ppłk dypl. rez. Kazimierz Baciak

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

(Dz.U. Nr 182, poz. 1228)





Nieobowiązująca

Ustawa z dnia 22 stycznia 1999 roku o ochronie informacji niejawnych

Tekst jednolity:

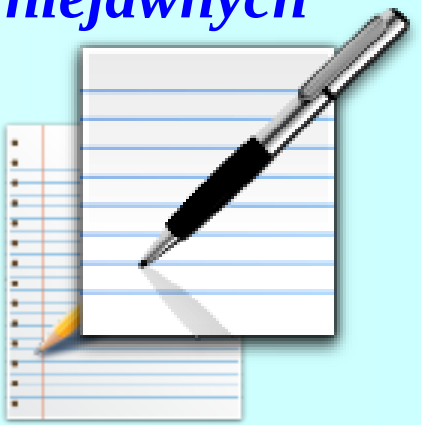
Obwieszczenie Marszałka Sejmu RP z dnia 22 września 2005 r. w sprawie ogłoszenia tekstu jednolitego ustawy o ochronie informacji niejawnych

[Dz.U. z 2005 r. Nr 196 Poz. 1631]



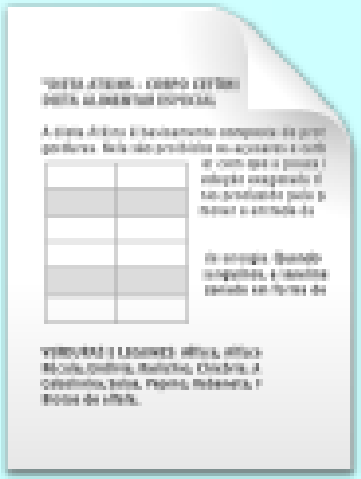
... Rana może być opatrzona, obelga darowana, ale ten, kto wyjawił tajemnicę, nie ma już nadziei …

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



1. *Przepisy ogólne*
2. *Klasyfikowanie informacji niejawnych*
3. *Organizacja ochrony informacji niejawnych*
4. *Szkolenie w zakresie ochrony informacji niejawnych*
5. *Bezpieczeństwo osobowe*
6. *Postępowanie odwoławcze i skargowe, wznowienie postępowania*
7. *Kancelarie tajne. Środki bezpieczeństwa fizycznego*
8. *Bezpieczeństwo teleinformatyczne*
9. *Bezpieczeństwo przemysłowe*
10. *Ewidencje i udostępnianie danych oraz akt postępowań sprawdzających, kontrolnych postępowań sprawdzających i postępowań bezpieczeństwa przemysłowego*
11. *Zmiany w przepisach obowiązujących*
12. *Przepisy przejściowe i końcowe*

1. Przepisy ogólne



1. Przepisy ogólne



Ustawa określa zasady ochrony informacji:

1) *klasyfikowania informacji niejawnych;*
2) *organizowania ochrony informacji niejawnych;*
3) *przetwarzania informacji niejawnych;*
4) *postępowania sprawdzającego prowadzonego w celu ustalenia, czy osoba nim objęta daje rękojmię zachowania tajemnicy, zwanego dalej odpowiednio „postępowaniem sprawdzającym” lub „kontrolnym postępowaniem sprawdzającym”;*
5) *organizacji kontroli stanu zabezpieczenia informacji niejawnych;*
6) *postępowania prowadzonego w celu ustalenia, czy przedsiębiorca nim objęty zapewnia warunki do ochrony informacji niejawnych, zwanego dalej „postępowaniem bezpieczeństwa przemysłowego”;*
7) *ochrony informacji niejawnych w systemach teleinformatycznych;*
8) *stosowania środków bezpieczeństwa fizycznego w odniesieniu do informacji niejawnych.*

Art. 1.

Przepisy ustawy mają zastosowanie do:

1) organów władzy publicznej, w szczególności:

a) Sejmu i Senatu,

b) Prezydenta Rzeczypospolitej Polskiej,

c) organów administracji rządowej,

d) organów jednostek samorządu terytorialnego, a także innych podległych im jednostek organizacyjnych lub przez nie nadzorowanych,

e) sądów i trybunałów,

f) organów kontroli państwowej i ochrony prawa;



2) jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych;

3) Narodowego Banku Polskiego;

4) państwowych osób prawnych i innych niż wymienione w pkt 1–3 państwowych jednostek organizacyjnych;

5) jednostek organizacyjnych podległych organom władzy publicznej lub nadzorowanych przez te organy;

6) przedsiębiorców zamierzających ubiegać się albo ubiegających się o zawarcie umów związanych z dostępem do informacji niejawnych lub wykonujących takie umowy albo wykonujących na podstawie przepisów prawa zadania związane z dostępem do informacji niejawnych.

3. **Przepisy ustawy o ochronie informacji niejawnych nie naruszają przepisów innych ustaw o ochronie tajemnicy zawodowej lub innych tajemnic prawnie chronionych, z zastrzeżeniem art. 5.**

Art. 2. W rozumieniu ustawy:

***1) jednostką organizacyjną** – jest podmiot wymieniony w art. 1 ust. 2;*

***2) rękojmią zachowania tajemnicy** – jest zdolność osoby do spełnienia ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem, stwierdzona w wyniku przeprowadzenia postępowania sprawdzającego;*

***3) dokumentem** – jest każda utrwalona informacja niejawna;*

***4) materiałem** – jest dokument lub przedmiot albo dowolna ich część, chronione jako informacja niejawna, a zwłaszcza urządzenie, wyposażenie lub broń wyprodukowane albo będące w trakcie produkcji, a także składnik użyty do ich wytworzenia;*

***5) przetwarzaniem informacji niejawnych** – są wszelkie operacje wykonywane w odniesieniu do informacji niejawnych i na tych informacjach, w szczególności ich wytwarzanie, modyfikowanie, kopiowanie, klasyfikowanie, gromadzenie, przechowywanie, przekazywanie lub udostępnianie;*

Art. 2. W rozumieniu ustawy:

6) systemem teleinformatycznym *– jest system teleinformatyczny w rozumieniu art. 2 pkt 3 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. Nr 144, poz. 1204, z późn. zm.[2]));*

7) dokumentem szczególnych wymagań bezpieczeństwa *– jest systematyczny opis sposobu zarządzania bezpieczeństwem systemu teleinformatycznego;*

8) dokumentem procedur bezpiecznej eksploatacji systemu teleinformatycznego *– jest opis sposobu i trybu postępowania w sprawach związanych z bezpieczeństwem informacji niejawnych przetwarzanych w systemie teleinformatycznym oraz zakres odpowiedzialności użytkowników systemu teleinformatycznego i pracowników mających do niego dostęp;*

9) dokumentacją bezpieczeństwa systemu teleinformatycznego *– jest dokument szczególnych wymagań bezpieczeństwa oraz dokument procedur bezpiecznej eksploatacji systemu teleinformatycznego, opracowane zgodnie z zasadami określonymi w ustawie;*

Art. 2. W rozumieniu ustawy:

10) akredytacją bezpieczeństwa teleinformatycznego – *jest dopuszczenie systemu teleinformatycznego do przetwarzania informacji niejawnych;*

11) certyfikacją – *jest proces potwierdzania zdolności urządzenia, narzędzia lub innego środka do ochrony informacji niejawnych;*

12) audytem bezpieczeństwa systemu teleinformatycznego – *jest weryfikacja poprawności realizacji wymagań i procedur, określonych w dokumentacji bezpieczeństwa systemu teleinformatycznego;*

13) przedsiębiorcą – *jest przedsiębiorca w rozumieniu art. 4 ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej (Dz. U. z 2007 r. Nr 155, poz. 1095, z późn. zm.[3])) lub każda inna jednostka organizacyjna, niezależnie od formy własności, którzy w ramach prowadzonej działalności gospodarczej zamierzają realizować lub realizują związane z dostępem do informacji niejawnych umowy lub zadania wynikające z przepisów prawa;*

14) kierownikiem przedsiębiorcy – *jest członek jednoosobowego zarządu lub innego jednoosobowego organu zarządzającego, a jeżeli organ jest wieloosobowy – cały organ albo członek lub członkowie tego organu wyznaczeni co najmniej uchwałą zarządu do pełnienia funkcji kierownika przedsiębiorcy, z wyłączeniem pełnomocników ustanowionych przez ten organ lub jednostkę; w przypadku spółki jawnej i spółki cywilnej kierownikiem przedsiębiorcy są wspólnicy prowadzący sprawy spółki, w przypadku spółki partnerskiej – wspólnicy prowadzący sprawy spółki albo zarząd, a w odniesieniu do spółki komandytowej i spółki komandytowo-akcyjnej – komplementariusze prowadzący sprawy spółki; w przypadku osoby fizycznej prowadzącej działalność gospodarczą kierownikiem przedsiębiorcy jest ta osoba; za kierownika przedsiębiorcy uważa się również likwidatora, a także syndyka lub zarządcę ustanowionego w postępowaniu upadłościowym; kierownik przedsiębiorcy jest kierownikiem jednostki organizacyjnej w rozumieniu przepisów ustawy;*

Art. 2. W rozumieniu ustawy:

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

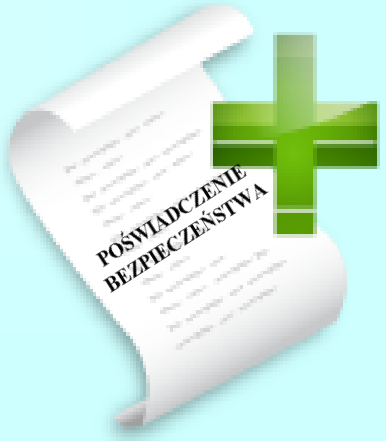
16) szacowaniem ryzyka – *jest całościowy proces analizy i oceny ryzyka;*

17) zarządzaniem ryzykiem – *są skoordynowane działania w zakresie zarządzania bezpieczeństwem informacji, z uwzględnieniem ryzyka;*

18) zatrudnieniem – *jest również odpowiednio powołanie, mianowanie lub wyznaczenie.*

Dostęp do informacji niejawnych

Art. 4. Informacje niejawne mogą być udostępnione wyłącznie osobie dającej rękojmię zachowania tajemnicy i tylko w zakresie niezbędnym do wykonywania przez nią pracy lub pełnienia służby na zajmowanym stanowisku albo wykonywania czynności zleconych



Rękojmia zachowania tajemnicy:

spełnienie ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem

2. Klasyfikowanie informacji niejawnych. Klauzule tajności



Tajemnicą państwową – jest informacja …

Tajemnicą służbową - jest informacja …

Informacje niejawne oznacza się klauzulą:

- **„Ściśle tajne"**
- **„Tajne„**
- **„Poufne"**
- **„Zastrzeżone"**



Klauzule tajności RP

NAZWA	OZNACZENIE
ŚCIŚLE TAJNE	„00”
TAJNE	„0”
POUFNE	„PF”
ZASTRZEŻONE	„Z”

2. Klasyfikowanie informacji niejawnych

Art. 5.

Informacjom niejawnym nadaje się klauzulę …

„ściśle tajne”, jeżeli ich nieuprawnione ujawnienie spowoduje wyjątkowo poważną szkodę dla Rzeczypospolitej Polskiej przez to, że …

„tajne”, jeżeli ich nieuprawnione ujawnienie spowoduje poważną szkodę dla Rzeczypospolitej Polskiej przez to, że …

„poufne”, jeżeli ich nieuprawnione ujawnienie spowoduje szkodę dla Rzeczypospolitej Polskiej przez to, że …

„zastrzeżone”, jeżeli nie nadano im wyższej klauzuli tajności, a ich nieuprawnione ujawnienie może mieć szkodliwy wpływ …

Informacjom niejawnym nadaje się klauzulę **„ŚCIŚLE TAJNE”,** jeżeli ich nieuprawnione ujawnienie spowoduje wyjątkowo poważną szkodę dla Rzeczypospolitej Polskiej przez to, że:

1. zagrozi niepodległości, suwerenności lub integralności terytorialnej Rzeczypospolitej Polskiej; zagrozi bezpieczeństwu wewnętrznemu lub porządkowi konstytucyjnemu Rzeczypospolitej Polskiej;
2. zagrozi sojuszom lub pozycji międzynarodowej Rzeczypospolitej Polskiej;
3. osłabi gotowość obronną Rzeczypospolitej Polskiej;



3. doprowadzi lub może doprowadzić do identyfikacji funkcjonariuszy, żołnierzy lub pracowników służb odpowiedzialnych za realizację zadań wywiadu lub kontrwywiadu, którzy wykonują czynności operacyjno-rozpoznawcze, jeżeli zagrozi to bezpieczeństwu wykonywanych czynności lub może doprowadzić do identyfikacji osób udzielających im pomocy w tym zakresie;
4. zagrozi lub może zagrozić życiu lub zdrowiu funkcjonariuszy, żołnierzy lub pracowników, którzy wykonują czynności operacyjno-rozpoznawcze, lub osób udzielających im pomocy w tym zakresie;
5. zagrozi lub może zagrozić życiu lub zdrowiu świadków koronnych lub osób dla nich najbliższych.



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

1. uniemożliwi realizację zadań związanych z ochroną suwerenności lub porządku konstytucyjnego Rzeczypospolitej Polskiej;
2. pogorszy stosunki Rzeczypospolitej Polskiej z innymi państwami lub organizacjami międzynarodowymi;
3. zakłóci przygotowania obronne państwa lub funkcjonowanie Sił Zbrojnych Rzeczypospolitej Polskiej;

4. utrudni wykonywanie czynności operacyjno - rozpoznawczych prowadzonych w celu zapewnienia bezpieczeństwa państwa lub ścigania sprawców zbrodni przez służby lub instytucje do tego uprawnione;
5. w istotny sposób zakłóci funkcjonowanie organów ścigania i wymiaru sprawiedliwości;
6. przyniesie stratę znacznych rozmiarów w interesach ekonomicznych Rzeczypospolitej Polskiej.

Informacjom niejawnym nadaje się klauzulę **„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 zagrozi bezpieczeństwu obywateli;
4. utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę bezpieczeństwa lub podstawowych interesów Rzeczypospolitej Polskiej;

1. utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę porządku publicznego, bezpieczeństwa obywateli lub ściganie sprawców przestępstw i przestępstw skarbowych oraz organom wymiaru sprawiedliwości;
2. zagrozi stabilności systemu finansowego Rzeczypospolitej Polskiej;
3. 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.



Klauzule tajności organizacji międzynarodowych

	NATO	UNIA EUROPEJSKA
ŚCIŚLE TAJNE	COSMIC TOP SECRET	TRÈS SECRET UE/ EU TOP SECRET
TAJNE	NATO SECRET	SECRET UE/ EU SECRET
POUFNE	NATO CONFIDENTIAL	CONFIDENTIEL UE/ EU CONFIDENTIAL
ZASTRZEŻONE	NATO RESTRICTED	RESTREINT UE/ EU RESTRICTED

COSMIC TOP SECRET (CTS) - nieupoważnione ujawnienie spowodowałoby wyjątkowo poważne straty dla NATO **(kolor czerwony)**;

NATO SECRET (NS) - nieupoważnione ujawnienie spowodowałoby poważne straty dla NATO **(kolor niebieski);**

NATO CONFIDENTIAL (NC) - nieupoważnione ujawnienie byłoby szkodliwe dla NATO **(kolor zielony)**;

NATO RESTRICTED (NR) - nieupoważnione ujawnienie byłoby szkodliwe dla interesów lub skuteczności NATO **(kolor szary).**

2. Klasyfikowanie informacji niejawnych



Art. 6.

Klauzulę tajności nadaje osoba, która jest uprawniona do podpisania dokumentu lub oznaczenia innego niż dokument materiału.

Zniesienie lub zmiana klauzuli tajności są możliwe wyłącznie po wyrażeniu pisemnej zgody przez uprawnioną osobę…





Prezes Rady Ministrów określi, w drodze rozporządzenia, sposób oznaczania materiałów umieszczania na nich klauzul tajności, a także tryb i sposób zmiany lub znoszenia nadanej klauzuli.

Informacje niejawne - Ochrona

2. Klasyfikowanie informacji niejawnych

Art. 7. (d. art. 25)

Chronione bez względu na upływ czasu …

1) dane mogące doprowadzić do identyfikacji funkcjonariuszy, ….;
2) dane mogące doprowadzić do identyfikacji osób, …;
3) informacje niejawne uzyskane od organów innych państw ….



