Warszawa, dnia 27 marca 2013 r.

Poz. 79

Służba Wywiadu Wojskowego

ZARZĄDZENIE Nr 47/2012
SZEFA SŁUŻBY WYWIADU WOJSKOWEGO

z dnia 20 grudnia 2012 r.

w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii tajnych oraz innych, niż kancelaria tajna, komórek organizacyjnych odpowiedzialnych za przetwarzanie materiałów niejawnych, sposobu i trybu przetwarzania informacji niejawnych oraz doboru i stosowania środków bezpieczeństwa fizycznego w Służbie Wywiadu Wojskowego

Na podstawie art. 47 ust. 3 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz.1228) zarządza się, co następuje:

Rozdział 1
Postanowienia ogólne

§ 1.

Zarządzenie określa:

1) organizację i funkcjonowanie kancelarii tajnych oraz innych, niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za przetwarzanie materiałów niejawnych w Służbie Wywiadu Wojskowego, z wyjątkiem, określonych w odrębnych przepisach, organizacji i funkcjonowania kancelarii kryptograficznej i stacji kryptograficznej;
2) obieg informacji niejawnych w Służbie Wywiadu Wojskowego, z wyjątkiem:
   a) materiałów związanych z ewidencją operacyjną,
   b) ewidencji archiwalnej, materiałów archiwalnych i dokumentacji niearchiwalnej gromadzonych w archiwum Służby Wywiadu Wojskowego oraz dokumentów stanowiących zasób biblioteki tajnej,
   c) materiałów i dokumentów kryptograficznych,
   d) dokumentów operacyjnych,

e) dokumentów wytwarzanych lub przesyłanych drogą elektroniczną.
– jeżeli ich obieg uregulowany został odrębnie;
3) dobór i zakres stosowania środków bezpieczeństwa fizycznego informacji niejawnych w SWW;
4) tryb komisyjnego otwierania urządzeń do przechowywania materiałów niejawnych;
5) tryb rozliczania żołnierzy, funkcjonariuszy i pracowników Służby Wywiadu Wojskowego z materiałów służbowych;
6) sposób ochrony informacji niejawnych w trakcie obrad, szkoleń i konferencji;
7) sposób sporządzania kopii i tłumaczeń z dokumentów zawierających informacje niejawne;
8) sprawozdawczość w zakresie materiałów niejawnych oraz postępowania w przypadku utraty takich materiałów.

§ 2.

Określenia użyte w zarządzeniu oznaczają:
1) SWW – Służbę Wywiadu Wojskowego;
2) ustawa – ustawę z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych;
3) jednostka organizacyjna SWW – jednostkę organizacyjną, o której mowa w statucie Służby Wywiadu Wojskowego stanowiącym załącznik do zarządzenia Ministra Obrony Narodowej z dnia 28 maja 2008 r. w sprawie nadania statutu Służbie Wywiadu Wojskowego (M.P. Nr 44, poz. 385, z 2009 r. Nr 6, poz. 65 oraz z 2012 r., poz. 481);
4) komórka organizacyjna – wydział, samodzielną sekcję, zespół lub inną komórkę wewnętrzną wchodzącą w skład jednostki organizacyjnej SWW;
5) punkt kontroli:
   a) sekretariat Szefa SWW lub jego zastępców, w przypadku utworzenia punktu kontroli,
   b) sekretariat kierownika jednostki organizacyjnej SWW, w przypadku utworzenia punktu kontroli,
   c) sekretariat kierownika komórki organizacyjnej, w przypadku utworzenia punktu kontroli,
   d) inne stanowiska w komórkach organizacyjnych, na których realizowane są zadania punktu kontroli;
6) funkcjonariusz:
   a) funkcjonariusza SWW mianowanego na podstawie przepisów ustawy z dnia 9 czerwca 2006 r. o służbie funkcjonariuszy Służby Kontrwywiadu Wojskowego oraz Służby Wywiadu Wojskowego (Dz. U. Nr 104, poz. 710, z późn. zm.[1)]) lub funkcjonariusza innej służby, wyznaczonego na stanowisko służbowe w SWW,
   b) żołnierza zawodowego wyznaczonego na stanowisko służbowe w SWW na podstawie przepisów ustawy z dnia 11 września 2003 r. o służbie wojskowej żołnierzy zawodowych (Dz. U. z 2010 r. Nr 90, poz. 593, z późn. zm.[2)]) lub skierowanego do służby w SWW,
   c) pracownika zatrudnionego w SWW na podstawie umowy o pracę, dopuszczonego do pracy na stanowisku związanym z dostępem do informacji niejawnych,
   d) osobę, której zlecono lub powierzono prace związane z dostępem do informacji niejawnych;
7) upoważniony funkcjonariusz pionu ochrony – naczelnika wydziału ochrony Biura Ochrony

[1)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2009 r. Nr 114, poz. 957, z 2010 r. Nr 113, poz. 745, Nr 182, poz. 1228, Nr 230, poz. 1510 i Nr 238, poz. 1578 oraz z 2011 r. Nr 117, poz. 677.
[2)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone Dz. U. z 2010 r. Nr 28, poz. 143, Nr 107, poz. 679, Nr 113, poz. 745, Nr 127, poz. 857, Nr 182, poz. 1228 i Nr 238, poz. 1578 oraz z 2011 r. Nr 22, poz. 114, Nr 112, poz. 654, Nr 122, poz. 696, Nr 171, poz. 1016 i Nr 236, poz. 1396.

i Osłony, naczelnika wydziału właściwego do spraw nadzoru nad kancelariami tajnymi Biura Ochrony i Osłony, kierownika kancelarii tajnej albo zastępującego ich funkcjonariusza pionu ochrony;

8) kancelaria tajna – wchodzące w skład wydziału właściwego do spraw nadzoru nad kancelariami tajnymi Biura Ochrony i Osłony: Główną Kancelarię Tajną, Kancelarię Tajną Międzynarodową i oddziały kancelarii;
9) GKT – Główną Kancelarię Tajną – kancelarię wysyłającą i przyjmującą przesyłki adresowane na Szefa SWW, jego zastępców i jednostki organizacyjne, obsługującą oddziały kancelarii oraz punkty kontroli;
10) KTM – Kancelarię Tajną Międzynarodową – kancelarię tajną odpowiedzialną za przyjmowanie, rejestrowanie, przechowywanie, obieg i udostępnianie dokumentów niejawnych wymienianych z innymi państwami i organizacjami międzynarodowymi, na podstawie zawartych przez Rzeczpospolitą Polską umów międzynarodowych;
11) oddział kancelarii – komórkę wykonującą zadania kancelarii tajnej na rzecz jednostek organizacyjnych SWW, których szczegółową właściwość i zadania określa pełnomocnik ochrony;
12) punkt obsługi dokumentów międzynarodowych – wydzieloną część oddziału kancelarii tajnej odpowiedzialną za przyjmowanie, rejestrowanie, przechowywanie, obieg i udostępnianie dokumentów niejawnych wymienianych z innymi państwami i organizacjami międzynarodowymi na podstawie zawartych przez Rzeczpospolitą Polską umów międzynarodowych;
13) pełnomocnik ochrony – pełnomocnika do spraw ochrony informacji niejawnych w SWW – dyrektora Biura Ochrony i Osłony;
14) kierownik kancelarii tajnej – funkcjonariusza podległego pełnomocnikowi ochrony, kierującego pracą kancelarii tajnej;
15) kancelista – funkcjonariusza pełniącego służbę lub zatrudnionego w kancelarii tajnej, podlegającego bezpośrednio kierownikowi kancelarii tajnej;
16) zastępca kierownika kancelarii tajnej – kancelistę zastępującego kierownika kancelarii tajnej podczas jego nieobecności;
17) wykonawca – funkcjonariusza zajmującego określone stanowisko służbowe, wykonującego zadania zgodnie z zakresem obowiązków, posiadającego stosowne poświadczenie bezpieczeństwa i przeszkolenie w zakresie ochrony informacji niejawnych;
18) przetwarzanie informacji niejawnych – wszelkie operacje wykonywane w odniesieniu do informacji niejawnych i na tych informacjach, w szczególności ich wytwarzanie, modyfikowanie, kopiowanie, klasyfikowanie, gromadzenie, przechowywanie, przekazywanie lub udostępnianie;
19) urządzenie ewidencyjne – księgę, dziennik, wykaz, spis, rejestr lub kartotekę o ustalonych rubrykach, służące do rejestrowania dokumentów zawierających informacje niejawne oraz umożliwiające kontrolę ich stanu i obiegu;
20) przesyłka – materiały w postaci odpowiednio zabezpieczonych, zaadresowanych i oznaczonych paczek lub listów;
21) strefa ochronna – pomieszczenia lub obszar, do którego dostęp objęty jest określonymi przez pełnomocnika ochrony restrykcjami, w celu uniemożliwienia osobom nieuprawnionym dostępu do informacji niejawnych;
22) strefa ochronna I – strefa, o której mowa w § 5 ust. 1 pkt 1 rozporządzenia Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz. U., poz. 683);

23) strefa ochronna II – strefa, o której mowa w § 5 ust. 1 pkt 2 rozporządzenia wymienionego w pkt 22;
24) strefa ochronna III – strefa, o której mowa w § 5 ust. 1 pkt 3 rozporządzenia wymienionego w pkt 22;
25) dekretacja – naniesienie przez właściwego przełożonego na opakowaniu przesyłki odręcznej adnotacji wskazującej adresata oraz naniesienie na pierwszej stronie dokumentu indywidualnie określonego adresata i daty, a także ewentualnej adnotacji informującej o sposobie dalszego postępowania;
26) nadawca – jednostkę organizacyjną SWW albo komórkę organizacyjną wysyłającą przesyłkę lub funkcjonariusza dokonującego dekretacji;
27) ostatni adresat – funkcjonariusza, na którego zaadresowana lub zadekretowana została przesyłka, niedokonującego dalszej dekretacji;
28) pokwitowanie – potwierdzenie odbioru materiału przez odbiorcę zawierające datę oraz podpis pozwalający na identyfikację funkcjonariusza;
29) stacja kryptograficzna – komórka organizacyjna lub stanowisko, realizująca zadania związane z ochroną kryptograficzną (szyfrowanie, deszyfrowanie) informacji niejawnych z wykorzystaniem urządzeń i narzędzi kryptograficznych;
30) naczelnik WKT – naczelnika wydziału właściwego do spraw nadzoru nad kancelariami tajnymi Biura Ochrony i Osłony;
31) metryka – metrykę elektronicznego nośnika informacji;
32) służba partnerska – organ i służbę, o której mowa w art. 9 ust. 1 ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz. U. Nr 104, poz. 709, z późn. zm.[3)]);
33) kopia – kopię oraz, jeżeli inaczej nie wynika z przepisów zarządzenia: odpis, wypis, wyciąg, wydruk i odwzorowanie cyfrowe;
34) dostępność informacji niejawnych – właściwość, o której mowa w § 2 pkt 1 rozporządzenia wymienionego w pkt 22;
35) integralność informacji niejawnych – właściwość, o której mowa w § 2 pkt 2 rozporządzenia wymienionego w pkt 22;
36) poufność informacji niejawnych – właściwość, o której mowa w § 2 pkt 3 rozporządzenia wymienionego w pkt 22;
37) poziom zagrożeń – określoną na zasadach, o których mowa w § 3 rozporządzenia wymienionego w pkt 22, ocenę prawdopodobieństwa wystąpienia zdarzeń związanych z bezpieczeństwem informacji niejawnych zagrażających ich poufności, dostępności lub integralności oraz konsekwencji związanych z ich nieuprawnionym ujawnieniem lub utratą;
38) incydent bezpieczeństwa – sytuację, o której mowa w § 2 pkt 4 rozporządzenia wymienionego w pkt 22;
39) pomieszczenie wzmocnione – pomieszczenie spełniające wymagania:
    a) zlokalizowane w budynku, co najmniej typu 3 wg kategorii środków bezpieczeństwa K-3 określonej w załączniku nr 1,
    b) zlokalizowane w strefie ochronnej I lub strefie ochronnej II,
    c) konstrukcji pomieszczenia, drzwi i okien, co najmniej typu 3 wg kategorii środków bezpieczeństwa K-2 określonej w załączniku wymienionym w lit. a;

[3)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2006 r. Nr 218, poz. 1592, z 2009 r. Nr 85, poz. 716, z 2010 r. Nr 182, poz. 1228, z 2011 r. Nr 22, poz. 114, Nr 53, poz. 273 i Nr 84, poz. 455 oraz z 2012 r., poz. 707.

40) plan ochrony – plan ochrony informacji niejawnych w SWW.

§ 3.

1. W kancelariach tajnych oprócz informacji niejawnych o klauzuli „Ściśle tajne” i „Tajne” przetwarza się informacje niejawne o klauzuli „Poufne” i „Zastrzeżone”.

2. W kancelariach tajnych przetwarza się informacje jawne.

3. Obieg informacji jawnych w SWW określają przepisy w sprawie obiegu informacji jawnych.

Rozdział 2
Organizacja i funkcjonowanie kancelarii tajnej oraz innej, niż kancelaria tajna komórki organizacyjnej odpowiedzialnej za rejestrowanie, przechowywanie, obieg i udostępnienie materiałów niejawnych

§ 4.

1. Oddziały kancelarii w jednostkach organizacyjnych SWW organizuje pełnomocnik ochrony na wniosek kierownika jednostki organizacyjnej SWW, w której ma być zlokalizowany oddział kancelarii, po zasięgnięciu opinii naczelnika WKT.

2. Naczelnik WKT i kancelarie tajne podlegają pełnomocnikowi ochrony.

3. Naczelnik WKT sprawuje nadzór nad prawidłowym funkcjonowaniem kancelarii tajnych i punktów kontroli, obiegiem dokumentów niejawnych oraz stosowaniem środków ochrony fizycznej.

4. Naczelnik WKT jest w szczególności odpowiedzialny za zorganizowanie i wdrożenie systemu oraz procedur obiegu i przesyłania informacji w ramach i poza SWW, szkolenie funkcjonariuszy kancelarii tajnych i punktów kontroli oraz prowadzenie wykazu osób upoważnionych do dostępu do informacji niejawnych, posiadających stosowne poświadczenia bezpieczeństwa, którego wzór określa załącznik nr 2.

5. Kierownika kancelarii tajnej wyznacza Szef SWW, po zasięgnięciu opinii pełnomocnika ochrony.

6. W przypadku nieobecności kierownika kancelarii tajnej obowiązki wykonuje zastępca kierownika kancelarii tajnej wskazany przez naczelnika WKT.

7. Utworzenie punktu kontroli odbywa się w trybie określonym w ust. 1.

8. Funkcjonariuszy pełniących służbę w punktach kontroli wyznaczają kierownicy właściwych jednostek organizacyjnych SWW albo komórek organizacyjnych spośród funkcjonariuszy odpowiednio tych jednostek organizacyjnych SWW albo komórek organizacyjnych, w porozumieniu z pełnomocnikiem ochrony.

9. Kierownicy kancelarii tajnych sprawują nadzór nad punktami kontroli właściwych jednostek organizacyjnych SWW w zakresie przestrzegania przepisów dotyczących obiegu informacji niejawnych.

10. Oddział kancelarii jednej jednostki organizacyjnej SWW może obsługiwać inne jednostki organizacyjne SWW lub komórki organizacyjne różnych jednostek usytuowane w tej samej strefie ochronnej.

§ 5.

1. GKT przyjmuje przesyłki adresowane na Szefa SWW, jego zastępców i jednostki organizacyjne SWW.

2. GKT wysyła i przyjmuje przesyłki za pośrednictwem Centrum Wsparcia Teleinformatycznego Sił Zbrojnych. GKT może, w uzasadnionych przypadkach, wysyłać i przyjmować przesyłki z pominięciem Centrum, w sposób określony w odrębnych przepisach.

3. Kancelarie tajne przyjmują przesyłki zaadresowane na obsługiwane przez nie jednostki organizacyjne SWW lub komórki organizacyjne.

4. Punkty kontroli przyjmują i przekazują przesyłki za pośrednictwem właściwych kancelarii tajnych, z zastrzeżeniem § 42 ust. 5.

5. Punkty kontroli jednostek organizacyjnych SWW albo komórek organizacyjnych, mających siedzibę poza Warszawą, mogą nadawać i odbierać przesyłki za pośrednictwem kancelarii tajnych jednostek wojskowych lub instytucji, przy których mają swoją siedzibę, na zasadach określonych w porozumieniach zawartych przez pełnomocnika ochrony z pełnomocnikami ochrony właściwych jednostek i instytucji.

§ 6.

1. Na stanowisko kierownika kancelarii tajnej wyznacza się funkcjonariusza pionu ochrony.

2. Kierownicy kancelarii tajnych w szczególności są odpowiedzialni za:
1) zapewnienie prawidłowej realizacji zadań przez kancelarię tajną;
2) nadzór nad przestrzeganiem przepisów dotyczących obiegu dokumentów niejawnych we właściwych jednostkach organizacyjnych SWW;
3) kontrolę właściwego oznaczenia, zabezpieczenia i ewidencjonowania obiegu dokumentów niejawnych przez punkty kontroli;
4) zapewnienie fizycznej ochrony dokumentów niejawnych w czasie godzin pracy kancelarii tajnej oraz w przypadku wystąpienia zdarzeń zakłócających przebieg służby;
5) zabezpieczenie materiałów niezbędnych do zapewnienia prawidłowego funkcjonowania systemu obiegu informacji niejawnych;
6) wykonywanie poleceń pełnomocnika ochrony.

3. Do obowiązków kierowników kancelarii tajnych w szczególności należy:

1) przyjmowanie, rejestrowanie, przechowywanie oraz przekazywanie materiałów niejawnych otrzymywanych, wysyłanych oraz wytwarzanych we właściwych jednostkach organizacyjnych SWW, według zasad ustalonych w zarządzeniu;
2) udostępnianie i wydawanie materiałów niejawnych osobom posiadającym stosowne poświadczenia bezpieczeństwa;
3) rozliczanie wykonawców z powierzonych im materiałów niejawnych;
4) kompletowanie dokumentów oraz przygotowywanie do archiwizacji akt znajdujących się w kancelarii tajnej;
5) prowadzenie ewidencji pieczęci urzędowych oraz służbowych używanych w SWW.

4. Do obowiązków kierownika KTM oraz kierowników kancelarii tajnych, w których zorganizowano punkty obsługi dokumentów międzynarodowych, należy ponadto prowadzenie na podstawie informacji otrzymywanych z Kancelarii Głównej Zagranicznej Ministerstwa Obrony Narodowej, wykazu kancelarii tajnych międzynarodowych i punktów obsługi dokumentów międzynarodowych.

5. Szczegółowe obowiązki kierownika KTM oraz kierowników kancelarii tajnych określa pełnomocnik ochrony.

§ 7.

1. Przekazanie obowiązków na stanowisku kierownika kancelarii tajnej następuje na podstawie protokołu zdawczo-odbiorczego, w obecności naczelnika WKT, osoby zdającej oraz osoby przejmującej obowiązki.

