5

ZARZĄDZENIE NR 2020 KOMENDANTA GŁÓWNEGO POLICJI

z dnia 30 grudnia 2010 r.

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

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
Przepisy ogólne

§ 1

Zarządzenie określa:

1) szczególny sposób organizacji kancelarii tajnych, w tym:
   a) sposób tworzenia i likwidacji kancelarii,
   b) podstawowe zadania kancelarii i jej oddziałów;
2) szczególny sposób funkcjonowania kancelarii tajnych, w tym:
   a) podstawowe zadania kierownika kancelarii tajnej,
   b) sposób przeprowadzania okresowych inwentaryzacji materiałów zawierających informacje niejawne oraz ich archiwizowania;
3) szczególny sposób organizacji i funkcjonowania innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za przetwarzanie materiałów niejawnych;
4) sposób i tryb przetwarzania informacji niejawnych w tym:
   a) sposób i tryb prowadzenia urządzeń ewidencyjnych,
   b) sposób i tryb ewidencjonowania materiałów zawierających informacje niejawne,
   c) wzory urządzeń ewidencyjnych i protokołów;
5) sposób i tryb przetwarzania informacji niejawnych na technicznych nośnikach informacji niejawnych, w tym sposób i tryb:
   a) ewidencjonowania, przechowywania i obiegu technicznych nośników informacji niejawnych,
   b) niszczenia i deklasyfikacji technicznych nośników informacji niejawnych;
6) dobór i stosowanie środków bezpieczeństwa fizycznego, w tym:
   a) warunki tworzenia stref ochronnych,
   b) rodzaje i zakres stosowania środków bezpieczeństwa fizycznego,
   c) elementy planu ochrony informacji niejawnych.

§ 2

1. Określenia użyte w zarządzeniu oznaczają:
   1) ustawa – ustawę z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych;
   2) jednostka organizacyjna – jednostkę Policji określoną odrębnymi przepisami regulującymi szczegółowe zasady organizacji i zakres działania komend, komisariatów i innych jednostek organizacyjnych Policji;
   3) komórka organizacyjna – wyodrębnioną część struktury jednostki organizacyjnej Policji;
   4) dokument – każdą utrwaloną informację niejawną;
   5) zbiór dokumentów niejawnych – logicznie uporządkowaną, wyodrębnioną grupę dokumentów niejawnych wraz ze spisem tych dokumentów;
   6) materiał – dokument lub przedmiot albo dowolną ich część chronioną jako informacja niejawna;
   7) pracownik – pracownika zatrudnionego lub policjanta pełniącego służbę w kancelarii lub oddziale kancelarii tajnej oraz innej niż kancelaria tajna komórce organizacyjnej odpowiedzialnej za przetwarzanie materiałów niejawnych;
   8) przesyłka – materiały w postaci odpowiednio zabezpieczonych, zaadresowanych i oznaczonych paczek lub listów;
   9) urządzenia ewidencyjne – rejestry, dzienniki, książki i inne urządzenia służące do ewidencji materiałów niejawnych;
   10) techniczny nośnik informacji niejawnych, zwany dalej „TNIN" – nośnik do którego odczytania bądź zapisania konieczne jest użycie odpowiedniego urządzenia;
   11) użytkownik – osobę z właściwym poświadczeniem bezpieczeństwa osobowego, posiadającą uprawniony dostęp do technicznych nośników informacji niejawnych lub do zasobów systemu, w którym są przetwarzane informacje niejawne;
   12) dysk twardy zwany dalej „HDD" – jeden z typów urządzeń pamięci masowej, wykorzystujący nośnik magnetyczny do przekazania danych;
   13) urządzenie pamięci masowej, zwane dalej „SSD" – urządzenie służące do przechowy-

wania danych zbudowane w oparciu o pamięć typu flash;

14) technologia MagnetoOptyczna zwana dalej „MO" – urządzenie wykorzystujące połączenia technologii magnetycznego i optycznego zapisu danych.

2. Ilekroć w zarządzeniu jest mowa o kancelarii tajnej, jeżeli przepisy zarządzania nie stanowią inaczej, należy przez to rozumieć oddział kancelarii tajnej, a także inną niż kancelaria tajna komórkę organizacyjną odpowiedzialną za przetwarzanie materiałów niejawnych.

§ 3

W kancelarii tajnej mogą być przetwarzane informacje niejawne o klauzuli „poufne" lub „zastrzeżone", za zgodą kierownika jednostki organizacyjnej.

Rozdział 2
Organizacja kancelarii tajnej

§ 4

1. Kancelarię tajną, zwaną dalej „kancelarią", tworzy kierownik jednostki organizacyjnej, w której są wytwarzane, przetwarzane, przekazywane lub przechowywane materiały zawierające informacje niejawne.
2. Kancelaria stanowi wyodrębnioną komórkę organizacyjną pionu ochrony, odpowiedzialną za rejestrowanie, przechowywanie, obieg i wydawanie materiałów osobom uprawnionym, obsługiwaną przez pracowników pionu ochrony, podległą bezpośrednio pełnomocnikowi do spraw ochrony informacji niejawnych, zwanemu dalej „pełnomocnikiem ochrony".
3. Kancelaria, ze względów organizacyjnych, może mieć swoje oddziały tworzone i funkcjonujące zgodnie z zasadami i na warunkach przewidzianych dla kancelarii.
4. Kancelaria, może obsługiwać więcej niż jedną jednostkę organizacyjną lub komórkę organizacyjną.
5. W przypadku uzasadnionym względami organizacyjnymi kierownik jednostki organizacyjnej może utworzyć więcej niż jedną kancelarię.
6. Kierownik jednostki organizacyjnej informuje Agencję Bezpieczeństwa Wewnętrznego o utworzeniu lub likwidacji kancelarii tajnej, z określeniem klauzuli tajności przetwarzanych w niej informacji niejawnych.

§ 5

Do podstawowych zadań wykonywanych w kancelarii należy:

1) przyjmowanie, ewidencjonowanie, przechowywanie, wydawanie, udostępnianie, przekazywanie i wysyłanie materiałów niejawnych;
2) prowadzenie urządzeń ewidencyjnych;
3) zapewnienie należytej ochrony materiałom niejawnym znajdującym się w kancelarii;
4) powiadamianie adresata o otrzymaniu dokumentu niejawnego;
5) przekazywanie lub udostępnianie, za pokwitowaniem, dokumentów niejawnych do właściwych jednostek lub komórek organizacyjnych albo dla pracowników oraz sprawowanie bieżącej kontroli postępowania z tymi dokumentami, a także egzekwowanie ich zwrotu;
6) przyjmowanie i rejestrowanie dokumentów niejawnych powielonych;
7) gromadzenie przepisów niejawnych oraz prowadzenie i aktualizowanie dziennika przepisów, a także udostępnianie i wydawanie przepisów;
8) odnotowywanie na dokumentach zawierających informacje niejawne oraz w urządzeniach ewidencyjnych zmiany lub zniesienia klauzuli tajności;
9) zwracanie wykonawcom dokumentów w celu ich uzupełnienia w przypadkach, gdy nie spełniają określonych wymogów;
10) realizacja czynności związanych z obowiązkiem rozliczania się policjantów i pracowników z posiadanych przez nich dokumentów niejawnych w przypadku rozwiązania stosunku służbowego lub stosunku pracy, przeniesienia lub delegowania do służby lub pracy w innej jednostce lub komórce organizacyjnej albo delegowania do służby lub pracy poza Policją;
11) rozliczanie wszystkich pozycji w prowadzonych urządzeniach ewidencyjnych; sporządzanie w razie potrzeby, wykazów dokumentów pobranych z kancelarii przez pracowników lub funkcjonariuszy komórek organizacyjnych, w celu ułatwienia rozliczenia dokumentów w urządzeniach ewidencyjnych;
12) przygotowywanie dokumentów niejawnych znajdujących się w kancelarii, w celu przekazania do archiwum lub składnicy akt Policji.

§ 6

1. W przypadku likwidacji kancelarii pełnomocnik ochrony powołuje komisję likwidacyjną i powiadamia o tym kierowników obsługiwanych komórek organizacyjnych.
2. W skład komisji wchodzi kierownik likwidowanej kancelarii lub pracownik wyznaczony do kierowania likwidowanym oddziałem kancelarii.
3. Do zadań komisji likwidacyjnej należy w szczególności:
   1) dokonanie przeglądu urządzeń ewidencyjnych prowadzonych w kancelarii, w celu porównania stanu faktycznego znajdujących się w kancelarii dokumentów niejawnych, pieczęci i stempli, ze stanem ewidencyjnym;
   2) wyszczególnienie nierozliczonych pozycji w urządzeniach ewidencyjnych;

3) wyszczególnienie dokumentów niejawnych, stanowiących dokumentację niearchiwalną kategorii „BC" oraz sporządzenie protokołów ich brakowania;
4) wyszczególnienie dokumentów niejawnych spraw zakończonych na dzień likwidacji kancelarii, ich opracowanie oraz sporządzenie spisów akt przekazanych zawierających informacje niejawne, w sposób określony w odrębnych przepisach dotyczących działalności archiwalnej w Policji;
5) przekazanie protokolarne teczek i dokumentów niejawnych, będących w realizacji wyznaczonemu następcy prawnemu;
6) przekazanie teczek dokumentów niejawnych, ostatecznie zakończonych do właściwego archiwum lub składnicy akt Policji;
7) rozliczenie i przekazanie na podstawie odrębnych przepisów dotyczących działalności archiwalnej w Policji, do archiwum lub składnicy akt Policji, prowadzonych urządzeń ewidencyjnych.

4. Komisja likwidacyjna sporządza protokół likwidacyjny w dwóch jednobrzmiących egzemplarzach, w którym zawiera informacje z przeprowadzonych czynności wskazanych w ust. 3. Pierwszy egzemplarz protokołu przekazuje pełnomocnikowi ochrony, drugi – wyznaczonemu następcy prawnemu, a w razie jego braku – do właściwego archiwum lub składnicy akt Policji.

Rozdział 3
Funkcjonowanie kancelarii tajnej

§ 7

1. Kancelarią kieruje kierownik kancelarii, zatrudniony przez kierownika jednostki organizacyjnej na wniosek pełnomocnika ochrony.
2. Kierownik kancelarii podlega pełnomocnikowi ochrony.
3. Oddziałem kancelarii kieruje pracownik wyznaczony przez kierownika kancelarii, w uzgodnieniu z pełnomocnikiem ochrony.

§ 8

Do zadań kierownika kancelarii należy w szczególności:
1) nadzór nad obiegiem dokumentów niejawnych w zakresie działania kancelarii;
2) organizowanie i koordynowanie pracy kancelarii oraz planowanie zadań;
3) prowadzenie okresowych kontroli w zakresie postępowania pracowników kancelarii z dokumentami niejawnymi, znajdującymi się w kancelarii;
4) przeprowadzanie okresowej kontroli stanu dokumentów niejawnych, znajdujących się w kancelarii;
5) egzekwowanie zwrotu dokumentów niejawnych;
6) informowanie pełnomocnika ochrony o zagrożeniach ujawnienia, utraty lub zagubienia dokumentów niejawnych, wynikających z nieprzestrzegania obowiązujących w tym zakresie przepisów bądź innych nieprawidłowościach związanych z ochroną informacji niejawnych;
7) nadzór nad właściwym oznaczaniem i ewidencjonowaniem dokumentów niejawnych, prowadzeniem urządzeń ewidencyjnych, odnotowywaniem zmiany lub zniesienia klauzuli tajności dokumentów niejawnych w urządzeniach ewidencyjnych;
8) nadzór nad wykorzystywaniem stempli i pieczęci znajdujących się na wyposażeniu kancelarii;
9) nadzór i koordynacja zadań, związanych z przekazywaniem do archiwum lub składnicy akt Policji dokumentów niejawnych, oraz ocena protokołów brakowania dokumentacji niearchiwalnej kategorii „BC", polegająca w szczególności na porównaniu dokumentów przeznaczonych do brakowania, z zapisami zawartymi w protokole brakowania, a w uzasadnionych przypadkach z zapisami w urządzeniach ewidencyjnych.