Art. 8. Informacje niejawne, którym nadano określoną klauzulę tajności:

1. mogą być udostępnione wyłącznie osobie uprawnionej, zgodnie z przepisami ustawy dotyczącymi dostępu do określonej klauzuli tajności;
2. muszą być przetwarzane w warunkach uniemożliwiających ich nieuprawnione ujawnienie, zgodnie z przepisami określającymi wymagania dotyczące kancelarii tajnych, bezpieczeństwa systemów teleinformatycznych, obiegu materiałów i środków bezpieczeństwa fizycznego, odpowiednich do nadanej klauzuli tajności;
3. muszą być chronione, odpowiednio do nadanej klauzuli tajności, z zastosowaniem środków bezpieczeństwa określonych w ustawie i przepisach wykonawczych wydanych na jej podstawie.

2. Klasyfikowanie informacji niejawnych

Art. 9.

1. Odbiorca materiału, w przypadku stwierdzenia zawyżenia lub zaniżenia klauzuli tajności może zwrócić się do osoby, która ją nadała, albo przełożonego tej osoby z wnioskiem o dokonanie stosownej zmiany.
2. W przypadku odmowy dokonania zmiany lub nieudzielenia odpowiedzi w ciągu 30 dni od daty złożenia wniosku, o którym mowa w ust. 1, odbiorca materiału może zwrócić się odpowiednio do ABW lub SKW o rozstrzygnięcie sporu.
3. Spór, o którym mowa w ust. 2, ABW lub SKW rozstrzyga w terminie 30 dni od daty złożenia wniosku o rozstrzygnięcie sporu.
4. Jeżeli stroną sporu, o którym mowa w ust. 2, jest ABW albo SKW, to spór rozstrzyga Prezes Rady Ministrów w terminie 30 dni od daty złożenia wniosku o rozstrzygnięcie sporu.
5. Prezes Rady Ministrów może upoważnić Szefa Kancelarii Prezesa Rady Ministrów, sekretarza stanu albo podsekretarza stanu w Kancelarii Prezesa Rady Ministrów do wykonywania czynności, o których mowa w ust. 4.

3. Organizacja ochrony informacji niejawnych





3. Organizacja ochrony informacji niejawnych

Art. 10.

ABW i SKW nadzorując funkcjonowanie systemu ochrony informacji niejawnych w jednostkach organizacyjnych pozostających w ich właściwości (MON- SKW, ABW inne):

1) prowadzą kontrolę ochrony informacji niejawnych i przestrzegania przepisów obowiązujących w tym zakresie;

2) realizują zadania w zakresie bezpieczeństwa systemów teleinformatycznych;

3) prowadzą postępowania sprawdzające, kontrolne postępowania sprawdzające oraz postępowania bezpieczeństwa przemysłowego;

4) zapewniają ochronę informacji niejawnych wymienianych między Rzeczpospolitą Polską a innymi państwami lub organizacjami międzynarodowymi;

5) prowadzą doradztwo i szkolenia w zakresie ochrony informacji niejawnych.





3. Organizacja ochrony informacji niejawnych

Art. 11.

Szef ABW pełni funkcję krajowej władzy bezpieczeństwa.

Szef ABW pełni funkcję krajowej władzy bezpieczeństwa w odniesieniu do MON za pośrednictwem Szefa SKW.



Prezes Rady Ministrów określi, w drodze rozporządzenia, zakres, tryb i sposób współdziałania , Szefa ABW i Szefa SKW w zakresie wykonywania funkcji krajowej władzy bezpieczeństwa przez Szefa ABW.

Art. 12.

Kontrole ABW i SKW (d. art.16)



Prezes Rady Ministrów określi, w drodze rozporządzenia:

- ✓ ***sposób przygotowania …***
- ✓ ***tryb uzgadniania …;***
- ✓ ***zadania funkcjonariuszy ABW oraz funkcjonariuszy lub żołnierzy SKW …;***
- ✓ ***sposób dokumentowania czynności kontrolnych.…***

3. Organizacja ochrony informacji niejawnych

Art. 13.

Współdziałanie kierownika jednostki organizacyjnej z ABW i SKW (d. art. 14 ust. 3)



Prezes Rady Ministrów określi, w drodze rozporządzenia:

- ✓ ***szczegółowy zakres, warunki, sposób i tryb przekazywania przez kierowników jednostek organizacyjnych służbom i instytucjom uprawnionym ….;***
- ✓ ***szczegółowy zakres, warunki, sposób i tryb udzielania przez Centralne Biuro Antykorupcyjne, zwane dalej „CBA”, Policję, Straż Graniczną, Żandarmerię Wojskową oraz organy kontroli skarbowej ….***

3. Organizacja ochrony informacji niejawnych



Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie przekazywania informacji, udostępniania dokumentów oraz udzielania pomocy służbom i instytucjom uprawnionym do prowadzenia poszerzonych postępowań sprawdzających, kontrolnych postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego [Dz.U. Nr 258, 1750]

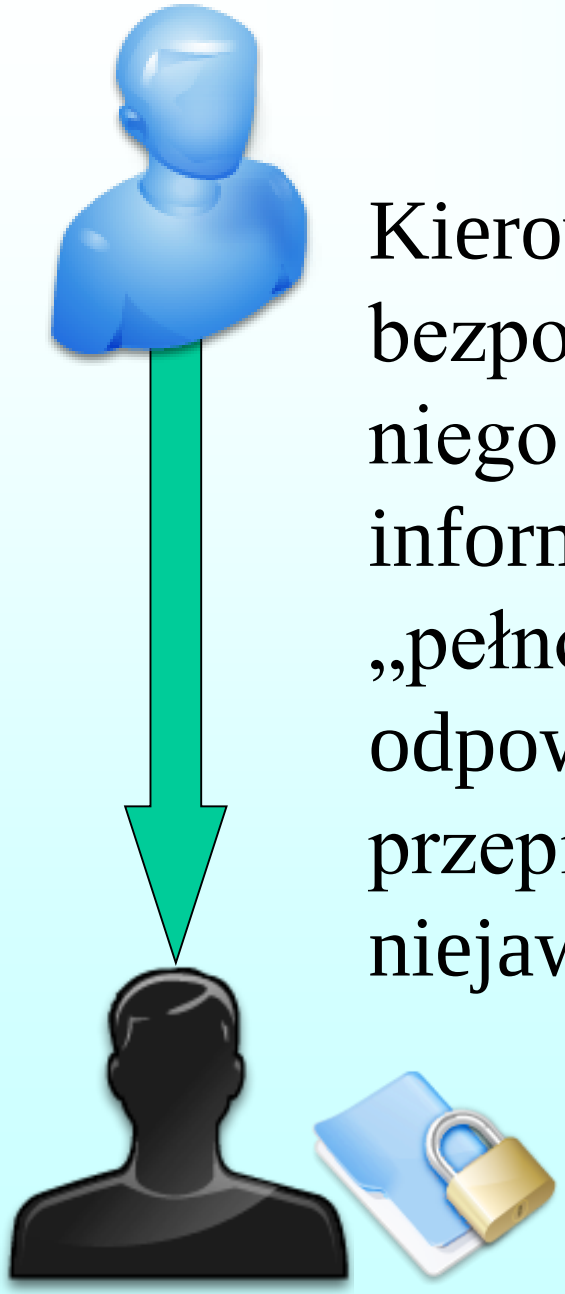
Art. 14.

Kierownik jednostki organizacyjnej, w której są przetwarzane informacje niejawne, odpowiada za ich ochronę, w szczególności za zorganizowanie i zapewnienie funkcjonowania tej ochrony.





Pełnomocnik ochrony



Kierownikowi jednostki organizacyjnej bezpośrednio podlega zatrudniony przez niego pełnomocnik do spraw ochrony informacji niejawnych, zwany dalej „pełnomocnikiem ochrony”, który odpowiada za zapewnienie przestrzegania przepisów o ochronie informacji niejawnych.

3. Organizacja ochrony informacji niejawnych

Art. 14.



Pełnomocnikiem ochrony może być osoba, która posiada:

1) obywatelstwo polskie;

2) wykształcenie wyższe*;

3) odpowiednie poświadczenie bezpieczeństwa wydane przez ABW albo SKW, a także przez były Urząd Ochrony Państwa lub byłe Wojskowe Służby Informacyjne;

4) zaświadczenie o przeszkoleniu w zakresie ochrony informacji niejawnych przeprowadzonym przez ABW albo SKW, a także przez byłe Wojskowe Służby Informacyjne.

Przepis stosuje się do pełnomocników ochrony i zastępców pełnomocników ochrony zatrudnionych po dniu wejścia w życie ustawy (Art. 183.**)*



Art. 15.

Do zadań pełnomocnika ochrony należy:

1) **zapewnienie ochrony informacji niejawnych, w tym stosowanie środków bezpieczeństwa fizycznego;**
2) **zapewnienie ochrony systemów teleinformatycznych, w których są przetwarzane informacje niejawne;**
3) **zarządzanie ryzykiem bezpieczeństwa informacji niejawnych, w szczególności szacowanie ryzyka;**
4) **kontrola ochrony informacji niejawnych oraz przestrzegania przepisów o ochronie tych informacji, w szczególności okresowa (co najmniej raz na trzy lata) kontrola ewidencji, materiałów i obiegu dokumentów;**

3. Organizacja ochrony informacji niejawnych

Art. 15.

Do zadań pełnomocnika ochrony należy:

5) opracowywanie i aktualizowanie, wymagającego akceptacji kierownika jednostki organizacyjnej, planu ochrony informacji niejawnych w jednostce organizacyjnej, w tym w razie wprowadzenia stanu nadzwyczajnego, i nadzorowanie jego realizacji;

6) prowadzenie szkoleń w zakresie ochrony informacji niejawnych;

7) prowadzenie zwykłych postępowań sprawdzających oraz kontrolnych postępowań sprawdzających;

8) prowadzenie aktualnego wykazu osób zatrudnionych lub pełniących służbę w jednostce organizacyjnej albo wykonujących czynności zlecone, które posiadają uprawnienia do dostępu do informacji niejawnych, oraz osób, którym odmówiono wydania poświadczenia bezpieczeństwa lub je cofnięto ...

3. Organizacja ochrony informacji niejawnych



Art. 16.

Pracownikiem pionu ochrony w jednostce organizacyjnej może być osoba, która posiada:

1) obywatelstwo polskie, z wyjątkiem pracowników pionu ochrony zatrudnionych u przedsiębiorców;

2) odpowiednie poświadczenie bezpieczeństwa lub upoważnienie;

3) zaświadczenie o odbytym przeszkoleniu w zakresie ochrony informacji niejawnych.



3. Organizacja ochrony informacji niejawnych

Art. 17.

W przypadku stwierdzenia naruszenia w jednostce organizacyjnej przepisów o ochronie informacji niejawnych pełnomocnik ochrony zawiadamia o tym kierownika jednostki organizacyjnej i podejmuje niezwłocznie działania zmierzające do wyjaśnienia okoliczności tego naruszenia oraz ograniczenia jego negatywnych skutków.

W przypadku stwierdzenia naruszenia przepisów o ochronie informacji niejawnych o klauzuli „poufne” lub wyższej pełnomocnik ochrony zawiadamia niezwłocznie również odpowiednio ABW lub SKW.

§ § § § § § § § § §

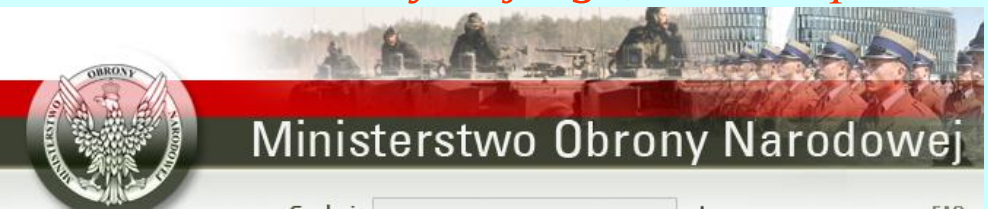


3. Organizacja ochrony informacji niejawnych

Art. 18.

Minister Obrony Narodowej określi, w drodze rozporządzenia:

1) *szczegółowe zadania pełnomocników ochrony w zakresie ochrony informacji niejawnych w jednostkach organizacyjnych jemu podległych lub przez niego nadzorowanych;*
2) *szczególne wymagania dotyczące stosowania środków bezpieczeństwa fizycznego przeznaczonych do ochrony informacji niejawnych;*
3) *miejsce i rolę Pełnomocnika Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych oraz pełnomocników ochrony kierowników bezpośrednio nadrzędnych jednostek organizacyjnych w resortowym systemie ochrony informacji niejawnych;*
4) *zakres, tryb i sposób współdziałania pełnomocników ochrony w zakresie ochrony informacji niejawnych z SKW;*
5) *rodzaje, szczegółowe cele oraz sposób organizacji szkoleń w zakresie ochrony informacji niejawnych;*
6) *zakres stosowania środków bezpieczeństwa fizycznego oraz kryteria tworzenia stref ochronnych;*
7) *tryb opracowywania oraz niezbędne elementy planów ochrony informacji niejawnych, w tym postępowanie z materiałami zawierającymi informacje niejawne oznaczone klauzulą „tajne” lub „ściśle tajne” w razie wprowadzenia stanu nadzwyczajnego, a także sposób nadzorowania ich realizacji.*



4. Szkolenie w zakresie ochrony informacji niejawnych



4. Szkolenie w zakresie ochrony informacji niejawnych

Art. 19.

Szkolenie w zakresie ochrony informacji niejawnych przeprowadza się w celu:

1) przepisami dotyczącymi ochrony informacji niejawnych oraz odpowiedzialności karnej, dyscyplinarnej i służbowej za ich naruszenie, w szczególności za nieuprawnione ujawnienie informacji niejawnych;

2) zasadami ochrony informacji niejawnych w zakresie niezbędnym do wykonywania pracy lub pełnienia służby, z uwzględnieniem zasad zarządzania ryzykiem bezpieczeństwa informacji niejawnych, w szczególności szacowania ryzyka;

3) sposobami ochrony informacji niejawnych oraz postępowania w sytuacjach zagrożenia dla takich informacji lub w przypadku ich ujawnienia.



4. Szkolenie w zakresie ochrony informacji niejawnych



Art. 19.

2. Szkolenie:

1) przeprowadzają odpowiednio ABW lub SKW – dla pełnomocników ochrony i ich zastępców oraz osób przewidzianych na te stanowiska, przedsiębiorców wykonujących działalność jednoosobowo, a także dla kierowników przedsiębiorców, u których nie zatrudniono pełnomocników ochrony;

2) przeprowadzają odpowiednio ABW lub SKW, wspólnie z pełnomocnikiem ochrony – dla kierownika jednostki organizacyjnej, w której są przetwarzane informacje niejawne o klauzuli „ściśle tajne” lub „tajne”;

3) organizuje pełnomocnik ochrony – dla pozostałych osób zatrudnionych, pełniących służbę lub wykonujących czynności zlecone w jednostce organizacyjnej;

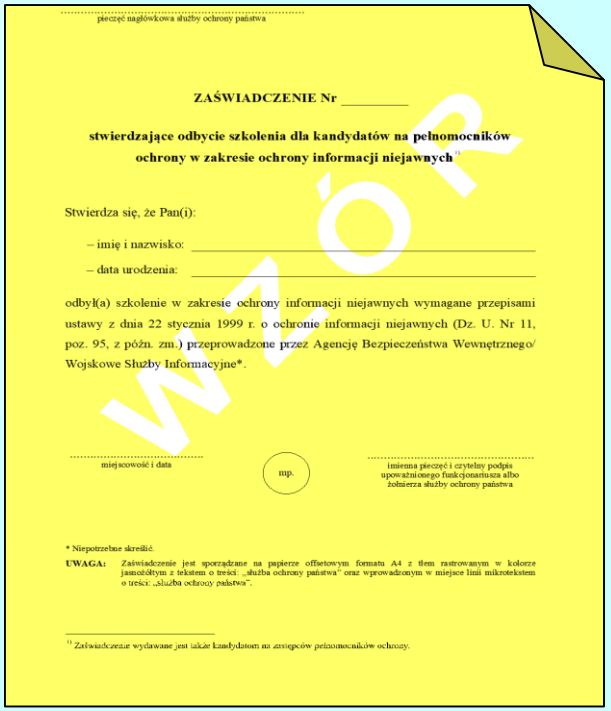
4) przeprowadza ABW – dla posłów i senatorów.

