



DZIENNIK URZĘDOWY

MINISTRA SPRAW ZAGRANICZNYCH

Warszawa, dnia 26 lipca 2013 r.

Poz. 18

ZARZĄDZENIE Nr 14

MINISTRA SPRAW ZAGRANICZNYCH¹⁾

z dnia 25 lipca 2013 r.

w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii tajnych oraz innych komórek organizacyjnych odpowiedzialnych za przetwarzanie materiałów niejawnych, sposobu i trybu przetwarzania informacji niejawnych oraz doboru i stosowania środków bezpieczeństwa fizycznego w Ministerstwie Spraw Zagranicznych oraz placówkach zagranicznych

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 I

Przepisy ogólne

§ 1. Zarządzenie określa:

- 1) wymagania w zakresie organizacji i funkcjonowania kancelarii tajnej, kancelarii tajnej międzynarodowej oraz innych komórek organizacyjnych odpowiedzialnych za przetwarzanie materiałów niejawnych;
- 2) strukturę organizacyjną systemu kancelaryjnego;
- 3) podstawowe zadania kierownika kancelarii tajnej, kancelarii tajnej międzynarodowej oraz pracownika prowadzącego obsługę kancelaryjną materiałów niejawnych;
- 4) sposób i tryb przetwarzania informacji niejawnych o klauzuli „poufne”, „tajne” i „ściśle tajne”;

¹⁾ Minister Spraw Zagranicznych kieruje działami administracji rządowej: sprawy zagraniczne oraz członkostwa Rzeczypospolitej Polskiej w Unii Europejskiej na podstawie § 1 ust. 2 rozporządzenia Prezesa Rady Ministrów z dnia 18 listopada 2011 r. w sprawie szczegółowego zakresu działania Ministra Spraw Zagranicznych (Dz. U. Nr 248, poz. 1492).

- 5) zasady doboru i zakres stosowania środków bezpieczeństwa fizycznego służących ochronie informacji niejawnych.

§ 2. Ilekczo w niniejszym zarządzeniu jest mowa o:

- 1) ustawie – należy przez to rozumieć ustawę z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228);
- 2) Ministerstwie – należy przez to rozumieć Ministerstwo Spraw Zagranicznych;
- 3) placówce zagranicznej – należy przez to rozumieć przedstawicielstwo dyplomatyczne, stałe przedstawicielstwo przy organizacji międzynarodowej, urząd konsularny, instytut polski lub inną placówkę podległą Ministrowi Spraw Zagranicznych, mającą siedzibę poza granicami Rzeczypospolitej Polskiej;
- 4) dyrektorze – należy przez to rozumieć dyrektora komórki organizacyjnej Ministerstwa;
- 5) kierownikowi placówki – należy przez to rozumieć pełnomocnego przedstawiciela Rzeczypospolitej Polskiej w innym państwie lub przy organizacji międzynarodowej, kierownika urzędu konsularnego, dyrektora instytutu polskiego oraz inną osobę wyznaczoną do kierowania placówką zagraniczną;
- 6) pełnomocnikowi ochrony – należy przez to rozumieć pełnomocnika lub zastępcę pełnomocnika do spraw ochrony informacji niejawnych w Ministerstwie;
- 7) pionie ochrony – należy przez to rozumieć wyodrębnioną komórkę organizacyjną Ministerstwa właściwą do spraw ochrony informacji niejawnych, podległą pełnomocnikowi ochrony;
- 8) PODN-Z – należy przez to rozumieć punkt obsługi dokumentów niejawnych stanowiący w placówce zagranicznej komórkę organizacyjną lub stanowisko pracy, których pracownicy zapewniają prawidłowe rejestrowanie, przechowywanie, wydawanie oraz obieg materiałów niejawnych o klauzuli „zastrzeżone” oraz „Restreint UE” i „NATO Restricted”;
- 9) PODN-Pf – należy przez to rozumieć punkt obsługi dokumentów niejawnych stanowiący w placówce zagranicznej komórkę organizacyjną lub stanowisko pracy, których pracownicy zapewniają w placówce zagranicznej prawidłowe rejestrowanie, przechowywanie, wydawanie oraz obieg materiałów niejawnych do klauzuli „poufne” włącznie;
- 10) PODN-T – należy przez to rozumieć punkt obsługi dokumentów niejawnych do klauzuli „tajne” stanowiący w placówce zagranicznej wyodrębnioną lokalizacyjnie komórkę organizacyjną, o której mowa w art. 44 ustawy, lub stanowisko pracy, których pracownicy zapewniają prawidłowe rejestrowanie, przechowywanie, wydawanie oraz obieg materiałów niejawnych do klauzuli „tajne” włącznie;

- 11) kancelarii tajnej – należy przez to rozumieć wyodrębnioną organizacyjnie i lokalizacyjnie komórkę organizacyjną, o której mowa w art. 42 ust. 4 ustawy, utworzoną w Ministerstwie;
- 12) kancelarii tajnej międzynarodowej – należy przez to rozumieć Główną Kancelarię Tajną NATO, UZE i UE dla sfery cywilnej RP, Podkancelarię Tajną NATO, UZE i UE w Ministerstwie, Punkty Kontroli NATO w placówkach zagranicznych, Podkancelarię Tajną NATO, UZE i UE w Stałym Przedstawicielstwie RP przy NATO, Podkancelarię Tajną NATO ATOMAL w Stałym Przedstawicielstwie RP przy NATO lub Podkancelarię Tajną NATO i UE w Stałym Przedstawicielstwie RP przy UE, akredytowane przez ABW i uprawnione do obsługi materiałów niejawnych UE lub NATO oznaczonych klauzulą stanowiącą odpowiednik klauzuli „poufne” lub wyższej;
- 13) sekretariacie komórki organizacyjnej – należy przez to rozumieć stanowisko pracy w komórce organizacyjnej Ministerstwa, właściwe do prowadzenia obsługi kancelaryjnej materiałów niejawnych i podległe bezpośrednio członkowi kierownictwa Ministerstwa lub dyrektorowi albo zastępcy dyrektora;
- 14) dokumencie niejawnym – należy przez to rozumieć dokument, o którym mowa w art. 2 pkt 3 ustawy;
- 15) materiale niejawnym – należy przez to rozumieć materiał, o którym mowa w art. 2 pkt 4 ustawy;
- 16) przesyłce niejawnej - należy przez to rozumieć odpowiednio zaadresowaną i oznaczoną kopertę, pakiet, paczkę lub pojemnik zawierające materiały niejawne, zabezpieczone zgodnie z zasadami określonymi w rozporządzeniu 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);
- 16) dekretacji – należy przez to rozumieć autoryzowaną, pisemną adnotację adresata, następcy prawnego adresata, osoby pisemnie przez niego upoważnionej lub właściwego przełożonego, zawierającą dyspozycje dotyczące sposobu dalszego postępowania z materiałem lub wskazanie osób, które powinny zapoznać się z zawartymi w nim informacjami niejawnymi;
- 17) strefie ochronnej I, II lub III – należy przez to rozumieć strefy, o których mowa w § 5 ust. 1 rozporządzenia Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych (Dz. U. poz. 683);
- 18) obsłudze kancelaryjnej materiałów niejawnych - należy przez to rozumieć zespół czynności wykonywanych w odniesieniu do materiałów niejawnych i na tych materiałach, w szczególności

rejestrwanie, przechowywanie, gromadzenie, zapewnienie ochrony, udostępnianie, wydawanie lub przekazywanie za pokwitowaniem osobom uprawnionym, nadzór nad obiegiem, kopiowanie oraz oznaczanie zmiany lub zniesienia klauzuli tajności;

- 19) dostępności informacji niejawnej - należy przez to rozumieć właściwość określającą, że informacja niejawna jest możliwa do wykorzystania na żądanie podmiotu uprawnionego w określonym czasie;
- 20) integralności informacji niejawnej - należy przez to rozumieć właściwość określającą, że informacja niejawna nie została zmodyfikowana w sposób nieuprawniony;
- 21) poufności informacji niejawnej - należy przez to rozumieć właściwość określającą, że informacja niejawna nie jest ujawniana podmiotom do tego nieuprawnionym.

§ 3. Nadzór nad wykonywaniem postanowień niniejszego zarządzenia sprawuje, w imieniu kierownika jednostki organizacyjnej, pełnomocnik ochrony.