§ 9

1. W przypadku zmiany na stanowisku kierownika kancelarii sporządza się protokół zdawczo-odbiorczy w dwóch jednobrzmiących egzemplarzach; pierwszy przechowywany jest w kancelarii, drugi – u pełnomocnika ochrony.
2. W przypadku zmiany pracownika wyznaczonego do kierowania oddziałem kancelarii sporządza się protokół zdawczo-odbiorczy w dwóch jednobrzmiących egzemplarzach; pierwszy przechowywany jest u pracownika przejmującego obowiązki, drugi – u kierownika kancelarii.
3. W przypadku zmiany na stanowisku kierownika innej niż kancelaria tajna komórki organizacyjnej odpowiedzialnej za przetwarzanie materiałów niejawnych sporządza się protokół zdawczo-odbiorczy w dwóch jednobrzmiących egzemplarzach; pierwszy przechowywany jest w innej niż kancelaria tajna komórce organizacyjnej odpowiedzialnej za przetwarzanie materiałów niejawnych, drugi – u kierownika komórki organizacyjnej.
4. Protokół, o którym mowa w ust. 1 i 2, powinien zawierać w szczególności:
   1) dane o urządzeniach ewidencyjnych, na podstawie których dokonano sprawdzenia stanu faktycznego dokumentów pozostających w ewidencji kancelarii lub oddziału kancelarii oraz pozycje zapisów w tych urządzeniach;

2) informacje dotyczące zgodności stanu ewidencyjnego przekazywanych urządzeń ewidencyjnych w porównaniu ze stanem faktycznym;
3) informacje dotyczące zgodności stanu faktycznego dokumentów ze stanem ewidencyjnym;
4) uwagi lub wnioski dotyczące ujawnionych nieprawidłowości w zakresie ewidencjonowania i obiegu dokumentów;
5) ewentualne informacje, dotyczące dokumentów, innych niż wymienione w pkt 1-4.

4. Wzór protokołu zdawczo-odbiorczego określa załącznik nr 1 do zarządzenia.
5. Przekazanie obowiązków, urządzeń ewidencyjnych, dokumentów niejawnych i innych materiałów, znajdujących się w kancelarii, odbywa się w obecności pełnomocnika ochrony – w przypadku przekazywania obowiązków przez kierownika kancelarii, bądź w obecności kierownika kancelarii – w przypadku przekazywania obowiązków przez pracownika wyznaczonego do kierowania oddziałem kancelarii, z zastrzeżeniem ust. 7 i 8.
6. Przekazanie obowiązków, urządzeń ewidencyjnych, dokumentów niejawnych i innych materiałów, znajdujących się w innej niż kancelaria tajna komórki organizacyjnej odpowiedzialnej za przetwarzanie materiałów niejawnych, odbywa się w obecności kierownika komórki organizacyjnej – w przypadku przekazywania obowiązków przez kierownika kancelarii.
7. W przypadku, gdy pełnomocnik ochrony nie uczestniczy w czynnościach, o których mowa w ust. 5, kierownik jednostki organizacyjnej powołuje komisję w celu przekazania obowiązków kierownika kancelarii. Protokół zdawczo-odbiorczy zatwierdza kierownik jednostki organizacyjnej.
8. Jeżeli kierownik kancelarii nie uczestniczy w czynnościach, o których mowa w ust. 5, pełnomocnik ochrony powołuje komisję w celu przekazania obowiązków pracownika wyznaczonego do kierowania oddziałem kancelarii. Protokół zdawczo-odbiorczy zatwierdza pełnomocnik ochrony.

§ 10

1. W przypadku czasowej nieobecności kierownika kancelarii jego obowiązki przejmuje, po powiadomieniu pełnomocnika ochrony, upoważniony pracownik kancelarii lub inny pracownik pionu ochrony. W razie ich braku kancelarię przejmuje protokolarnie inny pracownik wyznaczony przez kierownika jednostki lub komórki organizacyjnej po powiadomieniu pełnomocnika ochrony, posiadający stosowne poświadczenie bezpieczeństwa i przeszkolony w zakresie ochrony informacji niejawnych.
2. W przypadku, gdy nieobecność kierownika kancelarii przekracza 6 miesięcy, przekazanie obowiązków kierownika kancelarii pracownikowi, o którym mowa w ust. 1, odbywa się na zasadach, o których mowa w § 9.

§ 11

1. W celu dokonania okresowej kontroli ewidencji materiałów i obiegu dokumentów niejawnych kierownik jednostki organizacyjnej lub pełnomocnik ochrony, w terminie do dnia 31 stycznia każdego roku, w drodze decyzji powołuje komisję do spraw inwentaryzacji materiałów niejawnych, zwaną dalej „komisją".
2. W skład komisji nie powinny wchodzić osoby prowadzące urządzenia ewidencyjne jednostki lub komórki organizacyjnej, w której prowadzona jest inwentaryzacja.
3. Komisje, w terminie do dnia 15 marca każdego roku, przeprowadzają w swoich jednostkach i komórkach organizacyjnych kontrolę zgodności stanu faktycznego dokumentacji niejawnej ze stanem ewidencyjnym, za rok poprzedni określony w decyzji, o której mowa w ust. 1.
4. Inwentaryzacji mogą podlegać również materiały i dokumenty zaewidencjonowane w latach poprzedzających okres rozliczeniowy.

§ 12

Policjanci i pracownicy jednostek i komórek organizacyjnych sporządzają wykazy materiałów niejawnych pozostających w ich dyspozycji, które po podpisaniu przez sporządzającego i bezpośredniego przełożonego, przekazuje się komisji.

§ 13

1. Komisja dokonuje porównania zapisów w sporządzonych przez policjantów lub pracowników Policji wykazach z zapisami w ewidencjach prowadzonych w kancelarii, sprawdzając:
   1) czy w dyspozycji policjantów lub pracowników Policji znajdują się materiały niejawne niebędące na ich stanie ewidencyjnym;
   2) czy wykazy zawierają wszystkie materiały niejawne pozostające w ich dyspozycji.
2. Komisja sprawdza dokumenty, pozostające w dyspozycji policjantów lub pracowników Policji w celu stwierdzenia, czy liczba stron dokumentu lub innych jednostek miary oraz liczba egzemplarzy i jego ewentualnych załączników jest zgodna z zapisami w dokumencie i odpowiednich urządzeniach ewidencyjnych.
3. W przypadku stwierdzenia niezgodności zapisów komisja podejmuje czynności w celu wyjaśnienia przyczyn zaistniałych rozbieżności.

§ 14

1. Komisja po zakończeniu czynności inwentaryzacyjnych sporządza w dwóch egzemplarzach pro-

tokół, zawierający w szczególności informacje dotyczące:

1) zgodności stanu ewidencyjnego materiałów ze stanem faktycznym;
2) liczby materiałów objętych inwentaryzacją, odrębnie dla każdej klauzuli tajności;
3) stwierdzonych nieprawidłowości i podjętych w związku z tym czynności.

2. Komisja przekazuje w terminie do dnia 31 marca każdego roku jeden egzemplarz protokołu, o którym mowa w ust. 1, pełnomocnikowi ochrony, a drugi pozostaje w jednostce lub komórce organizacyjnej.

§ 15

Pełnomocnik ochrony w terminie do dnia 31 maja każdego roku przedstawia kierownikowi jednostki organizacyjnej do zatwierdzenia sprawozdanie z przeprowadzonych w jednostce i komórkach organizacyjnych czynności inwentaryzacyjnych.

§ 16

Dokumenty i zbiory dokumentów, dotyczące spraw ostatecznie zakończonych, mogą być przechowywane w kancelarii lub innym wydzielonym pomieszczeniu, zapewniającym ich ochronę odpowiednio do przyznanej im klauzuli tajności nie dłużej niż 2 lata. Po upływie tego okresu przekazuje się je do archiwum lub składnicy akt Policji, na podstawie spisów akt przekazanych, z wyjątkiem akt spraw operacyjno-rozpoznawczych, które powinny być przekazywane po zakończeniu sprawy.

§ 17

1. Policjanci i pracownicy jednostek i komórek organizacyjnych, przekazują sprawy ostatecznie zakończone zawierające informacje niejawne do kancelarii, po uporządkowaniu zbioru dokumentów zgodnie z odrębnymi przepisami o działalności archiwalnej w Policji, w szczególności po sporządzeniu spisu zawartości teczki oraz dokonaniu kwalifikacji i klasyfikacji zgodnie z Jednolitym Rzeczowym Wykazem Akt Policji.
2. W przypadku zaistnienia wątpliwości, czynności, o których mowa w ust. 1, powinny być wykonywane w uzgodnieniu z pracownikiem archiwum lub składnicy akt Policji.
3. Wszystkie dokumenty, zarejestrowane w urządzeniach ewidencyjnych kancelarii, bez względu na dokonane na nich skreślenia i adnotacje dotyczące zniesienia lub zmiany klauzuli tajności podlegają rozliczeniu w kancelarii.

Rozdział 4
Organizacja i funkcjonowanie innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za przetwarzanie materiałów niejawnych

§ 18

1. W Centralnym Biurze Śledczym Komendy Głównej Policji lub Biurze Spraw Wewnętrznych Komendy Głównej Policji mogą być tworzone inne niż kancelaria tajna komórki organizacyjne odpowiedzialne za przetwarzanie materiałów niejawnych, zorganizowane i funkcjonujące w następujący sposób:
   1) stan organizacyjno-etatowy innej niż kancelaria tajna komórki organizacyjne odpowiedzialnej za przetwarzanie materiałów niejawnych określi Komendant Główny Policji, na wniosek Dyrektora Centralnego Biura Śledczego Komendy Głównej Policji lub Dyrektora Biura Spraw Wewnętrznych Komendy Głównej Policji, po zasięgnięciu opinii pełnomocnika ochrony;
   2) podlegają Dyrektorowi Centralnego Biura Śledczego Komendy Głównej Policji lub Dyrektorowi Biura Spraw Wewnętrznych Komendy Głównej Policji, a w komórkach terenowych tych biur – kierownikom tych komórek;
   3) nie działają w ramach pionu ochrony;
   4) są kierowane przez kierownika komórki, wyznaczonego przez Komendanta Głównego Policji na wniosek Dyrektora Centralnego Biura Śledczego Komendy Głównej Policji lub Biura Spraw Wewnętrznych Komendy Głównej Policji, uzgodniony z pełnomocnikiem ochrony;
   5) w uzasadnionych przypadkach obowiązki kierownika innej niż kancelaria tajna komórki organizacyjnej odpowiedzialnej za przetwarzanie materiałów niejawnych, o których mowa w § 8 pkt 9, mogą być wykonywane przez pracownika wyznaczonego pisemnie przez Dyrektora Centralnego Biura Śledczego Komendy Głównej Policji lub Dyrektora Biura Spraw Wewnętrznych Komendy Głównej Policji;
   6) kontrolę realizacji zadań komórki zapewnia pełnomocnik ochrony;
   7) pracownika komórki wyznacza Dyrektor Centralnego Biura Śledczego Komendy Głównej Policji lub Dyrektor Biura Spraw Wewnętrznych Komendy Głównej Policji na wniosek kierownika właściwej komórki organizacyjnej Centralnego Biura Śledczego Komendy Głównej Policji i Biura Spraw Wewnętrznych Komendy Głównej Policji, w uzgodnieniu z pełnomocnikiem ochrony;
   8) pracownik innej niż kancelaria tajna komórki organizacyjnej odpowiedzialnej za przetwa-

rzanie materiałów niejawnych powinien spełniać, warunki określone w art. 16 ustawy, dla pracownika pionu ochrony;

9) inne niż kancelaria tajna komórki organizacyjne odpowiedzialne za przetwarzanie materiałów niejawnych, spełniają warunki przetwarzania materiałów niejawnych, o których mowa w art. 43 ust. 1 ustawy, oraz warunki fizycznego bezpieczeństwa informacji niejawnych, o których mowa w art. 46 w związku z art. 44 ust. 2 ustawy;
10) w razie likwidacji komórki, w skład komisji likwidacyjnej wchodzi przedstawiciel pionu ochrony wskazany przez pełnomocnika ochrony.

2. Inne niż kancelaria tajna komórki organizacyjne odpowiedzialne za przetwarzanie materiałów niejawnych mogą być tworzone w komendach wojewódzkich (Stołecznej) Policji, komendach powiatowych (miejskich, rejonowych) Policji, komisariatach Policji i komisariatach specjalistycznych Policji, oddziałach prewencji Policji, samodzielnych pododdziałach prewencji Policji, samodzielnych pododdziałach antyterrorystycznych Policji przy czym:
   1) utworzenie i ustalenie stanu organizacyjno-etatowego komórki nastąpi w porozumieniu z:
      a) Komendantem Głównym Policji, po wyrażeniu opinii przez pełnomocnika Komendanta Głównego Policji do spraw ochrony informacji niejawnych – w komendach wojewódzkich (Stołecznej) Policji,
      b) komendantem wojewódzkim Policji po wyrażeniu opinii przez pełnomocnika komendanta wojewódzkiego (Stołecznego) Policji do spraw ochrony informacji niejawnych – w pozostałych jednostkach organizacyjnych Policji;
   2) kontrolę realizacji zadań innej niż kancelaria tajna komórki organizacyjnej odpowiedzialnej za przetwarzanie materiałów niejawnych zapewnia pełnomocnik ochrony;
   3) pracownik innej niż kancelaria tajna komórki organizacyjnej odpowiedzialnej za przetwarzanie materiałów niejawnych powinien spełniać, warunki określone w art. 16 ustawy, dla pracownika pionu ochrony;
   4) inne niż kancelaria tajna komórki organizacyjne odpowiedzialne za przetwarzanie materiałów niejawnych spełniają warunki przetwarzania materiałów niejawnych, o których mowa w art. 43 ust. 1 ustawy oraz warunki fizycznego bezpieczeństwa informacji niejawnych, o których mowa w art. 46 w związku z art. 44 ust. 2 ustawy;
   5) w razie likwidacji innej niż kancelaria tajna komórki organizacyjnej odpowiedzialnej za przetwarzanie materiałów niejawnych, w skład komisji likwidacyjnej wchodzi przedstawiciel pionu ochrony wskazany przez pełnomocnika ochrony.