4. Szkolenie w zakresie ochrony informacji niejawnych

Art. 20.

Szkolenie, o którym mowa w art. 19 ust. 1, kończy się wydaniem zaświadczenia.

Odbierając zaświadczenie, osoba przeszkolona składa pisemne oświadczenie o zapoznaniu się z przepisami o ochronie informacji niejawnych.



pieczęć nagłówkowa służby ochrony państwa

ZAŚWIADCZENIE Nr _____

stwierdzające odbycie szkolenia dla kandydatów na pełnomocników ochrony w zakresie ochrony informacji niejawnych [1]

Stwierdza się, że Pan(i):

– imię i nazwisko: _____

– data urodzenia: _____

odbył(a) szkolenie w zakresie ochrony informacji niejawnych wymagane przepisami ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95, z późn. zm.) przeprowadzone przez Agencję Bezpieczeństwa Wewnętrznego/ Wojskowe Służby Informacyjne*.

WZÓR

miejscowość i data

m.p.

imienna pieczęć i czytelny podpis upoważnionego funkcjonariusza albo żołnierza służby ochrony państwa

* Niepotrzebne skreślić.

UWAGA: Zaświadczenie jest sporządzane na papierze offsetowym formatu A4 z tłem rastrowanym w kolorze jasnożółtym z tekstem o treści: „służba ochrony państwa" oraz wprowadzonym w miejsce linii mikrotekstem o treści: „służba ochrony państwa".

[1] Zaświadczenie wydawane jest także kandydatom na zastępców pełnomocników ochrony.

4. Szkolenie w zakresie ochrony informacji niejawnych





Prezes Rady Ministrów określi, w drodze rozporządzenia:

1) wzory zaświadczeń stwierdzających odbycie szkolenia w zakresie ochrony informacji niejawnych;

2) sposób rozliczania kosztów szkolenia, o których mowa w art. 19 ust. 4.

Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie wzorów zaświadczeń stwierdzających odbycie szkolenia w zakresie ochrony informacji niejawnych oraz sposobu rozliczania kosztów przeprowadzenia szkolenia przez Agencję Bezpieczeństwa Wewnętrznego lub Służbę Kontrwywiadu Wojskowego [DzU . Nr 258, poz.1751]

5. Bezpieczeństwo osobowe



5. Bezpieczeństwo osobowe



Art. 21.

Dopuszczenie do pracy lub pełnienia służby na stanowiskach albo zlecenie prac związanych z dostępem do informacji niejawnych o klauzuli „poufne” lub wyższej może nastąpić, z zastrzeżeniem art. 34 po:

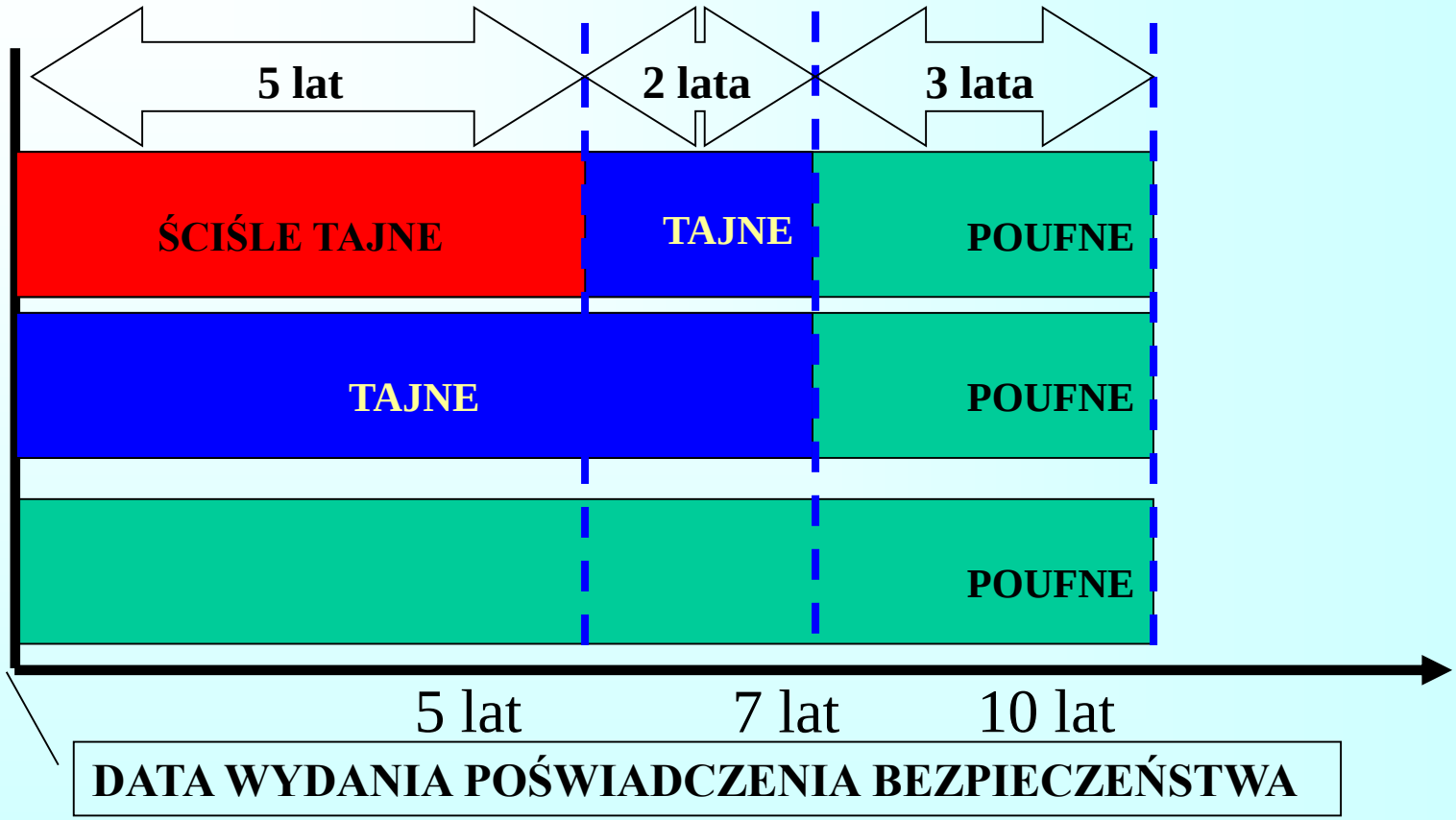
1) uzyskaniu poświadczenia bezpieczeństwa oraz

2) odbyciu szkolenia w zakresie ochrony informacji niejawnych.





Okres dostępu do informacji niejawnych



Poświadczenie bezpieczeństwa upoważniające do dostępu do informacji niejawnych o wyższej klauzuli tajności uprawnia do dostępu do informacji niejawnych o niższej klauzuli tajności, odpowiednio przez okresy jak wyżej także w odniesieniu do poświadczeń bezpieczeństwa organizacji międzynarodowych.

5. Bezpieczeństwo osobowe

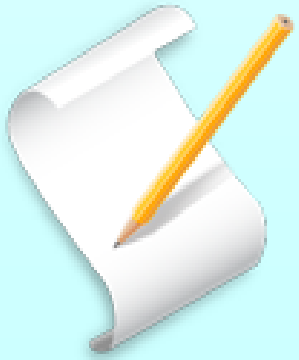


Art. 21.

Dopuszczenie do pracy lub pełnienia służby na stanowiskach albo zlecenie prac, związanych z dostępem danej osoby do informacji niejawnych o klauzuli „zastrzeżone” może nastąpić po:

1) pisemnym upoważnieniu przez kierownika jednostki organizacyjnej, jeżeli nie posiada ona poświadczenia bezpieczeństwa;

2) odbyciu szkolenia w zakresie ochrony informacji niejawnych.





Rodzaje postępowań sprawdzających



W zależności od stanowiska lub wykonywania czynności zleconych, o które ubiega się osoba, zwana dalej „osobą sprawdzaną”, przeprowadza się postępowanie sprawdzające: (Art. 22)



Zwykłe – „POUFNE”





Poszerzone –„TAJNE” i „ŚCIŚLE TAJNE” oraz POIN, KJO, umowy m. narodowe.

POSTĘPOWANIE SPRAWDZAJĄCE

MA NA CELU USTALENIE, CZY OSOBA SPRAWDZANA DAJE RĘKOJMIĘ ZACHOWANIA TAJEMNICY.

W TOKU POSTĘPOWANIA SPRAWDZAJĄCEGO USTALA SIĘ, CZY ISTNIEJĄ UZASADNIONE WĄTPLIWOŚCI DOTYCZĄCE:

1. **uczestnictwa, współpracy lub popierania przez osobę sprawdzaną działalności szpiegowskiej, terrorystycznej, sabotażowej albo innej wymierzonej przeciwko RP**
2. **zagrożenia osoby sprawdzanej ze strony obcych służb specjalnych w postaci prób werbunku lub nawiązania z nią kontaktu**
3. **przestrzegania porządku konstytucyjnego Rzeczypospolitej Polskiej**
4. **ukrywania lub świadomego niezgodnego z prawdą podawania w ankiecie bezpieczeństwa osobowego, lub postępowaniu sprawdzającym przez osobę sprawdzaną informacji mających znaczenie dla ochrony informacji niejawnych**
5. **wystąpienia związanych z osobą sprawdzaną okoliczności powodujących ryzyko jej podatności na szantaż lub wywieranie presji**
6. **niewłaściwego postępowania z informacjami niejawnymi**

W ZALEŻNOŚCI OD STANOWISKA LUB WYKONYWANIA CZYNNOŚCI ZLECONYCH, O KTÓRE UBIEGA SIĘ OSOBA, ZWANA DALEJ "OSOBĄ SPRAWDZANĄ", PRZEPROWADZA SIĘ:

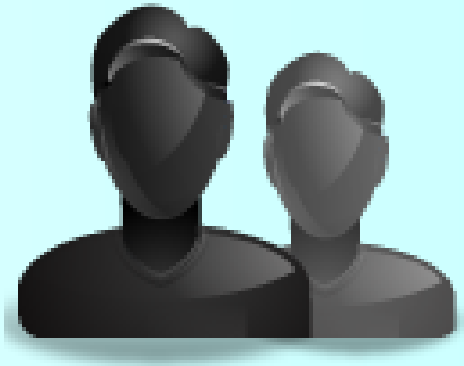
ZWYKŁE POSTĘPOWANIE SPRAWDZAJĄCE

- przy stanowiskach i pracach związanych z dostępem do informacji niejawnych o klauzuli "poufne"

POSZERZONE POSTĘPOWANIE SPRAWDZAJĄCE

- przy stanowiskach i pracach związanych z dostępem do informacji niejawnych o klauzuli "tajne" lub "ściśle tajne",
- wobec pełnomocników ochrony
- wobec kierowników jednostek organizacyjnych,
- wobec osób ubiegających się o dostęp do informacji niejawnych międzynarodowych

5. Bezpieczeństwo osobowe



Art. 23.

Postępowania sprawdzające …
{kto prowadzi? wobec kogo?}

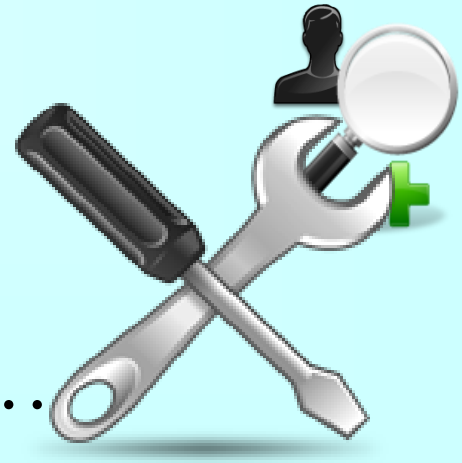


Art. 24.

Postępowania sprawdzające …
{cele, terminy}

Art. 25.

Zwykłe postępowanie sprawdzające …
{czynności}



Art. 26.

Poszerzone postępowanie sprawdzające …
{czynności}

Ankiety bezpieczeństwa osobowego

TRZY WZORY ANKIET BEZPIECZEŃSTWA OSOBOWEGO

(pieczęć instytucji … cej o sprawdzenie osoby upoważnianej do dost… rmacji niejawnych)

(odpowiednia klauzula tajności po wypełnieniu)
Egzemplarz pojedynczy

miejsce na aktualną fotografię 4 x 3,5 cm

ANKIETA
BEZPIECZEŃSTWA OSOBOWEGO

Niniejsza ankieta bezpieczeństwa osobowego wykorzystywana będzie zgodnie z ustawą na użyt… stępowania sprawdzającego w związku z upoważnieniem Pana (-i) do dostępu do informacji niejaw… no-wiących tajemnicę państwową, oznaczonych klauzulą (proszę zakreślić właściwe pole):

„Tajne” ☐

„Ściśle tajne” ☐

1. Osoba podlegająca sprawdz…
   a. Nazwisko ……
   b. Nazwisk… zednie (również nazwisko rodowe) ……
   c. …… ……

ŚCIŚLE TAJNE i TAJNE

(odpowiednia klauzula tajności po wypełnieniu)
Egzemplarz pojedynczy

miejsce na aktualną fotografię 4 x 3,5 cm

T A
… OBOWEGO

…ystywana będzie zgodnie z ustawą na użytek zwy-…iem Pana (-i) do dostępu do informacji niejawnych …ufne”.

……
……
……
……
……

POUFNE

(odpowiednia klauzula tajności po wypełnieniu)
Egzemplarz pojedynczy

miejsce na aktualną fotografię 4 x 3,5 cm

…NKIETA
…STWA OSOBOWEGO

…bowego wykorzystywana będzie zgodnie z ustawą na użytek zwy-…u z upoważnieniem Pana (-i) do dostępu do informacji niejawnych …ch klauzulą „zastrzeżone”.

……
…sko rodowe) ……
……
…zmiany) ……
……

……
(odpowiednia klauzula tajności po wypełnieniu)

Strona ----/----

ZASTRZEŻON…

Ankieta bezpieczeństwa osobowego

Załącznik do ustawy z dnia 5 sierpnia 2010 r.
ANKIETA BEZPIECZEŃSTWA OSOBOWEGO

Szanowna Pani, Szanowny Panie,

Rząd Rzeczypospolitej Polskiej, kierując się troską o bezpieczeństwo narodowe i mając na uwadze powinność jego ochrony, przedstawia tę ankietę w przekonaniu, iż zostanie ona wypełniona zgodnie z Pani (Pana) najlepszą wiedzą i wolą. Dziękując za współpracę, podkreślamy, że celem tej ankiety jest wyłącznie ochrona bezpieczeństwa narodowego przed zagrożeniami ze strony obcych służb specjalnych oraz ugrupowań terrorystycznych lub grup przestępczych. Prosimy uważnie przeczytać poniższą instrukcję, a w razie wątpliwości zwrócić się do pełnomocnika ochrony w Pani (Pana) jednostce organizacyjnej albo do Agencji Bezpieczeństwa Wewnętrznego bądź Służby Kontrwywiadu Wojskowego o pomoc w wypełnieniu ankiety.

Ankieta bezpieczeństwa osobowego, po wypełnieniu, stanowi tajemnicę prawnie chronioną i podlega ochronie przewidzianej dla informacji niejawnych o klauzuli tajności „poufne" w przypadku poszerzonego postępowania sprawdzającego lub „zastrzeżone" w przypadku zwykłego postępowania sprawdzającego. Jednocześnie informujemy Państwa, że informacje zawarte w niniejszej ankiecie są chronione ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.[90)]) i mogą być wykorzystane jedynie do celów postępowania sprawdzającego lub kontrolnego postępowania sprawdzającego, prowadzonego na podstawie przepisów ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr , poz.). Akta zakończonego postępowania sprawdzającego lub kontrolnego postępowania sprawdzającego mogą zostać udostępnione wyłącznie na żądanie sądu lub prokuratora w celu ścigania karnego lub podmiotom uprawnionym do prowadzenia postępowań sprawdzających, a także właściwemu organowi w celu rozpatrzenia odwołania lub dokonania sprawdzenia prawidłowości przeprowadzenia postępowania sprawdzającego oraz sądowi administracyjnemu w związku z rozpatrywaniem skargi.

Instrukcja

1. Przed wypełnieniem ankiety proszę się z nią dokładnie zapoznać.
2. Proszę wypełniać ankietę osobiście. Cudzoziemcy niewładający językiem polskim składają osobiście wypełnione ankiety w językach ojczystych, dołączając do nich tłumaczenie ich treści, wykonane przez tłumacza przysięgłego.