§ 4. Dyrektor oraz kierownik placówki sprawują bezpośredni nadzór nad przestrzeganiem przez podległych pracowników przepisów o ochronie informacji niejawnych, w tym przepisów niniejszego zarządzenia.

§ 5. Materiały niejawne podlegają oznaczeniu zgodnie z rozporządzeniem Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności (Dz. U. Nr 288, poz. 1692).

§ 6. Zasady przekazywania przesyłek niejawnych pocztą dyplomatyczną regulują odrębne przepisy.

§ 7. Zasady przetwarzania informacji niejawnych w akredytowanych systemach teleinformatycznych oraz wykorzystywania nośników danych cyfrowych regulują odrębne przepisy.

§ 8. Sposób i tryb przetwarzania w Ministerstwie oraz placówkach zagranicznych informacji niejawnych o klauzuli „zastrzeżone” regulują odrębne przepisy.

§ 9. Tryb przetwarzania oraz zasady niszczenia i archiwizacji szyfrogramów oraz niejawnych biuletynów, briefów, notatek informacyjnych i pilnych notatek określają odrębne przepisy, z zastrzeżeniem § 12 ust. 1.

§ 10. 1. Informacje niejawne mogą być udostępniane w Ministerstwie oraz placówkach zagranicznych wyłącznie osobie do tego uprawnionej, zgodnie z przepisami ustawy dotyczącymi dostępu do informacji niejawnych o określonej klauzuli tajności, i tylko

w zakresie niezbędnym do wykonywania przez tę osobę pracy na zajmowanym stanowisku albo wykonywania czynności zleconych.

2. Osoba spełniająca wymogi określone w ust. 1 powinna być adresatem określonej informacji niejawnej, następcą prawnym adresata lub powinna posiadać jego pisemne upoważnienie do odbioru, zapoznawania się i dekretacji informacji niejawnych albo powinna zostać upoważniona do zapoznania się z określoną informacją niejawną poprzez jej dekretację. Wzór upoważnienia stanowi załącznik nr 1 do niniejszego zarządzenia.

3. Osoba realizująca w Ministerstwie lub placówce zagranicznej zadania związane z dostępem do informacji niejawnych o klauzuli „poufne” lub wyższej, powinna dawać rękojmię zachowania tajemnicy w rozumieniu art. 2 pkt 2 ustawy.

Rozdział II

Organizacja i funkcjonowanie systemu kancelaryjnego

§ 11. 1. Na system kancelaryjny służący zapewnieniu w Ministerstwie i placówkach zagranicznych prawidłowej obsługi kancelaryjnej materiałów niejawnych składają się:

- 1) kancelaria tajna w Ministerstwie, z uwzględnieniem możliwości tworzenia jej oddziałów oraz komórka organizacyjna Ministerstwa właściwa do spraw przetwarzania, dystrybucji i ekspedycji materiałów niejawnych;
- 2) kancelarie tajne międzynarodowe w Ministerstwie i placówkach zagranicznych;
- 3) PODN-T w placówkach zagranicznych;
- 4) PODN-Pf w placówkach zagranicznych;
- 5) PODN-Z w placówkach zagranicznych;
- 6) sekretariaty komórek organizacyjnych w Ministerstwie uprawnione do prowadzenia obsługi kancelaryjnej materiałów niejawnych do klauzuli „poufne” włącznie.

2. System kancelaryjny organizuje Dyrektor Generalny Służby Zagranicznej poprzez zatwierdzanie przedkładanych przez pełnomocnika ochrony wniosków w sprawie utworzenia, przekształcenia, zawieszenia działalności lub likwidacji komórek organizacyjnych, o których mowa w ust. 1, albo powierzenia sekretariatom zadań w zakresie prowadzenia obsługi kancelaryjnej materiałów niejawnych. Pełnomocnik ochrony wnioskuje w tych sprawach po dokonaniu uzgodnień z właściwymi kierownikami placówek oraz dyrektorami.

3. W Ministerstwie kancelaria tajna, kancelaria tajna międzynarodowa oraz komórka organizacyjna właściwa do spraw przetwarzania, dystrybucji i ekspedycji materiałów niejawnych

podlegają bezpośrednio pełnomocnikowi ochrony, a sekretariat komórki organizacyjnej uprawniony do prowadzenia obsługi kancelaryjnej materiałów niejawnych właściwemu dyrektorowi.

4. W placówce zagranicznej kancelaria tajna międzynarodowa, PODN-T, PODN-Pf lub PODN-Z podlega bezpośrednio kierownikowi placówki.

§ 12. 1. W Ministerstwie dla obsługi kancelaryjnej materiałów niejawnych o klauzuli „poufne”, „tajne” lub „ściśle tajne” właściwą komórką jest kancelaria tajna, a dla szyfrogramów i innych dokumentów niejawnych o klauzuli „poufne”, o których mowa w § 9, kancelaria tajna lub sekretariat komórki organizacyjnej uprawniony do ich obsługi.

2. W uzasadnionych przypadkach materiały niejawne oznaczone klauzulą „poufne” oraz „tajne” mogą być pobierane przez uprawnionego pracownika z sekretariatu komórki organizacyjnej lub kancelarii tajnej na czas niezbędny do realizacji zadań związanych z dostępem do informacji niejawnych, z uwzględnieniem wymogów określonych w § 48 ust. 2 i 3.

3. W uzasadnionych przypadkach, za zgodą pełnomocnika ochrony, w kancelarii tajnej mogą być przetwarzane informacje niejawne o klauzuli „zastrzeżone”.

4. Obsługę kancelaryjną materiałów niejawnych oznaczonych klauzulą „EU Confidential/Confidentiel UE” lub „NATO Confidential” oraz wyższą zapewnia na podstawie odrębnych przepisów kancelaria tajna międzynarodowa.

§ 13. 1. W placówce zagranicznej obsługę kancelaryjną materiałów niejawnych o klauzuli :

- 1) „tajne” zapewnia PODN-T;
- 2) „poufne” zapewnia PODN-Pf lub PODN-T;
- 3) „zastrzeżone” oraz „Restreint UE” i „NATO Restricted” zapewnia PODN-Z, PODN-Pf lub PODN-T;
- 4) „EU Confidential/Confidentiel UE”, „NATO Confidential”, „NATO Confidential ATOMAL” lub wyższej zapewnia na podstawie odrębnych przepisów właściwa kancelaria tajna międzynarodowa.

2. Materiały niejawne o klauzuli „poufne” lub wyższej nie mogą być przechowywane w placówce zagranicznej poza PODN-T lub PODN-Pf.

3. W placówce zagranicznej, w której zorganizowano PODN-Pf, dopuszcza się za zgodą pełnomocnika ochrony krótkotrwałe przechowywanie zamkniętych i oznaczonych jako poczta dyplomatyczna przesyłek niejawnych zawierających materiały o klauzuli wyższej niż „poufne”.

4. W placówce zagranicznej, w której zorganizowano PODN-T, dopuszcza się za zgodą pełnomocnika ochrony krótkotrwałe przechowywanie zamkniętych i oznaczonych jako poczta dyplomatyczna przesyłek niejawnych zawierających materiały o klauzuli wyższej niż „tajne”.

§ 14. 1 W pomieszczeniach kancelarii tajnej, kancelarii tajnej międzynarodowej, PODN-T, PODN-Pf, można wydzielić miejsce, w którym osoby uprawnione będą zapoznawać się z materiałami niejawnymi, zwane czytelnią, zapewniające stały nadzór nad udostępnianymi materiałami niejawnymi przez osobę prowadzącą ich obsługę kancelaryjną.

2. W czytelnii nie instaluje się systemu monitoringu wizyjnego.

§ 15. 1. W Ministerstwie kancelarią tajną lub kancelarią tajną międzynarodową kieruje pracownik pionu ochrony wyznaczony przez Dyrektora Generalnego Służby Zagranicznej na stanowisko kierownika kancelarii, na wniosek pełnomocnika ochrony w uzgodnieniu z dyrektorem komórki właściwej w sprawach osobowych.

2. W placówce zagranicznej kancelarią tajną międzynarodową kieruje kierownik wyznaczony przez kierownika placówki w uzgodnieniu z dyrektorem komórki właściwej w sprawach osobowych oraz za zgodą pełnomocnika ochrony.