Rozdział 5
Przetwarzanie informacji niejawnych

§ 19

1. W kancelarii prowadzi się następujące urządzenia ewidencyjne:
   1) rejestr dzienników, książek ewidencyjnych i teczek, którego wzór określa załącznik nr 2 do zarządzenia;
   2) dziennik ewidencji, którego wzór określa załącznik nr 3 do zarządzenia;
   3) książkę doręczeń przesyłek miejscowych, której wzór określa załącznik nr 4 do zarządzenia;
   4) wykaz przesyłek nadanych, którego wzór określa załącznik nr 5 do zarządzenia;
   5) dziennik podawczy, którego wzór określa załącznik nr 6 do zarządzenia;
   6) dziennik ewidencji wydanych materiałów kancelaryjnych, zwany dalej DEWMK;
   7) dziennik przepisów.
2. W przypadkach uzasadnionych organizacją ochrony informacji niejawnych kancelaria może prowadzić odrębne urządzenia ewidencyjne, o których mowa w ust. 1 pkt 2, dla dokumentów oznaczonych różnymi klauzulami tajności.
3. Kancelaria może, w razie potrzeby, prowadzić odrębne urządzenia ewidencyjne dla poszczególnych komórek organizacyjnych lub dokumentów o określonym zakresie tematycznym. Przepis ust. 2 może być stosowany odpowiednio.
4. W przypadku wprowadzenia odrębnych urządzeń ewidencyjnych dla dokumentów oznaczonych różnymi klauzulami tajności, urządzenia ewidencyjne dla dokumentów oznaczonych klauzulą „ściśle tajne" oraz „tajne" oznacza się klauzulą „POUFNE", urządzenia ewidencyjne dla dokumentów oznaczonych klauzulą „poufne" i „zastrzeżone" oznacza się odpowiednio klauzulą „ZASTRZEŻONE".
5. Kancelaria może prowadzić inne urządzenia ewidencyjne niż wymienione w ust. 1, których wzór oraz klauzule tajności określa kierownik kancelarii.

§ 20

1. Wpisów do urządzeń ewidencyjnych, o których mowa w § 19 ust. 1 i 5 dokonuje się atramentem lub tuszem koloru czarnego lub niebieskiego, a ich zmianę lub anulowanie kolorem czerwonym, z datą i czytelnym podpisem pracownika dokonującego zmiany lub anulowania.

2. W przypadku anulowania pozycji w urządzeniach ewidencyjnych określonych w § 19 ust. 1 i 5 należy odnotować powód anulowania.
3. Zniesienie lub zmianę klauzuli tajności dokumentu niejawnego odnotowuje się we właściwych urządzeniach ewidencyjnych i na dokumentach, podając jednocześnie podstawę dokonania tej czynności.
4. Wpisy do urządzeń ewidencyjnych nie mogą być wycierane lub zamazywane.
5. Rejestrację dokumentów w urządzeniu ewidencyjnym, o którym mowa w § 19 ust. 1 pkt 1, należy rozpocząć od pierwszej pozycji w każdym kolejnym roku kalendarzowym.

§ 21

1. Urządzenia ewidencyjne określone w § 19 ust. 1 pkt 2, 3, 5-7 i ust. 5 podlegają zarejestrowaniu w rejestrze dzienników książek ewidencyjnych i teczek, który jest nadrzędnym urządzeniem ewidencyjnym w stosunku do innych urządzeń prowadzonych przez kancelarię i nie podlega ewidencjonowaniu.
2. Urządzenia ewidencyjne, o których mowa w § 19 ust. 1 pkt 2, 3, 5-7 i ust. 5, oraz ich kolejne tomy rejestruje się pod odrębnymi pozycjami.

§ 22

1. Informację o zarejestrowaniu urządzenia ewidencyjnego, o którym mowa w § 19, w rejestrze dzienników, książek ewidencyjnych i teczek odnotowuje się na karcie tytułowej tego urządzenia.
2. W lewym górnym rogu karty tytułowej urządzenia umieszcza się pieczęć z nazwą jednostki lub komórki organizacyjnej.
3. Strony lub karty urządzenia ewidencyjnego numeruje się, przeszywa, na ostatniej stronie urządzenia umieszcza się adnotację o sumarycznej ilości stron, opieczętowuje się pieczęcią „do pakietów", a osoba dokonująca zarejestrowania urządzenia w rejestrze dzienników, książek ewidencyjnych i teczek składa swój czytelny podpis oraz wpisuje datę zarejestrowania urządzenia.
4. W urządzeniach ewidencyjnych, zaznacza się początek i koniec roku kalendarzowego, a po zakończeniu roku dokonuje się adnotacji, na jakiej pozycji zakończono ewidencję dokumentów, potwierdzając ją datą i czytelnym podpisem kierownika kancelarii.
5. W urządzeniu ewidencyjnym, o którym mowa w § 19 ust. 1 pkt 2, w prawym górnym i dolnym rogu karty tytułowej i okładki umieszcza się odpowiednią klauzulę tajności.
6. Czynności, o których mowa w ust. 2-4, dokonuje się także w stosunku do urządzeń ewidencyjnych, o których mowa w § 19 ust. 1 pkt 2, 3 i 5-7 i ust. 5.

§ 23

Obieg dokumentów odnotowuje się, prowadząc ich ewidencję. Powinna ona odzwierciedlać:
1) przekazywanie dokumentów w obiegu wewnątrz jednostki lub komórki organizacyjnej;
2) przekazywanie dokumentów w obiegu zewnętrznym;
3) sposób ewidencjonowania dokumentów przez kancelarię.

§ 24

1. Przyjęcie w kancelarii przesyłek obejmuje:
   1) odebranie przesyłek od kuriera poczty specjalnej lub od innego przewoźnika;
   2) porównanie stanu faktycznego przesyłek z ich ewidencją w wykazie przesyłek nadanych;
   3) sprawdzenie prawidłowości zaadresowania i oznakowania zgodnie z przepisami oraz sprawdzenie stanu opakowania przesyłki w następujący sposób:
      a) w przypadku przyjmowania przesyłek na podstawie wykazu przesyłek nadanych – potwierdzenie podpisem, zapisem liczbowym i słownym liczby przyjętych przesyłek oraz odciskiem pieczęci „do pakietów",
      b) w przypadku przyjmowania przesyłki na podstawie książki doręczeń przesyłek miejscowych – porównanie jej numeru z numerem wykazanym w książce, pokwitowanie przyjęcia podpisem, datą i odciskiem okrągłej pieczęci „do pakietów";
   4) rozpakowanie przesyłek z kopert zewnętrznych;
   5) zaewidencjonowanie przesyłek w prowadzonych urządzeniach ewidencyjnych, ostemplowanie ich pieczęcią wpływu i wpisanie numeru z urządzenia ewidencyjnego oraz daty wpływu;
   6) wpisanie do wykazu przesyłek nadanych numeru z urządzenia ewidencyjnego, pod którym przesyłka została zarejestrowana;
   7) przekazanie przesyłek do kancelarii, które polega na:
      a) porównaniu przez pracownika odbierającego przesyłki stanu faktycznego przesyłek z ich ewidencją w urządzeniach ewidencyjnych, w obecności pracownika kancelarii,
      b) sprawdzeniu prawidłowości adresu, całości opakowania i zgodności numeru pisma na opakowaniu z numerem w urządzeniach ewidencyjnych;
   8) przekazywanie korespondencji pomiędzy kancelariami usytuowanymi w innych obiektach – na podstawie wykazu przesyłek nadanych, lub za książką doręczeń przesyłek miejscowych.

2. Pracownicy kancelarii, odbierający przesyłki powinni posiadać imienne upoważnienia, z podanym numerem pieczęci „do pakietów", podpisane przez pełnomocnika ochrony, zaś pracownik komórki organizacyjnej, o której mowa w § 18, podpisane przez kierownika komórki organizacyjnej.

§ 25

W przypadku stwierdzenia uszkodzenia otrzymanej przesyłki lub śladów jej otwierania pracownik kancelarii, kwitujący odbiór przesyłki sporządza w obecności doręczającego, w trzech jednobrzmiących egzemplarzach, protokół uszkodzenia przesyłki, którego wzór określa załącznik nr 7 do zarządzenia. Pierwszy egzemplarz przekazuje się nadawcy, drugi doręczającemu, a trzeci otrzymuje kancelaria przyjmująca przesyłkę.

§ 26

Wysłanie z kancelarii przesyłek na podstawie wykazu przesyłek nadanych obejmuje:

1) porównanie ilości przesyłek otrzymanych i przeznaczonych do wysłania z ilością pozycji w wykazie przesyłek nadanych;
2) sprawdzenie całości opakowania i prawidłowości oznaczenia oraz zaadresowania przesyłek;
3) zapakowanie przesyłki w kopertę zewnętrzną, i jej zaadresowanie, zabezpieczenie poprzez ostemplowanie pieczęcią do pakietów oraz oklejenie taśmą, a także ostemplowanie pieczęcią nagłówkową i oznaczenie numerem wykazu;
4) wpisanie przesyłki do wykazu przesyłek nadanych sporządzonego w dwóch egzemplarzach;
5) kontrolę ilości przesyłek z ilością pozycji w wykazie przesyłek nadanych;
6) przekazanie całości korespondencji wraz z jednym egzemplarzem wykazu przesyłek nadanych kurierowi poczty specjalnej, który potwierdza jej odbiór podpisem, zapisem liczbowym i słownym liczby przyjętych przesyłek oraz odciskiem pieczęci „do pakietów".

§ 27

1. Przyjęcie przesyłki w kancelarii i oddziałach kancelarii obejmuje:
   1) rozpakowanie przesyłki i sprawdzenie:
      a) zgodności odcisku pieczęci na opakowaniu z nazwą jednostki nadawcy,
      b) zgodności numeru na dokumencie z numerem na opakowaniu lub w książce doręczeń,
      c) zgodności ilości załączników, ich stron lub innych jednostek miary, z ilością wykazaną w piśmie;
   2) ostemplowanie otrzymanego dokumentu niejawnego pieczęcią wpływu na jej pierwszej stronie, wpisanie na niej numeru z urządzenia ewidencyjnego i daty wpływu; każdy z załączników podlega również ostemplowaniu pieczątką „załącznik nr" do pisma;
   3) zaewidencjonowanie dokumentu w dzienniku ewidencji z wpisaniem pozycji z książki doręczeń lub wykazu przesyłek;
   4) przedstawienie dokumentu po zarejestrowaniu adresatowi do zapoznania się i ewentualnie, zgodnie z jego dekretacją, przekazanie pracownikowi merytorycznemu za pokwitowaniem w dzienniku ewidencji, po uprzednim sprawdzeniu czy posiada ważne poświadczenie bezpieczeństwa upoważniające do dostępu do informacji niejawnych oznaczonych odpowiednią klauzulą tajności.
2. W przypadku stwierdzenia nieprawidłowości w wyniku czynności wymienionych w ust. 1 pkt 1, kierownik kancelarii lub pracownik kancelarii sporządza w trzech jednobrzmiących egzemplarzach protokół otwarcia przesyłki, którego wzór określa załącznik 8 do zarządzenia, zawierający opis nieprawidłowości. Pierwszy egzemplarz dołącza się do dokumentu, drugi przesyła nadawcy, a trzeci przechowywany jest w kancelarii.
3. Czynności, o których mowa w ust. 1 pkt 4, dokonuje się wyłącznie w pomieszczeniach kancelarii tajnej lub jej oddziałach.
4. W przypadku zapakowania kilku przesyłek ekspediowanych do jednego adresata w jedną kopertę zewnętrzną, konieczne jest wpisanie – po numerze wykazu – ilości kopert wewnętrznych.

§ 28

1. W przypadku nieobecności osoby, która pobrała dokumenty z kancelarii, dopuszcza się komisyjne otwarcie szafy, w której dokumenty te są przechowywane. Decyzję o jej komisyjnym otwarciu podejmuje przełożony pracownika lub upoważniona przez niego osoba.
2. Z czynności, o której mowa w ust. 1, sporządza się protokół otwarcia szafy w trzech jednobrzmiących egzemplarzach, którego wzór określa załącznik nr 9 do zarządzenia. Pierwszy egzemplarz protokołu, przechowywany jest w szafie dysponenta dokumentu, drugi u jego bezpośredniego przełożonego, a trzeci w kancelarii.