2. Protokół, o którym mowa w ust. 1, zawiera w szczególności:

1) nazwy i numery urządzeń ewidencyjnych, na podstawie których dokonano sprawdzenia stanu faktycznego dokumentów niejawnych pozostających na ewidencji kancelarii tajnej oraz pozycje zapisów w tych urządzeniach;
2) informacje dotyczące zgodności lub niezgodności stanu faktycznego dokumentów niejawnych ze stanem ewidencyjnym;
3) ewentualne uwagi osoby przyjmującej obowiązki, dotyczące ujawnionych nieprawidłowości w zakresie ewidencjonowania i obiegu dokumentów.

3. Protokół, o którym mowa w ust. 1, podpisują osoba zdająca i osoba przejmująca obowiązki, a zatwierdza pełnomocnik ochrony. Po zarejestrowaniu protokół przechowuje właściwa kancelaria tajna.

4. W przypadku, gdy osoba zdająca obowiązki nie może uczestniczyć w przejęciu obowiązków, czynność tę przeprowadza komisja powołana przez pełnomocnika ochrony. W skład komisji wchodzi naczelnik WKT.

5. W przypadku, o którym mowa w ust. 4, protokół, o którym mowa w ust. 1, podpisują członkowie komisji, o której mowa w ust. 4, i osoba przejmująca obowiązki, a zatwierdza pełnomocnik ochrony. Ust. 3 zdanie drugie stosuje się odpowiednio.

6. W przypadku zmiany funkcjonariusza punktu kontroli, ust. 1 i 2 stosuje się odpowiednio. Protokół po zarejestrowaniu przechowuje się w punkcie kontroli.

7. W okresie czasowej nieobecności, w szczególności z powodu urlopu lub wyjazdu służbowego, kierownika kancelarii tajnej zastępuje jego zastępca wyznaczony przez naczelnika WKT.

8. W przypadku braku możliwości wyznaczenia zastępcy, obowiązki zastępcy kierownika kancelarii tajnej wykonuje inna osoba pełniąca obowiązki służbowe w pionie ochrony, wyznaczona przez pełnomocnika ochrony. W takim przypadku kierownik kancelarii tajnej przekazuje tej osobie, protokolarnie, wyłącznie urządzenia ewidencyjne i materiały niezbędne do prowadzenia bieżącej pracy kancelarii tajnej. Szafy z pozostałymi dokumentami niejawnymi zamyka i oznakowuje swoją pieczęcią numerową.

9. W przypadku nieprzewidzianej nieobecności kierownika kancelarii tajnej, w szczególności, gdy nie można przewidzieć okresu trwania tej nieobecności, ust. 4 i 5 stosuje się odpowiednio.

10. W przypadku czasowej nieobecności funkcjonariusza pełniącego służbę w punkcie kontroli sporządza się protokół przekazania ewidencji, pieczęci oraz innych materiałów niezbędnych do funkcjonowania punktu kontroli, funkcjonariuszowi wyznaczonemu przez bezpośredniego przełożonego.

11. Protokół, o którym mowa w ust. 8 i 10, można sporządzić w formie pozwalającej na wielokrotne przekazywanie i zwrot dokumentacji ewidencyjnej, pieczęci oraz innych materiałów niezbędnych do funkcjonowania punktu kontroli. Protokół podlega rejestracji.

12. Ewidencje i pieczęcie, o których mowa w ust. 10, wyznaczony funkcjonariusz przechowuje w szafie metalowej pozostającej w jego dyspozycji.

Rozdział 3
Dobór i stosowanie środków bezpieczeństwa fizycznego

§ 8.

Kancelarie tajne lokalizuje się w pomieszczeniu lub zespole pomieszczeń znajdującym się w strefie ochronnej I lub w strefie ochronnej II.

§ 9.

1. Każda kancelaria tajna powinna być, w miarę możliwości, rozmieszczona w zespole trzech pomieszczeń z przeznaczeniem na:
1) pokój pracy dla kancelistów;
2) pomieszczenie magazynowe służące do przechowywania materiałów niejawnych poza szafami stalowymi;

3) pomieszczenie przeznaczone do zapoznawania się wykonawców z dokumentami niejawnymi – czytelnię. Czytelnia powinna być zorganizowana w sposób umożliwiający stały nadzór nad dokumentami ze strony kancelistów, jednakże zabrania się instalowania w niej systemu nadzoru wizyjnego.

2. W pomieszczeniu kancelarii tajnej, w którym przyjmowani są interesanci powinna być zainstalowana barierka oddzielająca ich od kancelistów i pozostałych pomieszczeń kancelarii.

§ 10.

1. Kancelarię tajną wyposaża się w urządzenia do niszczenia dokumentów oraz w pojemniki lub worki służące do przechowywania dokumentów niejawnych przeznaczonych do zniszczenia lub ewakuacji materiałów.

2. Kancelarię tajną można wyposażyć w sprzęt informatyczny przystosowany do odczytu informacji niejawnych zapisanych na elektronicznych nośnikach danych.

§ 11.

1. System bezpieczeństwa fizycznego informacji niejawnych w SWW ma na celu zapewnienie dostępności, integralności i poufności tych informacji.

2. Środki bezpieczeństwa fizycznego w SWW dobiera się adekwatnie do poziomu zagrożeń.

§ 12.

1. Cel, o którym mowa w § 11 ust. 1, osiąga się przez:
1) zapewnienie właściwego przetwarzania informacji niejawnych;
2) umożliwienie zróżnicowania dostępu do informacji niejawnych dla funkcjonariuszy zgodnie z posiadanymi przez nich uprawnieniami oraz uzasadnioną potrzebą dostępu do informacji niejawnych;
3) wykrywanie, udaremnianie lub powstrzymywanie działań nieuprawnionych;
4) uniemożliwianie lub opóźnianie wtargnięcia osób nieuprawnionych w sposób niezauważony lub z użyciem siły do pomieszczenia lub obszaru, w którym są przetwarzane informacje niejawne.

2. Środki bezpieczeństwa fizycznego stosuje się we wszystkich pomieszczeniach i obszarach, w których są przetwarzane informacje niejawne, z zastrzeżeniem § 17 ust. 4.

3. System środków bezpieczeństwa fizycznego obejmuje stosowanie rozwiązań organizacyjnych, wyposażenia i urządzeń służących ochronie informacji niejawnych oraz elektronicznych systemów pomocniczych wspomagających ochronę informacji niejawnych. W zależności od poziomu zagrożeń stosuje się odpowiednią kombinację następujących środków bezpieczeństwa fizycznego:
1) pion ochrony – wyodrębnioną i podległą pełnomocnikowi ochrony jednostkę organizacyjną SWW realizującą w jego imieniu zadania w zakresie ochrony informacji niejawnych, o których mowa w ustawie;

2) personel bezpieczeństwa – nadzorowane przez funkcjonariusza pionu ochrony osoby posiadające w razie konieczności odpowiednie uprawnienia do dostępu do informacji niejawnych i przeszkolenie, wykonujące czynności związane z fizyczną ochroną informacji niejawnych, w tym kontrolę dostępu do pomieszczeń lub obszarów, w których są przetwarzane informacje niejawne, nadzór nad systemem dozoru wizyjnego, a także reagowanie na alarmy lub sygnały awaryjne;
3) bariery fizyczne – środki chroniące granice miejsca, w którym są przetwarzane informacje niejawne, w szczególności ogrodzenia, ściany, bramy, drzwi i okna;
4) szafy i zamki – środki stosowane do przechowywania informacji niejawnych lub zabezpieczające te informacje przed nieuprawnionym dostępem;
5) system kontroli dostępu – obejmujący elektroniczny system pomocniczy lub rozwiązanie organizacyjne, stosowany w celu zagwarantowania uzyskiwania dostępu do pomieszczenia lub obszaru, w którym są przetwarzane informacje niejawne, wyłącznie przez osoby posiadające odpowiednie uprawnienia;
6) system sygnalizacji włamania – elektroniczny system pomocniczy stosowany w celu realizacji procedur ochrony informacji niejawnych oraz podwyższenia poziomu bezpieczeństwa, który zapewniają bariery fizyczne, a w pomieszczeniach i budynkach zastępujący lub wspierający personel bezpieczeństwa;
7) system dozoru wizyjnego – elektroniczny system pomocniczy stosowany w celu bieżącego monitorowania ochronnego lub sprawdzania incydentów bezpieczeństwa i sygnałów alarmowych przez personel bezpieczeństwa;
8) system kontroli osób i przedmiotów – obejmujący elektroniczny system pomocniczy lub rozwiązanie organizacyjne polegające na zwracaniu się o dobrowolne poddanie się kontroli lub udostępnienie do kontroli rzeczy osobistych, a także przedmiotów wnoszonych lub wynoszonych – stosowany w celu zapobiegania próbom nieuprawnionego wnoszenia na chroniony obszar rzeczy zagrażających bezpieczeństwu informacji niejawnych lub nieuprawnionego wynoszenia informacji niejawnych z budynków lub obiektów.

4. W celu zapewnienia dostępności, integralności i poufności informacji niejawnych za zgodą pełnomocnika ochrony można zastosować środki bezpieczeństwa fizycznego inne niż wymienione w ust. 3, jeżeli taka potrzeba wynika z analizy poziomu zagrożeń.

5. Jeżeli istnieje zagrożenie podglądu, także przypadkowego, informacji niejawnych, zarówno w świetle dziennym, jak i w warunkach sztucznego oświetlenia, podejmuje się działania w celu wyeliminowania takiego zagrożenia.

6. Elektroniczne systemy pomocnicze, o których mowa w ust. 3 pkt. 5-7, powinny posiadać wydane przez dostawcę, z uwzględnieniem przepisów o systemie oceny zgodności, poświadczenie zgodności z wymogami określonymi w załączniku nr 1 do zarządzenia.

7. Wejście do strefy ochronnej I lub strefy ochronnej II musi się odbywać, co najmniej ze strefy ochronnej III.

8. Metodykę doboru środków bezpieczeństwa fizycznego, o których mowa w ust. 3, określa załącznik nr 1.

§ 13.

1. Informacje niejawne o klauzuli „ściśle tajne” przetwarza się w strefie ochronnej I lub w strefie ochronnej II i przechowuje w sposób spełniający jedno z wymagań:

1) w szafach metalowych spełniających wymagania klasy odporności na włamanie S2 określone w Polskiej Normie PN-EN 14450 lub nowszej,
2) poza szafami metalowymi w pomieszczeniu wzmocnionym, z zastosowaniem jednego z poniższych środków uzupełniających:
   a) stała ochrona lub kontrola w nieregularnych odstępach czasu przez funkcjonariusza pionu ochrony posiadającego odpowiednie poświadczenie bezpieczeństwa, w szczególności z wykorzystaniem systemu dozoru wizyjnego z obowiązkową rejestracją w rozdzielczości nie mniejszej niż 400 linii telewizyjnych i przechowywaniem zarejestrowanego zapisu przez czas nie krótszy niż 30 dni;
   b) system sygnalizacji włamania obsługiwany przez pion ochrony z wykorzystaniem systemu dozoru wizyjnego, o którym mowa w lit. a.

2. Informacje niejawne o klauzuli „Tajne”, „Poufne” i „Zastrzeżone” przetwarza się w strefie ochronnej I lub w strefie ochronnej II i przechowuje ~~się~~ w szafach metalowych spełniających co najmniej wymagania klasy odporności na włamanie S1, określone w Polskiej Normie PN-EN 14450 lub nowszej, lub w pomieszczeniu wzmocnionym.

3. Na drzwiach szaf, o których mowa w ust. 1 pkt 1 oraz w ust. 2, nakleja się kartę informacyjną, której wzór określa załącznik nr 3.

§ 14.

Dopuszczalne jest przechowywanie w jednej szafie metalowej wspólnie materiałów niejawnych oznaczonych różnymi klauzulami oraz materiałów jawnych, pod warunkiem, że konstrukcja szafy pozwala na ich fizyczne rozdzielenie. Materiały nie są rozdzielane, jeżeli wchodzą w skład zbioru dokumentów.

§ 15.

W jednostkach i komórkach organizacyjnych SWW dopuszcza się przechowywanie materiałów niejawnych w szafach metalowych lub w odrębnie zamykanej skrytce stanowiącej część tej szafy oraz w zestawach kartotecznych, w pomieszczeniach innych niż kancelaria tajna, zlokalizowanych w strefie ochronnej I lub w strefie ochronnej II, w których przebywanie wiąże się z dostępem do informacji niejawnych.

§ 16.

1. W szczególnie uzasadnionych przypadkach, o ile jest to podyktowane potrzebami służby dopuszcza się przechowywanie materiałów zaewidencjonowanych na różnych funkcjonariuszy w tych samych szafach metalowych oraz zestawach kartotecznych.

2. W przypadku, o którym mowa w ust. 1, kierownik jednostki organizacyjnej SWW przedstawia pełnomocnikowi ochrony do akceptacji, szczegółowe rozwiązania w tym zakresie.

3. W Biurze Ochrony i Osłony rozwiązania, o których mowa w ust. 2, przedstawiają pełnomocnikowi ochrony do akceptacji kierownicy komórek organizacyjnych.

§ 17.

1. Przetwarzanie informacji niejawnych w systemach teleinformatycznych odbywa się w strefie ochronnej I lub w strefie ochronnej II, w warunkach uwzględniających wyniki procesu szacowania ryzyka, o którym mowa w art. 49 ust. 1 ustawy.

2. Przekazywanie informacji, o których mowa w ust. 1, odbywa się w strefie ochronnej, na podstawie wyników procesu szacowania ryzyka, o którym mowa w art. 49 ust. 1 ustawy.

3. Serwery, systemy zarządzania siecią, kontrolery sieciowe i inne newralgiczne elementy systemów teleinformatycznych umieszcza się, z uwzględnieniem wyników procesu szacowania ryzyka, o którym mowa w ust. 1, w strefie ochronnej I lub w strefie ochronnej II.

4. Przetwarzanie informacji niejawnych w części mobilnej zasobów systemu teleinformatycznego odbywa się na podstawie wyników procesu szacowania ryzyka, o którym mowa w art. 49 ust. 1 ustawy, w sposób określony w dokumentacji bezpieczeństwa systemu teleinformatycznego.

§ 18.

1. Po zakończeniu pracy kierownicy kancelarii tajnych oraz użytkownicy pomieszczeń służących do przetwarzania informacji niejawnych, zamykają i oznakowują swoimi pieczęciami numerowymi szafy metalowe służące do przechowywania materiałów niejawnych oraz pomieszczenia służbowe.

2. Czynności oznakowania dokonuje się przez czytelne odciśnięcie na wypełnieniu uchwytu plombującego treści indywidualnie przydzielonej funkcjonariuszowi pieczęci metalowej.

§ 19.

1. Zasady zdawania, przechowywania oraz wydawania kluczy użytku bieżącego i zapasowych do pomieszczeń służbowych oraz szaf metalowych określa plan ochrony.

2. Klucze i kody dostępu do szaf metalowych, pomieszczeń lub obszarów, w których są przetwarzane informacje niejawne, mogą być udostępnione tylko tym osobom, którym posiadanie kluczy lub znajomość kodów są niezbędne do wykonywania obowiązków służbowych. Kody zmienia się co najmniej raz w roku, a także w przypadku:

1) w nowo instalowanych zamkach szyfrowych i urządzeniach wyposażonych w zamki szyfrowe;
2) po każdej zmianie lub konserwacji zamka szyfrowego;
3) po każdej zmianie użytkownika urządzenia wyposażonego w zamek szyfrowy;
4) w przypadku ujawnienia kodu osobie nieupoważnionej.

§ 20.

1. Wykonawca otwierający pomieszczenie służbowe, szafę metalową w razie stwierdzenia uszkodzenia lub niezgodności plomby z treścią pieczęci, o której mowa w § 18 ust. 2, zawiadamia, za pośrednictwem bezpośredniego przełożonego, pełnomocnika ochrony, który podejmuje czynności wyjaśniające.

2. W przypadku utraty kluczy do szaf metalowych oraz pomieszczeń służących ochronie informacji niejawnych wykonawca zawiadamia, za pośrednictwem bezpośredniego przełożonego, pełnomocnika ochrony, który przeprowadza czynności wyjaśniające i określa sposób zabezpieczenia zgromadzonych w tych szafach lub pomieszczeniach materiałów.

§ 21.

1. Zabrania się wnoszenia do strefy ochronnej I lub strefy ochronnej II prywatnych urządzeń służących do przetwarzania obrazu i dźwięku.

2. W uzasadnionych przypadkach, za zgodą pełnomocnika ochrony dopuszcza się wnoszenie do strefy ochronnej I lub strefy ochronnej II urządzeń, o których mowa w ust. 1.

3. Procedurę uzyskiwania zgody, o której mowa w ust. 2, oraz zasady wnoszenia prywatnych urządzeń służących do przetwarzania obrazu i dźwięku do strefy ochronnej III określa plan ochrony.

§ 22.

Procedurę związaną z wnoszeniem i wynoszeniem ze stref ochronnych służbowych urządzeń służących do rejestracji obrazu, dźwięku, kopiowania oraz transmisji informacji określa plan ochrony.

§ 23.

Pomieszczenia służbowe, w których za zgodą pełnomocnika ochrony przechowywane są materiały i ewidencje niejawne oraz pieczęcie, zlokalizowane w obiektach SWW lub na terenie innych instytucji, niechronione całodobowo przez wewnętrzną służbę ochrony lub służbę dyżurną, należy zabezpieczyć dodatkowo systemami sygnalizacji włamania oraz systemem sygnalizacji pożarowej z zastrzeżeniem, iż muszą one w przypadkach zagrożenia zapewnić powiadomienie o alarmie osób wyznaczonych przez pełnomocnika ochrony.

§ 24.

1. Sprzątanie pomieszczeń kancelarii tajnych i innych pomieszczeń służących do przetwarzania informacji niejawnych, może odbywać się wyłącznie w obecności funkcjonariusza odpowiadającego za to pomieszczenie.

2. Na czas sprzątania funkcjonariusz, o którym mowa w ust. 1, zabezpiecza materiały niejawne w sposób uniemożliwiający przypadkowe ujawnienie ich treści osobom nieuprawnionym.

§ 25.

1. W terminie 2 lat od dnia wejścia w życie zarządzenia dostosowuje się kombinację środków bezpieczeństwa fizycznego oraz organizację stref ochronnych do wymagań określonych w zarządzeniu.

2. Certyfikaty, tabliczki znamionowe oraz poświadczenia, o których mowa w § 12 ust. 6, przyznane wyposażeniu i urządzeniom służącym ochronie informacji niejawnych, wydane przed dniem wejścia w życie zarządzenia, zachowują ważność.

Rozdział 4
Zasady rejestrowania, obiegu, kompletowania i niszczenia materiałów niejawnych

§ 26.