§ 16. Do zadań kierownika kancelarii tajnej oraz kierownika kancelarii tajnej międzynarodowej należy:

- 1) prowadzenie rejestru dzienników ewidencji i teczek;
- 2) bezpośredni nadzór nad prawidłowym rejestrowaniem przez pracowników kancelarii, przechowywaniem, udostępnianiem i obiegiem materiałów niejawnych oraz wydawaniem za pokwitowaniem materiałów niejawnych osobom do tego uprawnionym, które zapewniają odpowiednie warunki ich przechowywania;
- 3) prowadzenie i aktualizacja wykazu osób uprawnionych do dostępu do informacji niejawnych, obejmującego imię i nazwisko, termin upływu ważności uprawnień w odniesieniu do poszczególnych klauzul tajności, datę ostatniego szkolenia w zakresie ochrony informacji niejawnych;
- 4) każdorazowe sprawdzanie przed udostępnieniem materiału niejawnego uprawnień adresata lub osoby wskazanej w dekretacji do dostępu do informacji niejawnych o klauzuli tajności odpowiadającej klauzuli materiału niejawnego;
- 5) wydawanie za pokwitowaniem materiałów niejawnych osobom do tego uprawnionym, które zapewniają odpowiednie warunki do ich przechowywania;

- 6) zapewnienie możliwości ustalenia w każdych okolicznościach, gdzie znajduje się zarejestrowany materiał niejawnny;
- 7) weryfikacja prawidłowości oznaczania materiałów niejawnnych;
- 8) egzekwowanie zwrotu udostępnionych lub wydanych materiałów niejawnnych;
- 9) niezwłoczne powiadomianie o stwierdzonych nieprawidłowościach w zakresie obsługi kancelaryjnej materiałów niejawnnych oraz innych zdarzeniach związanych z przetwarzaniem informacji niejawnnych mogących stanowić naruszenie obowiązujących przepisów, w Ministerstwie pełnomocnika ochrony, a w placówce zagranicznej kierownika placówki;
- 10) wykonywanie innych czynności z zakresu obsługi kancelaryjnej materiałów niejawnnych;
- 11) nadzór nad realizacją przez podległych pracowników wymogu prawidłowego zabezpieczenia użytkowanych szaf metalowych i pomieszczeń po zakończeniu pracy.

§ 17. 1. Do zakresu obowiązków pracownika komórki organizacyjnej, o której mowa w § 11 ust. 1 należy w szczególności:

- 1) wykonywanie czynności z zakresu obsługi kancelaryjnej materiałów niejawnnych;
- 2) prowadzenie i aktualizacja wykazu osób uprawnionych do dostępu do informacji niejawnnych, obejmującego imię i nazwisko, termin upływu ważności uprawnień w odniesieniu do poszczególnych klauzul tajności, datę ostatniego szkolenia w zakresie ochrony informacji niejawnnych;
- 3) każdorazowe sprawdzanie przed udostępnieniem materiału niejawnego uprawnień adresata lub osoby wskazanej w dekretacji do dostępu do informacji niejawnnych o klauzuli tajności odpowiadającej klauzuli materiału niejawnego;
- 4) wydawanie za pokwitowaniem materiałów niejawnnych osobom do tego uprawnionym, które zapewniają odpowiednie warunki do ich przechowywania;
- 5) zapewnienie możliwości ustalenia w każdych okolicznościach, gdzie znajduje się zarejestrowany materiał niejawnny;
- 6) weryfikacja prawidłowości oznaczania materiałów niejawnnych;
- 7) egzekwowanie zwrotu udostępnionych lub wydanych materiałów niejawnnych;
- 8) niezwłoczne powiadomianie właściwego przełożonego o stwierdzonych nieprawidłowościach w zakresie obsługi kancelaryjnej materiałów niejawnnych oraz innych zdarzeniach związanych z przetwarzaniem informacji niejawnnych mogących stanowić naruszenie obowiązujących przepisów;

9) każdorazowe zabezpieczanie po zakończeniu pracy użytkowanych szaf metalowych i pomieszczeń.

2. W placówce zagranicznej pracownik PODN-T lub PODN-Pf oprócz zadań określonych w ust 1. prowadzi także rejestr dzienników ewidencji i teczek.

§ 18. 1. W Ministerstwie obsługę kancelaryjną materiałów niejawnych o klauzuli „poufne” lub wyższej prowadzi pracownik posiadający:

- 1) poświadczenie bezpieczeństwa uprawniające do dostępu do informacji niejawnych o klauzuli odpowiadającej najwyższej klauzuli obsługiwanych materiałów niejawnych;
- 2) aktualne zaświadczenie o odbytym szkoleniu w zakresie ochrony informacji niejawnych oraz informacji niejawnych UE i NATO,
- 3) zaświadczenie o odbytym specjalistycznym szkoleniu w zakresie prowadzenia obsługi kancelaryjnej materiałów niejawnych, zorganizowanym przez pełnomocnika ochrony.

2. W placówce zagranicznej obsługę kancelaryjną materiałów niejawnych o klauzuli „poufne” lub wyższej zapewnia pracownik wyznaczony przez kierownika placówki w uzgodnieniu z dyrektorem komórki właściwej w sprawach osobowych oraz za zgodą pełnomocnika ochrony, spełniający wymagania określone w ust. 1 pkt 1-3.

§ 19. 1. Przejęcie obowiązków w zakresie prowadzenia obsługi kancelaryjnej materiałów niejawnych odbywa się na podstawie protokołu zdawczo-odbiorczego, którego wzór określa załącznik nr 2 do niniejszego zarządzenia.

2. Protokół, o którym mowa w ust. 1, sporządza się:

- 1) w Ministerstwie - w egzemplarzu pojedynczym, który jest przekazywany do wiadomości pełnomocnikowi ochrony, a po dokonaniu zwrotu jest przechowywany we właściwym sekretariacie komórki organizacyjnej lub w kancelarii tajnej albo kancelarii tajnej międzynarodowej;
- 2) w placówce zagranicznej - w dwóch egzemplarzach, z których pierwszy przechowywany jest we właściwym PODN-T, PODN-Pf lub w kancelarii tajnej międzynarodowej, a drugi przekazywany jest pełnomocnikowi ochrony.

3. W przypadku czasowej nieobecności osoby prowadzącej obsługę kancelaryjną materiałów niejawnych jej obowiązki przejmuje na podstawie protokołu zdawczo-odbiorczego inny pracownik wyznaczony przez właściwego dyrektora lub kierownika placówki, spełniający wymagania określone w § 18 ust. 1 pkt 1-3, a o fakcie tym jest powiadamiany pełnomocnik ochrony. W takim przypadku protokół zdawczo-odbiorczy sporządza się w egzemplarzu pojedynczym, który jest przechowywany

we właściwym sekretariacie komórki organizacyjnej, PODN-T, PODN-Pf, kancelarii tajnej lub kancelarii tajnej międzynarodowej.

§ 20. 1. Otwarcia pomieszczenia i szaf metalowych służących do przechowywania materiałów niejawnych podczas nieobecności osoby prowadzącej ich obsługę kancelaryjną, może dokonać komisja składająca się co najmniej z dwóch osób spełniających wymagania określone w § 18 ust. 1 pkt 1-2.

2. Komisję powołuje odpowiednio pełnomocnik ochrony, dyrektor właściwej komórki organizacyjnej lub kierownik placówki zgodnie z § 11 ust. 3 i 4.

3. Wzór protokołu komisyjnego pobrania materiałów niejawnych określa załącznik nr 3 do niniejszego zarządzenia.

4. Z protokołem, o którym mowa w ust. 3 zapoznawana jest po powrocie do pracy osoba, o której mowa w ust. 1.

Rozdział III

Sposób i tryb przetwarzania materiałów niejawnych o klauzuli „poufne” lub wyższej

§ 21. Przesyłki przychodzące, zawierające materiały niejawne przyjmują za pokwitowaniem:

- 1) w Ministerstwie – komórki organizacyjne właściwe do spraw obsługi przesyłek przychodzących i po zarejestrowaniu wpływu przekazują za pokwitowaniem, bez otwierania kopert wewnętrznych, do kancelarii tajnej lub kancelarii tajnej międzynarodowej;
- 2) w placówce zagranicznej – PODN-Pf, PODN-T lub kancelaria tajna międzynarodowa.