CZĘŚĆ I: DANE OSOBOWE

KOLOROWE ZDJĘCIE OSOBY SPRAWDZANEJ (WYS. 5 cm × SZER. 4 cm)

1. NAZWISKO

2. PIERWSZE IMIĘ | 3. DRUGIE IMIĘ

4. NAZWISKO RODOWE | 5. INNE POPRZEDNIE NAZWISKA

6. DATA URODZENIA (DD-MM-RRRR) | 7. MIEJSCE URODZENIA (MIEJSCOWOŚĆ, PAŃSTWO)

8. POSIADANE OBYWATELSTWA (OD KIEDY?)

9. WCZEŚNIEJ POSIADANE OBYWATELSTWA (OD KIEDY – DO KIEDY?)

10. NR PESEL | 11. NIP

12.1. NR DOWODU OSOBISTEGO | 12.2. DATA WAŻNOŚCI DOWODU OSOBISTEGO

12.3. NAZWA ORGANU, KTÓRY WYDAŁ DOWÓD OSOBISTY

13. CZY POSIADA PANI (PAN) PASZPORT?
(PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić pkt 13.1. – 13.4.)

TAK ☐ NIE ☐

13.1. NR PASZPORTU | 13.2. DATA WAŻNOŚCI PASZPORTU

13.3. NAZWA ORGANU, KTÓRY WYDAŁ PASZPORT

13.4. CZY POSIADA PANI (PAN) INNY PASZPORT, NIŻ WSKAZANY W PKT 13.1. – 13.3.?
(PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę załączyć do ankiety dodatkowy arkusz wypełniony według schematu z pkt 13.1. – 13.3.)

TAK ☐ NIE ☐

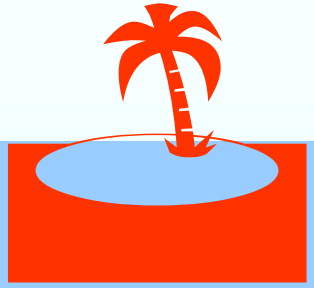
14. CZY JEST LUB BYŁA PANI (BYŁ PAN) OBJĘTA(OBJĘTY) POWSZECHNYM OBOWIĄZKIEM OBRONY?
(PROSZĘ ZAZNACZYĆ ODPOWIEDNIE POLE WYBORU – w przypadku zaznaczenia odpowiedzi „TAK" proszę wypełnić pkt 14.1. – 14.3.)

TAK ☐ NIE ☐

Art. 27. ZAWIESZENIE POSTĘPOWANIA SPRAWDZAJĄCEGO



długotrwała choroba osoby sprawdzanej (powyżej 30 dni),



wyjazd za granicę osoby sprawdzanej na okres przekraczający 30 dni

§ **gdy ocena dawania rękojmi zachowania tajemnicy zależy od uprzedniego rozstrzygnięcia zagadnienia przez inny organ, w szczególności w przypadku wszczęcia przeciwko osobie sprawdzanej postępowania karnego w sprawie o przestępstwo umyślne ścigane z oskarżenia publicznego lub umyślne przestępstwo skarbowe**

§ **gdy przeprowadzenie skutecznego postępowania sprawdzającego nie jest możliwe z innych przyczyn niezależnych od organu je prowadzącego**

5. Bezpieczeństwo osobowe

Art. 28.

Postępowanie sprawdzające kończy się:

1) wydaniem poświadczenia bezpieczeństwa;

2) odmową wydania poświadczenia bezpieczeństwa;

3) umorzeniem.

Art. 29.

Po zakończeniu postępowania sprawdzającego z wynikiem pozytywnym organ prowadzący postępowanie wydaje poświadczenie bezpieczeństwa …

WZÓR POŚWIADCZENIA BEZPIECZEŃSTWA

Załącznik nr 3

WZÓR

POŚWIADCZENIE BEZPIECZEŃSTWA NR _____

Na podstawie art. 28 pkt 1 w związku z art. 11 ust. 2 i 3 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228), po przeprowadzeniu na wniosek

_____
(nazwa wnioskodawcy)

przez _____
(nazwa i adres siedziby organu, który przeprowadził postępowanie)

poszerzonego postępowania sprawdzającego, stwierdza się, że Pani (Pan)

_____
(imię i nazwisko, data urodzenia)

daje rękojmię zachowania tajemnicy

w zakresie dostępu do informacji niejawnych
Organizacji Traktatu Północnoatlantyckiego / Unii Europejskiej*
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 pieczątka upoważnionej osoby)

*Niepotrzebne skreślić.

Zgodnie z art. 29 ust. 2 ustawy poświadczenie bezpieczeństwa powinno zawierać:



1) numer poświadczenia;

2) podstawę prawną;

3) wskazanie wnioskodawcy postępowania sprawdzającego;

4) określenie organu, który przeprowadził postępowanie sprawdzające;

5) datę i miejsce wystawienia;

6) imię, nazwisko i datę urodzenia osoby sprawdzanej;

7) określenie rodzaju przeprowadzonego postępowania sprawdzającego ze wskazaniem klauzuli tajności informacji niejawnych, do których osoba sprawdzana może mieć dostęp;

8) stwierdzenie, że osoba sprawdzana daje rękojmię zachowania tajemnicy;

9) termin ważności;

10) imienną pieczęć i podpis upoważnionego funkcjonariusza ABW albo funkcjonariusza lub żołnierza SKW, albo pełnomocnika ochrony, który przeprowadził postępowanie sprawdzające.

5. Bezpieczeństwo osobowe



Prezes Rady Ministrów określi, w drodze rozporządzenia, wzory:

- ✓ *poświadczenia bezpieczeństwa;*
- ✓ *poświadczeń bezpieczeństwa organizacji międzynarodowych.*

Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie wzorów poświadczeń bezpieczeństwa [Dz.U. Nr 258, poz. 1752]

Art. 31. UMORZENIE POSTĘPOWANIA SPRAWDZAJĄCEGO



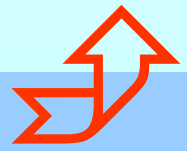
Śmierć osoby sprawdzanej



Rezygnacja osoby z ubiegania się o stanowisko lub wykonywanie prac, łączących się z dostępem do informacji niejawnych



Odstąpienie kierownika jednostki organizacyjnej od zamiaru obsadzenia osoby na stanowisku lub zlecenia prac związanych z dostępem do informacji niejawnych.



Gdy postępowanie z innej przyczyny stało się bezprzedmiotowe .

AW, CBA, Biuro Ochrony Rządu, Policja, Służba Więzienna, SWW, Straż Graniczna oraz Żandarmeria Wojskowa przeprowadzają samodzielnie postępowania sprawdzające oraz kontrolne postępowania sprawdzające odpowiednio wobec:

1) własnych funkcjonariuszy, żołnierzy i pracowników oraz osób ubiegających się o przyjęcie do służby lub pracy
2) osób wykonujących na ich rzecz czynności zlecone lub ubiegających się o wykonywanie tych czynności.

Zgodnie z art. 29 ust. 5 ustawy poświadczenia bezpieczeństwa wydane
w wyniku przeprowadzenia postępowań sprawdzających,
o których mowa w art. 23 ust. 5, zachowują ważność wyłącznie w okresie pracy lub służby w organie, który przeprowadził postępowanie sprawdzające.



5. Bezpieczeństwo osobowe

Art. 30.

Organ prowadzący postępowanie sprawdzające odmawia wydania poświadczenia bezpieczeństwa …



Prezes Rady Ministrów określi, w drodze rozporządzenia, wzór decyzji o odmowie wydania poświadczenia bezpieczeństwa.

Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie wzoru decyzji o odmowie wydania poświadczenia bezpieczeństwa [Dz.U. Nr 258, poz. 1753]

Art. 31.

Umorzenie postępowania sprawdzającego następuje …

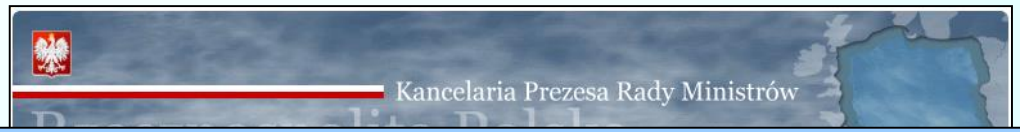
Art. 32.

Kolejne postępowanie sprawdzające …

5. Bezpieczeństwo osobowe

Art. 33.

Kontrolne postępowanie sprawdzające …



Prezes Rady Ministrów określi, w drodze rozporządzenia, wzór decyzji o cofnięciu poświadczenia bezpieczeństwa.

Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie wzoru decyzji o cofnięciu poświadczenia bezpieczeństwa. [Dz.U. Nr 258, poz. 1754]

Art. 34.

Nie przeprowadza się postępowania sprawdzającego …

Zgodnie z art. 30 ust. 3 ustawy decyzja o odmowie wydania poświadczenia bezpieczeństwa powinna zawierać:

1) podstawę prawną oraz uzasadnienie faktyczne i prawne;

2) wskazanie wnioskodawcy postępowania sprawdzającego;

3) określenie organu, który przeprowadził postępowanie sprawdzające;

4) datę i miejsce wydania;

5) imię, nazwisko i datę urodzenia osoby sprawdzanej;

6) określenie rodzaju przeprowadzonego postępowania sprawdzającego, ze wskazaniem klauzuli informacji niejawnych, do których osoba sprawdzana miała mieć dostęp;

7) stwierdzenie, że osoba sprawdzana nie daje rękojmi zachowania tajemnicy;

8) imienną pieczęć i podpis upoważnionego funkcjonariusza ABW albo funkcjonariusza lub żołnierza SKW, albo pełnomocnika ochrony, który przeprowadził postępowanie sprawdzające;

9) pouczenie o dopuszczalności i terminie wniesienia odwołania odpowiednio do Prezesa Rady Ministrów albo Szefa ABW lub Szefa SKW.

Zgodnie z art. 32 ust. 1 ustawy kolejne postępowanie sprawdzające jest przeprowadzane na pisemny wniosek kierownika jednostki organizacyjnej lub osoby uprawnionej do obsady stanowiska, złożony co najmniej na 6 miesięcy przed upływem terminu ważności poświadczenia bezpieczeństwa.



Zgodnie z art. 32 ust. 3 ustawy kolejne postępowanie sprawdzające powinno zostać zakończone przed upływem terminu ważności poświadczenia bezpieczeństwa.

Zgodnie z art. 33 ust. 1 ustawy kontrolne postępowanie sprawdzające jest przeprowadzane, w przypadku gdy o osobie, która posiada ważne poświadczenie bezpieczeństwa, zostaną ujawnione nowe informacje wskazujące, że nie daje ona rękojmi zachowania tajemnicy.



Zgodnie z art. 33 ust. 6 ustawy o wszczęciu kontrolnego postępowania sprawdzającego zawiadamia się:

1) kierownika jednostki organizacyjnej lub osobę uprawnioną do obsady stanowiska;

2) pełnomocnika ochrony w jednostce organizacyjnej;

3) osobę sprawdzaną.

Zgodnie z art. 33 ust. 11 ustawy kontrolne postępowanie sprawdzające kończy się:

1) decyzją o cofnięciu poświadczenia bezpieczeństwa;

2) poinformowaniem osób wymienionych w ust. 6 o braku zastrzeżeń w stosunku do osoby, którą objęto kontrolnym postępowaniem sprawdzającym,

3) decyzją o umorzeniu postępowania, w przypadku gdy postępowanie to nie zostanie zakończone przed upływem 12 miesięcy od dnia jego wszczęcia.

KONTROLNE POSTĘPOWANIE SPRAWDZAJĄCE

FAKTY WSKAZUJĄCE, ŻE OSOBA NIE DAJE RĘKOJMI ZACHOWANIA TAJEMNICY



OSOBA KTÓREJ WYDANO POŚWIADCZENIE BEZPIECZEŃSTWA

DECYZJA O COFNIĘCIU POŚWIADCZENIA BEZPIECZEŃSTWA

INFORMACJA O BRAKU ZASTRZEŻEŃ



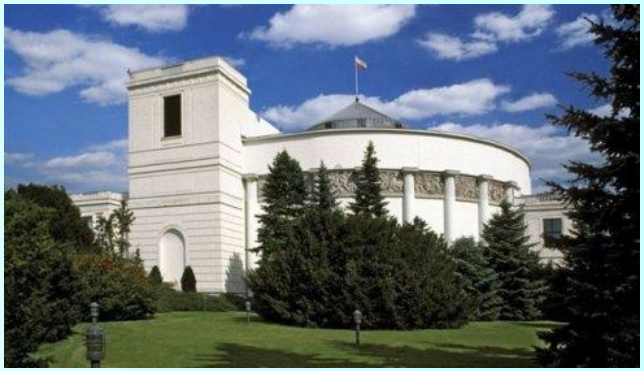
Zgodnie z art. 34 ust. 1 ustawy nie przep
się postępowania sprawdzającego, jeżeli osoba, której ma ono dotyczyć, przedstawi ważne poświadczenie bezpieczeństwa odpowiednie do wymaganej klauzuli tajności. Zasada ta nie dotyczy jednak poświadczeń bezpieczeństwa wydanych w wyniku przeprowadzenia postępowania sprawdzającego na podstawie art. 23 ust. 5 ustawy.



Zgodnie z art. 34 ust. 6 ustawy nie przeprowadza się postępowania sprawdzającego wobec osób dopuszczonych do informacji niejawnych w stanie nadzwyczajnym przez Prezydenta Rzeczypospolitej Polskiej lub Prezesa Rady Ministrów, każdego we własnym zakresie.



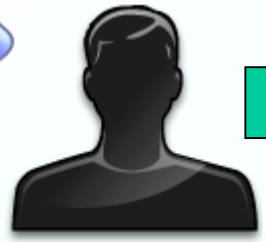
Zgodnie z art. 34 ust. 10 ustawy nie przeprowadza się postępowania sprawdzającego wobec:



Prezydenta RP oraz osoby wybranej na ten urząd, Marszałka Sejmu, Marszałka Senatu, Prezesa oraz członków Rady Ministrów, Prezesa NBP, Prezesa NIK, sędziów, prokuratorów i ławników, Rzecznika Praw Obywatelskich, Generalnego Inspektora Ochrony Danych Osobowych, członka RPP, członka KRRiT, Prezesa IPN, Szefów Kancelarii, posłów, senatorów, asesorów.

Zgodnie z art. 34 ust. 12 ustawy w stosunku do kandydatów na stanowiska, o których mowa w ust. 10 pkt 6-13, oraz wobec posłów lub senatorów, których obowiązki poselskie bądź senatorskie wymagają dostępu do informacji niejawnych o klauzuli "ściśle tajne", ABW przeprowadza poszerzone postępowanie sprawdzające.

UDOSTĘPNIANIE INFORMACJI NIEJAWNYCH (Z I PF)



KIEROWNIK J.O.

PISEMNA ZGODA (POLECENIE) UDOSTĘPNIENIA



KIEROWNIK KANCELARII TAJNEJ

UZASADNIONA POTRZEBA UDOSTĘPNIENIA DOKUMENTU

DOKUMENT NIEJAWNY

UDOSTĘPNIENIE DOKUMENTU



OSOBA (FIZYCZNA, PRAWNA) **WOBEC KTÓREJ WSZCZĘTO ZWYKŁE POSTĘPOWANIE SPRAWDZAJĄCE**

5. Bezpieczeństwo osobowe

Art. 34. ust. 5

Szefowie Kancelarii Prezydenta Rzeczypospolitej Polskiej, Kancelarii Sejmu, Kancelarii Senatu lub Kancelarii Prezesa Rady Ministrów albo minister właściwy dla określonego działu administracji rządowej, Prezes Narodowego Banku Polskiego, Prezes Najwyższej Izby Kontroli lub kierownik urzędu centralnego, a w przypadku ich braku ABW albo SKW, mogą:

1) w szczególnie uzasadnionych przypadkach, z zastrzeżeniem art. 4 ust. 2, wyrazić pisemną zgodę na jednorazowe udostępnienie określonych informacji niejawnych osobie nieposiadającej odpowiedniego poświadczenia bezpieczeństwa;

2) wyrazić pisemną zgodę na udostępnienie informacji niejawnych o klauzuli „tajne” lub „ściśle tajne” osobie, wobec której wszczęto poszerzone postępowanie sprawdzające.