1. GKT prowadzi następujące urządzenia ewidencyjne:
1) rejestr dzienników ewidencji i teczek;
2) dziennik ewidencyjny – dla dokumentów oznaczonych wszystkimi klauzulami tajności;
3) książkę doręczeń przesyłek miejscowych;
4) wykaz przesyłek nadanych;
5) rejestr wydanych przedmiotów służący do ewidencjonowania wydanych nośników informacji oraz innych przedmiotów

– których wzory określają przepisy wydane na podstawie art. 47 ust. 1 pkt 11 ustawy.

2. GKT prowadzi również następujące urządzenia ewidencyjne:
1) dziennik podawczy, którego wzór określa załącznik nr 4 – dla przesyłek oznaczonych wszystkimi klauzulami tajności;
2) książkę ewidencji pieczęci i stempli, której wzór określają przepisy w sprawie pieczęci i stempli oraz tablic urzędowych i informacyjnych używanych w SWW.

3.Oddziały kancelarii tajnych mogą prowadzić następujące urządzenia ewidencyjne:
1) dziennik ewidencyjny – dla dokumentów oznaczonych wszystkimi klauzulami tajności;
2) książkę doręczeń przesyłek miejscowych;
3) wykaz przesyłek nadanych;
4) rejestr wydanych przedmiotów służący do ewidencjonowania wydanych nośników informacji oraz innych przedmiotów;
5) dziennik podawczy.

4. Stacja kryptograficzna prowadzi dziennik ewidencji i doręczeń szyfrogramów, którego wzór określa załącznik nr 5, dziennik ewidencji i doręczeń szyfrofaksów, którego wzór określa załącznik nr 6, oraz rejestr wydanych przedmiotów służący do ewidencjonowania wydanych nośników informacji oraz innych przedmiotów.

5. Biuro Prawne prowadzi rejestr przepisów wydanych przez Szefa SWW, którego wzór określa załącznik nr 7.

6. Biuro Kadr prowadzi rejestr rozkazów wydanych przez Szefa SWW lub przez dyrektora Biura Kadr z upoważnienia Szefa SWW, którego wzór określa załącznik nr 8.

7. Jednostki organizacyjne SWW mogą prowadzić rejestr przepisów wydanych przez kierownika jednostki, którego wzór określa załącznik nr 7.

§ 27.

1. Punkty kontroli, o których mowa w § 2 pkt 5 lit. a i b, w celu rejestrowania obiegu dokumentów niejawnych prowadzą dziennik podawczy do przesyłek oznaczonych wszystkimi klauzulami tajności.

2. Punkty kontroli, o których mowa w § 2 pkt 5 lit. c i d, w celu dokumentowania obiegu przesyłek prowadzą:
1) dziennik ewidencyjny – dla dokumentów oznaczonych wszystkimi klauzulami tajności;
2) książkę doręczeń przesyłek miejscowych.
3) rejestr wydanych przedmiotów służący do ewidencjonowania wydanych nośników informacji oraz innych przedmiotów;

3. Punkty kontroli, w przypadku gdy są jedynymi punktami kontroli w jednostce organizacyjnej SWW, prowadzą:
1) dziennik ewidencyjny – dla dokumentów oznaczonych wszystkimi klauzulami tajności;
2) książkę doręczeń przesyłek miejscowych;
3) rejestr wydanych przedmiotów służący do ewidencjonowania wydanych nośników informacji oraz innych przedmiotów

dla wszystkich komórek organizacyjnych i nie muszą prowadzić dzienników podawczych.

§ 28.

1. Na wniosek kierownika jednostki organizacyjnej SWW, za zgodą pełnomocnika ochrony, oddziały kancelarii lub punkty kontroli mogą prowadzić w poszczególnych komórkach organizacyjnych jednostki organizacyjnej SWW dodatkowe:
1) dzienniki podawcze;
2) dzienniki ewidencyjne;
3) rejestry wydanych przedmiotów;
4) inne ewidencje.

2. Wniosek, o którym mowa w ust. 1, sporządza się na piśmie w egzemplarzu pojedynczym wraz z uzasadnieniem. Wniosek przechowywany jest w GKT.

3. W przypadku ćwiczeń, organizowanych przez kierownika jednostki organizacyjnej SWW, z wykorzystaniem ćwiczebnych materiałów, za zgodą pełnomocnika ochrony mogą zostać

wydane na czas ćwiczeń odrębne ewidencje niezbędne do prowadzenia ćwiczeń na zasadach określonych przez kierownika jednostki organizacyjnej SWW.

4. Po zakończeniu ćwiczeń ewidencje i materiały mogą zostać zniszczone przez organizatora ćwiczeń we własnym zakresie.

5. W przypadku ćwiczeń z wykorzystaniem ćwiczebnych materiałów, organizowanych przez Centrum Kształcenia, zgoda pełnomocnika ochrony, o której mowa w ust. 3, nie jest wymagana.

§ 29.

1. W celu rejestrowania przesyłek wpływających po godzinach pracy kancelarii tajnych, funkcjonariusz pełniący obowiązki oficera dyżurnego może prowadzić dziennik podawczy.

2. W celu rejestrowania przesyłek wpływających do Operacyjnego Centrum Monitoringu, po godzinach służby GKT, funkcjonariusz pełniący służbę oficera operacyjnego może prowadzić dziennik podawczy.

3. Oficer dyżurny i oficer operacyjny, przyjmują przesyłki, każdy według swojej właściwości.

§ 30.

1. W rejestrze dzienników ewidencji i teczek GKT rejestruje wszystkie urządzenia ewidencyjne dla potrzeb kancelarii tajnych oraz punktów kontroli.

2. Numer ewidencyjny dokumentu zarejestrowanego w rejestrze dzienników ewidencji i teczek składa się z sygnatury GKT, symbolu klauzuli tajności, pozycji zapisu w rejestrze dzienników ewidencji i teczek, łamanej przez rok kalendarzowy, w którym dokument zarejestrowano.

3. Wszystkie urządzenia ewidencyjne, o których mowa w § 26 i § 27 funkcjonariusze odpowiedzialni za ich prowadzenie, oznaczają odpowiednią klauzulą tajności, opisują, przeszywają, ich strony numerują, a następnie opieczętowują w GKT.

4. Wszystkie urządzenia ewidencyjne, o których mowa w § 26 – 28, jak również inne urządzenia ewidencyjne znajdujące się w dyspozycji funkcjonariuszy, powinny być prowadzone w sposób dający pełną i dokładną informację o każdym zarejestrowanym w nich dokumencie od momentu rejestracji, poprzez udostępnianie, odesłanie do wskazanego adresata, zniszczenie lub przerejestrowanie do innej ewidencji, aż do ostatecznego zdjęcia z obciążenia ewidencyjnego rejestru tego dokumentu, a następnie złożenia rejestru do archiwum lub zniszczenia zgodnie z jednolitym rzeczowym wykazem akt SWW.

5. Urządzenia ewidencyjne wydane przez GKT mogą zostać, po ich zakończeniu, złożone do archiwum lub wybrakowane. O powyższym należy poinformować niezwłocznie kierownika GKT celem zdjęcia ich z ewidencji.

§ 31.

1. W dzienniku ewidencyjnym rejestruje się dokumenty otrzymywane i wysyłane oraz wytworzone na potrzeby wewnętrzne jednostki organizacyjnej SWW lub komórki organizacyjnej, jak również załączniki odłączone od pism przewodnich.

2. Dopuszcza się rejestrowanie w jednym dzienniku ewidencyjnym dokumentów otrzymywanych i wysyłanych.

3. Dziennik ewidencyjny prowadzi się do całkowitego wykorzystania wszystkich kart. Po wykorzystaniu wszystkich stron dziennika ewidencyjnego, zakłada się następny tom i zachowuje ciągłość dotychczasowej numeracji.

§ 32.

1. W wykazie przesyłek nadanych wpisuje się przesyłki pocztowe przekazywane przewoźnikowi lub adresatowi, jeżeli są dostarczane bezpośrednio przez przedstawiciela nadawcy albo adresata.

2. Wykazów przesyłek nadanych nie ewidencjonuje się w żadnym urządzeniu ewidencyjnym. Wykazom nadaje się kolejne numery, zaczynając numerowanie w każdym roku kalendarzowym od cyfry „1".

3. Przewoźnik potwierdza przyjęcie przesyłek do przekazania na dwóch egzemplarzach wykazu, o którym mowa w ust. 1, zapisem liczbowym i słownym o ilości przyjętych przesyłek oraz uwierzytelnia podpisem i odciskiem pieczęci „Do pakietów", przy czym jeden egzemplarz wykazu pozostaje w kancelarii tajnej nadawcy, a drugi jest przeznaczony dla przewoźnika.

4. W przypadku przekazania przez kancelarię tajną materiałów niejawnych bezpośrednio upoważnionemu przedstawicielowi adresata, potwierdza on odbiór przesyłki podpisem i odciskiem pieczęci „Do pakietów" na drugim egzemplarzu wykazu przesyłek nadanych, przeznaczonym dla kancelarii tajnej nadawcy.

5. Jeżeli przesyłki są doręczane adresatowi przez upoważnionego przedstawiciela nadawcy, kierownik kancelarii tajnej sporządza wykaz przesyłek nadanych w trzech egzemplarzach, z których:

1) pierwszy egzemplarz, po pokwitowaniu przyjęcia przesyłki przez kierownika kancelarii tajnej adresata, osoba doręczająca zwraca do kancelarii tajnej nadawcy;
2) drugi egzemplarz, osoba doręczająca przekazuje wraz z przesyłką kierownikowi kancelarii tajnej adresata;
3) trzeci egzemplarz, zawierający pokwitowanie odbioru przesyłki przez osobę doręczającą, przechowuje się w kancelarii tajnej nadawcy i niszczy bezpośrednio po otrzymaniu egzemplarza, o którym mowa w pkt 1.

6. Kancelaria tajna potwierdza przyjęcie przesyłek od przewoźnika na dwóch egzemplarzach wykazu przesyłek wydanych, przy czym jeden egzemplarz wykazu pozostaje u przewoźnika, a drugi jest przeznaczony dla kancelarii tajnej.

7. Kancelaria tajna przechowuje wykazy, o których mowa w ust. 1 i 6, przez okres dwóch lat.

§ 33.

1. W książce doręczeń przesyłek miejscowych rejestruje się fakt doręczenia materiałów do kancelarii tajnej adresata, w tym samym kompleksie, bezpośrednio przez personel kancelarii tajnej nadawcy.

2. Kierownik kancelarii tajnej adresata potwierdza odbiór materiałów podpisem w odpowiedniej rubryce książki doręczeń oraz uwierzytelnionym odciskiem pieczęci „Do pakietów" lub „Do pokwitowań".

§ 34.

1. Udostępnienie dokumentu niejawnego może nastąpić tylko na pisemne, umieszczone na tym dokumencie polecenie kierownika jednostki organizacyjnej SWW, jego zastępcy lub bezpośredniego przełożonego funkcjonariusza, na którego stanie ewidencyjnym dany dokument się znajduje.

2. Fakt zapoznania się z dokumentem niejawnym potwierdza się, czytelnym podpisem i datą, na tym dokumencie albo w karcie zapoznania się z dokumentem, której wzór określają przepisy wydane na podstawie art. 47 ust. 1 pkt 10 ustawy.

3. Kart zapoznania się z dokumentem nie zakłada się dla urządzeń ewidencyjnych, notatników oraz brudnopisów dokumentów, o których mowa w ust. 1.

4. Kartę zapoznania się z dokumentem przesyła się, archiwizuje lub brakuje wraz z dokumentem, którego dotyczy.

5. Zapoznanie się z materiałami zgromadzonymi w Archiwum SWW, dokumentacją kartoteczną i ewidencyjną oraz dokumentami niejawnymi w:
1) procedurach operacyjnych;
2) aktach osobowych;
3) aktach postępowania sprawdzającego;
4) trwale oprawionych książkach, broszurach, reprodukcjach lub innych zbiorach dokumentów
– odnotowuje się na karcie zapoznania z teczką, której wzór określa załącznik nr 9.

§ 35.

1. Do elektronicznych nośników informacji zawierających dane niejawne przekazywanych poza SWW dołącza się metrykę elektronicznego nośnika informacji, której wzór określa załącznik nr 10.

2. W metryce umieszcza się dane dotyczące informacji niejawnych zapisanych na nośniku.

3. Funkcjonariusz, na którego stanie pozostaje nośnik, zakłada i rejestruje metrykę w kancelarii tajnej lub punkcie kontroli, w którym zarejestrowano nośnik w rejestrze wydanych przedmiotów.

4. Metryki nie zakłada się dla nośników przeznaczonych do użytku bieżącego wykonawców oraz w przypadku ich przekazywania służbie partnerskiej obcego państwa.

§ 36.

1. Kancelaria tajna oraz punkty kontroli przekazują materiały zawierające informacje niejawne oznaczone klauzulą „Poufne" lub wyższą wyłącznie wykonawcom posiadającym stosowne poświadczenia bezpieczeństwa albo pisemną zgodę osoby wymienionej w art. 34 ust. 5 i 9 ustawy, których pomieszczenia są zlokalizowane w strefie ochronnej I i strefie ochronnej II oraz wyposażone są w urządzenia do przechowywania dokumentów, o których mowa w § 13 ust. 1 pkt 1 albo ust. 2, za pokwitowaniem w dzienniku ewidencyjnym lub innym urządzeniu ewidencyjnym, z zastrzeżeniem ust. 4.

2. Kancelaria tajna lub punkt kontroli udostępniają lub przekazują materiały niejawne osobom, o których mowa w ust. 1, na podstawie zamieszczonej na materiale dekretacji kierownika jednostki organizacyjnej SWW, kierownika komórki organizacyjnej albo osoby upoważnionej przez kierownika jednostki organizacyjnej SWW do dekretowania dokumentów.

3. Urządzenia do przechowywania materiałów, o których mowa w § 13 ust. 1 pkt 1 oraz ust. 2, mogą być wykorzystywane wyłącznie przez jednego wykonawcę, chyba że konstrukcja urządzenia pozwala na fizyczne oddzielenie posiadanych przez wykonawców materiałów oraz zamknięcie ich w odrębnych skrytkach lub zostaną spełnione wymogi, o których mowa w § 16.

4. Zezwala się na udostępnienie materiałów niejawnych oznaczonych klauzulą „Poufne" lub „Tajne" wykonawcom nieposiadającym urządzeń, o których mowa w § 13 ust. 1 pkt 1 oraz ust. 2, jeżeli spełniają oni pozostałe warunki określone w ust. 1.

5. Wykonawca, któremu udostępniono materiały niejawne na zasadach określonych w ust. 4, ma obowiązek zachowania środków bezpieczeństwa uniemożliwiających dostęp do tych materiałów przez osoby nieuprawnione oraz zwrócić je do kancelarii tajnej przed zakończeniem dnia pracy.

6. Wykonawcom, których pomieszczenia służbowe znajdują się w strefie ochronnej III, materiały niejawne oznaczone klauzulą „Poufne" lub wyższą udostępnia się w kancelarii tajnej.

§ 37.

Dokumenty ostatecznie załatwionych spraw, zawierające informacje niejawne, otrzymane i wytworzone w jednostce organizacyjnej SWW podlegają:

1) skompletowaniu w teczki akt i przekazaniu do Archiwum SWW zgodnie z odrębnymi przepisami;
2) zwrotowi do nadawcy, jeżeli określił on taki sposób postępowania z przesłanymi materiałami;
3) brakowaniu, a następnie niszczeniu na zasadach określonych w odrębnych przepisach.

§ 38.

1. Fakt zniszczenia dokumentu potwierdza się w protokole zniszczenia, który zawiera w szczególności:
1) datę i miejsce zniszczenia dokumentów;
2) numer zezwolenia na zniszczenie dokumentów;
3) imienny skład komisji niszczącej dokumenty;
4) wykaz zniszczonych dokumentów.

2. Protokół, o którym mowa w ust. 1, stanowi dla kierownika kancelarii tajnej lub funkcjonariusza punktu kontroli podstawę do zdjęcia z ewidencji wyszczególnionych w nim dokumentów, poprzez naniesienie w odpowiednim urządzeniu ewidencyjnym adnotacji o treści: „Protokół zniszczenia nr ... z dnia ..., poz. nr ...", oraz uwierzytelnienie wpisu wpisaniem daty i podpisem.

3. Protokół, o którym mowa w ust. 1, jest przechowywany w kancelarii tajnej lub w punkcie kontroli jednostki organizacyjnej SWW albo komórki organizacyjnej.

4. Dokument uważa się za ostatecznie zniszczony, jeżeli został pocięty na paski o wymiarach maksymalnych 1,5 x 25 mm lub odpowiadającej im powierzchni o innych wymiarach, albo zmielony na miał papierowy.

5. Procedury niszczenia elektronicznych nośników informacji oraz informacji utrwalonych na tych nośnikach określają odrębne przepisy.

6. Zabrania się wywożenia częściowo zniszczonych dokumentów niejawnych oraz kopert i innych opakowań, w których otrzymano dokumenty niejawne, na wysypiska śmieci.

§ 39.

1. Do zadań funkcjonariusza pełniącego służbę w GKT należy:
1) przyjmowanie i przekazywanie przesyłek do kancelarii tajnej, punktów kontroli, kancelarii tajnych innych podmiotów, a także Centrum Wsparcia Teleinformatycznego Sił Zbrojnych;
2) sprawdzanie poprawności zapakowania i oznaczenia koperty zewnętrznej i wewnętrznej przesyłki; w przypadku stwierdzenia naruszenia zabezpieczeń przesyłki – powiadomienie kancelarii tajnej nadawcy i podjęcie czynności wyjaśniających;
3) pakowanie w koperty zewnętrzne przesyłek nadawanych poza strefę bezpieczeństwa, otwieranie kopert zewnętrznych przesyłek wpływających;
4) rejestrowanie przesyłek;
5) rejestrowanie prowadzonych ewidencji w rejestrze dzienników ewidencji i teczek oraz ich wydawanie kancelarii tajnej, punktom kontroli i innym użytkownikom.

2. Do zadań funkcjonariusza pełniącego służbę w oddziale kancelarii należy przyjmowanie i przekazywanie przesyłek do GKT i obsługiwanych punktów kontroli, a także wykonywanie czynności, o których mowa w ust. 1 pkt 2 – 4.

3. W kancelariach tajnych nie otwiera się kopert wewnętrznych, chyba że przesyłka została zadekretowana na kierownika kancelarii tajnej, kopertę taką może otworzyć kierownik kancelarii tajnej.

§ 40.

1. W kancelarii tajnej każdą przesyłkę rejestruje się pod kolejną pozycją w dzienniku podawczym poprzedzając ją cyfrowym lub literowym oznaczeniem klauzuli tajności, a następnie oznacza się pieczęcią wpływu, w obrębie której wpisuje się datę wpływu oraz numer pozycji z dziennika podawczego. W przypadku przesyłania w jednej kopercie więcej niż jednej pozycji dziennika ewidencyjnego, przesyłce nadaje się jeden numer dziennika podawczego z wyszczególnieniem w dzienniku podawczym wszystkich numerów znajdujących się na opakowaniu przesyłki.