§ 22. 1. W Ministerstwie, po godzinach urzędowania i w dni wolne od pracy, przesyłki o których mowa w § 21, przyjmuje za pokwitowaniem w książce dyżurów właściwy pracownik Centrum Operacyjnego spełniający wymagania określone w § 18 ust. 1 pkt 1-2.

2. Dyżurny Centrum Operacyjnego przekazuje przesyłkę w najbliższym dniu roboczym do kancelarii tajnej, lub kancelarii tajnej międzynarodowej.

§ 23. W przypadku stwierdzenia uszkodzenia przesyłki zawierającej materiały niejawne osoba kwitująca jej odbiór sporządza, wraz z doręczającym, protokół, o którym mowa w § 16 rozporządzenia Prezesa Rady Ministrów w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne.

§ 24. 1. Po otwarciu przesyłki zawierającej materiały niejawne, osoba prowadząca ich obsługę kancelaryjną sprawdza prawidłowość oznaczeń, zgodność zawartości przesyłki z wyszczególnionymi

na niej numerami ewidencyjnymi, zgodność liczby stron lub innych jednostek miary oraz liczby załączników z informacjami umieszczonymi na poszczególnych materiałach.

2. W przypadku stwierdzenia nieprawidłowości w zakresie, o którym mowa w ust. 1 osoba prowadząca obsługę kancelaryjną sporządza pisemne oświadczenie zawierające opis nieprawidłowości, które jest za pośrednictwem przełożonego niezwłocznie przekazywane pełnomocnikowi ochrony. Fakt powiadomienia pełnomocnika ochrony o stwierdzonych nieprawidłowościach odnotowuje się w odpowiednim dzienniku ewidencji w rubryce „informacje uzupełniające/uwagi”.

§ 25. Materiał niejawnny oznaczony klauzulą „poufne” lub równorzędną otrzymany podczas spotkań międzynarodowych poza terytorium Rzeczypospolitej Polskiej, powinien być przekazany do najbliższej placówki zagranicznej, zgodnie z § 21 pkt 2, a jeżeli nie jest to możliwe, dopuszczalny jest jego osobisty przewóz do Ministerstwa na zasadach określonych w § 23 rozporządzenia Prezesa Rady Ministrów w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne, zgodnie z § 21 pkt 1 oraz § 22 niniejszego zarządzenia.

§ 26. 1. Kancelaria tajna, kancelaria tajna międzynarodowa, PODN-T, PODN-Pf oraz sekretariat komórki organizacyjnej prowadzą dzienniki ewidencji określone w rozporządzeniu Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych, z zastrzeżeniem § 53 niniejszego zarządzenia.

2. W przypadkach uzasadnionych organizacją ochrony informacji niejawnych można prowadzić dodatkowo inne dzienniki ewidencji niż wymienione w ust. 1, w szczególności kartę obiegu materiału niejawnego, która podlega archiwizacji łącznie z dziennikiem ewidencji, w którym materiał został zarejestrowany. Fakt założenia karty obiegu materiału niejawnego odnotowuje się w odpowiednim dzienniku ewidencji w rubryce „informacje uzupełniające/uwagi”. Wzór karty obiegu materiału niejawnego określa załącznik nr 4 do niniejszego zarządzenia.

3. Dopuszcza się, za pisemną zgodą pełnomocnika ochrony, prowadzenie dzienników ewidencji w formie elektronicznej.

§ 27. 1. Każdą otrzymaną albo wysyłąną przesyłkę, bądź wytworzony dokument lub inny materiał niejawnny osoba prowadząca obsługę kancelaryjną niezwłocznie rejestruje w odpowiednim dzienniku ewidencji, w kolejności otrzymania lub wytworzenia w okresie roku kalendarzowego.

2. Materiały niejawne otrzymane w ramach wymiany z UE i NATO podlegają rejestracji w osobnych dziennikach ewidencji, prowadzonych odrębnie dla każdej organizacji międzynarodowej.

3. Obieg każdego materiału niejawnego podlega dokumentowaniu w odpowiednim dzienniku ewidencji, w szczególności poprzez potwierdzenie podpisami osób otrzymujących określone materiały niejawne faktu ich pobrania oraz potwierdzenie podpisem osoby prowadzącej obsługę kancelaryjną faktu dokonania ich zwrotu.

4. Do każdego materiału niejawnego o klauzuli „tajne” lub „ściśle tajne” z chwilą jego udostępnienia zakłada się kartę zapoznania się z dokumentem. W karcie odnotowuje się fakt każdorazowego udostępnienia materiału niejawnego osobie uprawnionej. Kartę archiwizuje się wraz z materiałem niejawnym lub z protokołem zniszczenia, albo pismem przewodnim o odesłaniu.

§ 28. 1. Zapisów w dziennikach ewidencji, o których mowa w § 26, dokonuje się atramentem lub tuszem w kolorze niebieskim lub czarnym. Zmian w zapisach dokonuje się atramentem lub tuszem w kolorze czerwonym, umieszczając datę, imię i nazwisko oraz podpis osoby dokonującej zmiany.

2. W przypadku anulowania pozycji w dziennikach ewidencji, o których mowa w § 26, podaje się powód anulowania oraz umieszcza się datę, imię i nazwisko oraz podpis osoby dokonującej anulowania. Anulowania pozycji dokonuje się atramentem lub tuszem w kolorze czerwonym.

3. Zabrania się wycierania, zamazywania lub nadpisywania zapisów dokonanych w dziennikach ewidencji, o których mowa w § 26.

§ 29. 1. Osoba prowadząca obsługę kancelaryjną nie otwiera przesyłek zawierających materiały niejawne, oznaczonych „do rąk własnych”. W odpowiednim dzienniku ewidencji umieszcza informacje o nadawcy, numerze i dacie wpływu przesyłki oraz jej oznaczeniu „do rąk własnych”. Na opakowaniu każdej przesyłki wpisuje datę wpływu i numer, pod którym została zarejestrowana.

2. Przesyłka, o której mowa w ust. 1, przekazywana jest w stanie zamkniętym, za pokwitowaniem adresatowi, następcy prawnemu adresata lub osobie pisemnie przez niego upoważnionej do odbioru.

3. Po otwarciu przesyłki, o której mowa w ust. 1, jej odbiorca wykonuje czynności określone w § 24.

4. Adresat przesyłki, o której mowa w ust. 1, może poprzez dekretację znieść oznaczenie „do rąk własnych”. Z chwilą zwrotu przesyłki osoba prowadząca obsługę kancelaryjną uzupełnia dane dotyczące przesyłki w odpowiednim dzienniku ewidencji.

§ 30. 1. Przesyłki zawierające materiały niejawne, wychodzące do adresatów zewnętrznych oraz dyrektorów komórek organizacyjnych zlokalizowanych w innych obiektach niż budynki Ministerstwa przy Al. J.Ch. Szucha 21, 23, 23A przekazuje za pokwitowaniem w wykazie przesyłek nadanych:

- 1) w Ministerstwie – kancelaria tajna, kancelaria tajna międzynarodowa lub sekretariat komórki organizacyjnej do komórki właściwej do spraw ekspedycji materiałów niejawnych lub do komórki właściwej do spraw poczty dyplomatycznej;
- 2) w placówce zagranicznej – kancelaria tajna międzynarodowa, PODN-T lub PODN-Pf, zgodnie z zasadami określonymi dla poczty dyplomatycznej.

2. Przekazanie materiałów niejawnych między komórkami organizacyjnymi zlokalizowanymi w budynkach Ministerstwa przy Al. J.Ch. Szucha 21, 23, 23A odbywa się wyłącznie za pośrednictwem kancelarii tajnej lub sekretariatu komórki organizacyjnej, za pokwitowaniem w książce doręczeń przesyłek miejscowych.

§ 31. Osoba, której wydano materiał niejawny, jest obowiązana dokonać jego zwrotu:

niezwłocznie po wykorzystaniu materiału;

- 1) na żądanie osoby prowadzącej obsługę kancelaryjną materiałów niejawnych lub pełnomocnika ochrony;
- 2) w przypadku zmiany zakresu obowiązków służbowych, przeniesienia na inne stanowisko pracy albo rozwiązania stosunku pracy.