§ 29

1. Dla każdego dokumentu o klauzuli „ściśle tajne" i „tajne", z chwilą zarejestrowania po raz pierwszy w jednostce organizacyjnej Policji zakłada się „Kartę zapoznania się z dokumentem", wpisując numer, pod którym dokument został zarejestrowany we właściwym urządzeniu ewidencyjnym. Kartę dołącza się do dokumentu, przechowuje wraz z dokumentem w jednostce organizacyjnej i nie przekazuje w przypadku wysłania dokumentu poza jednostkę organizacyjną.

2. Kartę archiwizuje się i brakuje wraz z dokumentem, do którego została założona, a w przypadku przekazania dokumentu do innej jednostki organizacyjnej karta zapoznania się z dokumentem podlega brakowaniu.
3. Kartę zapoznania można założyć do dokumentu, zawierającego informacje oznaczone klauzulą „poufne".
4. Do zbioru dokumentów załącza się jedną kartę zapoznania się z dokumentem.
5. Wzór karty zapoznania z dokumentem zawierającym informacje niejawne określają odrębne przepisy.

§ 30

1. W przypadku otrzymania przesyłki oznaczonej „Do rąk własnych" pracownik obowiązany jest do zarejestrowania jej w dzienniku ewidencji, wpisując: nadawcę, numer i datę wpływu, a w rubryce „Informacje uzupełniające/Uwagi" adnotację, że przesyłka była przeznaczona „Do rąk własnych". Przesyłkę po zarejestrowaniu przekazuje się bezpośrednio adresatowi lub osobie przez niego upoważnionej, za pokwitowaniem w dzienniku ewidencji.
2. Na opakowaniu przesyłek, o których mowa w ust. 1, odciska się pieczęć wpływu i wpisuje numer z dziennika ewidencji oraz datę wpływu przesyłki.
3. Przesyłkę, po wykorzystaniu adresat lub osoba upoważniona zwraca do kancelarii w stanie otwartym lub zamkniętym. Jeżeli przesyłka zwracana jest otwarta, pracownik kancelarii uzupełnia pozostałe rubryki w dzienniku ewidencji i odciska pieczęć wpływu bezpośrednio na dokumencie oraz ostemplowuje załączniki. Jeżeli przesyłka zwracana jest w stanie zamkniętym – osoba zwracająca przesyłkę zobowiązana jest:
   1) udzielić informacji czego dokument dotyczy;
   2) podać liczbę stron lub innych jednostek miary dokumentu;
   3) podać liczbę załączników oraz liczbę ich stron lub innych jednostek miary;
   4) odcisnąć pieczęć wpływu i wpisać wymagane informacje (datę wpływu, numer nadany w dzienniku ewidencji, ostemplować dołączone załączniki).

§ 31

1. Po godzinach pracy kancelarii przesyłki przyjmuje służba dyżurna jednostki organizacyjnej. Przesyłki te przekazuje się do kancelarii niezwłocznie po rozpoczęciu przez nią pracy.
2. O przyjęciu przesyłki „pilnej" lub „bardzo pilnej" służba dyżurna jednostki organizacyjnej zawiadamia jej adresata lub osobę przez niego upoważnioną; w przypadku przekazania przesyłki adresatowi lub osobie przez niego upoważnionej – informuje o tym kancelarię niezwłocznie po rozpoczęciu przez nią pracy. W tym przypadku obowiązek dostarczenia przesyłki do zarejestrowania spoczywa na adresacie lub osobie przez niego upoważnionej do odbioru.
3. Przesyłki pilne, telegramy i szyfrogramy doręcza się adresatom niezwłocznie po zarejestrowaniu. Przy kwitowaniu odbioru tych przesyłek odnotowuje się godzinę doręczenia.

§ 32

1. Ewidencjonowanie w kancelarii dokumentów niejawnych odbieranych ze Stacji Szyfrów w jednostce organizacyjnej obejmuje:
   1) sprawdzenie w obecności dyżurnego szyfranta prawidłowości zaadresowania, nadania numeru i liczby stron szyfrogramu;
   2) potwierdzenie odbioru szyfrogramu własnoręcznym podpisem w książce doręczeń szyfrogramów przez osobę upoważnioną z odnotowaniem godziny odbioru.
2. Pozostałe czynności dotyczące ewidencjonowania należy wykonywać zgodnie z przepisami § 27 ust. 1 pkt 2 i 3.
3. Po dokonaniu ewidencji szyfrogram należy niezwłocznie doręczyć adresatowi.

§ 33

1. Ewidencjonując w kancelarii dokumenty wysyłane, przed ich przyjęciem do wysłania i przed zarejestrowaniem w dzienniku, sprawdza się czy dokument:
   1) posiada właściwą sygnaturę literowo-cyfrową;
   2) posiada właściwy adres;
   3) posiada rozdzielnik;
   4) zawiera dane wykonawcze – nazwisko lub inne dane identyfikujące osobę sporządzającą i wykonującą dokument oraz ilość wykonanych egzemplarzy;
   5) wytworzono w takiej liczbie, jaką podano w rozdzielniku (dotyczy to również załączników);
   6) zawiera dane określające faktyczną liczbę załączników, stron lub innych jednostek miary załączników.
2. Ewidencjonowanie dokumentów wysyłanych odbywa się na zasadach określonych dla korespondencji otrzymanej, używa się pieczęci nagłówkowej oraz w odpowiednich rubrykach dziennika ewidencji wpisuje się adresata, liczbę stron lub innych jednostek miary dokumentu, liczbę załączników oraz liczbę stron lub innych jednostek miary załączników.
3. Po zaewidencjonowaniu przesyłkę zapakowaną w kopertę wewnętrzną należy wpisać do wykazu przesyłek nadanych, sporządzonego w dwóch egzemplarzach lub w trzech – jeżeli jednostka lub komórka organizacyjna znajduje się w innym obiekcie – i przekazać ją do kance-

larii lub oddziału kancelarii. W obiegu wewnętrznym oraz w szczególnie uzasadnionych przypadkach przekazywania przesyłki pomiędzy kancelariami usytuowanymi w innych obiektach odbywa się na podstawie książki doręczeń przesyłek miejscowych. Numer i pozycję z wykazu przesyłek lub książki doręczeń należy odnotować we właściwej rubryce dziennika ewidencji.

4. Jeśli dokument został sporządzony w jednym egzemplarzu przy jego wysyłce w rubryce „Informacje uzupełniające/Uwagi" należy dokonać wpisu o treści „tylko adresat".
5. W przypadku odłączenia od pisma przewodniego jednego lub więcej załączników, w rubryce „Informacje uzupełniające/Uwagi" dziennika ewidencji zamieszcza się adnotację, zawierającą jedną z następujących informacji:
   1) „załączniki odesłano przy piśmie nr ....." (należy podać numer z dziennika ewidencji, za którym przesłano pismo wraz z załącznikami);
   2) „załącznik nr ..... odesłano przy piśmie nr ....." (należy podać, który załącznik odesłano oraz jakim numerem oznaczono pismo w dzienniku ewidencji).

§ 34

Wadliwe wydruki, odbitki, klisze, matryce, kalki oraz brudnopisy powstałe w toku prac nad dokumentem niejawnym, osoba sporządzająca niszczy niezwłocznie, w sposób uniemożliwiający ich odczytanie lub odtworzenie.

§ 35

1. Wykonywanie kopii, odpisów, wypisów, wyciągów oraz tłumaczeń dokumentu niejawnego następuje na pisemne zlecenie sporządzającego dokument lub adresata, odnotowane na tym dokumencie lub odnotowane w zleceniu i wykonywane w warunkach gwarantujących ochronę informacji niejawnych. Wykonane kopie, odpisy, wypisy, wyciągi oraz tłumaczenia dokumentów ewidencjonuje się w dzienniku ewidencji.
2. Dokumenty, o których mowa w ust. 1, mogą być wykonywane wyłącznie przez osoby uprawnione do dostępu do informacji niejawnych.
3. W przypadku wykonywania kopii materiałów, stanowiących zbiór dokumentów (ponumerowanych i opisanych) dopuszcza się nadanie na cały zbiór jednego numeru z dziennika ewidencyjnego, który umieszcza się na obwolucie i pierwszym rejestrowanym dokumencie ze zbioru.
4. W przypadku wyłączenia przed kopiowaniem jakiegokolwiek dokumentu ze zbioru dokumentów, zbiór ten należy traktować jako odrębne dokumenty, z których każdy podlega odrębnej rejestracji w dzienniku ewidencyjnym.
5. Zgodność kopii z oryginałem potwierdza podpisem, na ostatniej stronie dokumentu lub zbioru dokumentów, kierownik jednostki lub komórki organizacyjnej albo inna osoba pisemnie przez nich upoważniona.

§ 36

1. Dokument niejawny otrzymany, mylnie skierowany, nie podlega rejestracji w kancelarii i powinien być zwrócony nadawcy.
2. Dokument niejawny otrzymany, mylnie skierowany, z błędnie zaadresowaną wewnętrzną kopertą, kancelaria lub oddział kancelarii, zwraca nadawcy łącznie z pierwotnym opakowaniem.

Rozdział 6
Przetwarzanie informacji niejawnych na technicznych nośnikach informacji niejawnych

§ 37

1. Techniczne nośniki informacji niejawnych muszą być zaewidencjonowane w DEWMK, w kancelarii tajnej komórki wprowadzającej nośnik do eksploatacji.
2. Dokumenty otrzymane w postaci technicznych nośników informacji niejawnych podlegają ewidencji w sposób określony w § 27.
3. Wydruki z technicznych nośników informacji niejawnych podlegają zarejestrowaniu w dzienniku ewidencji.
4. Dopuszcza się przesyłanie informacji niejawnych w postaci zapisu na technicznych nośnikach informacji niejawnych lub materiałach fotograficznych, jako załącznik do pisma przewodniego, w którym nadawca określa dyspozycję dotyczącą ewentualnego zwrotu nośnika.

§ 38

1. TNIN powinny posiadać:
   1) etykietę stałą lub trwale dołączoną do nośnika zawierającą naniesione w sposób trwały w szczególności poprzez ostemplowanie, nadrukowanie, naklejenie oznaczeń hologramowych lub wpisanie odręczne niezmywalnym środkiem:
      a) nazwy komórki organizacyjnej,
      b) numeru pod którym nośnik jest zarejestrowany w DEWMK,
      c) klauzuli tajności nośnika;
   2) dodatkową etykietę, zawierającą dyspozycję dla adresata w szczególności: polecenie zwrotu po wykorzystaniu, polecenie usunięcia informacji niejawnej.
2. TNIN w postaci indywidualnych dysków twardych komputera oraz TNIN będące elementami macierzy dyskowych powinny posiadać naniesione w sposób trwały oznaczenie zawierające:

1) numer pod którym nośnik jest zarejestrowany w DEWMK;
2) klauzulę tajności nośnika.

3. W DEWMK powinien być wpisany numer seryjny dysku twardego.
4. Na nośniki stanowiące macierz dyskową lub na nośniki w innych stanowiskach, w których nie ma dostępu do TNIN numer DEWMK umieszcza się na obudowie nośnika.
5. Dopuszcza się wykorzystywanie TNIN typu pendrive przez użytkowników określonego systemu teleinformatycznego, jeżeli dokumentacja bezpieczeństwa tego nie zabrania, ale tylko w niezbędnym zakresie oraz po spełnieniu następujących warunków:
   1) nośnik taki musi posiadać jednoznacznie odczytywalny numer seryjny, który jest zarejestrowany w DEWMK;
   2) dostęp do portów USB odbywa się tylko na dedykowanych do tego celu stanowiskach komputerowych, na których można przy użyciu odpowiedniego oprogramowania:
      a) zablokować dostęp dla nieuprawnionych nośników,
      b) zablokować możliwość zapisu informacji na nośnik,
      c) odczytać historię podłączeń urządzeń przez port USB.
6. W celu uwierzytelnienia nośnika na stanowisku, stosuje się oprogramowanie weryfikujące nośnik po jego numerze seryjnym, w innych przypadkach administrator każdorazowo udostępnia zablokowany port na czas niezbędny dla wykonania zadania a po zakończeniu pracy ponownie blokuje do niego dostęp. Fakt odblokowywania i blokowania portu jest każdorazowo zapisywany w odpowiednim dzienniku stanowiska komputerowego.
7. Dostęp do TNIN posiadają tylko specjalnie autoryzowani użytkownicy, posiadający odblokowany port USB przez administratora na czas pracy z TNIN lub posiadający nośnik uprawniony przez oprogramowanie weryfikujące numer seryjny nośnika do pracy na danym stanowisku i wyłącznie w sytuacjach, kiedy ich użycie jest niezbędne do przetwarzania danych w systemie.
8. W czasie, gdy nie zachodzi potrzeba używania TNIN, nośnik powinien być przechowywany na zasadach ogólnych tak jak w przypadku niejawnej dokumentacji papierowej.
9. Wszystkie TNIN oznaczone klauzulą „poufne" lub wyższą, wynoszone poza strefy ochronne, należy zabezpieczyć pod względem ochrony kryptograficznej środkami posiadającymi certyfikaty jednostki certyfikującej Agencji Bezpieczeństwa Wewnętrznego lub innymi certyfikatami uznanymi przez tę jednostkę.
10. W przypadku pozostałych nośników zalecanym jest zaszyfrowanie danych programem szyfrującym z użyciem algorytmu AES-256.