5. Bezpieczeństwo osobowe

Art. 34. ust. 9

Zgodę na udostępnienie informacji niejawnych o klauzuli „poufne” osobie, wobec której wszczęto postępowanie sprawdzające, może wyrazić, w formie pisemnej, kierownik jednostki organizacyjnej, w której ta osoba jest zatrudniona, pełni służbę lub wykonuje czynności zlecone.



6. Postępowanie odwoławcze i skargowe, wznowienie postępowania.



6. Postępowanie odwoławcze i skargowe, wznowienie postępowania

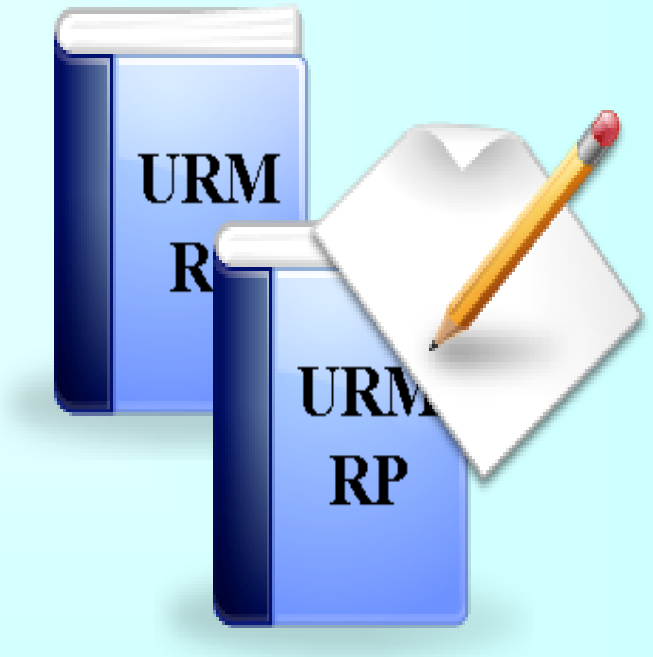
Art. 35.

Odwołanie od decyzji odmowy wydania …

{art.. 23, ust. 2 i 5}

Art. 36.

Prezes Rady Ministrów stwierdza, w drodze postanowienia …



Art. 36.

Prezes Rady Ministrów stwierdza, w drodze postanowienia …

Art. 36.

Odwołanie od wydanej przez pełnomocnika ochrony decyzji o odmowie wydania …

6. Postępowanie odwoławcze i skargowe, wznowienie postępowania



Art. 38.

Osobie sprawdzanej przysługuje skarga do sądu administracyjnego na decyzję lub postanowienie organu odwoławczego w terminie 30 dni od dnia doręczenia

Art. 39.

Prezes Rady Ministrów pełnomocnicy ochrony lub podmioty wymienione w art. 23 ust. 2 i 5 wznawiają postępowanie sprawdzające …

Art. 40.

Organ albo podmiot, o którym mowa w art. 39 ust. 1, po przeprowadzeniu postępowania określonego w art. 39 ust. 8 wydaje decyzję …

Art. 41.

Od decyzji o odmowie wznowienia postępowania, o którym mowa w … przysługuje odwołanie do …



OGÓLNE INFORMACJE NA TEMAT ANKIETY BEZPIECZEŃSTWA OSOBOWEGO

część I: „dane osobowe”, zawierająca podstawowe dane o osobie,

część II: „dane osobowe członków rodziny”, zawierająca podstawowe dane o członkach rodziny oraz dane współmieszkańców osoby sprawdzanej,

część III: „historia życia zawodowego i osobistego”, zawierająca dane dotyczące okresu po ukończeniu 18 roku życia o: 1) historii zatrudnienia, 2) dostępie do informacji niejawnych, 3) ostatniej ukończonej szkole oraz wszystkich szkołach ukończonych po 18 roku życia, a także kursach zagranicznych i posiadanym wykształceniu i tytułach naukowych, 4) członkostwie w organizacjach oraz radach fundacji, 5) adresach pobytu dłuższych niż 30 dni,

część IV: „dane dotyczące bezpieczeństwa”, zawierająca pytania o: 1) współpracę lub pracę w organach bezpieczeństwa PRL, 2) karalność za przestępstwa, 3) toczące się aktualnie wobec osoby sprawdzanej postępowania karne, 4) toczące się aktualnie wobec osoby sprawdzanej postępowania dyscyplinarne związane z naruszeniem przepisów dotyczących ochrony informacji niejawnych, 5) zainteresowania ze strony obcych służb specjalnych i/lub grup przestępczych, (także wobec członków rodziny i/lub współmieszkańców), 6) wypytywania przez obce władze na tematy związane z bezpieczeństwem i obronnością RP (także wobec członków rodziny i/lub współmieszkańców), 7) pobyty zagraniczne (także partnera) dłuższe niż 30 dni, 8) kontakty (także partnera) z obywatelami innych państw,

część V: „dane dotyczące stanu zdrowia”, zawierająca pytania o: 1) kategorię zdrowia (stwierdzoną w wyniku badania np. w wojsku), 2) przebyte lub aktualne choroby psychiczne, 3) przebyte lub aktualne dolegliwości psychiczne, 4) zażywanie środków odurzających i psychotropów, 5) spożywanie alkoholu w ilościach powodujących utratę świadomości, 6) problemy w pracy lub życiu prywatnym spowodowane spożyciem alkoholu, 7) leczenie się w związku ze spożywaniem alkoholu,

część VI: „dane dotyczące sytuacji majątkowo-finansowej”, zawierająca pytania o: 1) wynagrodzenie, 2) inne dochody, 3) łączne dochody za poprzedni rok, 4) składanie oświadczeń o stanie majątkowym, 5) osoby prowadzące wspólne gospodarstwo domowe z osobą sprawdzaną (w tym PESEL, NIP, dochody roczne), 6) liczbę osób na utrzymaniu osoby sprawdzanej, 7) posiadane nieruchomości (także innych osób ze wspólnego gospodarstwa domowego), 8) posiadane firmy lub udziały w firmie, 9) posiadane ruchomości, których koszt nabycia był wyższy, niż 20.000 zł, 10) posiadane rachunki bankowe, 11) zadłużenia i inne zobowiązania finansowe, 12) problemy związane z grami hazardowymi,

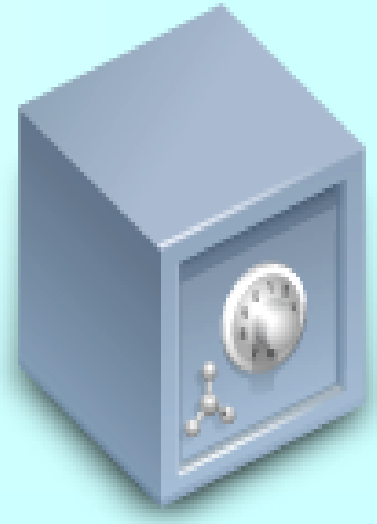
część VII: „osoby polecające”, zawierająca podstawowe dane o trzech osobach polecających, wpisywane dotychczas do pkt. 33 poprzedniej ankiety.

Integralną częścią ankiety jest instrukcja, zawierająca podstawowe informacje niezbędne do poprawnego wypełnienia ankiety.

CZY ANKIETĘ BEZPIECZEŃSTWA OSOBOWEGO NALEŻY OZNACZYĆ KLAUZULĄ TAJNOŚCI?
Zgodnie z art. 24 ust. 10 ustawy oraz z uwagi na zmianę definicji informacji niejawnych oraz, nie ma konieczności automatycznego nadawania ankiecie klauzuli tajności.



7. Kancelarie tajne. Środki bezpieczeństwa fizycznego



KANCELARIA TAJNA





Art. 42 Ustawy… **Kierownik jednostki organizacyjnej, w której są przetwarzane informacje niejawne o klauzuli „tajne” lub „ściśle tajne”, tworzy kancelarię, zwaną dalej „kancelarią tajną”, i zatrudnia jej kierownika ”.**

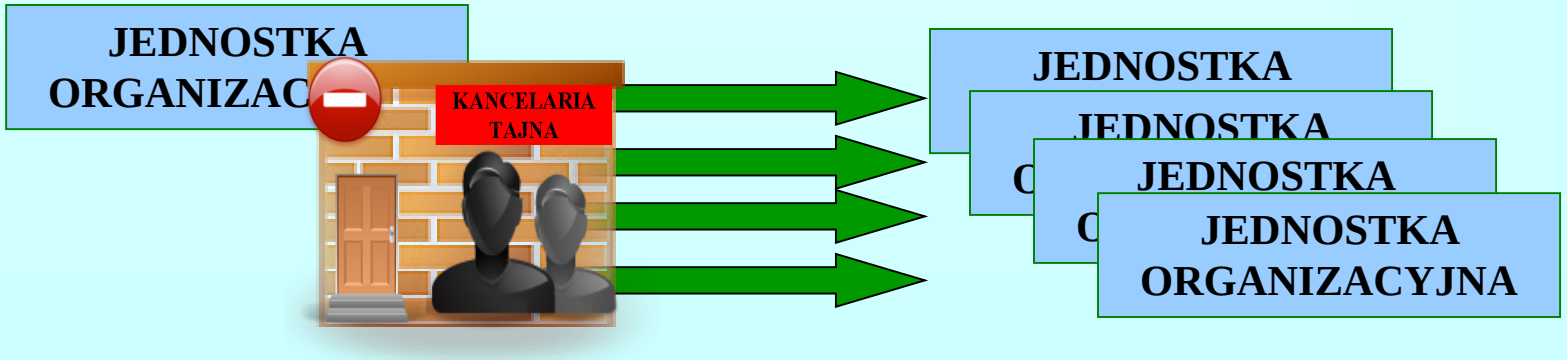
7. Kancelarie tajne. Środki bezpieczeństwa fizycznego

Art. 42.

W przypadku uzasadnionym względami organizacyjnymi kierownik jednostki organizacyjnej może utworzyć więcej niż jedną kancelarię tajną.

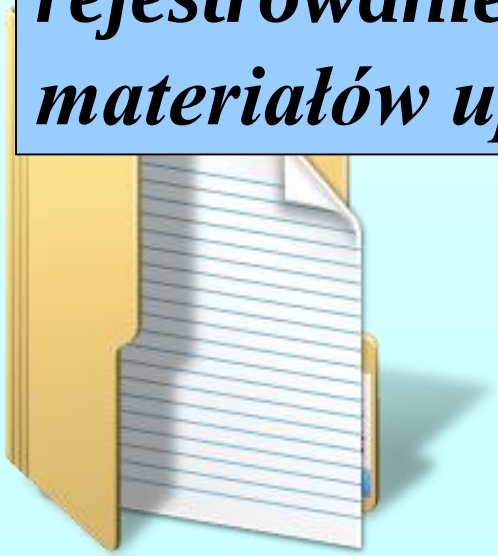
W uzasadnionych przypadkach, za zgodą odpowiednio ABW lub SKW, można utworzyć kancelarię tajną obsługującą dwie lub więcej jednostek organizacyjnych.

Podległość, obsada i zasady finansowania takiej kancelarii zostaną określone przez właściwych kierowników jednostek organizacyjnych.





Art. 42. Kancelaria - tajna stanowi wyodrębnioną komórkę organizacyjną, w zakresie ochrony informacji niejawnych podległą pełnomocnikowi ochrony, obsługiwaną przez pracowników pionu ochrony, odpowiedzialną za właściwe rejestrowanie, przechowywanie, obieg i wydawanie materiałów uprawnionym osobom.

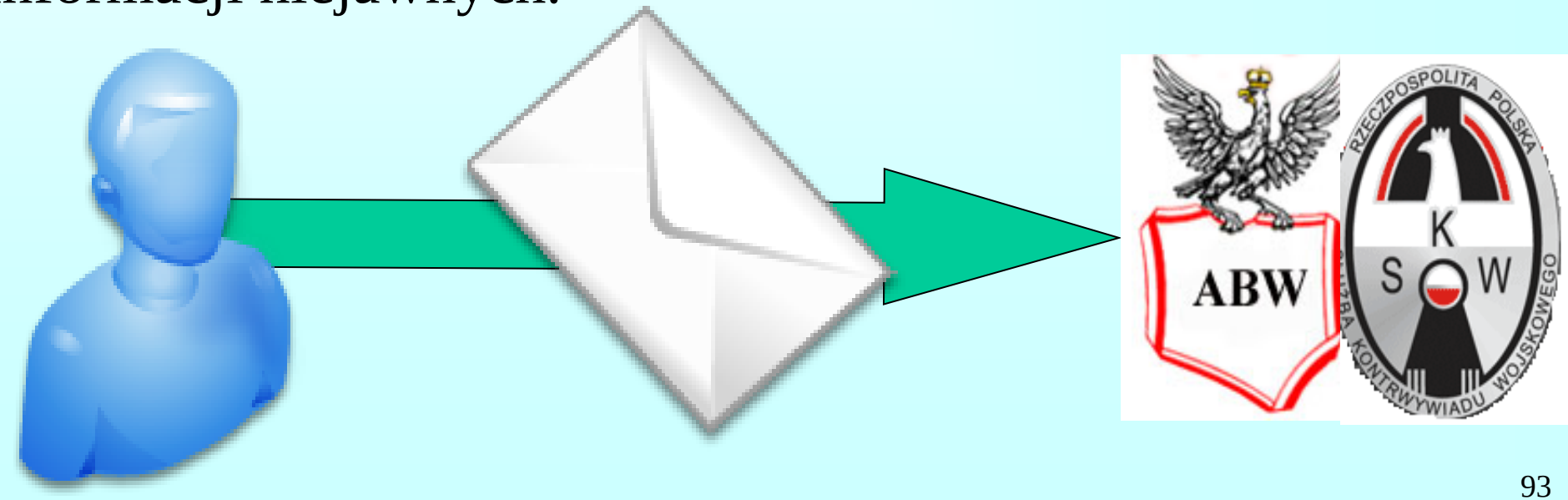




Art. 42.

Kierownik jednostki organizacyjnej może wyrazić zgodę na przetwarzanie w kancelarii tajnej informacji niejawnych o klauzuli „poufne” lub „zastrzeżone”.

Kierownik jednostki organizacyjnej informuje odpowiednio ABW lub SKW o utworzeniu lub likwidacji kancelarii tajnej, z określeniem klauzuli tajności przetwarzanych w niej informacji niejawnych.



Art. 43.

Organizacja pracy kancelarii tajnej zapewnia możliwość ustalenia w każdych okolicznościach, gdzie znajduje się materiał o klauzuli „tajne” lub „ściśle tajne” pozostający w dyspozycji jednostki organizacyjnej oraz kto z tym materiałem się zapoznał …



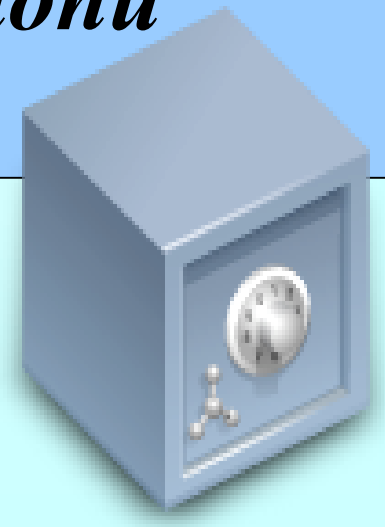
Kancelaria tajna powinna być:

- zorganizowana w odrębnym pomieszczeniu,

- zabezpieczona zgodnie z przepisami o środkach ochrony fizycznej,

- obsługiwana przez pracowników pionu ochrony.





Dokumenty niejawne o różnych klauzulach tajności przechowywane w kancelarii powinny być: od siebie fizycznie oddzielone



ŚCIŚLE TAJNE



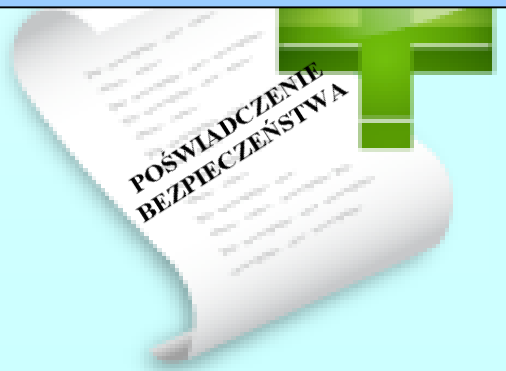
TAJNE



POUFNE

obsługiwane przez osobę posiadającą poświadczenie bezpieczeństwa odpowiednie do najwyższej klauzuli tajności dokumentów.