§ 32. Przekazywanie materiałów niejawnych bezpośrednio pomiędzy osobami, które są uprawnione do zapoznania się z informacjami niejawnymi zawartymi w tych materiałach, jest zabronione.

§ 33. Udostępnienie materiału niejawnego uprawnionej osobie spoza Ministerstwa lub placówki zagranicznej, może nastąpić na podstawie dekretacji właściwego członka kierownictwa Ministerstwa, dyrektora lub kierownika placówki. Dekretacja ta powinna określać sposób i zakres udostępnienia informacji niejawnych.

§ 34. 1. Dokumenty niejawne mogą być wytwarzane przez uprawnione osoby:

- 1) w odpowiednich, akredytowanych systemach teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych;
- 2) przy użyciu mechanicznych maszyn do pisania;
- 3) odręcznie.

§ 35. Wydruki, kopie, w tym odwzorowania cyfrowe, a także odpisy, wypisy, wyciągi, parafrazy i tłumaczenia dokumentów niejawnych mogą być wytwarzane wyłącznie na podstawie dekretacji właściwego dyrektora, jego przełożonego, kierownika placówki lub osoby pisemnie do tego upoważnionej.

§ 36. Zarejestrowany projekt dokumentu niejawnego, który nie został podpisany przez osobę uprawnioną, wykonawca niezwłocznie przekazuje:

- 1) w Ministerstwie – do kancelarii tajnej, sekretariatu komórki organizacyjnej lub kancelarii tajnej międzynarodowej;
- 2) w placówce zagranicznej – do PODN-Pf, PODN-T lub kancelarii tajnej międzynarodowej.

§ 37. 1. Materiały niejawne przechowywane w kancelarii tajnej, kancelarii tajnej międzynarodowej, PODN-T lub PODN-Pf podlegają komisijnemu przeglądowi pod kątem oceny ich dalszej przydatności, brakowania oraz wydzielenia materiałów archiwalnych w oparciu o „Jednolity Rzeczowy Wykaz Akt Ministerstwa Spraw Zagranicznych i placówek zagranicznych”. Przegląd dokonywany jest corocznie w I połowie roku kalendarzowego.

2. Materiały niejawne wytworzone w komórce organizacyjnej Ministerstwa lub placówce zagranicznej podlegają przeglądowi, o którym mowa w ust. 1, również w aspekcie ustalenia, czy spełniają ustawowe przesłanki ochrony. Za powiadomienie odbiorców materiałów niejawnych, w odniesieniu do których podjęto decyzję o zmianie lub zniesieniu klauzuli tajności, odpowiedzialny jest właściwy członek kierownictwa Ministerstwa, dyrektor lub kierownik placówki.

3. Komisję dla dokonania przeglądu materiałów niejawnych, o którym mowa w ust. 1 i 2, powołuje decyzją, której wzór określa załącznik nr 5 do niniejszego zarządzenia:

- 1) w Ministerstwie – pełnomocnik ochrony na wniosek właściwego członka kierownictwa Ministerstwa lub dyrektora;
- 2) w placówce zagranicznej – kierownik placówki.

4. Komisja z czynności, o których mowa w ust. 1 i 2, sporządza protokół, którego wzór określa załącznik nr 6 do niniejszego zarządzenia. W Ministerstwie protokół po zatwierdzeniu przez właściwego członka kierownictwa Ministerstwa lub dyrektora jest przedkładany do wiadomości pełnomocnikowi ochrony.

5. W skład komisji wchodzi co najmniej dwie osoby posiadające uprawnienia dostępu do informacji niejawnych o klauzuli odpowiadającej najwyższej klauzuli materiałów niejawnych przetwarzanych w komórce organizacyjnej Ministerstwa lub placówce zagranicznej. Komisji powinien przewodniczyć pracownik gwarantujący właściwą ocenę merytoryczną materiałów niejawnych. W skład komisji powinna wejść osoba prowadząca obsługę kancelaryjną materiałów niejawnych podlegających przeglądowi.

6. Materiały niejawne niszczy się komisyjnie w warunkach uniemożliwiających osobom nieupoważnionym wgląd do nich lub ich przejęcie, w odpowiednich urządzeniach w sposób

uniemożliwiający odczytanie lub odtworzenie treści zniszczonej informacji. Za całkowite zniszczenie materiałów odpowiada w szczególności przewodniczący komisji.

§ 38. Materiały niejawne wytworzone w placówce zagranicznej, których egzemplarz został przesłany do Ministerstwa, podlegają komisijnemu zniszczeniu w placówce zagranicznej.

§ 39. Osoba prowadząca obsługę kancelaryjną materiałów niejawnych odnotowuje fakt zniszczenia materiału niejawnego we właściwym dzienniku ewidencji poprzez umieszczenie informacji o numerze protokołu zniszczenia i numerze pozycji.

§ 40. Zasady niszczenia nośników danych cyfrowych zawierających informacje niejawne określają odrębne przepisy.

§ 41. Pracownik, który stwierdził fakt utraty, zagubienia lub przypadkowego zniszczenia materiału niejawnego albo innego naruszenia przepisów o ochronie informacji niejawnych, w szczególności nieuprawnionego ujawnienia informacji, jest obowiązany niezwłocznie powiadomić o zdarzeniu właściwego dyrektora lub kierownika placówki poprzez złożenie pisemnego oświadczenia o okolicznościach tego zdarzenia. Dyrektor lub kierownik placówki niezwłocznie powiadamia w formie pisemnej o zdarzeniu pełnomocnika ochrony, załączając oświadczenie pracownika.

§ 42. 1. Obieg materiałów niejawnych, przestrzeganie przepisów o ochronie informacji niejawnych oraz sprawdzenie, czy stan faktyczny materiałów niejawnych jest zgodny z ich stanem ewidencyjnym, są przedmiotem corocznych kontroli przeprowadzanych w Ministerstwie przez pełnomocnika ochrony, z których sprawozdania podlegają zatwierdzeniu przez Dyrektora Generalnego Służby Zagranicznej.

2. W placówce zagranicznej kierownik placówki powołuje w drodze pisemnej decyzji spośród podległych pracowników, posiadających uprawnienia dostępu do informacji niejawnych o klauzuli odpowiadającej najwyższej klauzuli przetwarzanych w placówce zagranicznej materiałów niejawnych, komisję do przeprowadzenia corocznej kontroli ochrony informacji niejawnych. Komisja sporządza w terminie do dnia 31 marca sprawozdanie o ochronie informacji niejawnych za rok ubiegły, podlegające zatwierdzeniu przez kierownika placówki. Jeden egzemplarz sprawozdania jest przekazywany pełnomocnikowi ochrony, a drugi jest przechowywany w placówce zagranicznej. Wzór sprawozdania stanowi załącznik nr 7 do niniejszego zarządzenia.

Rozdział IV

Zasady doboru i stosowania środków bezpieczeństwa fizycznego

§ 43. 1. W celu doboru adekwatnych środków bezpieczeństwa fizycznego w Ministerstwie i placówkach zagranicznych, dla pomieszczenia lub obszaru, w którym są przetwarzane informacje niejawne określa się poziom zagrożeń związanych z utratą poufności, integralności lub dostępności informacji niejawnych, zwany dalej „poziomem zagrożeń” .

2. Określenie poziomu zagrożeń wymaga dokonania analizy, w której uwzględnia się wszystkie istotne czynniki mogące mieć wpływ na bezpieczeństwo informacji niejawnych.

3. Poziom zagrożeń określa się przed rozpoczęciem przetwarzania informacji niejawnych, a także po każdej zmianie czynników, o których mowa w ust. 2, z uwzględnieniem § 54 niniejszego zarządzenia.

4. Rodzaje zagrożeń oraz podstawowe kryteria i sposób określania poziomu zagrożeń określa rozporządzenie Rady Ministrów w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych.

5. Za przeprowadzenie analizy, o której mowa w ust. 2, oraz sporządzenie i aktualizację dokumentacji określającej poziom zagrożeń i dobór adekwatnych środków bezpieczeństwa fizycznego odpowiada:

- 1) w Ministerstwie - pełnomocnik ochrony;
- 2) w placówce zagranicznej – kierownik placówki lub osoba przez niego wyznaczona, przy czym każdorazowo jeden egzemplarz dokumentacji przesyłany jest do pełnomocnika ochrony.