2. W kancelariach tajnych wydaje się, zgodnie z właściwościami, przesyłki kancelariom tajnym i punktom kontroli adresatów, za pokwitowaniem w dzienniku podawczym.

§ 41.

1. Funkcjonariusz pełniący służbę w stacji kryptograficznej rejestruje wysyłane i przyjmowane szyfrogramy w dzienniku ewidencji i doręczeń szyfrogramów.

2. Stacja kryptograficzna przekazuje do punktu kontroli albo KTM, zgodnie z właściwością, szyfrogramy przychodzące za pokwitowaniem w dzienniku ewidencji i doręczeń szyfrogramów.

3. Punkty kontroli albo KTM przekazują szyfrogramy wychodzące do stacji kryptograficznej, za pokwitowaniem w książce doręczeń przesyłek miejscowych.

4. Szyfrogramy wychodzące, po wysłaniu, stacja kryptograficzna przekazuje do punktu kontroli albo KTM nadawcy, za pokwitowaniem w dzienniku ewidencji i doręczeń szyfrogramów.

5. W przypadkach uzasadnionych potrzebami służby, stacja kryptograficzna może przekazać otrzymany szyfrogram bezpośrednio adresatowi, z pominięciem właściwego punktu kontroli, za pokwitowaniem w dzienniku ewidencji i doręczeń szyfrogramów.

6. W przypadku przekazania szyfrogramu w trybie, o którym mowa w ust. 5, nie później, niż na koniec danego miesiąca, stacja kryptograficzna przekazuje właściwemu punktowi kontroli pisemną informację na temat szyfrogramów przekazanych w tym trybie, z podaniem informacji o nadawcy szyfrogramu, numerze z dziennika ewidencji i doręczeń szyfrogramów oraz numerze ewidencyjnym szyfrogramu nadanym przez nadawcę.

7. Ustępy 1 – 6 stosuje się do szyfrofaksów, z tym że w miejsce dziennika ewidencji i doręczeń szyfrogramów wykorzystuje się dziennik ewidencji i doręczeń szyfrofaksów.

8. Szczegółowy obieg szyfrogramów i szyfrofaksów w SWW mogą określać odrębne przepisy.

§ 42.

1. Do zadań funkcjonariusza pełniącego służbę w punkcie kontroli należy:
1) przyjmowanie i przekazywanie przesyłek do kancelarii tajnej i punktów kontroli w ramach jednostki organizacyjnej SWW;
2) rejestrowanie przesyłek;
3) wydawanie przesyłek do dekretacji;
4) przekazywanie przesyłek od funkcjonariusza dokonującego dekretacji do adresata.

2. W punkcie kontroli można przechowywać przesyłki, do czasu ich wydania adresatowi określonemu w dekretacji.

3. W punkcie kontroli nie otwiera się kopert wewnętrznych, chyba że przesyłka została zadekretowana na funkcjonariusza punktu kontroli.

4. Przekazywanie materiałów niejawnych do kancelarii tajnej i między punktami kontroli w ramach jednostki organizacyjnej SWW, odbywa się za pokwitowaniem w książce doręczeń przesyłek miejscowych lub za wykazem przesyłek nadanych.

5. Przekazywanie zakopertowanych przesyłek, między punktami kontroli w ramach jednostki organizacyjnej SWW, może odbywać się z wyłączeniem kancelarii tajnej, za pokwitowaniem w książce doręczeń przesyłek miejscowych lub za wykazem przesyłek nadanych.

§ 43.

1. Funkcjonariusz pełniący służbę w punkcie kontroli, o którym mowa w § 2 pkt 5 lit. a i b, otrzymane z kancelarii tajnej przesyłki:
1) rejestruje pod kolejną pozycją w dzienniku podawczym, poprzedzając ją cyfrowym lub literowym oznaczeniem klauzuli tajności, a następnie oznacza na kopercie przesyłki, pieczęcią wpływu, w obrębie której wpisuje datę wpływu oraz numer pozycji z dziennika podawczego;
2) przekazuje przesyłkę właściwemu przełożonemu do dekretacji;
3) po zadekretowaniu przesyłki przekazuje ją, za pokwitowaniem zgodnie z naniesioną dekretacją.

2. Właściwy przełożony, po zadekretowaniu a następnie zaklejeniu lub przeszyciu przesyłki zwraca ją do punktu kontroli.

3. Funkcjonariusz, o którym mowa w ust. 1, jest obowiązany raz w tygodniu sprawdzić stan faktyczny przesyłek przekazanych do dekretacji Szefowi SWW lub jego zastępcom, kierownikowi jednostki organizacyjnej SWW lub jego zastępcom.

4. Każde dalsze przekazywanie przesyłki odbywa się wyłącznie za pośrednictwem punktu kontroli.

§ 44.

1. Funkcjonariusz pełniący służbę w punkcie kontroli, jeżeli został mu wydany dziennik ewidencyjny wychodzące przesyłki:
1) w obecności nadawcy, rejestruje pod kolejną pozycją we właściwym dzienniku ewidencyjnym, poprzedzając ją oznaczeniem klauzuli tajności i kopertuje;
2) na kopercie umieszcza:
   a) numer ewidencyjny, klauzulę tajności i ewentualne dodatkowe oznaczenia,
   b) określenie adresata,
   c) imię, nazwisko i podpis osoby kopertującej lub numer identyfikacyjny osoby kopertującej i jej podpis;
3) przekazuje za pokwitowaniem w książce doręczeń przesyłek miejscowych lub za wykazem przesyłek nadanych do kancelarii tajnej wraz z przygotowaną i otwartą kopertą zewnętrzną, z zastrzeżeniem § 42 ust. 5.

2. W obrębie jednego obiektu SWW dopuszczalne jest przesyłanie materiałów w pojedynczej kopercie.

3. W jednej kopercie wewnętrznej może znajdować się materiał zarejestrowany wyłącznie pod jedną pozycją dziennika ewidencji, z zastrzeżeniem ust. 5.

4. W kopercie zewnętrznej może znajdować się tylko jedna przesyłka zapakowana w kopertę wewnętrzną.

5. W uzasadnionych przypadkach, po uzgodnieniu z odbiorcą, dopuszcza się~~,~~ przesyłanie w jednej kopercie wewnętrznej większej ilości materiałów oznaczonych taką samą klauzulą, zarejestrowanych pod więcej niż jedną pozycją dziennika ewidencyjnego.

6. W przypadkach, o których mowa w ust. 5, na kopercie wewnętrznej umieszcza się wszystkie numery materiałów, pod którymi zostały one zarejestrowane w dzienniku ewidencyjnym.

§ 45.

1. Funkcjonariusz pełniący służbę w punkcie kontroli, jeżeli został mu wydany dziennik ewidencyjny, wpływające przesyłki:
1) rejestruje pod kolejną pozycją właściwego dziennika ewidencyjnego;
2) oznacza na kopercie przesyłki, pieczęcią wpływu, w obrębie której wpisuje datę oraz numer pozycji dziennika ewidencyjnego;
3) przekazuje do dekretacji.

2. Właściwy przełożony, po zadekretowaniu przesyłki zwraca ją do punktu kontroli po zaklejeniu lub przeszyciu.

3. Funkcjonariusz, o którym mowa w ust. 1, jest obowiązany ca najmniej raz w tygodniu sprawdzić stan faktyczny przesyłek przekazanych do dekretacji.

4. Funkcjonariusz pełniący służbę w punkcie kontroli:
1) wydaje przesyłki ostatnim adresatom, za pokwitowaniem w dzienniku ewidencyjnym;
2) dokonuje, przy udziale ostatniego adresata, pełnej rejestracji dokumentu zawartego w przesyłce w dzienniku ewidencyjnym.

5. Ostatni adresat na pierwszej stronie dokumentu odciska pieczęć wpływu, w obrębie której wpisuje:
1) datę wpływu;
2) numer dziennika ewidencyjnego;
3) liczbę załączników i liczbę stron załączników lub innych jednostek miary załączników.

§ 46.

1. Dekretujący i ostatni adresat obowiązani są sprawdzić:
1) prawidłowość adresu;
2) zgodność numeru ewidencyjnego przesyłki z numerem ewidencyjnym umieszczonym na kopercie;
3) zgodność liczby załączników i ich stron z liczbą podaną w dokumencie;
4) prawidłowość oznaczenia załączników.

2. W przypadku stwierdzenia w przesyłce braku dokumentów, załączników lub rozbieżności w numerach ewidencyjnych i oznaczeniach klauzulami tajności, dekretujący lub ostatni adresat wykonuje następujące czynności:
1) sporządza w dwóch egzemplarzach protokół z otwarcia przesyłki, z przeznaczeniem dla kancelarii tajnej adresata oraz nadawcy i przekazuje oba egzemplarze protokołu upoważnionemu funkcjonariuszowi pionu ochrony;
2) dokonuje zapisu o sporządzeniu protokołu we właściwym dzienniku ewidencyjnym, w rubryce „Informacje uzupełniające/uwagi”.

3. Upoważniony funkcjonariusz pionu ochrony:
1) przekazuje odpowiednio po jednym egzemplarzu protokołu do kancelarii tajnej adresata oraz nadawcy;
2) wyjaśnia sprawę z nadawcą przesyłki i sporządza notatkę służbową w tej sprawie;
3) powiadamia adresata i nadawcę o wynikach ustaleń, o których mowa w pkt 2.

§ 47.

1. Do ewidencjonowania korespondencji ze służbami partnerskimi, o ile zachodzi taka potrzeba, stosuje się odrębny dziennik ewidencyjny do materiałów oznaczonych wszystkimi klauzulami.

2. Dziennik, o którym mowa w ust. 1, prowadzony jest w punkcie kontroli komórki organizacyjnej, upoważnionej do koordynacji współpracy ze służbami partnerskimi.

3. Funkcjonariusz pełniący służbę w komórce organizacyjnej, o której mowa w ust. 2, lub inny upoważniony funkcjonariusz odbierający przesyłkę od przedstawiciela służby partnerskiej zobowiązany jest zarejestrować ją w kancelarii tajnej, a następnie w punkcie kontroli.

4. Przekazanie przesyłki przedstawicielowi służby partnerskiej przez funkcjonariusza pełniącego służbę w komórce organizacyjnej, o której mowa w ust. 2, może odbywać się z wyłączeniem kancelarii tajnej, za pokwitowaniem na egzemplarzu przesyłki pozostającym w jednostce organizacyjnej SWW lub w książce doręczeń przesyłek miejscowych albo przekazanie takie dokumentuje się notatką.

5. W przypadku przesyłek przekazywanych służbie partnerskiej, egzemplarz przeznaczony dla służby partnerskiej może zostać sporządzony zgodnie z przepisami właściwymi dla odbiorcy przesyłki, jak też może nie zawierać danych osoby podpisującej dokument i jej podpisu.

§ 48.

1. Mikrofilmy, negatywy, kalki, zeszyty, bruliony, elektroniczne nośniki informacji oraz inne materiały i przedmioty, zawierające informacje niejawne lub przeznaczone do zapisu informacji niejawnych, rejestruje się w rejestrze wydanych przedmiotów trwale nanosząc na nie numery z rejestru i klauzule tajności, a następnie wydaje uprawnionym osobom za pokwitowaniem w tym rejestrze.

2. Dopuszcza się przesyłanie informacji niejawnych w postaci nośników, o których mowa w ust. 1, jako załącznik do pisma przewodniego, w którym nadawca określa dyspozycję dotyczącą ewentualnego zwrotu nośnika.

3. Fizyczne niszczenie nośników, o których mowa w ust. 1, odbywa się na podstawie odrębnych przepisów.

4. Na materiałach, o których mowa w ust. 1, numer z rejestru wydanych przedmiotów powinien składać się z sygnatury literowo-cyfrowej złożonej z literowego oznaczenia jednostki organizacyjnej SWW lub komórki organizacyjnej, oznaczenia klauzuli tajności oraz numeru, pod którym materiał został zarejestrowany w rejestrze łamanym przez rok, w którym materiał został zarejestrowany, po których należy wpisać numer pozycji z rejestru dzienników i książek ewidencyjnych, pod którym dany rejestr wydanych przedmiotów został zarejestrowany; numer powinien być poprzedzony skrótem „RWP:”.

§ 49.

1. Odciski pieczęci tuszowych nanosi się kolorem innym niż czarny i czerwony.

2. Zapisów w ewidencjach dokonuje się atramentem (tuszem) czarnym lub niebieskim, a zmiany tych zapisów atramentem (tuszem) czerwonym z podaniem daty i czytelnym podpisem dokonującego zmiany. Dopuszcza się dokonywanie zapisów przy pomocy odcisków pieczęci oraz nanoszenie adnotacji o przekazaniu dokumentu do archiwum lub jego wybrakowaniu wyróżniającym kolorem, z wyjątkiem koloru czerwonego.

3. Anulowania zapisów w ewidencjach dokonuje się kolorem czerwonym, podając powód anulowania oraz umieszczając datę i czytelny podpis osoby dokonującej anulacji.

4. Wycieranie i zamazywanie zapisów w ewidencjach oraz na materiałach jest zabronione.

5. Zapisów w ewidencjach dokonuje się zgodnie z treścią poszczególnych rubryk. Stosowanie klamer i znaków powtórzeń jest zabronione.

6. Po dokonaniu wpisu po ostatniej pozycji w ewidencji zarejestrowanej w rejestrze, o którym mowa w § 26 ust. 1 pkt 1, należy:
1) na stronie tytułowej tej ewidencji wpisać datę i numer pozycji, na której daną ewidencję zakończono;
2) ostatni wpis podkreślić i dokonać adnotacji o treści „Dziennik (Książkę) zakończono pozycją nr … w dniu …", którą akceptuje właściwy przełożony składając podpis i odciskając imienną pieczęć;
3) potwierdzić zakończenie prowadzenia ewidencji poprzez umieszczenie przez kierownika GKT, pod adnotacją, o której mowa w pkt 2, podpisu i daty; fakt zakończenia prowadzenia ewidencji należy odnotować w rejestrze dzienników ewidencji i teczek.

7. Z końcem każdego roku kalendarzowego, ewidencje prowadzone w jednostce organizacyjnej SWW, należy zakończyć na zasadach określonych w ust. 6, z wyłączeniem ewidencji, o których mowa w § 26 ust. 1 pkt 1 i 5, ust. 2 pkt 2 oraz ust. 5 – 7.

8. W kolejnym dzienniku (książce) z danego roku kalendarzowego, wpisów w kolejnych pozycjach dokonuje się uwzględniając kontynuację numeracji z poprzedniego dziennika (książki), z wyłączeniem rejestru wydanych przedmiotów, w którym numeracja rozpoczyna się od pozycji nr 1.

9. W przypadku prowadzenia równolegle więcej niż jednego dziennika ewidencyjnego w kancelarii tajnej lub punkcie kontroli, na pismach po sygnaturze literowo-cyfrowej składającej się z literowego oznaczenia jednostki organizacyjnej SWW lub komórki organizacyjnej, oznaczenia klauzuli tajności oraz numeru, pod którym pismo zostało zarejestrowane w dzienniku ewidencyjnym łamanym przez rok, w którym pismo zostało sporządzone należy wpisać numer pozycji z rejestru dzienników ewidencji i teczek, pod którym dany dziennik ewidencyjny został zarejestrowany lub inny wyróżnik pozwalający na identyfikację dziennika ewidencyjnego, po uzyskaniu na to zgody pełnomocnika ochrony.

10. Z końcem każdego roku kalendarzowego ewidencje, o których mowa w § 26 ust. 1 pkt 1 i 5, ust. 2 pkt 2 oraz ust. 5 – 7 po dokonaniu ostatniego wpisu w danym roku należy:
1) ostatni wpis podkreślić i dokonać adnotacji o treści „Zakończono pozycją nr … w dniu …", którą akceptuje właściwy przełożony składając podpis i odciskając imienną pieczęć;

2) potwierdzić fakt zakończenia prowadzenia ewidencji w danym roku kalendarzowym poprzez umieszczenie przez funkcjonariusza pełniącego służbę w GKT, pod adnotacją, o której mowa w pkt 1, podpisu i daty.

11. W następnym roku kalendarzowym zapisy w ewidencjach, o których mowa w ust. 10, rozpoczyna się od pozycji nr 1.

§ 50.

1. Przesyłki wpływające do SWW po godzinach służby kancelarii tajnej przyjmują, potwierdzając ich odbiór, funkcjonariusze, o których mowa w § 29.

2. Funkcjonariusze, o których mowa w ust. 1, za pokwitowaniem w dzienniku podawczym, przekazują przesyłkę adresatowi, który jest zobowiązany zarejestrować ją niezwłocznie w GKT.

3. W przypadku nieobecności adresata funkcjonariusze, o których mowa w ust. 1, przekazują, za pokwitowaniem w dzienniku podawczym, przesyłkę GKT w najbliższym możliwym terminie.

4. O przesyłkach pilnych, wpływających do SWW po godzinach służby kancelarii tajnej, funkcjonariusze, o których mowa w ust. 1, informują niezwłocznie adresata, który decyduje o dalszym toku postępowania.

5. Kierownik jednostki, w której pełnią służbę funkcjonariusze, o których mowa w ust. 1, może pisemnie upoważnić tych funkcjonariuszy do otwierania pilnych przesyłek zawierających informacje niejawne oznaczone klauzulą „Zastrzeżone” i „Poufne”.

6. Przesyłki wychodzące z jednostek SWW po godzinach służby kancelarii tajnej przekazywane są adresatowi przez punkt kontroli nadawcy za wykazem przesyłek nadanych, pobranym od funkcjonariusza, o których mowa w § 29 ust. 1.

7. Egzemplarz nr 2 wykazu przesyłek nadanych po dostarczeniu przesyłki odbiorcy zwracany jest funkcjonariuszowi, o którym mowa w ust. 6, który następnego dnia roboczego przekazuje go GKT.

§ 51.

1. Rejestracji dokumentów dokonuje się po podpisaniu ich przez osobę upoważnioną.

2. Obowiązek rejestracji dokumentu spoczywa na osobie, która dokument sporządziła lub odpowiada za jego wysłanie.

3. Wadliwe wydruki, odbitki, klisze, matryce, kalki oraz brudnopisy powstałe w toku prac nad dokumentem funkcjonariusz, który je sporządził niszczy bezzwłocznie we własnym zakresie.

4. Zbędne zapisy zawierające informacje niejawne na nośnikach do zapisów informacji w postaci cyfrowej i taśmach elektromagnetycznych kasuje funkcjonariusz dokonujący tych zapisów.

5. Dokumenty zarejestrowane w dzienniku ewidencyjnym brakuje się na zasadach określonych odrębnymi przepisami.

Rozdział 5
Rozliczanie funkcjonariuszy z materiałów służbowych oraz komisyjny dostęp do urządzeń do przechowywania materiałów niejawnych

§ 52.

