieta Bezpieczeństwa Osobowego nastronach.

.....
/Podpis kierownika jednostki/

Miejscowość data.....

.....
Nazwa jednostki organizacyjnej

Pełnomocnik ds. Ochrony Informacji Niejawnych
W.....

POLECENIE WSZCZĘCIA ZWYKŁEGO POSTĘPOWANIA SPRAWDZAJACEGO

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

.....
/Pieczęć i podpis kierownika jednostki organizacyjnej/

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 przeprowadzanym zwykłym postępowaniem sprawdzającym wobec następującej osoby:

1. Nr PESEL
2. Nazwisko (w tym przybrane)
3. Imię (imiona)
4. Imię ojca
5. Imię matki
6. Nazwisko rodowe matki
7. Data urodzenia
8. Miejsce urodzenia
9. Adres zameldowania
10. 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

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 przekazuje 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:

- 11. Imię (imiona)
- 12. Nazwisko (w tym przybrane)
- 13. Nr PESEL
- 14. Imię ojca

Zapytanie proszę odesłać na adres:.....

.....
Pieczętka i podpis pełnomocnika ochrony lub zastępcy pełnomocnika ochrony

MINISTERSTWO SPRAWIEDLIWOŚCI
KRAJOWY REJESTR KARNY

Nazwa i adres podmiotu kierującego zapytanie
oraz numer urządzenia służącego do automatycznego
odbioru informacji

Data wpływu

Data wystawienia.....
znak opłaty

ZAPYTANIE O UDZIELENIE INFORMACJI O OSOBIE *

Numer PESEL _ _ _ _ _

1. Nazwisko rodowe
2. Nazwisko (w tym przybrane)
3. Imiona
4. Imię ojca
5. Imię matki
6. Data urodzenia
7. Nazwisko rodowe matki
8. Miejsce urodzenia
9. Obywatelstwo
10. Miejsce zamieszkania
11. Wskazanie postępowania , o którym mowa w art.6 pkt 4-6 i 8-10 ustawy z dnia 24 maja 2000r o Krajowym Rejestrze Karnym (Dz.U.Nr 50,poz.580 z późn. zm.), związku z którym zachodzi potrzeba uzyskania informacji o osobie – **art.25 ust.1 Ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U.Nr 182 ,poz.1228)**

12. Rodzaj danych, które maja być przedmiotem informacji o osobie:

- | | |
|---|-------------------------|
| 1. Kartoteka karna | 2. Kartoteka Nieletnich |
| 3. Kartoteka Osób Pozbawionych Wolności oraz Poszukiwanych Listem Gończym **) | |

1. Zakres danych, które maja być przedmiotem informacji o osobie.....

.....
(podpis osoby uprawnionej)

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:

1. Imię (imiona)
2. Nazwisko (w tym przybrane)
3. Nr PESEL
4. Imię ojca
5. Imię matki
6. Nazwisko rodowe matki
7. Data urodzenia
8. Miejsce urodzenia

.....

Pieczątka i podpis kierownika jednostki organizacyjnej

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 :

1. Imię
2. Nazwisko
3. 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 odpowiednia klauzule lub klauzule tajności

INFORMACJA DODATKOWA:

Zgodnie z art. 73 ust. 1 ustawy o ochronie informacji niejawnych, Agencja Bezpieczeństwa Wewnętrznego prowadzi ewidencje osób uprawnionych na podstawie przepisów ustawy do dostępu do informacji niejawnych o klauzuli „poufne” i wyższej (tj. poprzez poświadczenie bezpieczeństwa lub zgodę, o której mowa w art. 34 ust. 9 ustawy) oraz ewidencje osób, którym odmówiono wydania lub cofnięto poświadczenie bezpieczeństwa. Ewidencja ta prowadzona jest w oparciu o dane przekazywane do ABW przez pełnomocników ochrony na podstawie art. 15 ust. 1 pkt. 9 ustawy.

Wypełnione karty pełnomocnicy przesyłają do właściwej Delegatury ABW

Uwaga:

Kartę Informacyjną należy przesłać w przypadku:

- 1- Wydania Poświadczenia Bezpieczeństwa,
- 2- Odmowy wydania Poświadczenia Bezpieczeństwa,
- 3- Cofnięcia Poświadczenia Bezpieczeństwa,
- 4- Wydania zgody na udostępnienie informacji niejawnych w oparciu o art.34 ust.9.