Dokumenty niejawne zawierające informacje mogą być wydane poza kancelarię jedynie wtedy gdy odbiorca zapewnia warunki ochrony tych dokumentów przed nieuprawnionym ujawnieniem.



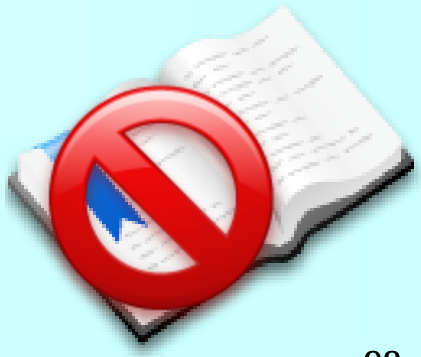






W razie wątpliwości, dokument może być udostępniony wyłącznie w kancelarii tajnej. Kancelaria odmawia wydania dokumentów niejawnych osobom nie posiadającym stosownego poświadczenia bezpieczeństwa.



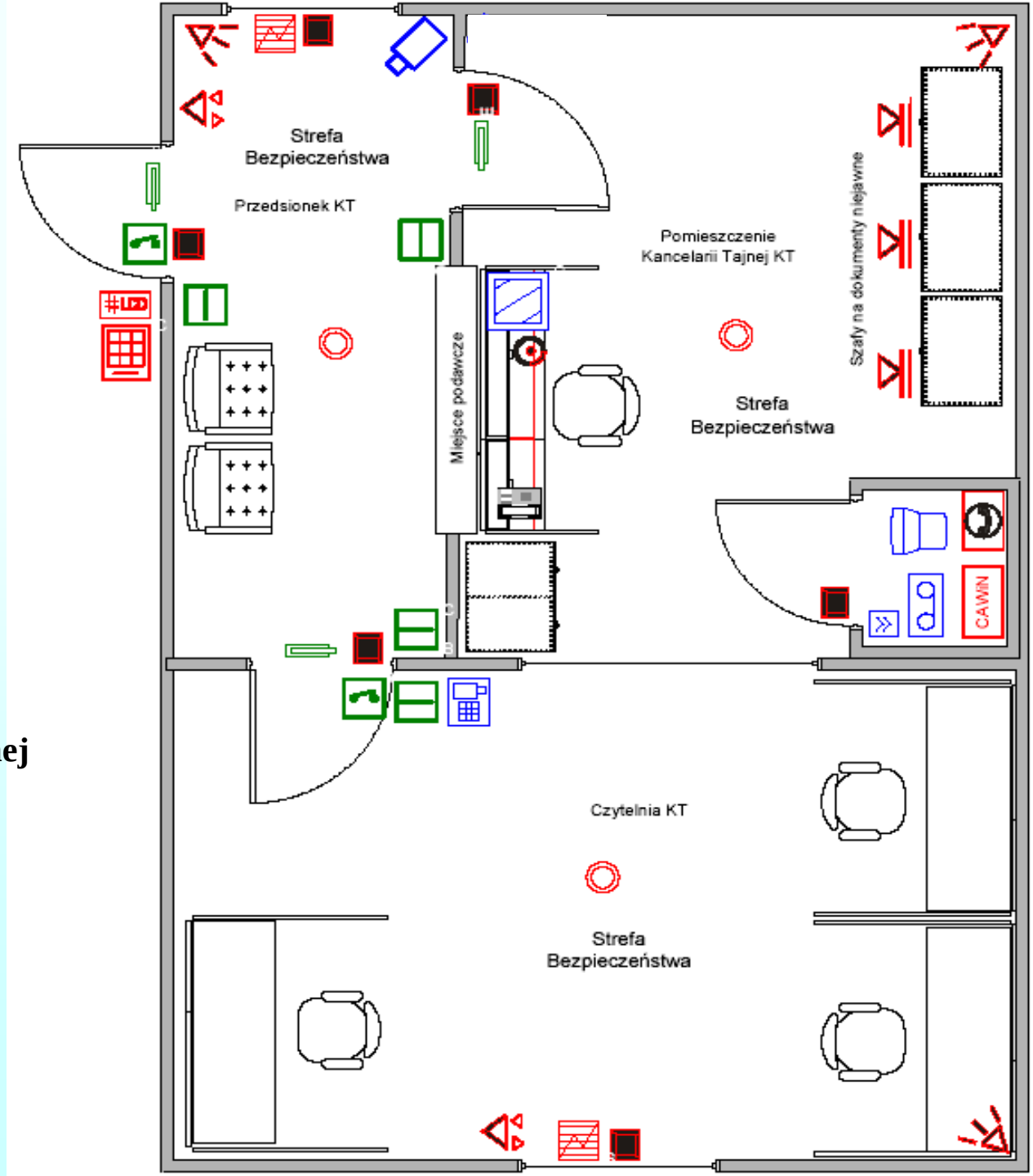


Kancelaria powinna spełniać wymagania w zakresie ochrony fizycznej



Wariant organizacji kancelarii tajnej

- wideo domofon
- szyfrator
- monitor
- czujka wstrząsowa
- przycisk napadowy
- czujka dualna
- czujka ppoż.
- kamera TV
- czujka podczerwieni pasywnej
- czujka magnetyczna
- czujka stłuczenia szkła
- samozamykacze
- zwora elektromagnetyczna
- przycisk ewakuacyjny

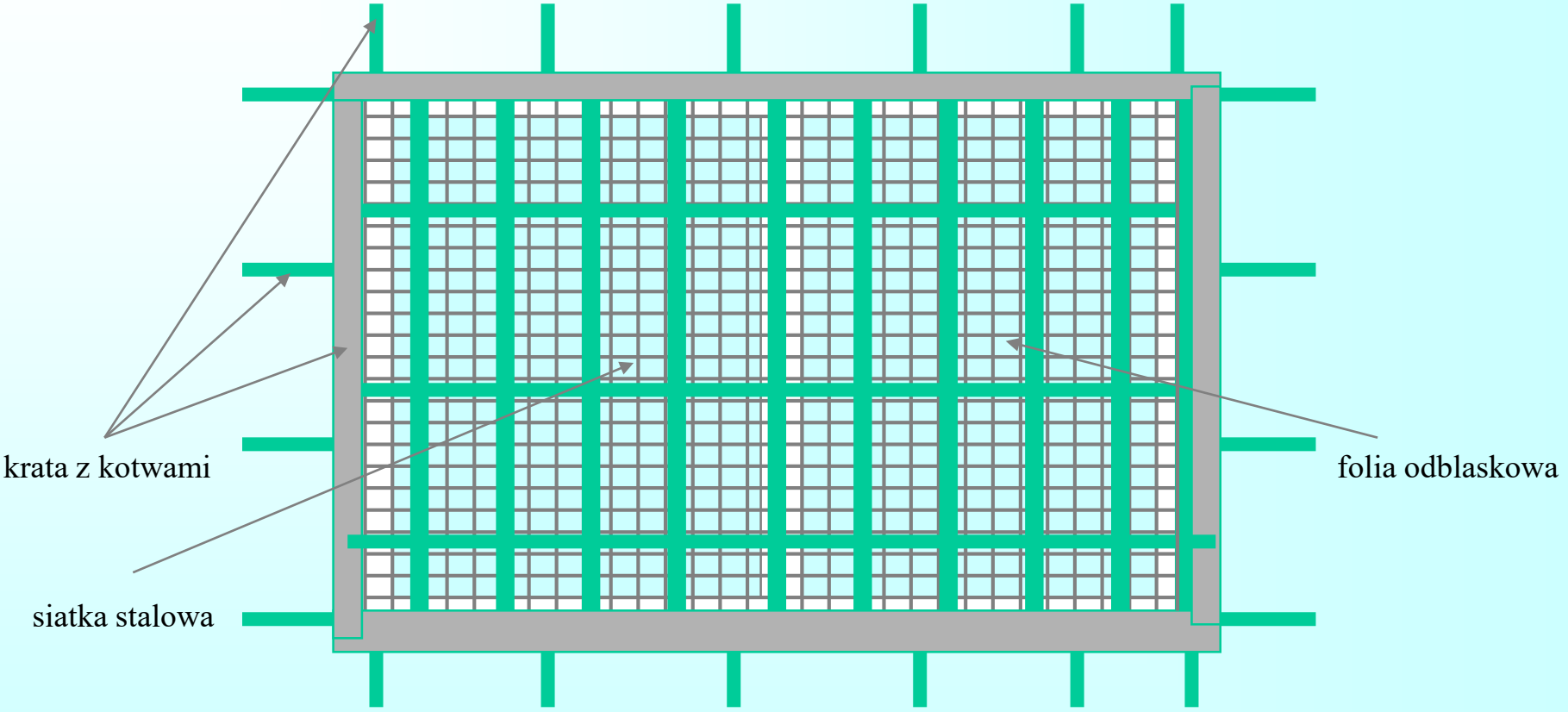


Drzwi wejściowe do kancelarii tajnej





Zabezpieczenia kancelarii tajnej



Zabezpieczenie zewnętrzne okien

Skrytki depozytowe

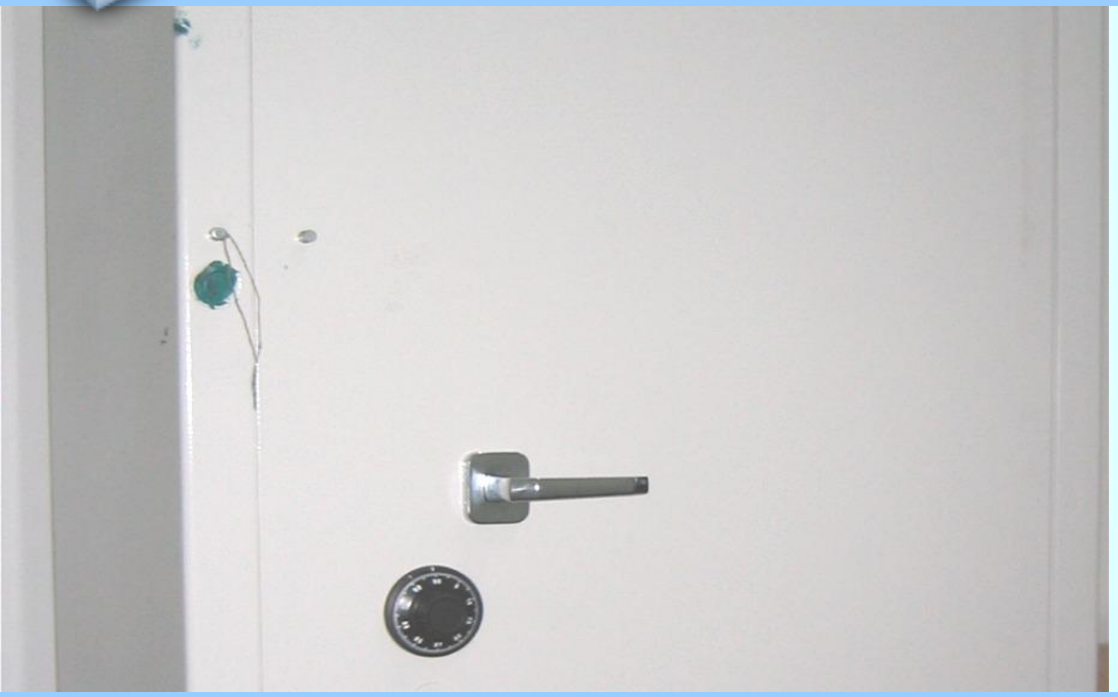


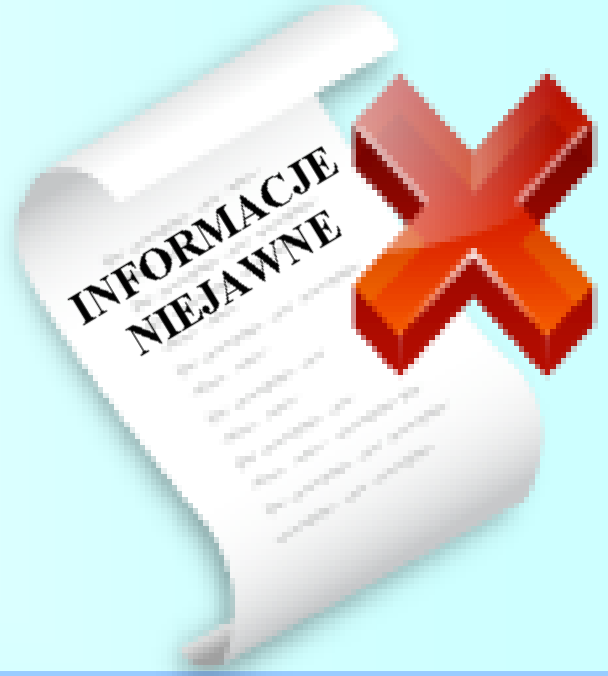


Czytelnia kancelarii tajnej

OCHRONA FIZYCZNA INFORMACJI NIEJAWNYCH

Urządzenia do przechowywania dokumentów niejawnych
SZAFY STALOWE





Klasa „C” - ŚCIŚLE TAJNE

Klasa „B” - TAJNE

Klasa „A” - POUFNE

Urządzenia do przechowywania dokumentów niejawnych
SZAFY STALOWE



Urządzenia do przechowywania dokumentów niejawnych
SZAFY STALOWE



Szyfratory do zamków





ŚCIŚLE TAJNE



TAJNE



POUFNE

Dokumenty i materiały oznaczone różnymi klauzulami tajności należy przechowywać w odrębnych pomieszczeniach lub szafach.

Można przechowywać razem jeżeli wchodzą one w skład zbioru dokumentów.

TAJNE



POUFNE

ŚCIŚLE TAJNE

7. Kancelarie tajne. Środki bezpieczeństwa fizycznego

Art. 43.

Kierownik jednostki organizacyjnej zatwierdza:

- ✓**sposób i tryb przetwarzania informacji niejawnych o klauzuli „poufne” …**
- ✓**instrukcję dotyczącą sposobu i trybu przetwarzania informacji niejawnych o klauzuli „zastrzeżone” …**
- ✓dokumentację określającą **poziom zagrożeń związanych z nieuprawnionym dostępem do informacji niejawnych lub ich utratą …**





Art. 44.

W jednostkach organizacyjnych dopuszcza się organizowanie innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za przetwarzanie materiałów niejawnych …





7. Kancelarie tajne. Środki bezpieczeństwa fizycznego

Art. 45.

Środki bezpieczeństwa fizycznego chroniące przed:

1) działaniem obcych służb specjalnych;

2) zamachem terrorystycznym lub sabotażem;

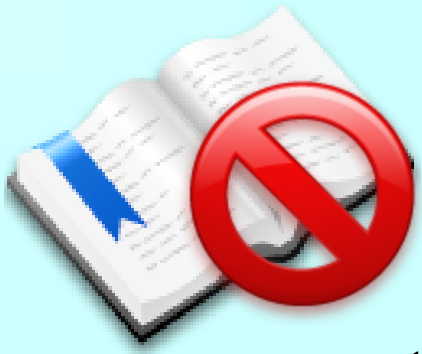
3) kradzieżą lub zniszczeniem materiału;

4) próbą wejścia osób nieuprawnionych do pomieszczeń, w których są przetwarzane informacje niejawne;

5) nieuprawnionym dostępem do informacji o wyższej klauzuli tajności niewynikającym z posiadanych uprawnień.









7. Kancelarie tajne.

Środki bezpieczeństwa fizycznego





Art. 46.