§ 39

1. Informacje niejawne wolno przetwarzać wyłącznie na zarejestrowanych TNIN przygotowanych według zasad określonych w § 37 i § 38. Nośniki typu pendrive oraz karty pamięci należy wcześniej sprawdzić pod kątem prawidłowości jednoznacznie odczytywalnego numeru seryjnego.
2. Zapisywanie informacji jawnych na zewnętrznych TNIN jest dozwolone, jeżeli tworzą razem z informacjami niejawnymi całość sprawy.
3. Formatowanie dysku twardego stanowiska systemu przetwarzającego informacje niejawne oraz wszystkie operacje wykonane na TNIN wymagają odnotowania tego faktu w odpowiednim dzienniku stanowiska komputerowego dla określonego systemu.
4. Zabrania się zapisu na TNIN informacji prywatnych.
5. Zabrania się rejestrowania prywatnych nośników jako TNIN.

§ 40

1. TNIN podlegają ochronie, stosownej do klauzuli tajności, jaką zostały oznaczone i należy je chronić analogicznie jak dokumenty niejawne.
2. TNIN należy chronić przed zniekształceniem bądź zniszczeniem zapisanej informacji pod wpływem temperatury, pól elektrycznych, magnetycznych i innych czynników.
3. Każdy wymienny TNIN powinien być przechowywany w opakowaniu ochronnym, jeżeli takie posiada, z wyraźnym oznaczeniem klauzuli tajności.
4. Każdy użytkownik zobowiązany jest do okresowej kontroli stanu technicznego posiadanych TNIN; w przypadku stwierdzenia nieprawidłowości polegającej na niemożliwości odczytu, zapisu lub innego uszkodzenia, powinien zgłosić ten fakt do pełnomocnika ochrony, który podejmie decyzję o dalszym postępowaniu.

§ 41

1. Przesyłanie TNIN za pośrednictwem poczty specjalnej przebiega przy zastosowaniu wymogów, o których mowa w przepisach w sprawie trybu i sposobu nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne, i zwalnia z zastosowania środków kryptograficznych.
2. Wynoszenie lub wywożenie TNIN poza komórkę organizacyjną w związku z naprawą lub konserwacją sprzętu komputerowego, przez firmy zewnętrzne, jest zabronione.
3. W przypadku cyklicznej wymiany informacji niejawnych z instytucjami spoza Policji zaleca

się używanie grupy nośników dedykowanych dla każdej z tych instytucji.

§ 42

1. Nośniki podlegają fizycznemu zniszczeniu jeżeli:
   1) ich stan techniczny uniemożliwia skuteczne usunięcie zawartych tam informacji;
   2) ich stan techniczny uniemożliwia odczytanie zawartych tam informacji;
   3) ich stan techniczny uniemożliwia ich dalszą eksploatację;
   4) posiadały klauzulę tajności i podjęto w stosunku do nich decyzję o wycofaniu z eksploatacji.
2. Nośniki przeznaczone do zniszczenia fizycznego powinny być pozbawione oznaczeń oraz, o ile to możliwe, zawartych tam informacji.
3. Niszczenie TNIN, zarządza kierownik komórki organizacyjnej Komendy Głównej Policji, w której zaewidencjonowano TNIN, powołując komisję, w skład której wchodzą:
   1) przedstawiciel komórki organizacyjnej, na której stanie jest zaewidencjonowany TNIN;
   2) kierownik kancelarii tajnej lub osoba przez niego upoważniona, a w uzasadnionych przypadkach inspektor bezpieczeństwa teleinformatycznego lub osoba przez niego upoważniona;
   3) użytkownik TNIN lub inna osoba upoważniona przez jego przełożonego;
   4) przedstawiciel pionu informatyki – gdy zachodzi konieczność wymontowania nośnika z chroniącej go obudowy.
4. W przypadku terenowych jednostek lub komórek organizacyjnych Policji, kierownik jednostki lub komórki, w porozumieniu z inspektorem bezpieczeństwa teleinformatycznego lub pełnomocnikiem ochrony powołuje komisję, o której mowa w ust. 3, w skład której wchodzą:
   1) przedstawiciel jednostki lub komórki organizacyjnej, na której stanie jest zaewidencjonowany TNIN;
   2) inspektor bezpieczeństwa teleinformatycznego lub wyznaczony przez pełnomocnika ochrony funkcjonariusz lub pracownik pionu ochrony celem merytorycznego nadzoru;
   3) lokalny przedstawiciel pionu informatyki, gdy zachodzi konieczność wymontowania nośnika z chroniącej go obudowy.
5. Kierownik jednostki lub komórki organizacyjnej, o której mowa w ust. 4, może nie powoływać komisji lecz przekazać zakwalifikowany do fizycznego zniszczenia TNIN do kancelarii tajnej macierzystej jednostki organizacyjnej.
6. Każdorazowo przed zniszczeniem nośników typu dysk twardy, dyskietka lub dysk magnetooptyczny, sam nośnik informacji musi zostać wymontowany z chroniącej go obudowy.
7. Komisja, o której mowa w ust. 3 i 4, każdorazowo określa konkretny sposób zniszczenia, w zależności od rodzaju i typu nośnika oraz innych lokalnych możliwości.
8. Zniszczenia nośników wykonanych z plastiku w szczególności CD, DVD, FDD, MO, kart magnetycznych i mikroprocesorowych, można dokonać w niszczarkach zapewniających odpowiedni do klauzuli stopień poziomu bezpieczeństwa według normy DIN32757-1.
9. Niszczarki, o których mowa w pkt. 8, powinny spełniać następujące normy:
   1) dla klauzuli „tajne" lub „ściśle tajne":
      a) poziom bezpieczeństwa 3-go stopnia: paski ≤ szer. 4 mm i dł. 80 mm lub fragmenty o powierzchni ≤ 320 mm^2,
      b) poziom bezpieczeństwa 2-go stopnia: paski ≤ szer. 6 mm lub fragmenty o powierzchni ≤ 800 mm^2 pod warunkiem zastosowania dodatkowych procedur ochrony (przykładowo wymieszania powstałej „masy plastikowej" z identyczną „masą plastikową" po nośnikach zawierających informacje jawne, następnie rozdzielenia całości i wrzucenie do kilku pojemników na odpady plastikowe);
   2) dla klauzuli „zastrzeżone" lub „poufne": poziom bezpieczeństwa 2-go stopnia: paski nie szersze niż 6 mm lub fragmenty o powierzchni ≤ 800 mm^2.
10. Zniszczenia TNIN na podłożu metalowym można dokonać poprzez mechaniczne usunięcie z metalowego podłoża warstwy magnetycznej zawierającej informacje lub spalenie, rozpuszczenie, rozdrobnienie (pocięcie) na kawałki ≤ szer. 4 mm i dł. 80 mm lub ≤ szer. 2 mm przy powierzchni ≤ 594 mm^2 lub fragmenty o powierzchni ≤ 320 mm^2.
11. Zniszczenia TNIN typu flash w szczególności pendrive, dyski SSD można dokonać poprzez rozpuszczenie, rozdrobnienie, mechaniczne zmiażdżenie prasą lub młotem.
12. Za zapewnienie koniecznej pomocy innych komórek organizacyjnych do zniszczenia TNIN odpowiada kierownik komórki organizacyjnej, na której stanie jest zaewidencjonowany TNIN.
13. Niszczenie nośników można przeprowadzić z wykorzystaniem urządzeń będących własnością innej jednostki organizacyjnej lub firmy świadczącej usługi w zakresie niszczenia i utylizacji nośników. W przypadku korzystania z usług firmy zewnętrznej należy sprawdzić czy dana firma posiada opracowane procedury niszczenia, przedstawia dokumentację przeprowadzenia procesu zniszczenia nośnika i utylizacji produktów zniszczenia. Nośniki HDD i SSD przekazywane do zniszczenia przez firmę zewnętrzną muszą być uszkodzone mechanicznie poprzez wywiercenie w nośniku minimum

5 otworów Φ 6 mm lub zdeformowanie mechaniczne wykonane młotem lub prasą, eliminujące możliwość bezpośredniego odczytania informacji po podłączeniu do komputera, a dokument przekazujący musi zawierać ich numery seryjne i numery rejestracji w DEWMK.

§ 43

1. Wycofanie TNIN z użycia lub jego deklasyfikacja jest możliwa wyłącznie po przeprowadzeniu skutecznego, nieodwracalnego usunięcia zapisanej informacji lub utraty cech funkcjonalnych nośnika. Skutecznego, nieodwracalnego usunięcia zapisanej informacji na nośnikach magnetycznych dokonuje się poprzez ich demagnetyzację, z wyjątkiem dysków magnetooptycznych, natomiast dla pozostałych nośników, z wyjątkiem dysków optycznych poprzez trzykrotne nadpisanie zapisanej tam informacji oraz pozostałej wolnej przestrzeni nośnika metodą US DoD 5220.22-M.
2. Deklasyfikacja polega na zmianie oznaczenia klauzuli tajności bądź jej zniesieniu. Deklasyfikacji nie podlegają nośniki optyczne i magnetooptyczne jednokrotnego ani wielokrotnego zapisu. Pomimo, że dysk twardy należy do nośników magnetycznych jego deklasyfikacji można dokonać jedynie poprzez trzykrotne nadpisanie zapisanej tam informacji oraz pozostałej wolnej przestrzeni nośnika metodą US DoD 5220.22-M, ponieważ konstrukcja dysku twardego zawiera elektroniczne znaczniki ścieżek, które podczas procesu demagnetyzacji są usuwane powodując niemożność dalszej jego eksploatacji. Poprawność deklasyfikacji należy po zakończeniu czynności zweryfikować.
3. Kancelaria tajna lub komórka organizacyjna, w której jest zaewidencjonowany zdeklasyfikowany TNIN prowadzi zatwierdzony przez pełnomocnika ochrony wykaz zdeklasyfikowanych nośników TNIN, który powinien zawierać typ nośnika, numer protokołu deklasyfikacji wraz z datą, nazwisko i imię osoby na której stanie znajduje się nośnik oraz nazwę komórki organizacyjnej.
4. Deklasyfikacji nie podlegają nośniki oznaczone klauzulą „tajne" lub „ściśle tajne".
5. Zwrot TNIN do kancelarii tajnej może nastąpić wyłącznie po usunięciu zapisanych tam informacji niejawnych z wyłączeniem nośników deponowanych tam tymczasowo lub podlegających archiwizacji.
6. Fakt zniszczenia lub deklasyfikacji nośnika TNIN potwierdza się protokołem deklasyfikacji lub zniszczenia, którego wzór określa załącznik nr 10 do zarządzenia. Kierownik kancelarii tajnej, odpowiedzialny za przetwarzanie materiałów niejawnych, w których jest zarejestrowany TNIN, na podstawie zatwierdzonego protokołu przeprowadza aktualizację rejestracji w DEWMK.

§ 44

Bieżąca kontrola użytkowania TNIN jest przeprowadzana przez inspektora bezpieczeństwa teleinformatycznego każdorazowo, podczas wykonywania czynności określonych w art. 52 ust. 1 pkt 1 ustawy oraz na każde polecenie kierownika jednostki organizacyjnej lub pełnomocnika ochrony.

Rozdział 7
Środki bezpieczeństwa fizycznego

§ 45

1. Tworzy się strefy ochronne:
   1) strefę I, w której przebywanie wiąże się z możliwością bezpośredniego dostępu do informacji niejawnych, w strefie I dokumenty niejawne oznaczone klauzulą „ściśle tajne" lub „tajne" można przechowywać poza szafami metalowymi w pomieszczeniach odpowiadających co najmniej klasie I odporności na włamanie według Polskiej Normy PN-EN-1143-1;
   2) strefę II, w której przebywanie nie wiąże się z bezpośrednim dostępem do informacji niejawnych, w strefie II dokumenty niejawne oznaczone klauzulą „ściśle tajne" lub „tajne" lub „poufne" muszą być przechowywane w szafach metalowych o odpowiedniej klasie odporności;
   3) strefę III służącą do kontroli osób, w której przebywanie nie wiąże się z dostępem do informacji niejawnych oznaczonych klauzulą „ściśle tajne" lub „tajne".
2. Wejście i wyjście ze strefy I lub II następuje wyłącznie ze strefy III.
3. Wymagania jakie powinny spełniać strefy ochronne określa załącznik nr 11 do zarządzenia.
4. Wymagania bezpieczeństwa fizycznego informacji niejawnych przetwarzanych w systemach teleinformatycznych określają odrębne przepisy.