6. Dokumentacja, o której mowa w ust. 5 podlega zatwierdzeniu w Ministerstwie przez Dyrektora Generalnego Służby Zagranicznej, a w placówce zagranicznej przez kierownika placówki.

§ 44. 1. We wszystkich pomieszczeniach i obszarach, w których są przetwarzane informacje niejawne, stosuje się środki bezpieczeństwa fizycznego odpowiednie dla określonego poziomu zagrożeń.

2. W zależności od poziomu zagrożeń stosuje się odpowiednią kombinację następujących środków bezpieczeństwa fizycznego:

- 1) personel ochrony - osoby przeszkolone, nadzorowane, wykonujące czynności związane z fizyczną ochroną obiektów, w tym reagowanie na alarmy lub sygnały awaryjne;
- 2) bariery fizyczne - środki chroniące granice obszarów lub pomieszczeń, w których są przetwarzane informacje niejawne, w szczególności ogrodzenia, bramy, ściany, drzwi i okna;

- 3) szafy i zamki - stosowane do przechowywania informacji niejawnych lub zabezpieczające te informacje przed nieuprawnionym dostępem;
- 4) system kontroli dostępu - obejmujący elektroniczny system pomocniczy lub rozwiązanie organizacyjne, stosowane w celu zagwarantowania uzyskiwania dostępu do pomieszczenia lub obszaru, w którym są przetwarzane informacje niejawne, wyłącznie przez osoby posiadające odpowiednie uprawnienia;
- 5) system sygnalizacji włamania i napadu - elektroniczny system pomocniczy stosowany w celu podwyższenie poziomu bezpieczeństwa, który zapewniają bariery fizyczne, a w pomieszczeniach i budynkach zastępujący lub wspierający pracowników ochrony;
- 6) system dozoru wizyjnego - elektroniczny system pomocniczy stosowany w celu bieżącego monitorowania ochronnego lub sprawdzania incydentów bezpieczeństwa i sygnałów alarmowych przez pracowników ochrony;
- 7) system kontroli osób, przedmiotów i pojazdów - rozwiązanie organizacyjne przy ew. wykorzystaniu elektronicznego systemu pomocniczego lub sprzętu, polegające na zapewnieniu kontroli osób, przedmiotów wnoszonych do lub wnoszonych z obiektu, a także pojazdów stosowane w celu zapobiegania próbom nieuprawnionego wnoszenia na chroniony obszar rzeczy zagrażających bezpieczeństwu informacji niejawnych lub nieuprawnionego wnoszenia materiałów niejawnych z budynków lub obiektów.

3. Zakres stosowania środków bezpieczeństwa fizycznego powinien odpowiadać co najmniej wartości arytmetycznej osiągniętej w wyniku zastosowania metodyki doboru środków bezpieczeństwa fizycznego określonej w załączniku nr 8 do niniejszego zarządzenia.

§ 45. 1. Kryteria tworzenia stref ochronnych określa rozporządzenie Rady Ministrów w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych.

2. Za wyznaczenie i organizację stref ochronnych odpowiada:

- 1) w Ministerstwie - pełnomocnik ochrony;
- 2) w placówkach zagranicznych - kierownik placówki po dokonaniu uzgodnień z komórką organizacyjną właściwą do spraw bezpieczeństwa dyplomatycznego i ochrony informacji niejawnych.

§ 46. W Ministerstwie lub placówce zagranicznej w strefie ochronnej I lub II można utworzyć pomieszczenie wzmocnione. Konstrukcja pomieszczenia powinna zapewniać ochronę równoważną ochronie zapewnianej przez odpowiednie szafy metalowe przeznaczone do przechowywania

materiałów niejawnych o określonej klauzuli tajności. W pomieszczeniu wzmocnionym dopuszczalne jest przechowywanie materiałów niejawnych poza wymaganymi szafami.

§ 47. Klucze i kody dostępu do szaf, 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 każdorazowo w przypadku:

- 1) zmiany składu osób znających kod;
- 2) zaistnienia podejrzenia, że osoba nieuprawniona mogła poznać kod;
- 3) gdy zamek poddano konserwacji lub naprawie.

§ 48. 1. W Ministerstwie informacje niejawne o klauzuli „ściśle tajne” przetwarza się w strefie ochronnej I lub II, zabezpieczonej systemem sygnalizacji włamania i napadu z wykorzystaniem systemu dozoru wizyjnego, oraz przechowuje w szafach metalowych, w których zastosowano środki bezpieczeństwa K1S1 typ 4 oraz K1S2 typ 4 określone w załączniku nr 8 do niniejszego zarządzenia, albo w pomieszczeniu wzmocnionym.

2. W Ministerstwie lub placówce zagranicznej informacje niejawne o klauzuli „tajne” przetwarza się w strefie ochronnej I lub II i przechowuje się w szafach metalowych w których zastosowano środki bezpieczeństwa K1S1 typ 4 lub typ 3 oraz K1S2 typ 4 lub typ 3 określone w załączniku nr 8 do niniejszego zarządzenia, albo w pomieszczeniu wzmocnionym.

3. W Ministerstwie lub placówce zagranicznej informacje niejawne o klauzuli „poufne” przetwarza się w strefie ochronnej I, II lub III i przechowuje się w strefie ochronnej I lub II w szafach metalowych lub w pomieszczeniu wzmocnionym.

§ 49. 1. W Ministerstwie i placówkach zagranicznych, w których są przetwarzane informacje niejawne, opracowuje się i aktualizuje plany ochrony informacji niejawnych.

2. Podstawowe elementy, które powinien zawierać plan ochrony, określa rozporządzenie Rady Ministrów w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych.

3. Plan ochrony informacji niejawnych w Ministerstwie jest opracowywany i aktualizowany przez pełnomocnika ochrony i podlega zatwierdzeniu przez kierownika jednostki organizacyjnej.

4. Plan ochrony informacji niejawnych w placówce zagranicznej jest opracowywany i aktualizowany przez kierownika placówki lub osobę przez niego wyznaczoną i podlega zatwierdzeniu przez kierownika placówki.

Rozdział V

Przepisy przejściowe i końcowe

§ 50. Przekształcenie Głównej Kancelarii Tajnej i jej oddziałów w Kancelarię Tajną Ministerstwa Spraw Zagranicznych oraz utworzenie w placówkach zagranicznych PODN-T, PODN-Pf, PODN-Z nastąpi do dnia 30 czerwca 2014 r.

§ 51. 1. Dyrektorzy przeprowadzą w terminie do dnia 31 grudnia 2013 r. przegląd materiałów niejawnych wytworzonych w podległych im komórkach organizacyjnych w okresie przed dniem 2 stycznia 2011 r., w celu ustalenia czy spełniają przesłanki ochrony określone w ustawie i stosownie do tego podejmą decyzje dotyczące obniżenia, zniesienia lub utrzymania klauzuli tajności. Przeglądowi podlegają materiały niejawne, które nie zostały przekazane do komórki właściwej w sprawach archiwum.

2. Kierownik placówki dokona przeglądu, o którym mowa w ust. 1 w odniesieniu do materiałów niejawnych wytworzonych i przechowywanych w placówce zagranicznej.

3. W przypadku materiału niejawnego wytworzonego i zniszczonego w placówce zagranicznej, którego egzemplarz został przesłany do Ministerstwa, przeglądu dokonuje dyrektor komórki organizacyjnej, do której materiał został przekazany. Decyzję dotyczącą obniżenia, zniesienia lub utrzymania klauzuli tajności podejmuje kierownik placówki na wniosek właściwego dyrektora.

§ 52. Szczegółowe zasady postępowania z materiałami niejawnymi w archiwum Ministerstwa zostaną określone w wytycznych dyrektora właściwego do spraw archiwum i zarządzania informacją, w uzgodnieniu z pełnomocnikiem ochrony, w terminie 90 dni od wejścia w życie niniejszego zarządzenia.

§ 53. 1. Wzory dzienników ewidencji, o których mowa w § 26, wprowadza się z dniem 1 stycznia 2014 roku.

2. W okresie do dnia 31 grudnia 2013 r. stosuje się dotychczasowe urządzenia ewidencyjne, zgodnie z § 12 rozporządzenia Rady Ministrów w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych.