1. W przypadku zmiany zakresu obowiązków, jeżeli wiąże się to z obowiązkiem przekazania materiałów służbowych innej osobie, a także w przypadku przeniesienia funkcjonariusza do innej komórki lub jednostki organizacyjnej SWW albo zwolnienia ze służby, bezpośredni przełożony sporządza w pojedynczym egzemplarzu polecenie rozliczenia materiałów służbowych, które w szczególności powinno zawierać:
1) sposób rozliczenia funkcjonariusza z materiałów, ze wskazaniem osób lub komórek, którym mają być przekazane;
2) termin, do którego funkcjonariusz powinien się rozliczyć;
3) potwierdzenie czytelnym podpisem funkcjonariusza faktu zapoznania się z poleceniem oraz datę tego zapoznania.

2. Rozliczenie się z materiałów służbowych może nastąpić poprzez:
1) przekazanie materiałów służbowych za pomocą protokołu zdawczo-odbiorczego;
2) przekazania materiałów zgodnie z pisemną dekretacją właściwego przełożonego umieszczoną na tych materiałach;
3) przeprowadzenie procedury archiwizacji lub brakowania materiałów.

3. W przypadku, gdy funkcjonariusz, w dniu wydania polecenia rozliczenia materiałów służbowych, nie posiada takich materiałów, umieszcza się na poleceniu stosowne oświadczenie potwierdzone podpisem funkcjonariusza punktu kontroli komórki organizacyjnej, w której pełni on służbę.

4. Polecenie, o którym mowa w ust. 1, oraz protokół, o którym mowa w ust. 2 pkt 1, przechowuje się, po zarejestrowaniu, we właściwej kancelarii tajnej lub punkcie kontroli.

5. Fakt przekazania materiałów odnotowuje się w urządzeniach ewidencyjnych punktu kontroli oraz kancelarii tajnych, w których funkcjonariusz pokwitował materiał jako ostatni adresat, poprzez przepisanie ich na innego funkcjonariusza bądź naniesienie adnotacji o wybrakowaniu lub zarchiwizowaniu materiału.

6. W przypadku czasowej nieobecności lub konieczności czasowego zastępstwa funkcjonariusza, przekazanie materiałów może nastąpić na podstawie polecenia, o którym mowa

w ust. 1, w oparciu o protokół, o którym mowa w ust. 2 pkt 1, bez konieczności odnotowania tego faktu w urządzeniach ewidencyjnych punktu kontroli oraz kancelarii tajnych.

§ 53.

1. W przypadkach uzasadnionych potrzebami służby, zezwala się na komisyjne otwarcie przydzielonego funkcjonariuszowi urządzenia do przechowywania materiałów niejawnych lub dostępu do informacji niejawnych zapisanych w wewnętrznej pamięci masowej jego komputera. Zezwolenie może wydać odpowiednio:
1) Szef SWW lub jego zastępca – w stosunku do wszystkich funkcjonariuszy;
2) kierownik jednostki organizacyjnej SWW lub jego zastępca – w stosunku do funkcjonariuszy podległej jednostki organizacyjnej SWW.

2. Z otwarcia urządzenia do przechowywania materiałów niejawnych lub z uzyskania dostępu do informacji niejawnych zapisanych w wewnętrznej pamięci masowej komputera, komisja sporządza protokół, który powinien, w szczególności, zawierać:
1) dane identyfikujące funkcjonariusza, który wydał polecenie otwarcia urządzenia do przechowywania materiałów niejawnych lub uzyskania dostępu do informacji niejawnych zapisanych w wewnętrznej pamięci masowej komputera;
2) dane identyfikujące członków komisji;
3) określenie zadań komisji;
4) czas i miejsce czynności;
5) dane identyfikujące funkcjonariusza, którego urządzenie do przechowywania materiałów niejawnych otwarto lub uzyskano dostęp do informacji niejawnych zapisanych w wewnętrznej pamięci masowej komputera;
6) opis zabezpieczenia otwieranej szafy lub uruchamianego komputera;
7) opis wykonanych przez komisję czynności, a w przypadku pobrania materiałów, dane identyfikujące funkcjonariusza, któremu zostały przekazane lub udostępnione;
8) treść pieczęci metalowej członka komisji, którą zabezpieczono urządzenie do przechowywania materiałów niejawnych lub podanie nowego hasła, którym zabezpieczono komputer;
9) podpisy członków komisji;
10) informację, o zatwierdzeniu protokołu przez osobę wydającą zezwolenie.

3. Protokół, po zarejestrowaniu, przechowuje się w punkcie kontroli obsługującym funkcjonariusza, którego dotyczyły czynności wymienione w ust. 2.

4. Z treścią protokołu zapoznaje funkcjonariusza, o którym mowa w ust. 1, bezpośredni przełożony. Fakt zapoznania się z protokołem funkcjonariusz potwierdza czytelnym podpisem i datą.

Rozdział 6
Ochrona informacji niejawnych w trakcie obrad, szkoleń i konferencji

§ 54.

1. Za ochronę informacji niejawnych w trakcie obrad, szkoleń i konferencji odpowiedzialny jest funkcjonariusz pionu ochrony lub inny funkcjonariusz wyznaczony, w porozumieniu z pełnomocnikiem ochrony, przez kierownika jednostki organizacyjnej SWW będącej ich organizatorem.

2. Uczestnicy obrad, szkoleń i konferencji sporządzają notatki, jeżeli organizator na to zezwolił, w brulionach wydawanych przez jednostkę organizującą przedsięwzięcie. W przypadku, gdy notatki sporządzone w brulionach zawierać będą informacje niejawne bruliony rejestruje się w rejestrze wydanych przedmiotów prowadzonym przez punkt kontroli organizatora. Z brulionami postępuje się jak z materiałami niejawnymi.

3. Jednostka organizacyjna organizująca obrady, szkolenia i konferencje, w trakcie przerw oraz po ich zakończeniu, zapewnia ich uczestnikom możliwość przechowywania brulionów, o których mowa w ust. 2.

4. Jednostka organizacyjna SWW organizująca obrady, szkolenia lub konferencje brakuje bruliony lub przesyła je, na prośbę uczestnika, do jego jednostki organizacyjnej lub jednostki organizacyjnej SWW.

5. Za ochronę informacji niejawnych podczas szkoleń organizowanych w Centrum Kształcenia SWW odpowiedzialny jest funkcjonariusz wyznaczony przez Komendanta Centrum Kształcenia SWW.

§ 55.

1. Pomieszczenie, w którym odbywają się obrady, szkolenia i konferencje, powinno być sprawdzone i zabezpieczone w celu wyeliminowania możliwości podglądu i podsłuchu.

2. Funkcjonariusze, o których mowa w § 54 ust. 1, mogą dokonać sprawdzenia tożsamości osób uczestniczących w obradach, szkoleniach i konferencjach każdorazowo, kiedy uznają to za wskazane.

3. Uczestnikom obrad, szkoleń i konferencji zabrania się wnoszenia do pomieszczeń, w których odbywają się obrady, szkolenia i konferencje, urządzeń do rejestracji obrazu lub dźwięku oraz łączności bezprzewodowej bez zgody funkcjonariuszy, o których mowa w § 54 ust. 1. W przypadku posiadania takich urządzeń i nie uzyskania zgody należy je zdeponować przed rozpoczęciem obrad, szkoleń i konferencji.

Rozdział 7
Kopie i tłumaczenia

§ 56.

1. Zezwolenie na sporządzanie kopii lub tłumaczeń z dokumentu, zawierającego informacje niejawne, wydaje na piśmie odpowiednio:
1) Szef SWW;
2) kierownik jednostki organizacyjnej SWW;
3) zastępca Szefa SWW, zastępca kierownika jednostki organizacyjnej SWW, doradca Szefa SWW, główny specjalista, naczelnik wydziału lub jego zastępca, kierownik samodzielnej sekcji albo, w szczególnie uzasadnionych przypadkach, każdy inny funkcjonariusz – po uzyskaniu pisemnego upoważnienia Szefa SWW.

2. Zezwolenie, o którym mowa w ust. 1, dekretuje się na pierwszej stronie dokumentu, z którego ma być sporządzona kopia lub tłumaczenie, lub na osobnym dokumencie, który po zarejestrowaniu dołącza się do dokumentu, z którego sporządza się kopię lub tłumaczenie.

3. Zgodność z oryginałem kopii lub tłumaczenia potwierdza się, na ostatniej stronie dokumentu wytworzonego w wyniku kopiowania lub tłumaczenia poprzez:
1) naniesienie napisu „Za zgodność”;
2) odciśnięcie pieczęci z nazwą jednostki organizacyjnej SWW, w której wykonano kopię lub tłumaczenie;
3) złożenie podpisu przez osobę, o której mowa w ust. 1 pkt 1 albo 2, albo – po uzyskaniu pisemnego upoważnienia Szefa SWW – przez funkcjonariusza innego, niż ta osoba, ze wskazaniem imienia i nazwiska lub innego oznaczenia wskazującego na składającego podpis.

4. Fakt sporządzenia kopii lub tłumaczenia odnotowuje się na ostatniej stronie dokumentu, z którego sporządzono kopię lub tłumaczenie, przez odcisk pieczęci lub umieszczenie adnotacji informującej o:
1) nazwie jednostki organizacyjnej SWW lub komórki organizacyjnej, w której sporządzono kopię lub tłumaczenie;
2) liczbie sporządzonych egzemplarzy kopii lub tłumaczeń;
3) dacie sporządzenia kopii lub tłumaczenia;
4) numerze, pod jakim kopia lub tłumaczenie zostały zarejestrowane w dzienniku ewidencyjnym.

5. Rejestracji kopii lub tłumaczenia dokonuje się w punkcie kontroli jednostki organizacyjnej SWW lub komórki organizacyjnej funkcjonariusza odpowiedzialnego za oryginał dokumentu.

6. Obowiązek rejestracji kopii lub tłumaczenia w dzienniku ewidencyjnym spoczywa na funkcjonariuszu:
1) dostarczającym dokument do kopiowania – w przypadku kopii;

2) sporządzającym odpis, wypis, wyciąg lub tłumaczenie – w przypadku odpisów, wypisów, wyciągów lub tłumaczeń.

7. Adnotacje, o których mowa w § 56 ust. 4 pkt 1 – 3, wpisuje się przed wykonaniem kopii lub tłumaczenia, natomiast numer, pod jakim zostały zarejestrowane w dzienniku ewidencyjnym, nanosi się po wykonaniu kopii lub tłumaczenia.

§ 57.

1. Wykonywanie kopii i tłumaczeń dokumentów dozwolone jest w pomieszczeniach usytuowanych w strefie ochronnej I lub II.

2. Kopiowanie i drukowanie dokumentu odbywa się w obecności funkcjonariusza dostarczającego dokument do kopiowania lub drukowania.

Rozdział 8
Sprawozdawczość i postępowanie w przypadku utraty materiału niejawnego

§ 58.

1. Do 30 stycznia każdego roku pełnomocnik ochrony powołuje, w drodze decyzji, komisję inwentaryzacyjną, w celu przeprowadzenia inwentaryzacji materiałów niejawnych za rok ubiegły, połączonej z kontrolą ewidencji.

2. W decyzji powołującej komisję inwentaryzacyjną, pełnomocnik ochrony określa zakres i sposób przeprowadzenia kontroli, o której mowa w ust. 1.

3. O nieprawidłowościach stwierdzonych podczas kontroli, o której mowa w ust. 1, pełnomocnik ochrony informuje Szefa SWW i kierowników jednostek organizacyjnych SWW, w których stwierdzono nieprawidłowości.

4. W terminie 2 tygodni od zatwierdzenia protokołu kontroli, kierownik jednostki organizacyjnej SWW, w której stwierdzone zostały nieprawidłowości zobowiązany jest do usunięcia nieprawidłowości stosując się do zaleceń pokontrolnych.

§ 59.

1. W przypadku utraty kontroli nad materiałem funkcjonariusz, który stwierdził jego brak jest zobowiązany złożyć za pośrednictwem bezpośredniego przełożonego pisemny raport kierownikowi jednostki organizacyjnej SWW.

2. Kierownik jednostki organizacyjnej SWW jest zobowiązany niezwłocznie powiadomić pełnomocnika ochrony o utracie kontroli nad materiałem, podając wszelkie możliwe do ustalenia jego dane, okoliczności, w jakich ujawniono utratę oraz plan czynności wyjaśniających mających na celu jego odnalezienie. Do powiadomienia dołącza się raport, o którym mowa w ust. 1.

3. O wyniku czynności wyjaśniających, o których mowa w ust. 2, należy poinformować pełnomocnika ochrony, wskazując jednocześnie na charakter utraty oraz podając dodatkowe informacje dotyczące utraconego materiału wynikające z ustaleń poczynionych w trakcie czynności wyjaśniających.

4. W przypadku potwierdzenia faktu utraty kontroli nad materiałem i po przeprowadzeniu czynności, o których mowa w ust. 1 – 3, fakt ten należy odnotować w ewidencji, w postaci numeru dokumentu, za którym przekazano pełnomocnikowi ochrony informację o wyniku przeprowadzonych czynności wyjaśniających.

5. Pełnomocnik ochrony może zlecić przeprowadzenie dodatkowych czynności, mających na celu wyjaśnienie okoliczności utraty kontroli nad materiałem oraz miejsca jego przechowywania.

Rozdział 9
Przepisy końcowe

§ 60.

1. W przypadku dokumentacji wytwarzanej poza granicami kraju i braku możliwości zastosowania wymogów niniejszego zarządzenia, dopuszcza się stosowanie innych rozwiązań określonych odrębnymi przepisami, z zastrzeżeniem ust. 2.

2. Kierownik jednostki organizacyjnej SWW nadzorujący wykonawców w przypadku, o którym mowa w ust. 1, opracowuje wytyczne w zakresie ochrony informacji niejawnych, a w szczególności w zakresie ich przetwarzania.

3. Wytyczne, o których mowa w ust. 2, wraz z uzasadnieniem przyjętych rozwiązań wymagają akceptacji pełnomocnika ochrony oraz zatwierdzenia przez Szefa SWW.

§ 61.

Traci moc zarządzenie nr 45/2011 Szefa Służby Wywiadu Wojskowego z dnia 5 grudnia 2011 r. w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii tajnych oraz innych, niż kancelaria tajna, komórek organizacyjnych odpowiedzialnych za przetwarzanie materiałów niejawnych, sposobu i trybu przetwarzania informacji niejawnych oraz doboru i stosowania środków bezpieczeństwa fizycznego w Służbie Wywiadu Wojskowego (Dz. Urz. MON Nr 24, poz. 362).

§ 62.

Zarządzenie wchodzi w życie z dniem 1 stycznia 2013 r.

m. p.

SZEF
SŁUŻBY WYWIADU WOJSKOWEGO
gen. bryg. Radosław KUJAWA

Załączniki do zarządzenia Nr 47/MON
Ministra Obrony Narodowej
z dnia 20 grudnia 2012 r. (poz. 79)

Załącznik nr 1

METODYKA DOBORU ŚRODKÓW BEZPIECZEŃSTWA FIZYCZNEGO

Część I. Instrukcja

1. Proces doboru środków bezpieczeństwa fizycznego zapewnia elastyczność ich stosowania w zależności od określonego dla danego pomieszczenia lub obszaru poziomu zagrożeń.

2. W częściach II – IV przedstawiono najbardziej odpowiednie i ekonomiczne kombinacje środków bezpieczeństwa fizycznego zapewniające wielopoziomową ochronę informacji niejawnych oraz spełniające wymagania określone w § 4 – 7 zarządzenia.

3. Środki bezpieczeństwa fizycznego określone w części III „Klasyfikacja środków bezpieczeństwa fizycznego" zostały podzielone na 6 kategorii, z których każda dotyczy określonego aspektu bezpieczeństwa fizycznego. Aby ułatwić odczytywanie informacji, wykaz środków został sporządzony w formie tabeli z przypisanymi im wartościami liczbowymi.

4. Pierwszym etapem procesu doboru środków bezpieczeństwa fizycznego jest odczytanie z tabeli w części II „Podstawowe wymagania bezpieczeństwa fizycznego" minimalnej łącznej sumy punktów wymaganych do osiągnięcia założonego poziomu ochrony informacji w wyniku zastosowania odpowiednich kombinacji środków bezpieczeństwa fizycznego. Liczba wymaganych do uzyskania punktów zależy od najwyższej klauzuli tajności informacji niejawnych przetwarzanych w danej lokalizacji oraz określonego poziomu zagrożeń.

5. Drugim etapem jest odczytanie z tej samej tabeli w części II, odpowiadającej założonemu poziomowi ochrony informacji, minimalnej liczby punktów koniecznych do uzyskania w każdej z grup obejmującej kategorie wymaganych do zastosowania środków bezpieczeństwa fizycznego (oznaczonej „obowiązkowo").

6. Trzecim etapem jest dokonanie wyboru określonych środków bezpieczeństwa fizycznego, przy którym należy posługiwać się tabelą z części III „Klasyfikacja środków bezpieczeństwa fizycznego". W tej tabeli należy odczytać liczbę punktów odpowiadającą wybranemu środkowi bezpieczeństwa i wpisać ją w odpowiednie miejsce w tabeli w części IV „Punktacja zastosowanych środków bezpieczeństwa fizycznego". Niezastosowanie danego środka jest jednoznaczne z przyznaniem za niego liczby punktów „0". Przy dokonywaniu wyboru konieczne jest uwzględnienie wymagań określonych w zarządzeniu, jak też w samej tabeli z części III „Klasyfikacja środków bezpieczeństwa fizycznego". Dobór adekwatnych środków bezpieczeństwa fizycznego w konkretnym przypadku musi zapewnić uzyskanie zarówno minimalnej łącznej sumy punktów wymaganych do osiągnięcia założonego

poziomu ochrony informacji niejawnych (w zależności od najwyższej klauzuli tajności informacji przetwarzanych w danej lokalizacji oraz poziomu zagrożeń), jak również uzyskanie minimalnej liczby punktów odpowiadających każdej z grup kategorii środków bezpieczeństwa fizycznego (oznaczonych jako „obowiązkowo"). W przypadku, gdy liczba punktów uzyskanych po zastosowaniu środka należącego do grup kategorii oznaczonych jako „obowiązkowo" jest mniejsza od minimalnej łącznej sumy punktów wymaganych do osiągnięcia założonego poziomu ochrony informacji niejawnych, należy zastosować środki z kategorii oznaczonych „dodatkowo" zapewniające uzyskanie minimalnej łącznej sumy punktów.

7. Za zastosowanie produktów, które posiadają ważne certyfikaty wydane przed wejściem w życie zarządzenia oraz rozporządzenia, o którym mowa w § 2 pkt 22 zarządzenia, przyznaje się liczbę punktów odpowiednio do spełnianych przez nie wymagań określonych w tabeli z części III „Klasyfikacja środków bezpieczeństwa fizycznego".