§ 46

1. W zależności od nadanej klauzuli tajności, dokumenty niejawne lub materiały przechowywane są:
   1) „ściśle tajne" – w szafach metalowych klasy C;
   2) „tajne" – w szafach metalowych klasy B;
   3) „poufne" – w szafach metalowych klasy A;
   4) „zastrzeżone" – w meblach drewnianych lub szafach zamykanych na klucz.
2. Klasyfikację szaf oraz rodzaj środków ochrony fizycznej określa załącznik nr 12 do zarządzenia.
3. W uzasadnionych przypadkach kierownik jednostki organizacyjnej może wyrazić zgodę na przechowywanie materiałów, o których mowa

w ust. 1 pkt 3, w niecertyfikowanych szafach metalowych.

§ 47

1. Do ochrony informacji niejawnych oznaczonych klauzulą „ściśle tajne" lub „tajne" stosuje się elektroniczne systemy zabezpieczeń:
   1) systemy sygnalizacji włamania i napadu wyposażone w urządzenia transmisji alarmu;
   2) systemy telewizji dozorowanej stosowane w zabezpieczeniach;
   3) systemy kontroli dostępu stosowane w zabezpieczeniach, wyłącznie w przypadku braku całodobowej ochrony obiektu;
   4) systemy sygnalizacji pożarowej.
2. Elektroniczne systemy zabezpieczeń wykorzystywane do ochrony informacji niejawnych mogą funkcjonować jako podsystemy innego elektronicznego systemu zabezpieczeń.
3. W elektronicznych systemach zabezpieczeń stosuje się wyłącznie urządzenia elektroniczne posiadające certyfikaty wydane przez akredytowaną jednostkę certyfikującą lub deklaracje zgodności producenta potwierdzające zgodność tych urządzeń z obowiązującymi dokumentami normatywnymi.
4. Systemy wykonane według Polskiej Normy PN-93/E-08390 w klasie SA3 i SA4 mogą być wykorzystywane nadal do zabezpieczenia informacji niejawnych oznaczonych klauzulą „ściśle tajne" lub „tajne" pod warunkiem, że system określa rodzaje czynności przewidzianych dla drugiego stopnia zabezpieczenia według Polskiej Normy PN-EN-50133-1.

§ 48

1. Dokumenty oznaczone różnymi klauzulami tajności powinny być przechowywane w kancelarii w odrębnych szafach lub pomieszczeniach chyba, że wchodzą one w skład zbioru dokumentów.
2. Dokumenty, o których mowa w ust. 1, powinny być przechowywane w kancelarii, w jednej szafie lub pomieszczeniu pod warunkiem ich fizycznego oddzielenia. W takim przypadku szafa lub pomieszczenie musi spełniać wymagania dla najwyższej klauzuli tajności przechowywanych w nich dokumentów.
3. Kierownik jednostki organizacyjnej Policji lub inna upoważniona przez niego osoba, a w Komendzie Głównej Policji kierownik komórki organizacyjnej albo inna upoważniona przez niego osoba, mogą wyrazić pisemną zgodę na przechowywanie dokumentów poza pomieszczeniami kancelarii na czas niezbędny do realizacji zadań związanych z dostępem do tych dokumentów.

§ 49

1. W pomieszczeniach kancelarii można wydzielić miejsce, w którym osoby upoważnione mogą zapoznawać się z dokumentami niejawnymi zwane dalej „czytelnią".
2. Czytelnia powinna być zorganizowana w sposób umożliwiający stały nadzór ze strony pracowników kancelarii.
3. W czytelni nie instaluje się systemu nadzoru wizyjnego.

§ 50

1. Po zakończeniu pracy kierownik kancelarii lub upoważniony pracownik kancelarii jest obowiązany sprawdzić prawidłowość zamknięcia szaf i pomieszczeń kancelarii.
2. Kody dostępu, szyfry zmienia się:
   1) w urządzeniach nowo instalowanych oraz w odstępach czasowych nieprzekraczających 6 miesięcy;
   2) po każdej naprawie lub konserwacji zamka;
   3) po przekazaniu obowiązków na stanowisku kierownika kancelarii lub innej upoważnionej osoby;
   4) w przypadku ujawnienia kodu osobie nieupoważnionej.
3. Nieprawidłowości związane z naruszeniem przepisów ust. 2. należy niezwłocznie zgłaszać pełnomocnikowi ochrony.
4. Przepisy ust. 1-2 obowiązują odpowiednio w stosunku do innych pomieszczeń, w których są przechowywane dokumenty niejawne.

§ 51

1. Kierownik jednostki organizacyjnej zatwierdza plan ochrony informacji niejawnych, który powinien zawierać w szczególności:
   1) opis granic strefy ochronnej;
   2) zastosowane środki bezpieczeństwa fizycznego;
   3) szczegółowy sposób zdawania, przechowywania i wydawania kluczy oraz ich duplikatów do pomieszczeń oraz szaf kancelarii, a także sposób ustalania, zmiany i deponowania haseł i szyfrów, w przypadku stosowania zamków szyfrowych;
   4) procedury przyznawania uprawnień do wejścia, wyjścia i przebywania w strefie ochronnej I i II, w tym dla pracowników obsługi technicznej, interesantów lub gości;
   5) sposób interwencji osób odpowiedzialnych za ochronę fizyczną w przypadkach wywołania alarmu;
   6) procedury ewakuacji i niszczenia informacji niejawnych (w tym w razie wprowadzenia stanu nadzwyczajnego).
2. Kierownicy terenowych komórek organizacyjnych Centralnego Biura Śledczego Komendy Głównej Policji lub Biura Spraw Wewnętrznych

Komendy Głównej Policji w porozumieniu z właściwym miejscowo pełnomocnikiem ochrony przygotują plany ochrony zawierające informacje, o których mowa w ust. 1. Plany te będą stanowiły załączniki do planów ochrony informacji niejawnych komend wojewódzkich Policji.

Rozdział 8
Przepisy przejściowe i końcowe

§ 52

Kancelarie tajne utworzone na podstawie § 4 zarządzenia nr 1579 Komendanta Głównego Policji z dnia 30 grudnia 2005 r. w sprawie szczególnego sposobu organizacji kancelarii tajnych, stosowania środków ochrony fizycznej oraz obiegu informacji niejawnych w Policji (Dz. Urz. KGP z 2006 r. Nr 1 poz. 3 i Nr 12 poz. 74) funkcjonują, nie dłużej niż do dnia 30 czerwca 2011 r., zgodnie z dotychczasowymi przepisami.

§ 53

1. Środki bezpieczeństwa fizycznego informacji niejawnych należy dostosować do przepisów zarządzenia w terminie 12 miesięcy od dnia wejścia w życie zarządzenia.
2. Urządzenia ewidencyjne należy dostosować do przepisów zarządzenia w terminie 6 miesięcy od dnia wejścia w życie zarządzenia.

§ 54

Zarządzenie wchodzi w życie z dniem 2 stycznia 2011 r.

Komendant Główny Policji
gen. insp. Andrzej Matejuk

DZIENNIK URZĘDOWY
KOMENDY GŁÓWNEJ POLICJI

Warszawa, dnia 8 października 2012 r.

Poz. 52

ZARZĄDZENIE NR 132
KOMENDANTA GŁÓWNEGO POLICJI

z dnia 5 października 2012 r.

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

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:

§ 1. W zarządzeniu nr 2020 Komendanta Głównego Policji z dnia 30 grudnia 2010 r. w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii tajnych i innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za przetwarzanie materiałów niejawnych, sposobu i trybu przetwarzania informacji niejawnych oraz doboru i stosowania środków bezpieczeństwa fizycznego informacji niejawnych w Policji (Dz. Urz. KGP z 2011 r. Nr 1, poz. 5) wprowadza się następujące zmiany:

1) w § 1:

a) w pkt 4 uchyla się lit. c,

b) pkt 6 otrzymuje brzmienie:

„6) dobór i stosowanie środków bezpieczeństwa fizycznego.";

2) w § 2 ust. 1 uchyla się pkt 4, 6, 10 i 12-14;

3) w § 19:

a) ust. 1 otrzymuje brzmienie:

„1. W kancelarii prowadzi się następujące urządzenia ewidencyjne:

1) rejestr dzienników ewidencji i teczek;

2) dziennik ewidencyjny;

3) książkę doręczeń przesyłek miejscowych;

4) wykaz przesyłek nadanych;

5) rejestr wydanych przedmiotów.",

b) po ust. 1 dodaje się ust. 1a w brzmieniu:

„1a. Wzory urządzeń ewidencyjnych, o których mowa w ust. 1, określają odpowiednio załączniki nr 1, 2, 4, 5 i 6 do rozporządzenia Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych (Dz. U. Nr 276, poz. 1631).";

4) § 21 otrzymuje brzmienie:

„1. Urządzenia ewidencyjne określone w § 19 ust. 1 pkt 2, 3, 5 i ust. 5 podlegają zarejestrowaniu w rejestrze dzienników ewidencji i teczek, który jest nadrzędnym urządzeniem ewidencyjnym w stosunku do innych urządzeń prowadzonych przez kancelarię i nie podlega ewidencjonowaniu.

2. Urządzenia ewidencyjne, o których mowa w § 19 ust. 1 pkt 2, 3, 5 i ust. 5, oraz ich kolejne tomy rejestruje się pod odrębnymi pozycjami.";

5) w § 22:

a) ust. 1 otrzymuje brzmienie:

„1. Informację o zarejestrowaniu urządzenia ewidencyjnego, o którym mowa w § 19, w rejestrze dzienników ewidencji i teczek odnotowuje się na karcie tytułowej tego urządzenia.",

b) ust. 5 otrzymuje brzmienie:

„5. W urządzeniu ewidencyjnym, o którym mowa w § 19 ust. 1 pkt 2, umieszcza się na środku na górze i dole karty tytułowej i okładki odpowiednią klauzulę tajności.",

c) ust. 6 otrzymuje brzmienie:

„6. Czynności, o których mowa w ust. 2-4, dokonuje się także w stosunku do urządzenia ewidencyjnego, o którym mowa w § 19 ust. 1 pkt 2, 3, 5 i ust. 5.";

6) § 25 otrzymuje brzmienie:

„§ 25. 1. W przypadku stwierdzenia uszkodzenia otrzymanej przesyłki lub śladów jej otwierania pracownik kancelarii kwitujący odbiór przesyłki sporządza w obecności doręczającego, w trzech jednobrzmiących egzemplarzach, protokół w sprawie uszkodzenia przesyłki. Pierwszy egzemplarz przekazuje się nadawcy, drugi doręczającemu, a trzeci pozostaje w kancelarii przyjmującej przesyłkę.

2. Wzór protokołu w sprawie uszkodzenia przesyłki określa załącznik nr 1 do rozporządzenia Prezesa Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne (Dz. U. Nr 271, poz. 1603).";

7) § 26 otrzymuje brzmienie:

„§ 26. Wysłanie z kancelarii przesyłek na podstawie wykazu przesyłek nadanych obejmuje:

1) porównanie ilości przesyłek otrzymanych i przeznaczonych do wysłania z ilością pozycji w wykazie przesyłek nadanych;

2) sprawdzenie całości opakowania i prawidłowości oznaczenia oraz zaadresowania przesyłek;

3) zapakowanie przesyłki w kopertę zewnętrzną i jej zaadresowanie, zabezpieczenie w sposób uniemożliwiający nieuprawniony dostęp do zawartości, a także ostemplowanie pieczęcią nagłówkową i oznaczenie numerem wykazu;

4) wpisanie przesyłki do wykazu przesyłek nadanych sporządzonego w dwóch egzemplarzach;

5) kontrolę ilości przesyłek z ilością pozycji w wykazie przesyłek nadanych;

6) przekazanie całości korespondencji wraz z jednym egzemplarzem wykazu przesyłek nadanych kurierowi poczty specjalnej, który potwierdza jej odbiór podpisem, zapisem liczbowym i słownym ilości przyjętych przesyłek oraz odciskiem pieczęci "do pakietów".";

8) w § 29 ust. 5 otrzymuje brzmienie:

„5. Wzór karty zapoznania się z dokumentem określa załącznik nr 3 do rozporządzenia, o którym mowa w § 19 ust. 1a.";

9) w § 33 ust. 5 otrzymuje brzmienie:

„5. W przypadku odłączenia od pisma przewodniego jednego lub więcej załączników, w rubryce dziennika ewidencyjnego "Adnotacje o wysłaniu dokumentu lub załącznika (pozycja w książce doręczeń przesyłek miejscowych/ pozycja wykazu przesyłek nadanych/załącznik do pisma nr...)" zamieszcza się adnotację, zawierającą jedną z następujących informacji:

1) "załączniki odesłano przy dokumencie nr ..." (należy podać numer z dziennika ewidencyjnego, za którym przesłano dokument wraz z załącznikami);

2) "załącznik nr ... odesłano przy dokumencie nr ..." (należy podać, który załącznik odesłano oraz jakim numerem oznaczono dokument w dzienniku ewidencyjnym).";

10) Rozdział 6 otrzymuje brzmienie:

„Rozdział 6

Przetwarzanie informacji niejawnych na informatycznych nośnikach danych

§ 37. 1. Informatyczne nośniki danych, zwane dalej w skrócie „IND", z utrwalonymi na nich dokumentami elektronicznymi podlegają rejestracji w rejestrze wydanych przedmiotów w kancelarii tajnej komórki wprowadzającej IND do eksploatacji.