§ 54. Dokumentacja określająca poziom zagrożeń i dobór adekwatnych środków bezpieczeństwa fizycznego oraz plany ochrony informacji niejawnych w Ministerstwie i placówkach zagranicznych, zostaną opracowane i zatwierdzone w terminie do dnia 30 czerwca 2015 r.

§ 55. Dostosowanie w Ministerstwie i placówkach zagranicznych kombinacji środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych do wskazanego poziomu zagrożeń oraz organizacji stref ochronnych do wymagań określonych w rozporządzeniu Rady Ministrów w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych nastąpi do dnia 30 czerwca 2015 r.

§ 56. Tracą moc:

- 1) zarządzenie Nr 16 Ministra Spraw Zagranicznych z dnia 28 czerwca 2000 roku w sprawie szczególnych zasad organizacji kancelarii tajnych, stosowania środków ochrony fizycznej oraz obiegu informacji niejawnych w Ministerstwie Spraw Zagranicznych, przedstawicielstwach dyplomatycznych, stałych przedstawicielstwach przy organizacjach międzynarodowych, urzędach konsularnych i instytutach polskich;
- 2) decyzja Nr 11 Ministra Spraw Zagranicznych z dnia 13 kwietnia 2006 r. w sprawie określenia stanowisk oraz rodzajów prac zleconych w Ministerstwie Spraw Zagranicznych, z którymi może łączyć się dostęp do informacji niejawnych;
- 3) decyzja Nr 6 Dyrektora Generalnego z dnia 23 grudnia 2002 r. w sprawie utworzenia i organizacji Głównej Kancelarii Tajnej w Ministerstwie Spraw Zagranicznych.

§ 57. Zarządzenie wchodzi w życie z dniem ogłoszenia.

Minister Spraw Zagranicznych: *Radostaw Sikorski*

**Załącznik nr 1
do zarządzenia Nr 14
Ministra Spraw Zagranicznych
z dnia 25 lipca 2013 r.**

Egz. pojedynczy

.....
(nazwa komórki organizacyjnej / placówki zagranicznej)

.....
(sygnatura dokumentu)

UPOWAŻNIENIE

Zgodnie z § 10 ust.2 zarządzenia nr Ministra Spraw Zagranicznych z dnia 2013 roku w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii tajnych oraz innych komórek organizacyjnych odpowiedzialnych za przetwarzanie materiałów niejawnych, sposobu i trybu przetwarzania informacji niejawnych oraz doboru i stosowania środków bezpieczeństwa fizycznego w Ministerstwie Spraw Zagranicznych oraz placówkach zagranicznych, upoważniam Panią/Pana,

(imię i nazwisko, stanowisko)

posiadającą(-ego)poświadczenie bezpieczeństwa nr ważne do dnia oraz zaświadczenie o odbyciu szkolenia w zakresie ochrony informacji niejawnych wydane w dniu, do odbioru/zapoznawania się/ dekretacji* materiałów niejawnych oznaczonych klauzulą, które są adresowane do mnie,

w tym „do rąk własnych”*. Upoważnienie to jest ważne w okresie od..... do...../podczas mojej nieobecności*.

.....
(imię i nazwisko oraz podpis pełnomocnika ochrony
/dyrektora/ kierownika placówki)

* niepotrzebne skreślić

**Załącznik nr 2
do zarządzenia Nr 14
Ministra Spraw Zagranicznych
z dnia 25 lipca 2013 r.**

.....
(nazwa komórki organizacyjnej/ placówki)

..... dnia

.....
(sygnatura dokumentu)

Egz. nr
(lub egzemplarz pojedynczy)

ZATWIERDZAM

.....
(imię i nazwisko oraz podpis kierownika placówki lub dyrektora
/ pełnomocnika ochrony)

**PROTOKÓŁ ZDAWCZO – ODBIORCZY
z komisyjnego przekazania materiałów niejawnych**

W
(nazwa komórki organizacyjnej / placówki)

Wyznaczona zgodnie z § 19 ust. 1 zarządzenia nr Ministra Spraw Zagranicznych z dnia 2013 roku w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii tajnych oraz innych komórek organizacyjnych odpowiedzialnych za przetwarzanie materiałów niejawnych, sposobu i trybu przetwarzania informacji niejawnych oraz doboru i stosowania środków bezpieczeństwa fizycznego w Ministerstwie Spraw Zagranicznych oraz placówkach zagranicznych, komisja w składzie:

przewodniczący:
..... - przekazujący
..... - przyjmujący

dokonała w dniu przekazania materiałów przechowywanych w PODN-Z/
PODN-Pf/PODN-T/ kancelarii tajnej/kancelarii tajnej międzynarodowej*:

1. Dzienniki ewidencji zarejestrowane w rejestrze dzienników ewidencji i teczek pod pozycjami:

1).....
(nazwa dziennika oraz numer pozycji w rejestrze)

2).....
(nazwa dziennika oraz numer pozycji w rejestrze)

2. Materiały niejawne:

1) z roku zarejestrowane w, pozycje o numerach:...../od nr.... do nr....*
(nazwa dziennika i numer)

2) z roku zarejestrowane w, pozycje o numerach:...../od nr.... do nr....*
(nazwa dziennika i numer)

3. Pieczęcie i klucze zaewidencjonowane w, pozycje o numerach:...../od nr.... do nr....*
(nazwa dziennika i numer)

4. Ew. inne materiały podlegające przekazaniu:

Komisja stwierdza, że materiały niejawne pobrane z PODN-Z/PODN-Pf/PODN-T/kancelarii tajnej/kancelarii tajnej międzynarodowej* zostały zwrócone. (Jeżeli nie zostały zwrócone, to należy wskazać, w czym są posiadaniu)

Komisja stwierdza, że stan faktyczny materiałów niejawnych jest zgodny/nie jest zgodny* ze stanem ewidencyjnym. (Jeżeli stan nie jest zgodny, należy wyszczególnić braki oraz wskazać przyczynę nieprawidłowości).

Ew. uwagi komisji lub osoby zatwierdzającej protokół:

Podpisy członków komisji:

przewodniczący:

przekazujący:

przyjmujący:

Wykonano w 2 egzemplarzach (lub w egzemplarzu pojedynczym- do wiadomości Pełnomocnik ds. Ochrony Informacji Niejawnych)*:

Egz. nr 1- a/a

(PODN-Z/PODN-Pf/PODN-T/ KTM, a w ministerstwie KT/KTM/sekretariat)

Egz. nr 2 – Pełnomocnik ds. Ochrony Informacji Niejawnych (tylko w przypadku placówek zagranicznych)*

*niepotrzebne skreślić

**Załącznik nr 3
do zarządzenia Nr 14
Ministra Spraw Zagranicznych
z dnia 25 lipca 2013 r.**

Egz. pojedynczy

.....
(nazwa komórki organizacyjnej / placówki zagranicznej)

.....
(sygnatura dokumentu)

ZATWIERDZAM

.....
(imię i nazwisko oraz podpis pełnomocnika ochrony
/dyrektora/ kierownika placówki)

PROTOKÓŁ KOMISYJNEGO POBRANIA MATERIAŁÓW NIEJAWNYCH

W dniu....., komisja w składzie:

1.
(imię i nazwisko)

2.
(imię i nazwisko)

dokonała otwarcia pomieszczenia nr...../szafy metalowej/sejfu/mebla biurowego*, użytkowanego(-ej) przez
.....
(imię i nazwisko, stanowisko)

Zostały pobrane następujące materiały niejawne:

1.
(należy podać nazwę materiału i numer pozycji w dzienniku ewidencji)

Wyżej wymienione materiały są w dyspozycji Pani/Pana
(imię i nazwisko)

Pomieszczenie/szafę metalową/mebel biurowy* zamknięto w obecności członków komisji.

Pomieszczenie/szafę metalową zabezpieczono.

Klucze do pomieszczenia / szafy metalowej zdeponowano
(należy podać rodzaj/ sposób zabezpieczenia)

Podpisy członków komisji:

1.

2.