8. Spis użytych w metodyce norm obowiązujących w dniu wejścia w życie zarządzenia:
   - PN-EN 1627 – Okna, drzwi, żaluzje. Odporność na włamanie. Wymagania i klasyfikacja
   - PN-EN 14450 – Pomieszczenia i urządzenia do przechowywania wartości. Wymagania, klasyfikacja i metody badań odporności na włamanie. Pojemniki bezpieczne i szafy
   - PN-EN 1300 – Pomieszczenia i urządzenia do przechowywania wartości. Klasyfikacja zamków o wysokim stopniu zabezpieczenia z punktu widzenia odporności na nieuprawnione otwarcie
   - PN-EN 50131-1 – Systemy alarmowe. Systemy sygnalizacji włamania i napadu. Wymagania systemowe
   - PN-EN 50133-1 – Systemy alarmowe. Systemy kontroli dostępu. Część 1: Wymagania systemowe
   - PN-EN 12209 – Okucia budowlane. Zamki. Zamki mechaniczne wraz z zaczepami. Wymagania i metody badań
   - PN-EN 1143-1 – Pomieszczenia i urządzenia do przechowywania wartości. Wymagania, klasyfikacja i metody badań odporności na włamanie. Część 1: Szafy, szafy ATM, pomieszczenia i drzwi do pomieszczeń.

Część II. Podstawowe wymagania bezpieczeństwa fizycznego

Najwyższa klauzula tajności informacji przetwarzanych w jednostce organizacyjnej	Poziom zagrożeń		
	Niski	Średni	Wysoki
ŚCIŚLE TAJNE			
Obowiązkowo: kategorie K1+K2+K3*	10	15	20
Obowiązkowo: kategorie K4+K5**	6	7	7
Dodatkowo: kategoria K6	4	5	5
Łącznie suma punktów	**20**	**27**	**32**
TAJNE			
Obowiązkowo: kategorie K1+K2+K3	8	12	15
Obowiązkowo: kategorie K4+K5***	4	5	5
Dodatkowo: kategoria K6	4	5	5
Łącznie suma punktów	**16**	**19**	**25**
POUFNE			
Obowiązkowo: kategorie K1+K2+K3	6	10	12
Obowiązkowo: kategorie K4+K5	2	3	3
Dodatkowo: kategoria K6	3	3	4
Łącznie suma punktów	**11**	**14**	**16**
ZASTRZEŻONE			
Obowiązkowo: kategorie K1+K2+K3	6	6	6
Dodatkowo: kategoria K4, K5 lub K6	-	1	2
Łącznie suma punktów	**6**	**7**	**8**

* tylko jedna z wartości może być równa 0.
** żadna z wartości nie może być mniejsza od 2.
*** żadna z wartości nie może być równa 0.

Część III. Klasyfikacja środków bezpieczeństwa fizycznego

KATEGORIA K1: Szafy do przechowywania informacji niejawnych
Środek bezpieczeństwa K1S1 – Konstrukcja szafy

Uznaje się, że szafy spełniające wymagania klasy „C" określone na podstawie wcześniej obowiązujących przepisów tj. rozporządzenia Rady Ministrów z dnia 18 października 2005 r. w sprawie organizacji i funkcjonowania kancelarii tajnych (Dz. U. Nr 208, poz. 1741), rozporządzenia Rady Ministrów z dnia 1 czerwca 2010 r. w sprawie organizacji i funkcjonowania kancelarii tajnych (Dz. U. Nr 114, poz. 765), zarządzenia nr 25/MON z dnia 17 listopada 2005 r. w sprawie szczególnego sposobu organizacji kancelarii tajnych oraz innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za rejestrowanie, przechowywanie, obieg i udostępnianie materiałów niejawnych, stosowania środków ochrony fizycznej oraz obiegu informacji niejawnych (Dz. Urz. MON Nr 21, poz. 203) są równoważne z wymaganiami dla typu 3.
Uznaje się, że szafy spełniające wymagania klasy „B" określone na podstawie ww. przepisów są równoważne z wymaganiami dla typu 2.
Uznaje się, że szafy spełniające wymagania klasy „A" określone na podstawie ww. przepisów są równoważne z wymaganiami dla typu 1.

Typ/ Punktacja	Funkcje lub cechy
Typ 4 4 pkt	Szafa spełnia co najmniej wymagania klasy odporności na włamanie „0" określone w Polskiej Normie PN-EN 1143-1;
Typ 3 3 pkt	Szafa spełnia co najmniej wymagania klasy odporności na włamanie S2 określone w Polskiej Normie PN-EN 14450;
Typ 2 2 pkt	Szafa spełnia co najmniej wymagania klasy odporności na włamanie S1 określone w Polskiej Normie PN-EN 14450;
Typ 1 1 pkt	Szafa charakteryzuje się następującymi cechami: 1) jest to zamykany na klucz mebel biurowy, nie wyposażony w żadne szczególne funkcje zabezpieczające, ale charakteryzujący się umiarkowaną odpornością na nieuprawnione próby otwarcia; 2) jest zabezpieczona zamkiem typu 1 lub 2 z Kategorii K1S2.

Środek bezpieczeństwa K1S2 – Zamek do szafy

Typ/ Punktacja	Funkcje lub cechy
Typ 4 4 pkt	Zamek charakteryzuje się wysokim poziomem odporności na fachowe i profesjonalne działania osoby nieuprawnionej posługującej się wyjątkowo zaawansowanymi narzędziami i umiejętnościami, które nie są powszechnie dostępne. Zamek jest zamkiem szyfrowym i spełnia co najmniej wymagania klasy B określone w Polskiej Normie PN-EN 1300. Rozróżnia się: 1) zamek mechaniczny szyfrowy co najmniej trzytarczowy, o cichym, przesuwie, posiadający min. 100 podziałek na pokrętle i skali nastawień, przy której w przypadku każdej tarczy zamek trzytarczowy nie otworzy się, jeżeli pokrętło jest przekręcone więcej niż o 1 kreskę podziałki po obu stronach właściwej kreski podziałki, a w przypadku zamka czterotarczowego wartość ta wynosi 1,25. Zamek powinien być odporny na manipulację przez eksperta, również przy użyciu specjalistycznych narzędzi, przez okres 20 roboczogodzin. Zamek powinien być zabezpieczony przed działaniem destrukcyjnym, w tym przed przewierceniem i prześwietleniem (atakiem) radiologicznym (promieniowanie z radioaktywnego źródła nie przekraczającego równowartości 10 curie, Co-60 z odległości 760 mm przez 20 godzin). Zmiana kombinacji powinna być blokowana i uaktywniana kluczem od tyłu obudowy zamka. Szafa powinna być wyposażona w dwa komplety kluczy od ustawiania szyfru; 2) zamek elektroniczny szyfrowy spełnia te same wymagania co zamek mechaniczny szyfrowy oraz nie generuje sygnałów, które mogą być wykorzystane do otwarcia zamka przez okres 20 roboczogodzin.
Typ 3 3 pkt	Zamek charakteryzuje się wysokim poziomem odporności na fachowe i profesjonalne działania osoby nieuprawnionej posługującej się wyjątkowo zaawansowanymi narzędziami i umiejętnościami, dostępnymi powszechnie dla profesjonalistów. Zamek jest zamkiem szyfrowym i spełnia co najmniej wymagania klasy B określone w Polskiej Normie PN-EN 1300. Rozróżnia się: 1) zamek mechaniczny szyfrowy co najmniej trzytarczowy, o cichym przesuwie, posiadający min. 100 podziałek na pokrętle i skali nastawień, przy której w przypadku każdej

	tarczy zamek trzytarczowy nie otworzy się, jeżeli pokrętło jest przekręcone więcej niż o 1 kreskę podziałki po obu stronach właściwej kreski podziałki, a w przypadku zamka czterotarczowego wartość ta wynosi 1,25. Zmiana kombinacji powinna być blokowana i uaktywniana kluczem od tyłu obudowy zamka. Zamek powinien być zabezpieczony przed działaniem destrukcyjnym, w tym przed przewierceniem. Z szafą powinny być dostarczone dwa komplety kluczy do zmiany kodu; 2) zamek elektroniczny szyfrowy spełnia te same wymagania co zamek mechaniczny szyfrowy oraz nie generuje sygnałów, które mogą być wykorzystane do otwarcia zamka przez okres 20 roboczogodzin.
Typ 2 **2 pkt**	Zamek charakteryzuje się odpornością na sprawne działania osoby nieuprawnionej, posługującej się zwykłymi, powszechnie dostępnymi środkami. Zamek spełnia co najmniej wymagania klasy A określone w Polskiej Normie PN-EN 1300.
Typ 1 **1 pkt**	Zamek charakteryzuje się umiarkowaną odpornością na nieuprawnione próby otwarcia i może być wykorzystywany wyłącznie w szafach typu 1. Zamek spełnia co najmniej wymagania kategorii 4 określone w Polskiej Normie PN-EN 12209.

KATEGORIA K2: Pomieszczenia

Kategoria K2 opisuje pomieszczenia, w których informacje niejawne przechowywane są w szafach opisanych w kategorii K1, i nie dotyczy pomieszczeń wzmocnionych. W przypadku pomieszczeń wzmocnionych obowiązują dodatkowe wymagania, o których mowa w § 5 ust. 1.

O zaklasyfikowaniu pomieszczenia do danego typu decyduje najsłabszy element (ściana, podłoga, strop, drzwi, okna), strefa ochronna lub poziom na jakim pomieszczenie się znajduje. W przypadku pomieszczeń zlokalizowanych w strefie ochronnej I lub strefie ochronnej II, lub znajdujących się w tych strefach na poziomie powyżej 5 m nad gruntem lub innym elementem budynku (np. balkonem lub balustradą), bądź gdy nie znajduje się ono na ostatniej kondygnacji (poddaszu) stosuje się wymagania obniżone o jeden pkt (np. pomieszczenia typ 3 uzyskują 4 pkt).

Środek bezpieczeństwa K2S1 – Konstrukcja pomieszczenia

W przypadku zespołu pomieszczeń wymagania dotyczą wyłącznie konstrukcji zewnętrznych.

Typ/ Punktacja	**Funkcje lub cechy**
Typ 4 **4 pkt**	Konstrukcja pomieszczenia charakteryzuje się następującymi cechami: 1) zapewnia wysoką odporność na próby sforsowania z wykorzystaniem wielu różnych zaawansowanych narzędzi ręcznych i zasilanych prądem; 2) zapewnia wysoki poziom odporności na potajemne próby uzyskania nieuprawnionego dostępu; 3) jest usytuowane w budynku o konstrukcji murowanej, betonowej lub innej o podobnych właściwościach (parametrach) konstrukcyjnych; 4) jest oddzielone od innych pomieszczeń stałymi przegrodami budowlanymi o rozwiązaniach konstrukcyjno-materiałowych zapewniających bezpieczeństwo pożarowe i bezpieczeństwo konstrukcji, pozbawionymi zbędnych otworów, 5) w przypadku gdy ściany zewnętrzne lub stropy stanowią jednocześnie granicę strefy ochronnej III powinny posiadać konstrukcję murowaną, betonową lub inną o podobnych właściwościach o grubości nie mniejszej, niż: – stropy monolityczne z betonu lub o konstrukcji stalowo-ceramicznej np. Kleina o grubości co najmniej 20 cm. O innej konstrukcji z pustką powietrzną o grubości co najmniej 30 cm; – ściany betonowe 15 cm; – ściany murowane 25 cm. **UWAGA:** do ww. wymiarów wlicza się warstwę wykończeniową (tynk, szlichta, itp.).
Typ 3 **3 pkt**	Konstrukcja pomieszczenia charakteryzuje się następującymi cechami: 1) zapewnia wysoką odporność na działania osoby nieuprawnionej próbującej uzyskać dostęp siłą lub za pomocą różnorodnych narzędzi ręcznych; 2) zapewnia wysoki poziom odporności na potajemne próby uzyskania nieuprawnionego dostępu; 3) jest usytuowane w budynku o konstrukcji murowanej, betonowej lub innej o podobnych właściwościach (parametrach) konstrukcyjnych; 4) jest oddzielone od innych pomieszczeń stałymi przegrodami budowlanymi o rozwiązaniach konstrukcyjno-materiałowych zapewniających bezpieczeństwo konstrukcji, pozbawionymi zbędnych otworów, 5) w przypadku gdy ściany zewnętrzne lub stropy stanowią jednocześnie granicę strefy ochronnej III powinny posiadać konstrukcję murowaną, betonową lub inną o podobnych właściwościach o grubości nie mniejszej niż: – stropy monolityczne z betonu lub o konstrukcji stalowo-ceramicznej np. Kleina o grubości co najmniej 15 cm. O innej konstrukcji z pustką powietrzną o grubości co najmniej 25 cm; – ściany betonowe 15 cm; – ściany murowane 25 cm.

	UWAGA: do ww. wymiarów wlicza się warstwę wykończeniową (tynk, szlichta, itp.).
Typ 2 **2 pkt**	Konstrukcja pomieszczenia charakteryzuje się następującymi cechami: 1) zapewnia względną odporność na działania osoby nieuprawnionej próbującej uzyskać dostęp siłą lub za pomocą ograniczonej liczby narzędzi ręcznych; 2) zapewnia odporność na potajemne próby uzyskania nieuprawnionego dostępu; 3) zbudowane zostało z elementów murowanych, betonu lub innych materiałów o podobnych właściwościach (parametrach) konstrukcyjnych; 4) jest oddzielone od innych pomieszczeń stałymi przegrodami budowlanymi o rozwiązaniach konstrukcyjno-materiałowych zapewniających bezpieczeństwo konstrukcji, pozbawionymi zbędnych otworów, 5) w przypadku gdy ściany zewnętrzne lub stropy stanowią jednocześnie granicę strefy ochronnej III powinny posiadać konstrukcję murowaną, betonową lub inną o podobnych właściwościach o grubości nie mniejszej niż: – stropy monolityczne z betonu lub o konstrukcji stalowo-ceramicznej np. Kleina o grubości co najmniej 10 cm. O innej konstrukcji z pustką powietrzną o grubości co najmniej 20 cm; – ściany betonowe 10 cm; – ściany murowane 15 cm. **UWAGA:** do ww. wymiarów wlicza się warstwę wykończeniową (tynk, szlichta, itp.).
Typ 1 **1 pkt**	Konstrukcja pomieszczenia charakteryzuje się następującymi cechami: 1) zbudowane zostało z cegły lekkiej, kartongipsu, drewna (materiałów pochodnych) lub innego materiału o podobnej wytrzymałości; 2) zapewnia odporność na próby uzyskania nieuprawnionego dostępu; 3) jest oddzielone od innych pomieszczeń stałymi przegrodami budowlanymi; **UWAGA:** Jeżeli wymagane jest, by takie pomieszczenie było zabezpieczone przed długotrwałymi potajemnymi próbami uzyskania dostępu (na przykład w nocy lub podczas weekendu), standard drzwi i ich zamków oraz standard zabezpieczenia okien powinien być odpowiednio wyższy, adekwatnie do poziomu zagrożeń.

Środek bezpieczeństwa K2S2 – Konstrukcja drzwi pomieszczenia

Typ/ Punktacja	Funkcje lub cechy
Typ 4 **4 pkt**	Drzwi spełniają najwyższe wymagania odporności na włamanie określone w aktualnych normach branżowych i są odporne na próby otwarcia z wykorzystaniem wielu różnych zaawansowanych narzędzi ręcznych i zasilanych prądem;
Typ 3 **3 pkt**	Drzwi spełniają średnie wymagania odporności na włamanie określone w aktualnych normach branżowych i są odporne na działania osoby nieuprawnionej próbującej uzyskać dostęp siłą lub za pomocą różnorodnych narzędzi ręcznych;
Typ 2 **2 pkt**	Drzwi spełniają podstawowe wymagania odporności na włamanie określone w aktualnych normach branżowych i są odporne na działania osoby nieuprawnionej próbującej uzyskać dostęp siłą lub za pomocą ograniczonej liczby narzędzi ręcznych;
Typ 1 **1 pkt**	Drzwi wewnętrzne pełne, o konstrukcji drewnianej lub z materiałów pochodnych, wyposażone w dwa zamki, z których jeden spełnia, co najmniej średnie wymagania odporności antywłamaniowej określone w aktualnie obowiązujących normach branżowych.

Środek bezpieczeństwa K2S3 – Zamek do drzwi pomieszczenia

Typ/ Punktacja	Funkcje lub cechy
Typ 4 **4 pkt**	Zamek spełniający najwyższe wymagania odporności antywłamaniowej określone w aktualnie obowiązujących normach branżowych.
Typ 3 **3 pkt**	Zamek spełniający wysokie wymagania odporności antywłamaniowej określone w aktualnie obowiązujących normach branżowych.
Typ 2 **2 pkt**	Zamek spełniający średnie wymagania odporności antywłamaniowej określone w aktualnie obowiązujących normach branżowych..
Typ 1 **1 pkt**	Zamek spełniający podstawowe (niskie) wymagania odporności antywłamaniowej określone w aktualnie obowiązujących normach branżowych.

Środek bezpieczeństwa K2S4 – Konstrukcja okien do pomieszczenia

W przypadku okien których dolna krawędź zlokalizowana jest powyżej 5m nad poziomem gruntu lub więcej niż 3m od powierzchni dachu, bądź też zlokalizowanych w miejscu znacznie utrudniającym do nich dostęp oraz okien o powierzchni otworu wewnętrznego ościeżnicy mniejszej niż 250 cm^2 – dla okien typu 1 przyznaje się 2 pkt.

Typ/ Punktacja	Funkcje lub cechy
Typ 4 4 pkt	Okna spełniają wysokie wymagania odporności na włamanie określone w aktualnie obowiązującej normie branżowej lub okna standardowe (bezklasowe) wyposażone w stalowe kraty o konstrukcji oraz sposobie montażu do konstrukcji ściany zapewniającym wysoką odporność na próby sforsowania z wykorzystaniem wielu różnych zaawansowanych narzędzi ręcznych i zasilanych prądem. Kraty muszą spełniać wysokie wymagania odporności na włamanie określone w aktualnie obowiązującej normie branżowej
Typ 3 3 pkt	Okna spełniają średnie wymagania odporności na włamanie określone w aktualnie obowiązującej normie branżowej lub okna standardowe (bezklasowe) wyposażone w kraty o konstrukcji oraz sposobie montażu do konstrukcji ściany zapewniającym wysoką odporność na działania osoby nieuprawnionej próbującej uzyskać dostęp siłą lub za pomocą różnorodnych narzędzi ręcznych. Kraty muszą spełniać średnie wymagania odporności na włamanie określone w aktualnie obowiązującej normie branżowej.
Typ 2 2 pkt	Okna spełniają podstawowe (niskie) wymagania odporności na włamanie określone w aktualnie obowiązującej normie branżowej lub okna standardowe (bezklasowe) wyposażone w kraty o konstrukcji oraz sposobie montażu do konstrukcji ściany zapewniającym względną odporność na działania osoby nieuprawnionej próbującej uzyskać dostęp siłą lub za pomocą ograniczonej liczby narzędzi ręcznych. Kraty muszą spełniać podstawowe (niskie) wymagania odporności na włamanie określone w aktualnie obowiązującej normie branżowej.
Typ 1 1 pkt	Standardowe (bezklasowe) okna z szyb zespolonych o konstrukcji drewnianej lub PCV zamykane (blokowane) kluczem. **UWAGA:** w przypadku okien których dolna krawędź zlokalizowana jest powyżej 5m nad poziomem gruntu lub więcej niż 3m od powierzchni dachu, bądź też zlokalizowanych w miejscu znacznie utrudniającym do nich dostęp - dla okien Typu 1 przyznaje się 2 pkt.