2. Otrzymane IND z utrwalonymi na nich dokumentami elektronicznymi podlegają procedurze określonej w § 27. Przesyłanie IND odbywa się za pismem.

3. Dokumenty elektroniczne podlegają zaewidencjonowaniu w dzienniku ewidencyjnym. Dokumenty elektroniczne i dokumenty nieelektroniczne posiadające tę samą treść oznaczane są tą samą sygnaturą literowo-cyfrową.

4. Wydruki dokumentów elektronicznych z IND podlegają zarejestrowaniu w dzienniku ewidencyjnym.

5. Klauzulę tajności nanosi się, o ile to możliwe, na dokumencie elektronicznym.

6. W rejestrze wydanych przedmiotów powinien być wpisany numer seryjny IND.

§ 38. 1. Dokument elektroniczny oznacza się metryką, o której mowa w rozporządzeniu Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie oznaczania materiałów i umieszczania na nich klauzul tajności (Dz. U. Nr 288, poz. 1692).

2. Treść metryki dokumentu elektronicznego określają przepisy rozporządzenia, o którym mowa w ust. 1.

3. Metryka dokumentu elektronicznego stanowi jego integralną część.

4. IND w postaci dysków twardych indywidualnych oraz będących elementami macierzy dyskowych, służące do przetwarzania informacji niejawnych powinny posiadać naniesione w sposób trwały oznaczenie zawierające:

1) numer, pod którym IND jest zarejestrowany w rejestrze wydanych przedmiotów;

2) klauzulę tajności IND.

5. Na IND stanowiące macierz dyskową lub na IND w innych stanowiskach, w których nie ma dostępu do IND, numer rejestru wydanych przedmiotów umieszcza się na obudowie IND.

6. Sposób postępowania z materiałami zawierającymi informacje niejawne wykorzystywane w urządzeniach lub systemach przeznaczonych do wykonywania czynności operacyjno-rozpoznawczych, w szczególności z urządzeniami, częściami urządzeń lub IND określono w rozporządzeniu, o którym mowa w ust.1.

7. Dopuszcza się wykorzystywanie IND przeznaczonych do utrwalania informacji niejawnych w postaci dokumentów elektronicznych przez użytkowników określonego systemu teleinformatycznego, jeżeli dokumentacja bezpieczeństwa systemu teleinformatycznego tego nie zabrania, ale tylko w niezbędnym zakresie oraz po spełnieniu, w przypadku IND typu pamięć USB lub karta pamięci, następujących warunków:

1) IND musi posiadać jednoznacznie odczytywalny numer seryjny;

2) system operacyjny jest tak skonfigurowany, iż tylko dopuszczone IND są przez niego wykrywane.

8. Dopuszcza się wykorzystanie IND do przetwarzania informacji jawnych, w systemach niejawnych, w celu realizacji niezbędnych zadań Policji po zaewidencjonowaniu ich w wykazie prowadzonym przez kierownika komórki organizacyjnej, który dla IND określonych w ust. 7 pkt 1 musi zawierać ich numer seryjny.

9. Wynoszenie lub wywożenie niejawnych IND poza strefy ochronne powinno być dozwolone jedynie pod warunkiem zastosowania certyfikowanych, kryptograficznych metod ochrony lub przez spełnienie wymagań określonych w przepisach rozporządzenia, o którym mowa w § 25 ust. 2.

10. W przypadku niejawnych IND zalecane jest szyfrowanie znajdujących się na nich informacji algorytmem AES-256 z 8-znakowym hasłem dla informacji o klauzuli niższej niż tajne i 14-znakowym hasłem w innych przypadkach.

§ 39. 1. Informacje niejawne w postaci dokumentów elektronicznych wolno przetwarzać wyłącznie na zarejestrowanych IND przygotowanych według zasad określonych w § 37 i § 38. IND typu pamięć USB oraz karta pamięci należy uprzednio sprawdzić pod kątem prawidłowości jednoznacznie odczytywalnego numeru seryjnego.

2. Zapisywanie dokumentów jawnych na IND jest dozwolone, jeżeli tworzą razem z utrwalonymi na nich niejawnymi dokumentami elektronicznymi całość sprawy.

3. Formatowanie IND w postaci dysku twardego stanowiska systemu przetwarzającego informacje niejawne oraz wszystkie operacje wykonane na tym IND wymagają odnotowania tego faktu w odpowiednim dzienniku stanowiska komputerowego dla określonego systemu.

4. Zabrania się zapisu na IND informacji prywatnych.

5. Zabrania się rejestrowania prywatnych IND.

§ 40. 1. IND z utrwalonymi na nich dokumentami elektronicznymi należy chronić przed zniekształceniem bądź zniszczeniem zapisanej informacji pod wpływem temperatury, pól elektrycznych, magnetycznych i innych czynników.

2. IND z utrwalonymi na nich dokumentami elektronicznymi powinny być przechowywane w opakowaniu ochronnym.

3. Każdy użytkownik zobowiązany jest do okresowej kontroli stanu technicznego posiadanych IND, przy czym w przypadku stwierdzenia nieprawidłowości polegającej na niemożliwości odczytu, zapisu lub innego uszkodzenia, powinien zgłosić ten fakt do pełnomocnika ochrony, który podejmie decyzję o dalszym postępowaniu.

§ 41. 1. Zabronione jest wynoszenie lub wywożenie niejawnych IND poza jednostkę organizacyjną, w związku z naprawą lub konserwacją sprzętu komputerowego przez podmioty zewnętrzne.

2. W przypadku cyklicznej wymiany informacji niejawnych z instytucjami spoza Policji zaleca się używanie grupy IND dedykowanych dla każdej z tych instytucji.

§ 42. 1. Uszkodzone niejawne IND podlegają zniszczeniu fizycznemu, przy czym przed fizycznym zniszczeniem IND należy, o ile jest to możliwe, dokonać usunięcia z niego danych.

2. Niszczenie niejawnych IND zarządza kierownik komórki organizacyjnej Komendy Głównej Policji, w której zaewidencjonowano IND z dokumentem elektronicznym, powołując komisję, w skład której wchodzą:

1) przedstawiciel komórki organizacyjnej, na której stanie jest zaewidencjonowany IND;

2) kierownik kancelarii tajnej lub osoba przez niego upoważniona, a w uzasadnionych przypadkach inspektor bezpieczeństwa teleinformatycznego lub osoba przez niego upoważniona;

3) użytkownik IND lub inna osoba upoważniona przez jego przełożonego;

4) przedstawiciel pionu informatyki – gdy zachodzi konieczność wymontowania IND z chroniącej go obudowy.

3. W przypadku terenowych jednostek organizacyjnych lub komórek organizacyjnych kierownik tej jednostki lub komórki, w porozumieniu z inspektorem bezpieczeństwa teleinformatycznego lub pełnomocnikiem ochrony, powołuje komisję, o której mowa w ust. 2, w skład której wchodzą:

1) przedstawiciel jednostki organizacyjnej lub komórki organizacyjnej, na której stanie jest zaewidencjonowany niejawny IND;

2) inspektor bezpieczeństwa teleinformatycznego lub wyznaczony przez pełnomocnika ochrony policjant lub pracownik pionu ochrony celem merytorycznego nadzoru;

3) lokalny przedstawiciel pionu informatyki, gdy zachodzi konieczność wymontowania IND z chroniącej go obudowy.

4. Kierownik jednostki organizacyjnej lub komórki organizacyjnej, o której mowa w ust. 3, może nie powoływać komisji, lecz przekazać zakwalifikowany do fizycznego zniszczenia niejawny IND do kancelarii tajnej macierzystej jednostki organizacyjnej lub komórki organizacyjnej.

5. Każdorazowo przed zniszczeniem niejawnego IND w postaci dysku twardego, dyskietki lub dysku magnetooptycznego, sam nośnik informacji musi zostać wymontowany z chroniącej go obudowy.

6. Komisja, o której mowa w ust. 2 i 3, każdorazowo określa konkretny sposób zniszczenia, w zależności od rodzaju i typu IND oraz innych lokalnych możliwości.

§ 43. 1. Zniszczenia niejawnych IND wykonanych z plastiku, w szczególności: CD, DVD, FDD, MO, kart magnetycznych i mikroprocesorowych, można dokonać w niszczarkach zapewniających odpowiedni do klauzuli tajności stopień poziomu bezpieczeństwa według normy DIN32757-1.

2. Niszczarki, o których mowa w ust. 1, powinny spełniać następujące normy:

1) dla klauzuli "tajne" lub "ściśle tajne":

a) poziom bezpieczeństwa 3-go stopnia: paski ≤ szer. 4 mm i dł. 80 mm lub fragmenty o powierzchni ≤ 320 mm^2,

b) poziom bezpieczeństwa 2-go stopnia: paski ≤ szer. 6 mm lub fragmenty o powierzchni ≤ 800 mm^2 pod warunkiem zastosowania dodatkowych procedur ochrony (przykładowo wymieszania powstałej masy plastikowej z identyczną masą plastikową po nośnikach zawierających informacje jawne, następnie rozdzielenia całości i wrzucenia do kilku pojemników na odpady plastikowe);

2) dla klauzuli zastrzeżone lub poufne - poziom bezpieczeństwa 2-go stopnia: paski nie szersze niż 6 mm lub fragmenty o powierzchni ≤ 800 mm^2.

3. Zniszczenia IND na podłożu metalowym można dokonać poprzez mechaniczne usunięcie z metalowego podłoża warstwy magnetycznej zawierającej informacje lub spalenie, rozpuszczenie, rozdrobnienie (pocięcie) na kawałki ≤ szer. 4 mm i dł. 80 mm lub ≤ szer. 2 mm przy powierzchni ≤ 594 mm^2 lub fragmenty o powierzchni ≤ 320 mm^2.

4. Zniszczenia IND można dokonać poprzez rozpuszczenie, rozdrobnienie, mechaniczne zmiażdżenie prasą lub młotem.

5. Kierownik jednostki organizacyjnej lub kierownik komórki organizacyjnej, w której jest zaewidencjonowany IND, odpowiada za zapewnienie koniecznej pomocy do jego zniszczenia przez, odpowiednio, inne jednostki organizacyjne lub podmioty świadczące usługi w zakresie niszczenia i utylizacji nośników albo inne komórki organizacyjne.

6. W przypadku niszczenia IND przy wykorzystaniu urządzeń podmiotu zewnętrznego należy sprawdzić czy ten podmiot posiada opracowane procedury niszczenia, przedstawia dokumentację przeprowadzenia procesu zniszczenia IND i utylizacji produktów zniszczenia.

7. Niejawne IND w postaci:

1) dysków twardych;

2) pamięci typu „flash" - pamięci pozwalającej na zapisywanie i kasowanie wielu komórek pamięci podczas operacji programowania,

przed przekazaniem do zniszczenia podmiotowi zewnętrznemu muszą być uszkodzone mechanicznie poprzez wywiercenie w nośniku minimum 5 otworów Φ 6 mm lub zdeformowanie mechaniczne wykonane młotem lub prasą, eliminujące możliwość bezpośredniego odczytania informacji po

podłączeniu do komputera, a dokument przekazujący musi zawierać ich numery seryjne i numery rejestracji w rejestrze wydanych przedmiotów.

§ 44. 1. Deklasyfikacja IND polega na zmianie oznaczenia klauzuli tajności bądź jej zniesieniu.

2. Deklasyfikacja IND dopuszczalna jest tylko dla informacji niejawnych oznaczonych klauzulą "zastrzeżone" oraz "poufne".

3. Niedopuszczalna jest deklasyfikacja IND, na których były przetwarzane informacje niejawne oznaczane klauzulą "tajne" lub "ściśle tajne".

§ 45. 1. Wycofanie niejawnego IND z użycia lub jego deklasyfikacja jest możliwa wyłącznie po przeprowadzeniu skutecznego, nieodwracalnego usunięcia zapisanych tam dokumentów elektronicznych lub utraty cech funkcjonalnych IND.