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

1) zorganizować strefy ochronne;

2) wprowadzić system kontroli wejść i wyjść ze stref ochronnych;

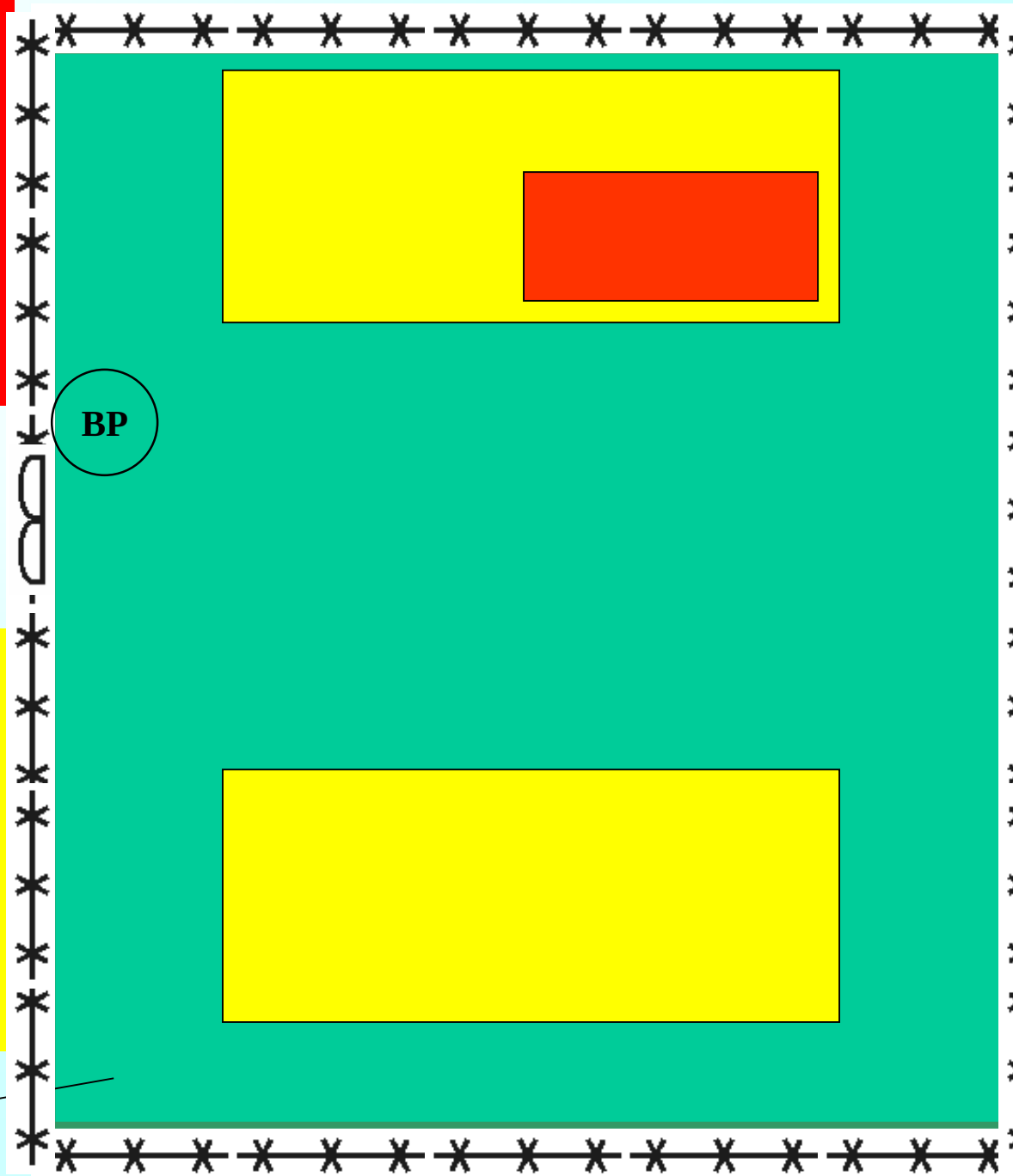
3) określić uprawnienia do przebywania w strefach ochronnych;

4) stosować wyposażenie i urządzenia służące ochronie informacji niejawnych, którym przyznano certyfikaty.

SPECJALNA STREFA BEZPIECZEŃSTWA

STREFA BEZPIECZEŃSTWA

STREFA ADMINISTRACYJNA



KONTROLA STREF BEZPIECZEŃSTWA I STREFY ADMINISTRACYJNEJ

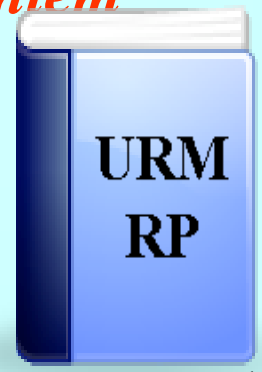


7. Kancelarie tajne. Środki bezpieczeństwa fizycznego

Art. 47.

Rada Ministrów określi, w drodze rozporządzenia:

1) *podstawowe kryteria i sposób określania poziomu zagrożeń oraz dobór środków bezpieczeństwa fizycznego odpowiednich do wskazanego poziomu zagrożeń;*
2) *wymagania w zakresie organizacji i funkcjonowania kancelarii tajnych;*
3) *rodzaje zagrożeń, które należy uwzględnić przy określaniu poziomu zagrożeń;*
4) *podstawowe elementy, które powinien zawierać plan ochrony informacji niejawnych;*
5) *zakres stosowania środków bezpieczeństwa fizycznego;*
6) *kryteria tworzenia stref ochronnych;*
7) *strukturę organizacyjną kancelarii tajnej, z uwzględnieniem możliwości tworzenia jej oddziałów;*
8) *podstawowe zadania kierownika kancelarii;*
9) *sposób i tryb przetwarzania informacji niejawnych;*
10) *wzór karty zapoznania się z dokumentem;*
11) *wzory dzienników ewidencji.*



7. Kancelarie tajne. Środki bezpieczeństwa fizycznego

Art. 47.

Ministrowie właściwi do spraw wewnętrznych, administracji publicznej, spraw zagranicznych, finansów publicznych, budżetu i instytucji finansowych, ***Minister Obrony Narodowej,*** *Minister Sprawiedliwości, Prezes Narodowego Banku Polskiego, Prezes Najwyższej Izby Kontroli, Pierwszy Prezes Sądu Najwyższego, Prokurator Generalny, Szefowie Kancelarii Prezydenta Rzeczypospolitej Polskiej, Sejmu, Senatu oraz Prezesa Rady Ministrów, Szef Agencji Bezpieczeństwa Wewnętrznego, Szef Agencji Wywiadu, Szef Służby Kontrwywiadu Wojskowego, Szef Służby Wywiadu Wojskowego, Szef Centralnego Biura Antykorupcyjnego, Komendant Główny Policji, Komendant Główny Straży Granicznej, Szef Biura Ochrony Rządu, a także Prezes Instytutu Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu,*

określą, w drodze zarządzenia, każdy w zakresie swojego działania, szczególny sposób organizacji i funkcjonowania kancelarii tajnych oraz komórek organizacyjnych, o których mowa w art. 44 ust. 1, sposób i tryb przetwarzania informacji niejawnych oraz dobór i stosowanie środków bezpieczeństwa fizycznego.

7. Kancelarie tajne. Środki bezpieczeństwa fizycznego



Art. 47.

Prezes Rady Ministrów określi, w drodze rozporządzenia:

1) tryb i sposób nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów;

2) sposób postępowania nadawców przesyłek zawierających informacje niejawne oraz wymogi, jakie muszą spełniać te przesyłki;

3) sposób postępowania podmiotów, które wykonują zadania przewoźników tych materiałów, z przesyłkami zawierającymi informacje niejawne;

4) sposób dokumentowania przyjmowania przez przewoźników przesyłek oraz ich wydawania adresatom, wraz z załącznikami w postaci wzorów niezbędnych formularzy;

5) warunki ochrony i sposoby zabezpieczenia przesyłek przez przewoźnika oraz warunki, jakie muszą spełniać wykorzystywane przez niego środki transportu i uczestniczące w konwojach osoby;

6) sposób postępowania w przypadku zaistnienia nieprzewidzianych okoliczności mogących mieć wpływ na bezpieczeństwo przesyłki;

7) warunki przewożenia materiałów poza granicami Rzeczypospolitej Polskiej.



8. Bezpieczeństwo teleinformatyczne



8. Bezpieczeństwo teleinformatyczne



Art. 48.

Systemy teleinformatyczne, w których mają być przetwarzane informacje niejawne, podlegają akredytacji bezpieczeństwa teleinformatycznego …

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



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

Akredytacja bezpieczeństwa teleinformatycznego

- dopuszczenie systemu lub sieci teleinformatycznej do wytwarzania, przetwarzania, przechowywania lub przekazywania informacji niejawnych, na zasadach określonych w ustawie



Dokumentacja bezpieczeństwa

systemu lub sieci informatycznej:

Szczególne Wymagania Bezpieczeństwa

oraz

Procedury Bezpiecznej Eksploatacji



8. Bezpieczeństwo teleinformatyczne

Art. 49.

✓Dokument szczególnych wymagań bezpieczeństwa systemu teleinformatycznego powinien zawierać w szczególności wyniki procesu szacowania ryzyka …

✓Kierownik jednostki organizacyjnej akceptuje wyniki procesu szacowania ryzyka dla bezpieczeństwa informacji niejawnych oraz jest odpowiedzialny za właściwą organizację bezpieczeństwa teleinformatycznego …







POJĘCIE BEZPIECZEŃSTWA TELEINFORMATYCZNEGO

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.

Bezpieczeństwo teleinformatyczne zapewnia się przed rozpoczęciem oraz w trakcie przetwarzania informacji niejawnych w systemie lub sieci teleinformatycznej.





Podstawowe wymagania stawiane systemom teleinformatycznym

POUFNOŚĆ

INTEGRALNOŚĆ

DOSTĘPNOŚĆ

Dodatkowe wymagania stawiane systemom teleinformatycznym

ROZLICZALNOŚĆ

AUTENTYCZNOŚĆ

NIEZAWODNOŚĆ

8. Bezpieczeństwo teleinformatyczne



Prezes Rady Ministrów określi, w drodze rozporządzenia, podstawowe wymagania bezpieczeństwa teleinformatycznego, jakim powinny odpowiadać systemy teleinformatyczne, niezbędne dane, jakie powinna zawierać dokumentacja bezpieczeństwa systemów informatycznych oraz sposób opracowania tej dokumentacji.

Rozporządzenie Prezesa Rady Ministrów
z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego. [Dz.U. Nr 159 poz. 948]

POJĘCIE BEZPIECZEŃSTWA TELEINFORMATYCZNEGO

Z pojęciem bezpieczeństwa teleinformatycznego wiążą się trzy podstawowe problemy:



Co ma być chronione ?

Przed czym ma być chronione ?

Jak ma być chronione i ile trzeba za to zapłacić?

Przed czym ma być chronione?





Informacja niejawna chroniona jest przed nieuprawnionym dostępem oraz jego rozmaitymi konsekwencjami.







Jak ma być chronione i ile trzeba za to zapłacić?



Poprzez zastosowanie urządzenia technic procedur niezbędnych do zapewnienia wym narzuconych systemowi w którym przetwarzane są informacje niejawne.

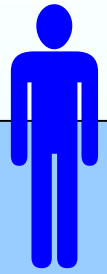


Koszty rozwiązań ujętych dokumentach bezpieczeństwa systemu.

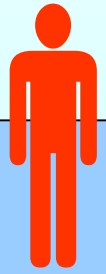


OSOBY ODPOWIEDZIALNE ZA BEZPIECZEŃSTWO TELEINFORMATYCZNE W JEDNOSTCE ORGANIZACYJNEJ





Administrator systemu teleinformatycznego



Inspektor bezpieczeństwa teleinformatycznego



Przetwarzanie informacji niejawnych w systemach teleinformatycznych



AKREDYTACJA BEZPIECZEŃSTWA TELEINFORMATYCZNEGO

KIEROWNIK JO.

ABW/SKW

ABW/SKW







ZGODA NA PRZETWARZANIE INFORMACJI NIEJAWNYCH

CERTYFIKAT SYSTEMU

Ochrona systemu



Ochrona fizyczna



Ochrona elektromagnetyczna



Ochrona kryptograficzna

Ochrona fizyczna

Umieszczenie urządzeń systemu w strefie kontrolowanego dostępu w zależności od klauzuli tajności, ilości, zagrożeń dla poufności, integralności lub dostępności informacji niejawnych.

Zastosowaniu środków zapewniających ochronę fizyczną przed nieuprawnionym dostępem, podglądem, podsłuchem.

Ochrona elektromagnetyczna



- ***Emisja - energia elektromagnetyczna rozchodząca się od źródła przez promieniowanie (w postaci fal elektromagnetycznych) lub przewodzenie.***

- ***Emisja ujawniająca - niepożądana emisja sygnału, którego pewne cechy związane są z informacją nadawaną, odbieraną, przechowywaną i przetwarzaną.***
- ***<u>Emisja ujawniająca promieniowana</u>***
- ***<u>Emisja ujawniająca przewodzona</u>***

Ochrona elektromagnetyczna

Instalacja sprzętu zgodnie z zaleceniami technicznymi Służb Ochrony Państwa



Komputer TEMPEST

BSK lub Kabina ekranująca





Komputer standardowy



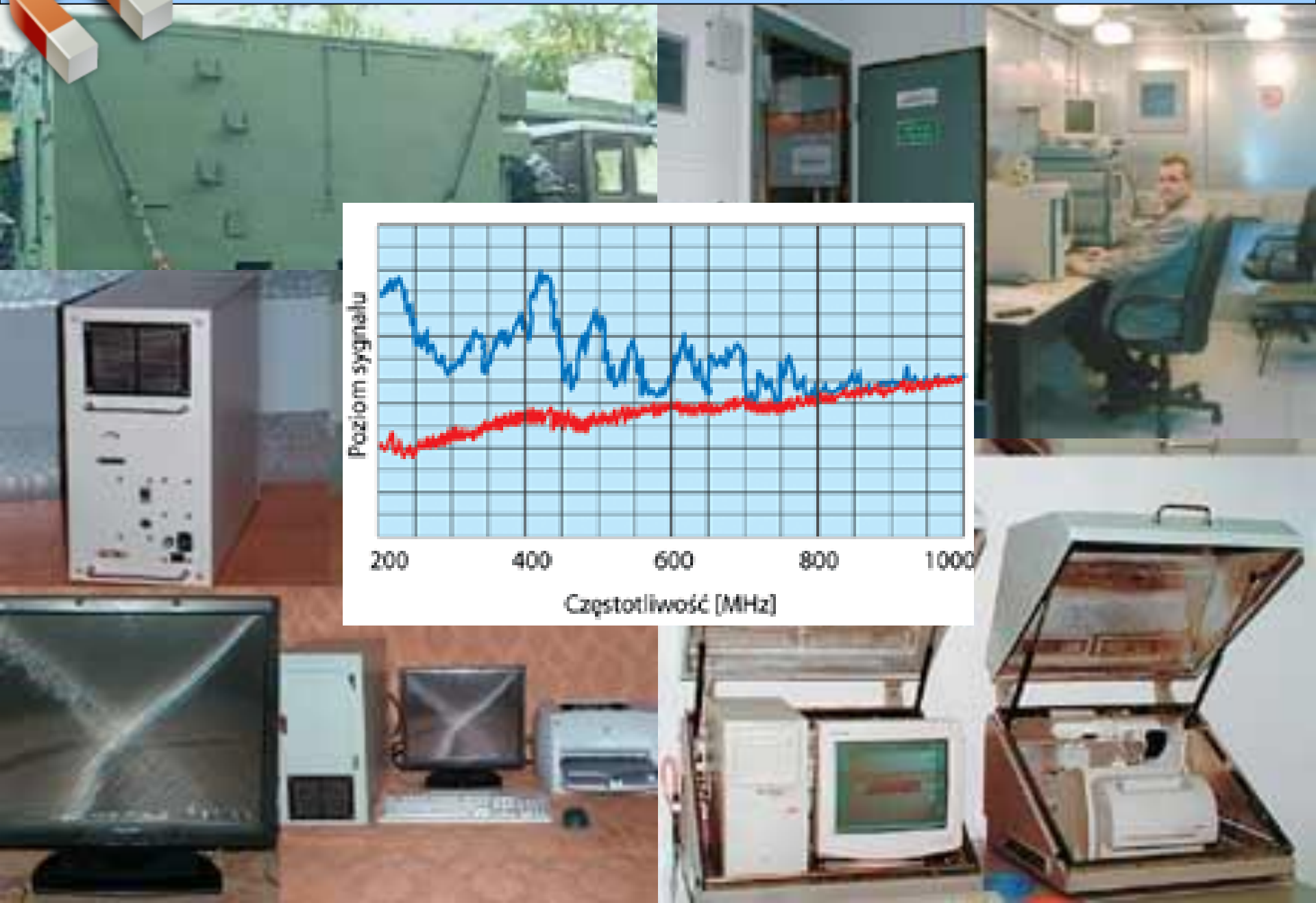
Urządzenie podsłuchowe lub zakłócające

0 1 2 3

Granica strefy kontrolowanej (administracyjnej)

Strefa ochrony elektromagnetycznej

Ochrona elektromagnetyczna



Bezpieczne kabiny kontenerowe







Kryptografia - dziedzina wiedzy zajmująca się metodami utajnionego (bezpiecznego) zapisywania i przesyłania wiadomości



POUFNOŚĆ **INTEGRALNOŚĆ** **UWIERZYTELNIENIE**

Ochrona kryptograficzna





9. Bezpieczeństwo przemysłowe.



Art. 54.