Aktualny wzór Karty Informacyjnej można pobrać na stronie:

http://www.bip.abw.gov.pl/portal/bip/76/151/INFORMACJA_NA_TEMAT_KART_INFORMACYJNYCH.html

ZAŁĄCZNIK NR 3 - protokół oceny dokumentacji niearchiwalnej

.....
(nazwa jednostki organizacyjnej)

PROTOKÓŁ OCENY DOKUMENTACJI NIEARCHIWALNEJ

Komisja w składzie:

.....
imię i nazwisko, stanowisko

.....
imię i nazwisko, stanowisko

.....
imię i nazwisko, stanowisko

dokonała oceny i wydzielenia przeznaczonej do przekazania na makulaturę lub zniszczenie dokumentacji niearchiwalnej w ilościmb. i stwierdziła, że stanowi ona dokumentację niearchiwalną dla celów praktycznych jednostki organizacyjnej, oraz że upłynęły terminy jej przechowywania określone w jednolitym rzeczowym wykazie akt.

Przewodniczący komisji:

Członkowie komisji :

.....
.....

Załączniki:

.....kart spisu

.....pozycji spisu

ZAŁĄCZNIK NR 4 - spis dokumentacji niearchiwalnej przeznaczonej na makulaturę lub zniszczenie

.....
nazwa i adres jednostki organizacyjnej

**SPIS DOKUMENTACJI NIEARCHIWALNEJ PRZEZNACZONEJ NA MAKULATURĘ
LUB ZNISZCZENIE**

L.p.	Tytuł teczki	Symbol z wykazu rzeczowego	Daty skrajne	Uwagi

ZAŁĄCZNIK NR 5- protokół komisyjnego zniszczenia dokumentów niearchiwalnych

**PROTOKÓŁ
KOMISYJNEGO ZNISZCZENIA DOKUMENTÓW NIEARCHIWALNYCH**

W dniu komisja w składzie:

1.Przewodniczący komisji.....

(kierownik lub pracownik archiwum zakładowego)

2. Członek komisji.....

(przedstawiciel komórek org., których dokumenty są brakowane),

3. Członek komisji.....

(Pełnomocnik ochrony lub pracownik pionu ochrony),

dokonała zniszczenia dokumentów niearchiwalnych, w oparciu o zgodę Archiwum Państwowego – pismo nr..... z dnia..... wydana na podstawie Protokołu oceny dokumentacji niearchiwalnej oraz Spis dokumentacji niearchiwalnej przeznaczonej na makulaturę lub zniszczenie, pismo nr..... z dnia.....

Dokumenty zostały komisyjnie zniszczone w dniu..... przez *(spalenie, zmielenie itp.)*

Podpisy członków komisji:

1. Przewodniczący komisji.....

2. Członek komisji.....

3. Członek komisji.....

ZAŁĄCZNIK NR 6 - wymagania w zakresie ochrony informacji niejawnych stanowiących tajemnicę służbową oznaczonych klauzulą „zastrzeżone”

**WYMAGANIA W ZAKRESIE OCHRONY INFORMACJI NIEJAWNYCH
STANOWIĄCYCH TAJEMNICĘ SŁUŻBOWĄ OZNACZONYCH KLAUZULĄ
„ZASTRZEŻONE”**

I. DEFINICJA INFORMACJI NIEJAWNYCH OZNACZONYCH KLAUZULĄ „ZASTRZEŻONE”.

1. 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.
2. Informacje niejawne , którym przyznano klauzulę „zastrzeżone” są chronione zgodnie z przepisami ustawy z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych (Dz.U.Nr 182,poz.1228).

Oznacza to w szczególności , e informacje takie:

- 1) mogą być udostępnione wyłącznie osobie uprawnionej do dostępu do informacji niejawnych oznaczonych klauzulą „zastrzeżone”,
- 2) muszą być wytwarzane , przetwarzane lub przechowywane w warunkach uniemożliwiających ich nieuprawnione ujawnienie,
- 3) muszą być odpowiednio chronione.

II. OZNACZANIE INFORMACJI ZASTRZEŻONYCH.

1. Propozycje przyznania klauzuli niejawności na wykonywanym dokumencie przedstawia osoba sporządzająca dokument,
2. Klauzulę niejawności na danym dokumencie przyznaje osoba która jest upoważniona do odpisania dokumentu,
3. Rękopisy sporządzanych dokumentów niejawnych oznaczonych klauzulą „zastrzeżone” powinny być opracowywane w brulionach (zeszytach pracy) uprzednio zarejestrowanych kancelarii materiałów niejawnych.

4. Dokumenty niejawne oznaczone klauzulą „zastrzeżone” powinny być opisane i oznaczone zgodnie Rozporządzeniem 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 z 2010 roku , poz.1069) Wzór sposobu opisanania dokumentu stanowi załącznik do Planu .