2. Skutecznego, nieodwracalnego usunięcia zapisanych dokumentów elektronicznych na IND magnetycznych dokonuje się poprzez ich demagnetyzację, z wyjątkiem dysków magnetooptycznych, natomiast dla pozostałych IND, z wyjątkiem dysków optycznych, poprzez trzykrotne nadpisanie zapisanej tam informacji oraz pozostałej wolnej przestrzeni IND metodą US DoD 5220.22-M.

3. Deklasyfikacji nie podlegają niejawne IND optyczne i magnetooptyczne jednokrotnego ani wielokrotnego zapisu.

4. Deklasyfikacji dysku twardego (pomimo że dysk twardy należy do nośników magnetycznych) można dokonać jedynie poprzez trzykrotne nadpisanie zapisanej tam informacji oraz pozostałej wolnej przestrzeni IND metodą US DoD 5220.22-M, ponieważ konstrukcja dysku twardego zawiera elektroniczne znaczniki ścieżek, które podczas procesu demagnetyzacji są usuwane, powodując niemożność dalszej jego eksploatacji, przy czym poprawność deklasyfikacji dysku twardego należy po zakończeniu czynności zweryfikować.

§ 46. 1. Kancelaria tajna lub komórka organizacyjna, w której jest zaewidencjonowany zdeklasyfikowany niejawny IND, prowadzi zatwierdzony przez pełnomocnika ochrony wykaz zdeklasyfikowanych IND, który powinien zawierać typ IND, numer protokołu deklasyfikacji wraz z datą, nazwisko i imię osoby, na której stanie znajduje się IND, oraz nazwę komórki organizacyjnej.

2. Zwrot IND do kancelarii tajnej może nastąpić wyłącznie po usunięciu zapisanych tam dokumentów elektronicznych z wyłączeniem IND deponowanych tam tymczasowo lub podlegających archiwizacji.

§ 47. 1. Usuwanie zapisanych na IND dokumentów elektronicznych odbywa się na zasadach jak dla dokumentów nieelektronicznych.

2. Fakt deklasyfikacji lub zniszczenia niejawnego IND potwierdza się protokołem deklasyfikacji lub zniszczenia, którego wzór określa załącznik nr 10 do zarządzenia.

§ 48. Kierownik lub pracownik kancelarii tajnej, odpowiedzialny za przetwarzanie materiałów niejawnych, w których jest zarejestrowany IND, na podstawie zatwierdzonego protokołu przeprowadza aktualizację rejestracji w rejestrze wydanych przedmiotów.

§ 49. Bieżąca kontrola użytkowania IND zarejestrowanego w rejestrze wydanych przedmiotów jest przeprowadzana przez inspektora bezpieczeństwa teleinformatycznego każdorazowo, podczas wykonywania czynności określonych w art. 52 ust. 1 pkt 1 ustawy oraz na każde polecenie kierownika jednostki organizacyjnej lub kierownika komórki organizacyjnej albo pełnomocnika ochrony.";

11) Rozdział 7 otrzymuje brzmienie:

„Rozdział 7

Dobór i stosowanie środków bezpieczeństwa fizycznego

§ 50. 1. System bezpieczeństwa informacji niejawnych obejmuje środki bezpieczeństwa fizycznego stosowane w celu zapewnienia poufności, integralności i dostępności tych informacji.

2. W zależności od określonego w jednostkach organizacyjnych poziomu zagrożeń dla pomieszczeń lub obszarów, należy stosować odpowiednią kombinację następujących środków bezpieczeństwa fizycznego:

1) personel bezpieczeństwa – osoby przeszkolone, nadzorowane, a w razie konieczności posiadające odpowiednie uprawnienie do dostępu do informacji niejawnych, wykonujące czynności związane z fizyczną ochroną informacji niejawnych, w tym:

   a) kontrolę dostępu do pomieszczeń lub obszarów, w których przetwarzane są informacje niejawne,

   b) nadzór nad systemem dozoru wizyjnego,

   c) reagowanie na zagrożenia, alarmy lub sygnały awaryjne;

2) bariery fizyczne – środki chroniące granice miejsca, w którym przetwarzane są informacje niejawne, w szczególności:

   a) drzwi,

   b) zamki,

   c) okna,

   d) ściany,

   e) bramy,

   f) ogrodzenia;

3) szafy i zamki – stosowane do przechowywania informacji niejawnych lub zabezpieczające te informacje przed nieuprawnionym dostępem;

4) system kontroli dostępu – stosowany w celu zagwarantowania dostępu do pomieszczenia lub obszaru, w którym przetwarzane są informacje niejawne, wyłącznie przez osoby posiadające odpowiednie uprawnienia, obejmujący:

   a) rozwiązania organizacyjne,

   b) elektroniczny system pomocniczy;

5) system sygnalizacji włamania i napadu – elektroniczny system pomocniczy stosowany w celu realizacji procedur ochrony informacji niejawnych oraz podwyższenia poziomu bezpieczeństwa, który zapewniają:

   a) bariery fizyczne,

   b) zastępujący lub wspierający personel bezpieczeństwa w pomieszczeniach i budynkach;

6) system dozoru wizyjnego – elektroniczny system pomocniczy stosowany w celu bieżącego monitorowania ochronnego lub sprawdzania incydentów bezpieczeństwa i sygnałów alarmowych przez personel bezpieczeństwa;

7) system kontroli osób i przedmiotów – stosowany w celu zapobiegania próbom nieuprawnionego wnoszenia na chroniony obszar rzeczy zagrażających bezpieczeństwu informacji niejawnych lub nieuprawnionego wynoszenia informacji niejawnych z obiektów, obejmujący:

   a) rozwiązania organizacyjne polegające na dobrowolnym poddaniu się kontroli lub udostępnieniu do kontroli rzeczy osobistych,

   b) elektroniczny system pomocniczy.

3. W celu zapewnienia poufności, integralności i dostępności informacji niejawnych można zastosować również środki bezpieczeństwa fizycznego inne niż wymienione w ust. 2, jeżeli taka potrzeba wynika z analizy poziomu zagrożeń.

4. Środki bezpieczeństwa fizycznego zalecane do stosowania w strefach ochronnych określa załącznik nr 1 do zarządzenia.

§ 51. Kierownicy terenowych komórek organizacyjnych Centralnego Biura Śledczego Komendy Głównej Policji lub Biura Spraw Wewnętrznych Komendy Głównej Policji w porozumieniu z właściwymi miejscowo pełnomocnikami ochrony przygotują plany ochrony informacji niejawnych. Plany te będą stanowiły załączniki do planów ochrony informacji niejawnych komend wojewódzkich (Stołecznej) Policji.";

12) uchyla się załączniki nr 2 – 7 oraz 11 i 12;

13) dodaje się załącznik nr 13 w brzmieniu określonym w załączniku nr 1 do niniejszego zarządzenia;

14) załącznik nr 10 otrzymuje brzmienie określone w załączniku nr 2 do niniejszego zarządzenia;

15) użyte w zarządzeniu w różnych przypadkach wyrazy „dziennik ewidencji" zastępuje się wyrazami „dziennik ewidencyjny".

§ 2. 1. Formularze urządzeń ewidencyjnych stosowane według dotychczasowych wzorów mogą być wykorzystywane do wyczerpania zapasów, nie dłużej jednak niż do dnia 31 grudnia 2013 r.

2. Kierownicy jednostek organizacyjnych, w terminie 3 lat od dnia wejścia w życie zarządzenia, określą dobór i stosowanie środków bezpieczeństwa fizycznego zgodnie z niniejszym zarządzeniem.

§ 3. Zarządzenie wchodzi w życie po upływie 14 dni od dnia podpisania.

Komendant Główny Policji

z up. Zastępca Komendanta Głównego Policji
nadinsp. Andrzej ROKITA

Załączniki do zarządzenia nr 132
Komendanta Głównego Policji
z dnia 5 października 2012 r.

Załącznik nr 1

ŚRODKI BEZPIECZEŃSTWA FIZYCZNEGO
ZALECANE DO STOSOWANIA W STREFACH OCHRONNYCH

STREFA OCHRONNA	POZIOM ZAGROŻENIA	ŚRODKI BEZPIECZEŃSTWA FIZYCZNEGO
STREFA III	POZIOM NISKI	Kontrola dostępu do pomieszczeń i obszarów lub stosowanie barier fizycznych chroniących granice miejsca.
	POZIOM ŚREDNI	1. Kontrola dostępu do pomieszczeń i obszarów lub stosowanie barier fizycznych chroniących granice miejsca. 2. Reagowanie na zagrożenia, alarmy lub sygnały awaryjne.
	POZIOM WYSOKI	1. Kontrola dostępu do pomieszczeń i obszarów lub stosowanie barier fizycznych chroniących granice miejsca. 2. Reagowanie na zagrożenia, alarmy lub sygnały awaryjne. 3. Inne środki bezpieczeństwa fizycznego wynikające z określonego poziomu zagrożeń.
STREFA II	POZIOM NISKI	1. Kontrola dostępu do pomieszczeń i obszarów lub system kontroli dostępu. 2. Szafy i zamki. 3. Inne środki bezpieczeństwa fizycznego wynikające z określonego poziomu zagrożeń.
	POZIOM ŚREDNI	1. Kontrola dostępu do pomieszczeń i obszarów lub system kontroli dostępu. 2. Reagowanie na zagrożenia, alarmy lub sygnały awaryjne. 3. Szafy i zamki. 4. Inne środki bezpieczeństwa fizycznego wynikające z określonego poziomu zagrożeń.
	POZIOM WYSOKI	1. Kontrola dostępu do pomieszczeń i obszarów lub system kontroli dostępu. 2. Nadzór nad systemem dozoru wizyjnego. 3. Reagowanie na zagrożenia, alarmy lub sygnały awaryjne. 4. Szafy i zamki. 5. Inne środki bezpieczeństwa fizycznego wynikające z określonego poziomu zagrożeń.
STREFA I	POZIOM NISKI	1. System kontroli dostępu. 2. Bariery fizyczne, tj. drzwi, zamki, okna (na parterze zabezpieczone) i ściany. 3. Inne środki bezpieczeństwa fizycznego wynikające z określonego poziomu zagrożeń.
	POZIOM ŚREDNI	1. System kontroli dostępu. 2. Bariery fizyczne, tj. drzwi, zamki, okna (na parterze zabezpieczone) i ściany. 3. Szafy i zamki. 4. Inne środki bezpieczeństwa fizycznego wynikające z określonego poziomu zagrożeń.
	POZIOM WYSOKI	1. System kontroli dostępu. 2. Bariery fizyczne, tj. drzwi, zamki, okna (na parterze zabezpieczone) i ściany. 3. Szafy i zamki. 4. System dozoru wizyjnego. 5. Inne środki bezpieczeństwa fizycznego wynikające z określonego poziomu zagrożeń.

Załącznik nr 2

„WZÓR"

Egzemplarz nr .....

Protokół nr .../...

deklasyfikacji/zniszczenia*) IND

W dniu ..... w miejscowości ..... komisja w składzie:

1. ..... /.....

(Imię i nazwisko, / stanowisko, nazwa komórki organizacyjnej)

2. ..... /.....

(Imię i nazwisko, / stanowisko, nazwa komórki organizacyjnej)

3. ..... /.....

(Imię i nazwisko, / stanowisko, nazwa komórki organizacyjnej)

dokona deklasyfikacji / zniszczenia*) nośników IND

.....

(nazwa komórki organizacyjnej i jednostki organizacyjnej, na której stanie był zarejestrowany IND)

Nr RWP/ Liczba dziennika*)	Typ nośnika	Klauzula Tajności	Sposób deklasyfikacji/zniszczenia*)	Zastosowane urządzenie lub oprogramowanie *typ i nr urządzenia lub nazwę użytego oprogramowania i nr wersji*	Nośnik zarejestrowano w wykazie nośników zdeklasyfikowanych pod poz. nr:

Uwagi:

.....

.....

Podpisy członków komisji:

1. ..... 2. ..... 3. .....

Zgoda na deklasyfikację/zniszczenie

....

(podpis kierownika komórki organizacyjnej) (podpis pełnomocnika ochrony)

Komisja w dniu ..... dokonała deklasyfikacji / zniszczenia wymienionych nośników IND ww. metodą.

Podpisy członków komisji:

1. ..... 2. ..... 3. .....

IND zdjęto z ewidencji ..... / .. zarejestrowano w .....*)

(typ ewidencji) (typ ewidencji i nr pod jakim zarejestrowano)

.....

(podpis kierownika KT lub komórki organizacyjnej prowadzącej RWP)

*) Niepotrzebne skreślić.

wykonano w 2 egz.

egz. nr 1 – kancelaria tajna lub inna komórka organizacyjna prowadząca RWP.

egz. nr 2 – komórka organizacyjna / jednostka organizacyjna