✓Warunkiem dostępu przedsiębiorcy do informacji niejawnych w związku z wykonywaniem umów albo zadań wynikających z przepisów prawa, zwanych dalej „umowami”, jest zdolność do ochrony informacji niejawnych.

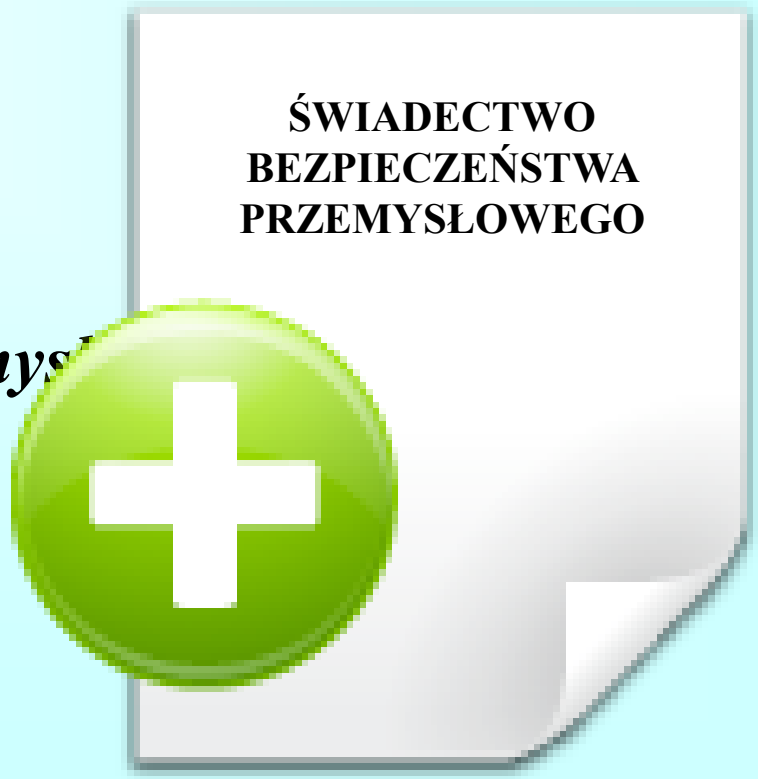
✓Dokumentem potwierdzającym zdolność do ochrony informacji niejawnych o klauzuli „poufne” lub wyższej jest świadectwo bezpieczeństwa przemysłowego, zwane dalej „świadectwem”, wydawane przez ABW albo SKW po przeprowadzeniu postępowania bezpieczeństwa przemysłowego.

Art. 55.

W zależności od stopnia zdolności do ochrony informacji niejawnych o klauzuli „poufne” lub wyższej wydaje się świadectwo odpowiednio:

- ✓pierwszego stopnia,
- ✓drugiego stopnia,
- ✓trzeciego stopnia.







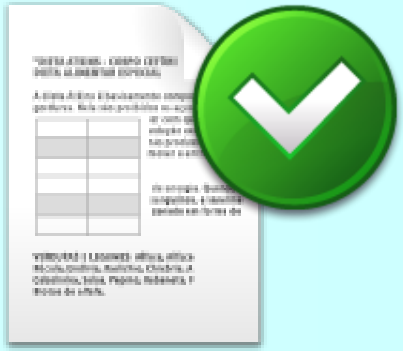
Art. 56.

Postępowanie bezpieczeństwa przemysłowego jest prowadzone na wniosek przedsiębiorcy. …



Art. 57.

Postępowanie bezpieczeństwa przemysłowego obejmuje …



Art. 58.

Sprawdzenia przedsiębiorcy i osób wymienionych w art. 57 przeprowadza się na podstawie . …

9. Bezpieczeństwo przemysłowe



Art. 59.

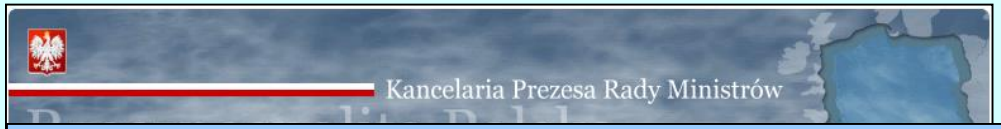
Postępowanie bezpieczeństwa przemysłowego powinno być zakończone w terminie nie dłuższym niż …

Art. 60.

W przypadku postępowania bezpieczeństwa przemysłowego prowadzonego w celu wydania świadectwa, o którym mowa w art. 55 ust. 1 pkt 3 …

Art. 61.

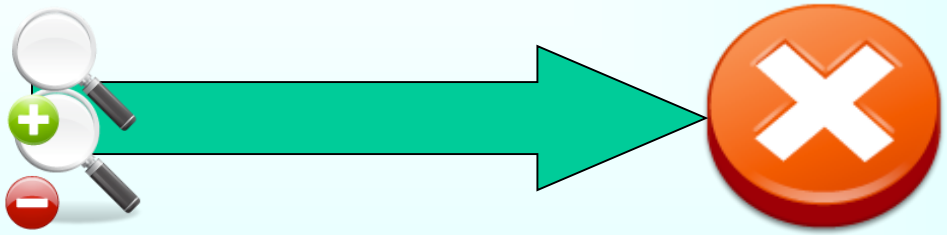
Za przeprowadzenie sprawdzenia przedsiębiorcy oraz postępowań sprawdzających wobec osób wymienionych w art. 57 ust. 3, z wyjątkiem postępowań sprawdzających, o których mowa w art. 32 ust. 4 i art. 33 ust. 1, ABW albo SKW przysługuje zwrot zryczałtowanych kosztów …



Prezes Rady Ministrów określi, w drodze rozporządzenia, wysokość zryczałtowanych kosztów, o których mowa w ust. 1, oraz tryb ich zwrotu …

Art. 62.

Umorzenie postępowania bezpieczeństwa przemysłowego …



Art. 63.

Zawieszenie postępowania bezpieczeństwa przemysłowego …



9. Bezpieczeństwo przemysłowe

Art. 64.

Postępowanie bezpieczeństwa przemysłowego kończy się …

Art. 65.

ABW albo SKW, w okresie ważności świadectwa, może przeprowadzić z urzędu sprawdzenie przedsiębiorcy …

Art. 66.

Wyniki sprawdzenia przedsiębiorcy z urzędu lub ustalenia kontroli ochrony informacji niejawnych mogą stanowić podstawę wydania decyzji o cofnięciu świadectwa …

Art. 67.

Świadectwo, decyzja o odmowie wydania świadectwa oraz decyzja o cofnięciu świadectwa …

9. Bezpieczeństwo przemysłowe



Prezes Ministrów określi, w drodze rozporządzenia, wzory:

- ✓ ***kwestionariusza;***
- ✓ ***świadectwa;***
- ✓ ***decyzji o odmowie wydania świadectwa;***
- ✓ ***decyzji o cofnięciu świadectwa.***

Rozporządzenie Rady Ministrów z dnia 5 kwietnia 2011 r. w sprawie wzorów kwestionariusza bezpieczeństwa przemysłowego, świadectwa bezpieczeństwa przemysłowego, decyzji o odmowie wydania świadectwa bezpieczeństwa przemysłowego oraz decyzji o cofnięciu świadectwa bezpieczeństwa przemysłowego [Dz.U. Nr 86, poz. 470]

9. Bezpieczeństwo przemysłowe

Art. 69.

Od decyzji o umorzeniu postępowania bezpieczeństwa przemysłowego, odmowie wydania oraz o cofnięciu świadectwa przedsiębiorcy przysługuje odwołanie do Prezesa Rady Ministrów …

Art. 70.

Przedsiębiorca, w czasie trwania postępowania bezpieczeństwa przemysłowego, a także w okresie ważności świadectwa, ma obowiązek informowania …

INSTRUKCJA BEZPIECZEŃSTWA PRZEMYSŁOWEGO

Art. 71.

Jednostka organizacyjna zawierająca umowę związaną z dostępem do informacji niejawnych o klauzuli „poufne” lub wyższej jest odpowiedzialna za wprowadzenie do umowy instrukcji bezpieczeństwa przemysłowego …



10. Ewidencje i udostępnianie danych oraz akt postępowań sprawdzających, kontrolnych postępowań sprawdzających i postępowań bezpieczeństwa przemysłowego.



10. Ewidencje i udostępnianie danych oraz akt postępowań sprawdzających, kontrolnych postępowań sprawdzających i postępowań bezpieczeństwa przemysłowego



Art. 72.

Akta postępowań sprawdzających lub kontrolnych postępowań sprawdzających przeprowadzonych przez służby i instytucje uprawnione do prowadzenia poszerzonych postępowań sprawdzających i akta postępowań bezpieczeństwa przemysłowego są udostępniane do wglądu lub przekazywane wyłącznie na pisemne żądanie.

Art. 73.

ABW i SKW prowadzą ewidencję osób uprawnionych na podstawie przepisów ustawy do dostępu do informacji niejawnych o klauzuli „poufne” i wyższej oraz ewidencję osób, którym odmówiono wydania poświadczenia bezpieczeństwa, a także osób, wobec których podjęto decyzję o cofnięciu poświadczenia bezpieczeństwa ….



11. Zmiany w przepisach obowiązujących

Art. 74.

….

…..

……

…….

§ § § § §

{zmiany w ustawach}

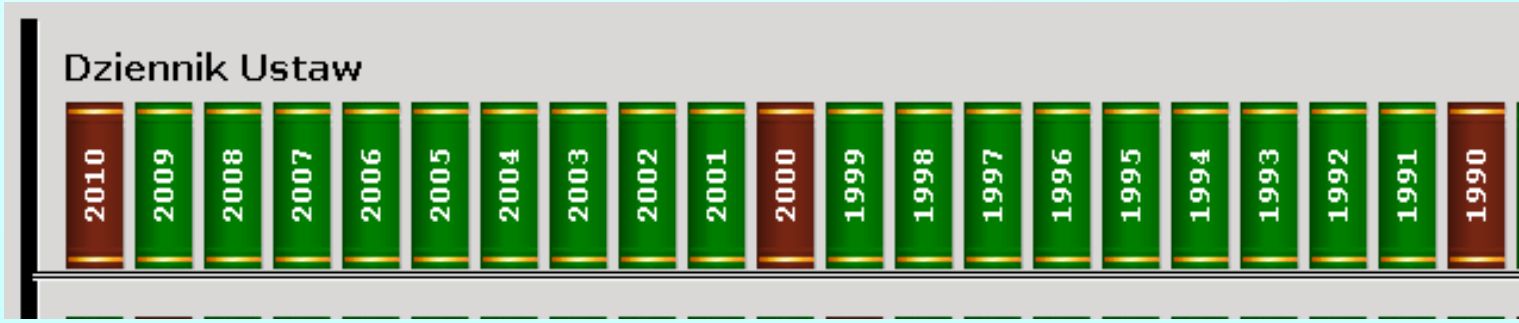
……..

……..

……..

……..

Art. 180.





12. Przepisy przejściowe i końcowe





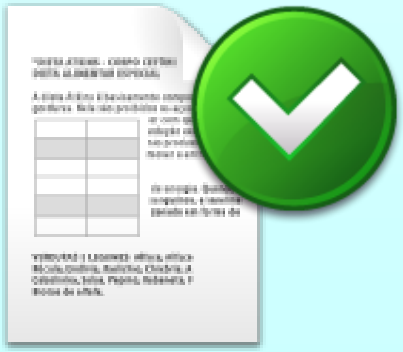
Art. 181.

Kierownicy jednostek organizacyjnych przeprowadzą, w terminie 36 miesięcy od dnia wejścia w życie ustawy, przegląd wytworzonych w podległych im jednostkach organizacyjnych materiałów zawierających informacje niejawne w celu ustalenia, czy spełniają ustawowe przesłanki ochrony na podstawie ustawy, i dokonają w razie potrzeby zmiany lub zniesienia klauzuli tajności …



Art. 182.

Poświadczenia bezpieczeństwa wydane na podstawie przepisów dotychczasowych zachowują ważność przez okres wskazany w tych przepisach.





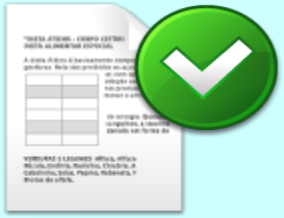
Art. 183.

Przepis art. 14 ust. 3 pkt 2 stosuje się do pełnomocników ochrony i zastępców pełnomocników ochrony zatrudnionych po dniu wejścia w życie ustawy.



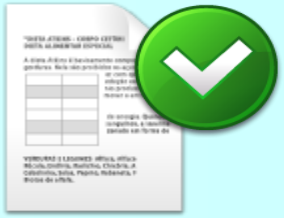
Art. 184.

Kierownicy jednostek organizacyjnych, w których w dniu wejścia w życie ustawy funkcjonują kancelarie tajne, informują o nich w terminie do 3 miesięcy od tej daty odpowiednio ABW lub SKW, z określeniem klauzuli tajności przetwarzanych informacji niejawnych.



Art. 185.

Akredytacje systemów teleinformatycznych udzielone przed dniem wejścia w życie ustawy zachowują ważność do czasu dokonania w systemie teleinformatycznym zmian, które mogą mieć istotny wpływ na bezpieczeństwo teleinformatyczne, nie dłużej jednak niż przez okres 5 lat od dnia wejścia w życie ustawy.



Art. 186.

Świadectwa bezpieczeństwa przemysłowego wydane na podstawie przepisów dotychczasowych, ważne w dniu wejścia w życie ustawy, potwierdzające zdolność do ochrony informacji niejawnych …

Art. 187.

Przedsiębiorcy wykonujący umowy związane z dostępem do informacji niejawnych o klauzuli „poufne”, nieposiadający w dniu wejścia w życie ustawy ważnego świadectwa bezpieczeństwa przemysłowego powinni uzyskać takie świadectwo w terminie 12 miesięcy od dnia wejścia w życie ustawy.

Art. 188.

Do postępowań sprawdzających, kontrolnych postępowań sprawdzających i postępowań bezpieczeństwa przemysłowego wszczętych i niezakończonych przed dniem wejścia w życie ustawy stosuje się przepisy dotychczasowe.

12. Przepisy przejściowe i końcowe

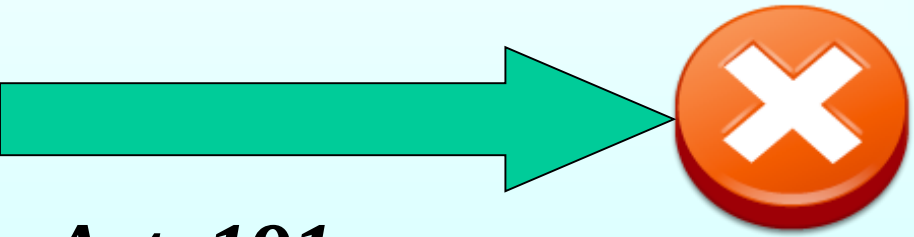


Art. 189.

Dotychczasowe przepisy wykonawcze wydane na podstawie art. 14 ust. 4, art. 17 ust. 2, **art. 18a ust. 2**, art. 23 ust. 3, art. 36 ust. 3, art. 53 ust. 1–4, art. 55, art. 62 ust. 1, art. 63 ust. 4, art. 74 i art. 74a ust. 2 **ustawy, o której mowa w art. 190, zachowują moc do dnia wejścia w życie przepisów wykonawczych wydanych na podstawie** art. 6 ust. 9, art. 12 ust. 6, art. 13 ust. 4, **art. 18 ust. 1**, art. 20 ust. 2, art. 29 ust. 6, art. 30 ust. 8, art. 33 ust. 12, art. 47 ust. 1, 3 i 5, art. 49 ust. 9, art. 53 ust. 4, art. 61 ust. 2 i art. 68 ust. 1 **niniejszej ustawy, nie dłużej jednak niż przez okres 12 miesięcy od dnia jej wejścia w życie.**

Art. 190.

Traci moc ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 2005 r. Nr 196, poz. 1631, z późn. zm.).



Art. 191.

Ustawa wchodzi w życie po upływie 3 miesięcy od dnia ogłoszenia z wyjątkiem art. 131, który wchodzi w życie z dniem 1 stycznia 2013 r.





DZIĘKUJĘ ZA UWAGĘ