III. PRZEKAZYWANIE NA ZEWNĄTRZ INFORMACJI ZASTRZEŻONYCH.

1. Materiały zawierające informacje niejawne oznaczone klauzulą „zastrzeżone”, nadawane w postaci listów , przekazuje się jako listy polecone, w dwóch nieprzezroczystych mocnych kopertach, materiały nadawane w postaci paczek, przekazuje się jako paczki wartościowe w dwóch nieprzezroczystych warstwach mocnego papieru, które oznaczają się w sposób następujący:

- na wewnętrznej kopercie (listu) lub wewnętrznej warstwie papieru (paczki) muszą być umieszczone:
 - klauzula tajności ewentualnie dodatkowe oznaczenie,
 - znak pisma,
 - imienne określenie adresata,
 - imię , nazwisko i podpis osoby pakującej.
- na zewnętrznej kopercie (listu) lub zewnętrznej warstwie papieru (paczki) muszą być umieszczone:
 - nazwa jednostki organizacyjnej adresata,
 - adres siedziby adresata,
 - znak pisma, jednak bez umieszczania informacji , że korespondencja zawiera informacje „zastrzeżone”, tj. bez symbolu „**Z**”, po literowym oznaczeniu komórki organizacyjnej twórcy dokumentu,
 - nazwa jednostki organizacyjnej nadawcy.

IV. WYTWARZANIE INFORMACJI ZASTRZEŻONYCH Z WYKORZYSTANIEM SPRZĘTU KOMPUTEROWEGO.

1. Dokumenty oznaczone klauzulą „zastrzeżone” mogą być wytwarzane pod warunkiem zastosowania niezbędnych czynności i zabezpieczeń określonych w rozdziale 8 (BEZPIECZENSTWO TELEINFORMATYCZNE) ustawy o ochronie informacji niejawnych.
2. Pełnomocnik określi osoby ,które posiadają poświadczenia bezpieczeństwa lub upoważnienia nadane przez kierownika jednostki i są uprawnione do wytwarzania materiałów zastrzeżonych.
3. Wykaz osób uprawnionych do wytwarzania materiałów oznaczonych klauzulą ”zastrzeżone” prowadzony jest przez Pełnomocnika w formie rejestru.
4. Należy dokonać akredytacji bezpieczeństwa teleinformatycznego systemu i sieci teleinformatycznej, w których będą wytwarzane , przetwarzane, przechowywane lub przekazywane informacje niejawne oznaczone klauzulą „zastrzeżone”.
5. Po akredytacji, należy wydzielić stanowisko komputerowe, które będzie służyło do wytwarzania tych dokumentów.
6. Dokumenty szczególnych wymagań bezpieczeństwa oraz procedury bezpiecznej eksploatacji systemów i sieci teleinformatycznych , w których mają być wytwarzane , przetwarzane, przechowywane lub przekazywane informacje niejawne oznaczone klauzulą „zastrzeżone” są akredytowane przez kierownika jednostki a następnie przedstawiane właściwej służbie ochrony państwa. ABW może wnieść w ciągu 30 dni od przedstawienia dokumentacji poprawki do określonych procedur.

V. KOPIE ZAPASOWE:

1. Zaleca się wykonywanie kopii zapasowych wykonanych dokumentów oznaczonych klauzulą „zastrzeżone”,
2. Sposób przechowywania zapasowych kopii, w przypadku gdy nośnikiem informacji jest materiał inny niż pismo, jest taki sam jak sposób przechowywania dokumentów wykonanych w tradycyjnej formie, zaewidencjonowanie kopii zapasowych polega na tym, że klauzulę tajności i sygnaturę literowo-cyfrową umieszcza się przez ostemplowanie, nadrukowanie, wpisanie odręczne, trwałe dołączenie metek, nalepek, kalkomanii lub w inny

sposób, bezpośrednio, a jeżeli jest to nie możliwe na ich obudowie lub opakowaniu.

VI. PRZECHOWYWANIE INFORMACJI ZASTRZEŻONYCH W KOMÓRKACH ORGANIZACYJNYCH LUB NA STANOWISKACH PRACY.

1. Informacje niejawne oznaczone klauzulą „zastrzeżone” podlegają ochronie w sposób określony Ustawą o ochronie informacji niejawnych do czasu , gdy osoba , która nadała klauzulę niejawności nie zniesie okresu ochronnego.
2. Dokumentacja zawierająca informacje niejawne oznaczone klauzulą „zastrzeżone” może być przechowywana w kancelarii materiałów niejawnych lub w pomieszczeniach na stanowiskach pracy w meblach biurowych zamykanych na klucz (zabezpieczone przed dostępem osób nieuprawnionych).