KATEGORIA K3: Budynki

O zaklasyfikowaniu budynku do danego typu decyduje najsłabszy jego element zewnętrzny.

Typ/ Punktacja	Funkcje lub cechy
Typ 4 4 pkt	Budynek charakteryzuje się wytrzymałą konstrukcją oraz następującymi cechami: 1) jest murowany, betonowy lub wykonany z innych materiałów o podobnych właściwościach (parametrach) konstrukcyjnych i zapewnia wysoki poziom odporności na próby włamania; 2) wszystkie okna zlokalizowane poniżej 5 m są typu co najmniej 3, a drzwi wejściowe znajdują się pod bezpośrednim, całodobowym nadzorem personelu bezpieczeństwa bądź pozostają zamknięte; 3) nie jest wykorzystywany przez inne podmioty; 4) jest zlokalizowany wewnątrz strefy ochronnej III; 5) otoczenie oraz dach są stale monitorowane przez personel bezpieczeństwa.
Typ 3 3 pkt	Budynek charakteryzuje się następującymi cechami: 1) jest murowany, betonowy lub wykonany z innych materiałów o podobnych właściwościach (parametrach) konstrukcyjnych i zapewnia średni poziom odporności na próby włamania; 2) wszystkie okna zlokalizowane poniżej 5 m są typu co najmniej 2, a drzwi wejściowe znajdują się pod całodobowym nadzorem personelu bezpieczeństwa bądź pozostają zamknięte; 3) jeżeli jest on wykorzystywany przez inne podmioty, podlegają one procedurom bezpieczeństwa określonym przez pion ochrony SWW; 4) wejście do budynku możliwe jest wyłącznie przez strefę ochronną III; 5) otoczenie oraz dach są stale monitorowane przez personel bezpieczeństwa.
Typ 2 2 pkt	Budynek charakteryzuje się następującymi cechami: 1) stanowi lekką konstrukcję, zazwyczaj z pojedynczego rzędu cegieł lub lekkich bloczków i zapewnia średni poziom odporności na próby włamania; 2) jest wykorzystywany przez inne podmioty, nie podlegające procedurom bezpieczeństwa określonym przez pion ochrony SWW;
Typ 1 1 pkt	Budynek jest lekką konstrukcją przeznaczoną do ochrony zawartości i osób znajdujących się wewnątrz tylko przed działaniem czynników zewnętrznych (deszcz, niska temperatura, wiatr itd.).

KATEGORIA K4: Kontrola dostępu
Środek bezpieczeństwa K4S1 – Systemy kontroli dostępu

Typ/ Punktacja	Funkcje lub cechy
Typ 4 4 pkt	Elektroniczny automatyczny system kontroli dostępu o następujących cechach: 1) spełnia najwyższe wymagania w klasie rozpoznania i w klasie dostępu określone w aktualnie obowiązującej normie branżowej, 2) jest to automatyczny system zapewniający właściwy stopień ochrony, wymagający jedynie minimalnego nadzoru przez personel bezpieczeństwa; 3) jest stosowany w połączeniu z barierą dostępu uniemożliwiającą powrót (anti-passback), działającą na zasadzie uniemożliwiającej otwarcie danego przejścia kontrolowanego, jeżeli wcześniej nie nastąpiło wyjście ze strefy, do której zamierza się wejść, bądź bez uprzedniego wejścia do poprzedzającej go strefy; 4) sygnały ostrzeżeń i alarmów z systemu przekazywane są do stacji monitoringu obsługiwanej przez personel bezpieczeństwa; 5) obejmuje wszystkie wejścia i wyjścia kontrolowanego pomieszczenia lub obszaru; 6) okres archiwizacji danych powinien wynosić, co najmniej 12 miesięcy, 7) jest wspomagany przez system telewizji dozorowej.
Typ 3 3 pkt	Elektroniczny automatyczny system kontroli dostępu o następujących cechach: 1) spełnia najwyższe wymagania w klasie rozpoznania i w klasie dostępu określone w aktualnie obowiązującej normie branżowej, 2) wstęp kontrolowany jest przez odpowiednią barierę, która może wymagać bezpośredniego nadzoru przez personel bezpieczeństwa; 3) obejmuje wszystkie wejścia i wyjścia kontrolowanego pomieszczenia lub obszaru. 4) sygnały ostrzeżeń i alarmów z systemu przekazywane są do stacji monitoringu obsługiwanej przez personel bezpieczeństwa; 5) okres archiwizacji danych powinien wynosić, co najmniej 12 miesięcy, 6) jest wspomagany przez system telewizji dozorowej.
Typ 2 2 pkt	Polega na zastosowaniu jednego z poniższych rozwiązań: 1) elektroniczny automatyczny system kontroli dostępu o następujących cechach: a) spełnia średnie wymagania w klasie rozpoznania i w klasie dostępu określone w aktualnie obowiązującej normie branżowej; b) wstęp kontrolowany jest przez odpowiednią barierę, która może wymagać bezpośredniego nadzoru personelu bezpieczeństwa; c) obejmuje wszystkie wejścia i wyjścia kontrolowanego obszaru; d) okres archiwizacji danych powinien wynosić, co najmniej 6 miesięcy, lub 2) system kontroli dostępu obejmujący wszystkie wejścia i wyjścia z kontrolowanego obszaru, wymagający: a) obecności personelu bezpieczeństwa; b) zastosowania dokumentu z fotografią lub systemu wstępu na podstawie unikalnych przepustek; w zależności od ustaleń związanych z przyznawaniem wstępu akceptowane mogą być również inne dokumenty identyfikacyjne, na przykład legitymacja służbowa. **UWAGA:** W przypadku wejścia na zasadach określonych w pkt. 2 do strefy ochronnej I lub strefy ochronnej II należy prowadzić ewidencję wejść i wyjść. Dane z ewidencji są przechowywane co najmniej przez okres 12 miesięcy od wprowadzenia ostatniej pozycji.
Typ 1 1 pkt	Poniższe systemy mogą być stosowane wyłącznie do zabezpieczania obszarów, w których przetwarzane są informacje niejawne najwyżej o klauzuli "poufne". 1) Elektroniczny system kontroli dostępu oparty na zamkniętych drzwiach pomieszczenia lub obszaru do którego można uzyskać dostęp za pomocą kodów (zamki szyfrowe) - spełniający niskie wymagania w klasie rozpoznania i w klasie dostępu określone w aktualnie obowiązującej normie branżowej lub 2) kluczy wydawanych przez personel bezpieczeństwa, za pokwitowaniem, uprawnionym osobom. **UWAGA:** Dane z ewidencji, o której mowa w pkt. 2 są przechowywane co najmniej przez okres 12 miesięcy od wprowadzenia ostatniej pozycji.

Środek bezpieczeństwa K4S2 – Kontrola osób nieposiadających stałego upoważnienia do wejścia na obszar jednostki organizacyjnej (interesantów)

Typ/ Punktacja	Funkcje lub cechy
Eskorta 3 pkt	Kontrolę interesantów organizuje się w następujący sposób: 1) wprowadzani interesanci przez cały czas swojej wizyty przebywają pod nadzorem personelu bezpieczeństwa lub funkcjonariusza, z którym związana jest ich wizyta; 2) jeżeli interesanci muszą odwiedzić kilka różnych działów lub funkcjonariuszy, powinni formalnie przechodzić spod nadzoru jednej osoby pod nadzór innej, z zapewnieniem wszelkiej dokumentacji dotyczącej takiej wizyty i zmiany towarzyszących osób uprawnionych;

	3) interesanci są zobligowani do noszenia odpowiedniego identyfikatora odróżniającego ich od funkcjonariuszy; 4) wszyscy interesanci wchodzący do strefy ochronnej I lub strefy ochronnej II poddawani są kontroli osobistej i bagaży pod kątem wnoszonych lub wynoszonych przedmiotów. Odmowa poddania się kontroli uniemożliwia wejście do ww. stref. W indywidualnych przypadkach za zgodą dyrektora BOiO lub upoważnionej przez niego osoby odstępuje się od kontroli. 5) interesanci bez zgody dyrektora BOiO nie mogą wnosić do strefy ochronnej I i strefy ochronnej II telefonów komórkowych oraz innych urządzeń do gromadzenia lub transmisji danych. W indywidualnych przypadkach, za zgodą Dyrektora BOiO lub upoważnionej przez niego osoby, z nadzoru można zrezygnować (z zachowaniem pkt 3 w stosunku do osób dysponujących poświadczeniem bezpieczeństwa do klauzuli „Tajne" lub „Ściśle tajne".
Przepustka 1 pkt	Kontrolę interesantów organizuje się w następujący sposób: 1) interesanci mogą uzyskać prawo wstępu na dany obszar bez konieczności nadzoru osoby uprawnionej; 2) interesanci są zobligowani do noszenia plakietki z przepustką, która ich identyfikuje, jako osoby nie posiadające stałego upoważnienia do wejścia na obszar jednostki organizacyjnej, i tym samym odróżnia ich od funkcjonariuszy. **UWAGA:** należy pamiętać, że system oparty na wydawaniu interesantom przepustek, jest skuteczny, jeżeli wszyscy funkcjonariusze jednostki organizacyjnej również noszą identyfikatory.

KATEGORIA K5: Personel bezpieczeństwa i systemy sygnalizacji napadu i włamania
Środek bezpieczeństwa K5S1 – Pion ochrony i personel bezpieczeństwa

Typ/ Punktacja	Funkcje lub cechy
Typ 5 5 pkt	Zadania w zakresie ochrony fizycznej realizowane są przez funkcjonariuszy pionu ochrony lub personel bezpieczeństwa spełniający następujące warunki: 1) personel bezpieczeństwa składa się z funkcjonariuszy zatrudnionych w SWW; 2) pracownicy cywilni samodzielnie nadzorują wyłącznie dostęp do strefy ochronnej III; 3) organizuje się częsty, wewnętrzny patrol kontrolujący wnętrze budynku po losowo wybranych trasach i przeprowadzany w nieregularnych odstępach czasu, jednak nie rzadziej niż co dwie godziny; 4) personel bezpieczeństwa wykorzystuje do nadzoru system telewizji dozorowej, system sygnalizacji włamania i napadu oraz system p.poż. 5) wartownicy mają przydzielone określone zadania do wykonania podczas patrolu.
Typ 4 4 pkt	Personel bezpieczeństwa organizuje się w następujący sposób: 1) personel bezpieczeństwa składa się z osób zatrudnionych na czas nieokreślony w SWW; 2) organizuje się wewnętrzny patrol kontrolujący wnętrze budynku po losowo wybranych trasach i przeprowadzany w nieregularnych odstępach czasu nie przekraczających 6 godzin, co umożliwia odbycie 2 lub 3 patroli w nocy i przeprowadzenie okresowych kontroli zabezpieczeń podczas weekendów lub dni wolnych od pracy.
Typ 3 3 pkt	Personel bezpieczeństwa organizuje się w następujący sposób: 1) zadania personelu bezpieczeństwa mogą wykonywać pracownicy zatrudnieni przez instytucję na terenie której znajduje się placówka SWW; 2) patrol ograniczony jest do kontroli terenu i jego granic, podczas którego strażnicy sprawdzają zabezpieczenia budynków, ale nie mają do nich dostępu; 3) częstotliwość patroli powinna zależeć od środowiska operacyjnego i poziomu zagrożenia.
Typ 2 2 pkt	Personel bezpieczeństwa organizuje się w następujący sposób: 1) w obiekcie funkcjonują strażnicy "stacjonarni", którzy nie są zobowiązani do przeprowadzania patroli, ale nadzorują chroniony obszar za pośrednictwem elektronicznych systemów pomocniczych; 2) zadania te mogą wykonywać pracownicy cywilni lub pracownicy firmy zewnętrznej.
Typ 1 1 pkt	Personel bezpieczeństwa organizuje się w następujący sposób: 1) w obiekcie funkcjonują strażnicy "sporadyczni", którzy są zatrudnieni do odwiedzania terenu nocą i podczas weekendów w celu przeprowadzenia podstawowej kontroli ogrodzenia; 2) strażnicy nie mają uprawnień dostępu do danego obiektu lub budynku, ale w przypadku podejrzenia włamania zareagują poprzez wezwanie osoby posiadającej klucze.

Środek bezpieczeństwa K5S2 – Systemy sygnalizacji napadu i włamania

Typ/ Punktacja	Funkcje lub cechy
Typ 4 **4 pkt**	System, charakteryzuje się następującymi cechami: 1) spełnia najwyższe wymagania bezpieczeństwa określone w aktualnej normie branżowej; 2) obejmuje ochroną cały chroniony obszar, w tym szafy służące do przechowywania informacji niejawnych i sygnalizuje co najmniej: a) otwarcie drzwi, okien i innych zamknięć chronionego obszaru, b) penetrację drzwi, okien i innych zamknięć chronionego obszaru bez ich otwierania, c) penetrację ścian, sufitów i podłóg, d) poruszanie się w chronionym obszarze (pułapkowe - nadzór nad wybranymi miejscami, w których występuje wysokie prawdopodobieństwo wykrycia), e) atak na szafy służące do przechowywania informacji niejawnych; 3) stosowany jest wraz z systemem dozom wizyjnego z obowiązkową rejestracją w rozdzielczości nie mniejszej niż 400 linii telewizyjnych i przechowywaniem zarejestrowanego zapisu przez czas nie krótszy niż 30 dni, nie obejmującym pomieszczeń służących wyłącznie jako pomieszczenia przeznaczone do spotkań; 4) stan systemu sygnalizacji napadu i włamania oraz systemu dozoru wizyjnego, w tym generowane ostrzeżenia i alarmy, jest stale monitorowany przez personel bezpieczeństwa. **UWAGA**: 4 pkt przyznaje się również w przypadku obszarów, w których przez 24 godziny na dobę przebywają funkcjonariusze.
Typ 3 **3 pkt**	System charakteryzuje się następującymi cechami: 1) spełnia wysokie wymagania bezpieczeństwa określone w aktualnej normie branżowej; 2) obejmuje ochroną otwory wejściowe i wnętrze obszaru oraz sygnalizuje co najmniej: a) otwarcie drzwi, okien i innych zamknięć chronionego obszaru, b) penetrację drzwi, okien i innych zamknięć chronionego obszaru bez ich otwierania, c) poruszanie się w chronionym obszarze (pułapkowe – nadzór nad wybranymi miejscami, w których występuje wysokie prawdopodobieństwo wykrycia), d) atak na szafy służące do przechowywania informacji niejawnych; 3) stan systemu, w tym generowane ostrzeżenia i alarmy, jest stale monitorowany przez personel bezpieczeństwa. **UWAGA:** 3 pkt przyznaje się również w przypadku systemu wykonanego przed wejściem w życie zarządzenia wymaganiami systemu co najmniej klasy SA3 określonymi w Polskiej Normie PN-93/E-08390, pod warunkiem spełnienia wymagań w zakresie ochrony i nadzoru określonych w pkt 2 dla typu 4.
Typ 2 **2 pkt**	System charakteryzuje się następującymi cechami: 1) spełnia średnie wymagania bezpieczeństwa określone w aktualnej normie branżowej i zapewnia identyfikację użytkowników włączających i wyłączających system lub jego część; 2) obejmuje ochroną miejsca, w których informacje niejawne są przechowywane oraz całą granicę obszaru (okna, drzwi i inne otwory) i sygnalizuje co najmniej: a) otwarcie drzwi, okien i innych zamknięć chronionego obszaru, b) poruszanie się w chronionym obszarze (pułapkowo – nadzór nad wybranymi miejscami, w których występuje wysokie prawdopodobieństwo wykrycia); 3) stan systemu, w tym generowane ostrzeżenia i alarmy, jest stale monitorowany przez personel bezpieczeństwa. **UWAGA**: 2 pkt przyznaje się również w przypadku systemu wykonanego przed wejściem w życie rozporządzenia, zgodnie z wymaganiami systemu co najmniej klasy SA2 określonymi w Polskiej Normie PN-93/E-08390, pod warunkiem spełnienia wymagań w zakresie ochrony i nadzoru określonych w pkt 2 dla typu 3.
Typ 1 **1 pkt**	System charakteryzuje się następującymi cechami: 1) spełnia podstawowe (niskie) wymagania bezpieczeństwa określone w aktualnej normie branżowej; 2) obejmuje ochroną miejsca, w których informacje niejawne są przechowywane i sygnalizuje co najmniej: a) otwarcie drzwi do chronionego obszaru, b) poruszanie się w chronionym obszarze (pułapkowo - nadzór nad wybranymi miejscami, w których występuje wysokie prawdopodobieństwo wykrycia). **UWAGA:** 1 pkt przyznaje się również w przypadku systemu wykonanego przed wejściem w życie rozporządzenia, zgodnie z wymaganiami systemu co najmniej klasy SA1 określonymi w Polskiej Normie PN-93/E-08390, pod warunkiem spełnienia wymagań w zakresie ochrony i nadzoru określonych w pkt 2 dla typu 2.