VII. NADAWANIE , ZMIANA I ZNOSZENIE KLAUZULI „ZASTRZEŻONE”.

1. Klauzulę przyznaje osoba, która jest upoważniona do podpisania dokumentu lub oznaczenia innego niż dokument materiału. Uprawnienie do przyznania , obniżania i znoszenia klauzuli tajności przysługuje wyłącznie w zakresie posiadanego dostępu do informacji niejawnych.
2. Zawyżanie lub zaniżanie klauzuli tajności jest niedopuszczalne.
3. Odbiorca materiału zgłasza osobie , która przyznała daną klauzulę , albo jej przełożonemu fakt wyraźnego zawyżenia lub zaniżenia klauzuli tajności. W przypadku gdy osoba lub jej przełożony zdecyduje o zmianie klauzuli, powinna o tym poinformować odbiorców tego materiału. Odbiorcy materiału, którzy przekazali go kolejnym odbiorcom ,są odpowiedzialni za poinformowanie o ich zmianie klauzuli.
4. Zmiany nadanej klauzuli dokonuje się przez jej skreślenie i wpisanie obok niej nowej z podaniem:
 - a) daty,
 - b) imienia i nazwiska,
 - c) podpisu osoby dokonującej zmiany.
5. Skreślenie bez wpisania daty , imienia i nazwiska oraz podpisu dokonującego zmiany uważa się za nie dokonane.
6. Skreślenia oraz pozostałych wpisów dokonuje się kolorem czerwonym . Wycieranie , wywabianie lub zamazywanie klauzuli , która podlega zmianie i dokonanych zmian jest

niedozwolone. Fakt dokonania zmian klauzuli należy odnotować w odpowiednich dziennikach ewidencyjnych lub rejestrach materiałów niejawnych, z podaniem przyczyny zmiany.

7. Uprawnienia osoby o której mowa w pkt.1 , w zakresie przyznawania , obniżania lub znoszenia klauzuli tajności materiału oraz określenia okresu jaki informacja niejawna podlega ochronie , przechodzą w przypadku rozwiązania, zniesienia, likwidacji, przekształcenia lub reorganizacji dotyczącej stanowiska lub funkcji tej osoby, na jej następcę prawnego. W razie braku następcy prawnego, uprawnienia w tym zakresie przechodzą na właściwą służbę ochrony państwa.

ZAŁĄCZNIK NR 7 - Instrukcja alarmowa w przypadku zgłoszenia o podłożeniu lub znalezieniu ładunku wybuchowego w urzędzie.

**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, i mogą to być ładunki wybuchowe , nie wolno dotykać. O ich umiejscowieniu należy natychmiast powiadomić administratora obiektu i policję .

5. W przypadku , gdy użytkownicy pomieszczeń faktycznie stwierdza 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. WSPÓŁPRACA 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.

ZAŁĄCZNIK NR 8 - Instrukcja postępowania w przypadku otrzymania przesyłki niewiadomego pochodzenia.

**INSTRUKCJA POSTĘPOWANIA W PRZYPADKU OTRZYMANIA PRZESYŁKI
NIEWIADOMEGO POCHODZENIA.**

W przypadku otrzymania jakiejkolwiek przesyłki niewiadomego pochodzenia lub budzącej podejrzenia z jakiegokolwiek innego powodu:

- Brak nadawcy,
- Brak adresu nadawcy,
- Przesyłka pochodzi od nadawcy lub z miejsca z którego nie spodziewamy się ,
- Inne podejrzenia,

Nie należy otwierać tej przesyłki

Należy:

- 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 pożarna- nr 998.

Służby 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 wąchać 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 pożarna- nr 998.

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

PROTOKÓŁ OTWARCIA SEJFU (Szafy)

W dniu.....

Komisja w składzie :

1.

(imię i nazwisko)

2.

(imię i nazwisko)

3.

(imię i nazwisko)

dokonała otwarcia sejfu (szafy) znajdującej się w pomieszczeniu nr, którego użytkownikiem jest.....

(imię i nazwisko oraz stanowisko służbowe)

Z sejfu (szafy) zostały zabrane następujące dokumenty (materiały, przedmioty):

1.

2.

3.

którymi obecnie dysponuje Pan/i

.....

(imię i nazwisko oraz stanowisko służbowe)

Sejf (szafę) zamknięto i zaplombowano pieczęcią (*referentka do plasteliny nr.....*) w obecności członków komisji.

Podpisy członków komisji:

1.

2.

3.