KATEGORIA K6: Granice
Środek bezpieczeństwa K6S1 – Ogrodzenie

Typ/ Punktacja	Funkcje lub cechy
Typ 4 **4 pkt**	Ogrodzenie charakteryzuje się następującymi cechami: 1) zapewnia wysoki poziom zabezpieczenia, maksymalnie utrudnia i opóźnia działania profesjonalnego i zdeterminowanego intruza/włamywacza, który dysponuje szeroką wiedzą i zaawansowanymi narzędziami; 2) projekt i konstrukcja ogrodzenia zapewniają wysoki poziom odporności na ataki dokonywane poprzez wspinanie się na ogrodzenie lub wyłamanie ogrodzenia; 3) minimalna wysokość wynosi 250 cm; 4) górna część jest zabezpieczona z obu stron przed wspinaniem się i przechodzeniem przez ogrodzenie; 5) zapewnia łatwe monitorowanie; 6) jest przeważnie wspomagane innymi systemami zabezpieczenia ogrodzenia, takimi jak system dozoru wizyjnego, system wykrywania naruszenia ogrodzenia; 7) jeśli to możliwe, między budynkami a zewnętrznym ogrodzeniem zachowana jest wolna przestrzeń o szerokości nie mniejszej niż 5 m. **UWAGA:** 4 pkt przyznaje się również w przypadku podwójnego ogrodzenia tworzącego obwodnicę.
Typ 3 **3 pkt**	Ogrodzenie charakteryzuje się następującymi cechami: 1) zapewnia średni poziom zabezpieczenia, jest zaprojektowane w celu utrudnienia i opóźnienia działań dobrze przygotowanego intruza/włamywacza, który dysponuje ograniczoną liczbą narzędzi ręcznych; 2) projekt i konstrukcja ogrodzenia zapewniają odporność na próby wspinania się na ogrodzenie lub wyłamanie ogrodzenia; 3) minimalna wysokość wynosi 230 cm; 4) górna część jest zabezpieczona przed wspinaniem się i przechodzeniem przez ogrodzenie; 5) zapewnia łatwe monitorowanie; 6) jeśli to możliwe, między budynkami a ogrodzeniem zachowana jest wolna przestrzeń o szerokości 5 m.
Typ 2 **2 pkt**	Ogrodzenie charakteryzuje się następującymi cechami: 1) zabezpiecza przed włamaniem, zapewnia umiarkowany poziom odporności na próby wspinania się na ogrodzenie lub wyłamanie ogrodzenia przez nieprofesjonalnego włamywacza/intruza, niedysponującego określonymi umiejętnościami i posługującego się powszechnie dostępnymi, typowymi narzędziami; 2) minimalna wysokość wynosi 2 m.
Typ 1 **1 pkt**	Ogrodzenie jest zaprojektowane bez uwzględnienia żadnych szczególnych wymagań w zakresie bezpieczeństwa; takie ogrodzenie służy wyłącznie do wyznaczenia granic terenu i zapewnienia minimalnego zabezpieczenia przed osobami innymi niż zdeterminowany włamywacz/intruz.

Środek bezpieczeństwa K6S2 – Kontrola w punktach dostępu

Typ/ Punktacja	Funkcje lub cechy
TAK=1 pkt **NIE=0 pkt**	Bramy i wejścia są zbudowane zgodnie z tym samym standardem bezpieczeństwa co ogrodzenie oraz zapewniona jest kontrola dostępu. **UWAGA:** skuteczność każdego ogrodzenia zależy w dużym stopniu od poziomu bezpieczeństwa zapewnionego przy punktach dostępu umieszczonych w ogrodzeniu. **UWAGA:** w przypadku bram i wejść spełniających powyższe kryteria i tworzących „śluzę" (podwójne zabezpieczenie) przyznaje się 2 pkt.

Środek bezpieczeństwa K6S3 – System kontroli osób i przedmiotów przy wejściu/wyjściu

Typ/ Punktacja	Funkcje lub cechy
TAK=1 pkt **NIE=0 pkt**	Elektroniczny system pomocniczy lub rozwiązanie organizacyjne polegające na zwracaniu się o dobrowolne poddanie się kontroli lub udostępnienie do kontroli rzeczy osobistych, a także przedmiotów wnoszonych lub wynoszonych - stosowany w celu zapobiegania próbom nieuprawnionego wnoszenia na chroniony obszar rzeczy zagrażających bezpieczeństwu informacji niejawnych lub nieuprawnionego wynoszenia informacji niejawnych z budynków lub obiektów.

Środek bezpieczeństwa K6S4 – System wykrywania naruszenia ogrodzenia

Typ/ Punktacja	Funkcje lub cechy
TAK=1 pkt **NIE=0 pkt**	System: 1) jest stosowany przy ogrodzeniu w celu zwiększenia poziomu bezpieczeństwa zapewnionego przez ogrodzenie; 2) jest instalowany w formie zamaskowanych urządzeń bądź też widocznego sprzętu, co działa jako czynnik odstraszający. Ponieważ może wywoływać fałszywe alarmy, należy go stosować tylko w połączeniu z systemem weryfikacji alarmu, takim jak na przykład system dozoru wizyjnego.

Środek bezpieczeństwa K6S5 – Oświetlenie chronionego obszaru

Typ/ Punktacja	Funkcje lub cechy
TAK=1 pkt **NIE=0 pkt**	Oświetlenie jest czynnikiem odstraszającym potencjalnych intruzów, jak również zapewniającym widoczność wymaganą, aby można było skutecznie - bezpośrednio (personel bezpieczeństwa) lub pośrednio (dozór wizyjny) - kontrolować obszar. Charakteryzuje się następującymi cechami: 1) standard oświetlenia jest zgodny z minimalnymi wymaganiami określonymi dla systemu dozoru wizyjnego (jeżeli taki system zastosowano); 2) instalacja oświetlenia uwzględnia warunki ukształtowania terenu i zabudowy.

Środek bezpieczeństwa K6S6 – System dozoru wizyjnego granic

Typ/ Punktacja	Funkcje lub cechy
TAK=1 pkt **NIE=0 pkt**	System z obowiązkową rejestracją w rozdzielczości nie mniejszej niż 400 linii telewizyjnych i przechowywaniem zarejestrowanego zapisu przez czas nie krótszy niż 30 dni. Systemem są nadzorowane newralgiczne dla bezpieczeństwa miejsca takie jak: bramy, wejścia do budynków, elewacje budynków z oknami, powierzchnie dachów, depozytory itp.

Część IV. Punktacja zastosowanych środków bezpieczeństwa fizycznego

ŚRODEK BEZPIECZEŃSTWA	PKT
KATEGORIA K1: Szafy do przechowywania informacji niejawnych	
Środek bezpieczeństwa K1S1 – Konstrukcja szafy	
Liczba punktów za środek bezpieczeństwa (K1S1 = 4, 3, 2 lub 1 pkt)	
Środek bezpieczeństwa K1S2 – Zamek do szafy	
Liczba punktów za środek bezpieczeństwa (K1S2 = 4, 3, 2 lub 1 pkt)	
Liczba punktów za kategorię K1 stanowiąca iloczyn liczby punktów za oba powyższe środki bezpieczeństwa (K1=K1S1xK1S2)	
KATEGORIA K2: Pomieszczenia	
Środek bezpieczeństwa K2S1 – Konstrukcja pomieszczenia	
Liczba punktów za środek bezpieczeństwa (K2S1 = 4, 3, 2 lub 1 pkt)	
Środek bezpieczeństwa K2S2 – Konstrukcja drzwi pomieszczenia	
Liczba punktów za środek bezpieczeństwa (K2S2 = 4, 3, 2 lub 1 pkt)	
Środek bezpieczeństwa K2S3 – Zamek do drzwi pomieszczenia	
Liczba punktów za środek bezpieczeństwa (K2S3 = 4, 3, 2 lub 1 pkt)	
Środek bezpieczeństwa K2S4 – Konstrukcja okien do pomieszczenia	
Liczba punktów za środek bezpieczeństwa (K2S3 = 4, 3, 2 lub 1 pkt)	
Liczba punktów za kategorię K2 stanowiąca sumę liczby punktów za powyższe środki bezpieczeństwa (K2=K2S1+K2S2+K2S3+K2S4)	
KATEGORIA K3: Budynki	
Liczba punktów za kategorię (K3 = 4, 3, 2 lub 1 pkt)	
KATEGORIA K4: Kontrola dostępu	
Środek bezpieczeństwa K4S1 – Systemy kontroli dostępu	
Liczba punktów za środek bezpieczeństwa (K4S1 = 4, 3, 2 lub 1 pkt)	
Środek bezpieczeństwa K4S2 – Kontrola osób nieposiadających stałego upoważnienia do wejścia na obszar jednostki organizacyjnej (interesantów)	
Liczba punktów za środek bezpieczeństwa (K4S2 = 3 lub 1 pkt)	
Liczba punktów za kategorię K4 stanowiąca sumę liczby punktów za oba powyższe środki bezpieczeństwa (K4=K4S1+K4S2)	
KATEGORIA K5: Personel bezpieczeństwa i systemy sygnalizacji napadu i włamania	
Środek bezpieczeństwa K5S1 – Personel bezpieczeństwa	
Liczba punktów za środek bezpieczeństwa (K5S1 = 5, 4, 3, 2 lub 1 pkt)	
Środek bezpieczeństwa K5S2 – Systemy sygnalizacji napadu i włamania	
Liczba punktów za środek bezpieczeństwa (K5S2 = 4, 3, 2 lub 1 pkt)	
Liczba punktów za kategorię K5 stanowiąca sumę liczby punktów za oba powyższe środki bezpieczeństwa (K5=K5S1+K5S2)	
KATEGORIA K6: Granice	
Środek bezpieczeństwa K6S1 – Ogrodzenie	
Liczba punktów za środek bezpieczeństwa (K6S1 = 4, 3, 2 lub 1 pkt)	
Środek bezpieczeństwa K6S2 – Kontrola w punktach dostępu	
Liczba punktów za środek bezpieczeństwa (K6S2 = 1 lub 0 pkt)	
Środek bezpieczeństwa K6S3 – System kontroli osób i przedmiotów przy wejściu/wyjściu	
Liczba punktów za środek bezpieczeństwa (K6S3 = 1 lub 0 pkt)	

Środek bezpieczeństwa K6S4 – System wykrywania naruszenia ogrodzenia	
Liczba punktów za środek bezpieczeństwa (K6S4 = 1 lub 0 pkt)	
Środek bezpieczeństwa K6S5 – Oświetlenie chronionego obszaru	
Liczba punktów za środek bezpieczeństwa (K6S5 = 1 lub 0 pkt)	
Środek bezpieczeństwa K6S6 – System dozoru wizyjnego granic	
Liczba punktów za środek bezpieczeństwa (K6S6 = 1 lub 0 pkt)	
Liczba punktów za kategorię K6 stanowiąca sumę liczby punktów za powyższe środki bezpieczeństwa (K6=K6S1+K6S2+K6S3+K6S4+K6S5+K6S6)	
Ogólna liczba punktów stanowiąca sumę punktów za wszystkie kategorie PUNKTY=K1+K2+K3+K4+K5+K6	

. . . . . .
klauzula

WYKAZ

osób .....

(nazwa jednostki organizacyjnej))

upoważnionych do dostępu do informacji niejawnych

Lp.	Stopień	Imię i nazwisko, imię ojca Nr PESEL	Nazwa komórki organizacyjnej	Zakres i nr poświadczenia bezpieczeństwa	Termin ważności poświadczenia bezpieczeństwa do klauzuli			UWAGI
					Ściśle tajne	Tajne	Poufne / Zastrzeżone	
1	2	3	4	5	6	7	8	9

Załącznik nr 3

STRZEŻ INFORMACJI NIEJAWNYCH

SZAFA nr fabryczny . . . . .

Odpowiedzialny : **nr pieczęci . . . . . .**
nr pieczęci . . . . . .
nr pieczęci . . . . . .
nr pieczęci . . . . . .

PRZED OPUSZCZENIEM MIEJSCA PRACY SPRAWDŹ ZABEZPIECZENIE POWIERZONYCH CI DOKUMENTÓW

Załącznik nr 4

. . . . . .

(pieczęć nagłówkowa)
(numer ewidencyjny)

DZIENNIK PODAWCZY

. . . . . .

(jednostka organizacyjna)

Rozpoczęto dnia . . . . . .

od pozycji nr . . . . . .

Zakończono dnia . . . . . .

na pozycji nr . . . . . .

"l e w a s t r o n a d o k u m e n t u"

Oznaczenie klauzuli	Numer kolejny zapisu	Data wpływu	Nadawca	Numer przesyłki	Dokąd skierowano (jednostka, stanowisko lub imię i nazwisko)	Data i ewent. godzina odbioru	Pokwitowanie odbioru (czytelny podpis)	UWAGI
1	2	3	4	5	6	7	8	9

"p r a w a s t r o n a d o k u m e n t u"

Oznaczenie klauzuli	Numer kolejny zapisu	Data wpływu	Nadawca	Numer przesyłki	Dokąd skierowano (jednostka, stanowisko lub imię i nazwisko)	Data i ewent. godzina odbioru	Pokwitowanie odbioru (czytelny podpis)	UWAGI
1	2	3	4	5	6	7	8	9

"o s t a t n i a s t r o n a d o k u m e n t u"

Rozliczenie ilościowe zarejestrowanych dokumentów wg klauzul:

ŚCIŚLE TAJNE - . . . . . .

TAJNE - . . . . . .

POUFNE - . . . . . .

ZASTRZEŻONE - . . . . . .

RAZEM - . . . . . .

Niniejszy dziennik zawiera . . . . . / . . . . . stron
(słownie)

ponumerowanych, przesznurowanych i opieczętowanych.

. . . . . .
(miejscowość i data)

. . . . . .
(podpis)

…… ……

(pieczęć nagłówkowa i numer ewidencyjny) (klauzula)

DZIENNIK

EWIDENCJI I DORĘCZEŃ

SZYFROGRAMÓW

……

(jednostka organizacyjna)

Rozpoczęto dnia ……

od pozycji nr ……...

Zakończono dnia ……

na pozycji nr ……..…..

……

(klauzula)

„lewa strona dokumentu”

Oznaczenie klauzuli	Kolejny numer wch. lub wych.	Nr wych. nadawcy	Data i godzina otrzymania	NADAWCA	ADRESAT	NAZWISKO OPERATORA	Liczba		Nr egzemplarza	Liczba		
							Egz.	stron jednego.egz.		załączników	stron załączników	nośników
1	2	3	4	5	6	7	8	9	10	11	12	13

Strona ………./……….

„prawa strona dokumentu”

Numer nośnika wg. RWP	Potwierdzenie odbioru szyfrogramu, nośnika				Informacje uzupełniające, UWAGI
	Jedn. / Komórka organizacyjna odbiorcy	Data (godzina i minuta)	Nazwisko i imię osoby odbierającej	Podpis	
14	15	16	17	18	19

Niniejszy dziennik zawiera …….. / …….. stron
(słownie)

ponumerowanych, przesznurowanych i opieczętowanych.

…… ……..
(miejscowość i data) *(podpis)*

„strona tytułowa dokumentu” Załącznik nr 6

…… ……
(pieczęć nagłówkowa i numer ewidencyjny) (klauzula)

DZIENNIK

EWIDENCJI I DORĘCZEŃ SZYFROFAKSÓW

……
(jednostka organizacyjna)

Rozpoczęto dnia ……..poz. ……

Zakończono dnia ……..poz. ……

……
(klauzula)

„lewa strona dokumentu”

Numer i klauzula tajności szyfrofaksu wysyłanego	Numer i klauzula tajności szyfrofaksu otrzymanego	Liczba dziennika lub numer i klauzula tajności szyfrofaksu nadawcy	Ilość stron	Stopień pilności	Czas przyjęcia do wysłania		Dokąd (do kogo)
					Data	Godz. i min.	
1	2	3	4	5	6	7	8

Strona ……/……

„prawa strona dokumentu”

Skąd (od kogo)	Kto wysłał lub odebrał			Pokwitowanie odbioru			Uwagi
	Nazwisko	Data	Godz. i min.	Nazwisko i imię	Data	Godz. i min.	
9	10	11	12	13	14	15	16

„ostatnia strona dokumentu”

Niniejszy dziennik zawiera …….. / …….. stron
(słownie)

ponumerowanych, przesznurowanych i opieczętowanych.

……. ……..
(miejscowość i data) *(podpis)*

. . . .

(pieczęć nagłówkowa)
(numer ewidencyjny)

(klauzula)

REJESTR PRZEPISÓW WYDANYCH

. . . . . .

(jednostka organizacyjna)

Rozpoczęto dnia . . . . . .

Zakończono dnia . . . . . .

. . . . . .

(klauzula)

"l e w a s t r o n a d o k u m e n t u"

Data wydania przepisu	Jednostka merytorycznie odpowiedzialna	Numer kolejny wpisu (z uwzględnieniem klauzuli tajności)					Tytuł aktu prawnego	Uwagi
		Zarządzenia	Decyzji	Wytycznych	Porozumienia	Inne		

"p r a w a s t r o n a d o k u m e n t u"

Data wydania przepisu	Jednostka merytorycznie odpowiedzialna	Numer kolejny wpisu (z uwzględnieniem klauzuli tajności)					Tytuł aktu prawnego	Uwagi
		Zarządzenia	Decyzji	Wytycznych	Porozumienia	Inne		

Rejestr zawiera . . . . / . . . . stron
(słownie)

ponumerowanych, przesznurowanych i opieczętowanych.

. . . .
(miejscowość i data)   *(podpis)*

. . . .

(pieczęć nagłówkowa)
(numer ewidencyjny)

(klauzula)

REJESTR ROZKAZÓW

. . . . . .

(komórka organizacyjna)

Rozpoczęto dnia: . . . . . .

od pozycji nr . . . . . .

Zakończono dnia: . . . . . .

na pozycji nr . . . . . .

. . . . . .

(klauzula)

"lewa strona dokumentu"

Oznaczenie klauzuli rozkazu	Numer kolejny zapisu	Data podpisania rozkazu	Adnotacje dot. przedłużenia okresu ochrony, zniesienia, bądź zmiany klauzuli tajności	Określenie osoby podpisującej	Określenie, czego rozkaz dotyczy	Nazwisko wykonawcy	Liczba stron rozkazu	Pozycja Dziennika ewidencji oryginału rozkazu
1	2	3	4	5	6	7	8	9

"prawa strona dokumentu"

Egz. nr (miejsce przeznaczenia)	Pokwitowanie odbioru oryginału rozkazu	Liczba powielonych kopii / Pozycja Dziennika ewidencji	Kopia egz. nr (miejsce przeznaczenia)	Pokwitowanie odbioru kopii rozkazu		Uwagi
	Czytelny podpis i data			Data	Numer pozycji z książki doręczeń / wykazu przesyłek nadanych lub czytelny podpis odbierającego	
10	11	12	13	14	15	16

"o s t a t n i a s t r o n a d o k u m e n t u"

Niniejszy rejestr zawiera . . . . . / . . . . . stron
(słownie)

ponumerowanych, przesznurowanych i opieczętowanych.

. . . . . .
(miejscowość i data)

. . . . . .
(podpis)

Załącznik nr 9

KARTA ZAPOZNANIA Z TECZKĄ

. . . . . .
(sygnatura archiwalna)

Lp.	Stopień, imię i nazwisko	Stanowisko służbowe i nazwa jedn. org.	Cel zapoznania się z materiałami	Data	Podpis

Lp.	Stopień, imię i nazwisko	Stanowisko służbowe i nazwa jedn. org.	Cel zapoznania się z materiałami	Data	Podpis

METRYKA ELEKTRONICZNEGO NOŚNIKA INFORMACJI

. . . . . .

(rodzaj i nr ewidencyjny nośnika)

Do pakietów

Lp.	Nazwa dokumentu lub krótki opis zawartości nośnika	Ilość folderów / Ilość plików	Zajętość nośnika w jm.	Imię i nazwisko osoby utrwalającej informacje	Data i podpis	Adnotacje o zniszczeniu nośnika lub usunięciu pliku / folderu
1	2	3	4	5	6	7