* niepotrzebne skreślić

**Załącznik nr 4
do zarządzenia Nr 14
Ministra Spraw Zagranicznych
z dnia 25 lipca 2013 r.**

KARTA OBIEGU MATERIAŁU NIEJAWNEGO

NR:

Lp.	Imię i nazwisko osoby, której udostępniono lub wydano materiał	Data udostępnienia/wydania	Potwierdzenie pobrania materiału	Data zwrotu materiału	Potwierdzenie zwrotu materiału	Uwagi

**Załącznik nr 5
do zarządzenia Nr 14
Ministra Spraw Zagranicznych
z dnia 25 lipca 2013 r.**

..... dnia

(nazwa komórki organizacyjnej/ placówki zagranicznej)

..... Egz. pojedynczy
(sygnatura dokumentu)

DECYZJA NR/.....

.....
(nazwa stanowiska osoby powołującej komisję)
W SPRAWIE POWOŁANIA KOMISJI DLA DOKONANIA PRZEGLĄDU MATERIAŁÓW NIEJAWNYCH

Na podstawie § 37 zarządzenia nr Ministra Spraw Zagranicznych z dnia 2013 roku w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii tajnych oraz innych komórek organizacyjnych odpowiedzialnych za przetwarzanie materiałów niejawnych, sposobu i trybu przetwarzania informacji niejawnych oraz doboru i stosowania środków bezpieczeństwa fizycznego w Ministerstwie Spraw Zagranicznych oraz placówkach zagranicznych, powołuję komisję dla dokonania przeglądu materiałów niejawnych przetwarzanych przez w składzie:
(nazwa komórki organizacyjnej/placówki zagranicznej)

przewodniczący:

członkowie:

..... - przedstawiciel pełnomocnika ochrony*

Komisja rozpocznie pracę w terminie określonym przez jej przewodniczącą.

Protokół przeglądu materiałów niejawnych – po zatwierdzeniu przez

.....
(imię i nazwisko
dyrektora)

przewodniczący komisji przekaze do wiadomości pełnomocnikowi ochrony.*

.....
...
(imię i nazwisko oraz podpis
pełnomocnika ochrony/kierownika
placówki)

* nie dotyczy placówek zagranicznych

**Załącznik nr 6
do zarządzenia Nr 14
Ministra Spraw Zagranicznych
z dnia 25 lipca 2013 r.**

.....
(nazwa komórki organizacyjnej/placówki zagranicznej)

....., dnia.....

.....
(nr ewidencyjny)

Egz. pojedynczy

ZATWIERDZAM

.....

.....
(stanowisko, imię i nazwisko, podpis dyrektora/
kierownika placówki)

ZAPOZNAŁEM SIĘ**

Pełnomocnik ds. Ochrony
Informacji Niejawnych

.....
(podpis)

PROTOKÓŁ PRZEGLĄDU MATERIAŁÓW NIEJAWNYCH

Powołana przez, decyzją nr z dnia
(stanowisko)

komisja w składzie:

przewodniczący:

członkowie:
.....

w dniach dokonała przeglądu materiałów niejawnych przechowywanych w sekretariacie komórki organizacyjnej/PODN-Z/PODN-Pf/PODN-T/kancelarii tajnej/kancelarii tajnej międzynarodowej* i zakwalifikowała:

1) **do zniszczenia*** - materiały niejawne kategorii „B” wymienione w załączonym spisie, zawierającym pozycji (załącznik nr 1). Komisja stwierdziła, że stanowią one dokumentację nieprzydatną do celów służbowych oraz, że upłynęły terminy ich przechowywania określone w Jednolitym Rzeczowym Wykazie Akt Ministerstwa Spraw Zagranicznych i placówek zagranicznych.

2) **do dalszego przechowywania*** w sekretariacie komórki organizacyjnej/PODN-Z/PODN-Pf/PODN-T/kancelarii tajnej/kancelarii tajnej międzynarodowej* - materiały niejawne kategorii „B”/ „A” * wymienione w załączonym spisie, zawierającym pozycji (załącznik nr 2). Komisja stwierdziła, że stanowią one dokumentację przydatną do celów służbowych.

3) **do przekazania*** do komórki organizacyjnej właściwej do spraw archiwum materiały niejawne, wymienione w załączonym spisie zdawczo-odbiorczym zawierającym ogółem pozycji (załączniki nr 3-4). Komisja stwierdziła, że przedstawiają one trwałą lub czasową wartość archiwalną w świetle Jednolitego Rzeczowego Wykazu Akt Ministerstwa Spraw Zagranicznych i placówek zagranicznych.

*- niewłaściwe skreślić

** - nie dotyczy placówki zagranicznej

Ponadto komisja dokonała przeglądu materiałów niejawnych wytworzonych w w aspekcie utrzymania, zmiany lub zniesienia
(nazwa komórki organizacyjnej/placówki zagranicznej)

klauzuli tajności i zakwalifikowała je zgodnie z załączonym spisem stanowiącym załącznik nr 4 do niniejszego protokołu. *

Po uzyskaniu zezwolenia dyrektora/kierownika placówki* komisja dokona zniszczenia wskazanych materiałów niejawnych, a fakt ten zostanie udokumentowany poprzez wypełnienie oświadczenia (załącznik nr 6).

Załączniki:

- Zał. nr 1 - kart spisu materiałów niejawnych przeznaczonych do zniszczenia;
- Zał. nr 2 - kart spisu materiałów niejawnych przeznaczonych do dalszego przechowywania w sekretariacie komórki organizacyjnej/PODN-Z/PODN-Pf/PODN-T/ kancelarii tajnej/kancelarii tajnej międzynarodowej*;
- Zał. nr 3 - kart spisu zdawczo odbiorczego materiałów niejawnych kat. „A” za rok
- Zał. nr 4 - kart spisu zdawczo odbiorczego materiałów niejawnych kat. „B” za rok....
- Zał. nr 5 - kart spisu materiałów niejawnych, w odniesieniu do których dokonano przeglądu w aspekcie utrzymania, zmiany lub zniesienia klauzuli tajności.

Po zatwierdzeniu protokołu zostanie dołączony:

- Zał. nr 6 - oświadczenie komisji potwierdzające fakt zniszczenia materiałów niejawnych, które zostały wskazane w załączniku nr 1.

Przewodniczący:

Członkowie:

.....

*- niewłaściwe skreślić

Załącznik nr 1 do protokołu przeglądu materiałów niejawnych nr.....

.....
(nazwa komórki organizacyjnej/placówki)

Egz. pojedynczy

ZEZWALAM NA ZNISZCZENIE

.....
(imię i nazwisko oraz podpis dyrektora/
kierownika placówki)

Spis materiałów niejawnych przeznaczonych do zniszczenia

Lp.	Numer ewidencyjny	Nazwa materiału	Numer egzemplarza	Ilość stron	Uwagi
1.					
2.					
3.					
4.					
5.					

Załączniki: kart zapoznania się z dokumentem

Przewodniczący:

Członkowie:

.....

Wykonano w egzemplarzu pojedynczym – a/a sekretariat/PODN-Z/PODN-Pf/PODN-T/KT/KTM*

*- *niewłaściwe skreślić*

Załącznik nr 2 do protokołu przeglądu materiałów niejawnych nr

.....
(nazwa komórki organizacyjnej/placówki)

Egz. pojedynczy

AKCEPTUJĘ:

.....
(podpis dyrektora/kierownika placówki)

Spis materiałów niejawnych przeznaczonych do dalszego przechowywania

W
(sekretariacie komórki organizacyjnej/PODN-Z/PODN-Pf/PODN-T/kancelarii tajnej/kancelarii tajnej międzynarodowej*)

Lp.	Numer ewidencyjny	Nazwa materiału	Numer egzemplarza	Ilość stron	Uwagi
1.					
2.					
3.					
4.					
5.					

Przewodniczący:

Członkowie:

.....

Wykonano w egzemplarzu pojedynczym – a/a sekretariat/PODN-Z/PODN-Pf/PODN-T/KT/KTM*

*- niewłaściwe skreślić

Załącznik nr 3 do protokołu przeglądu materiałów niejawnych nr

.....
(nazwa komórki organizacyjnej/placówki)

Egz. nr.....

AKCEPTUJĘ:

.....
(podpis dyrektora/kierownika
placówki zdającej akta)

**SPIS ZDAWCZO ODBIORCZY NR
MATERIAŁÓW NIEJAWNYCH KAT. „A” za rok**

L.p.	Numer ewidencyjny	Nazwa materiału	Teczka	Wiązka	Uwagi	Adnotacje Archiwum
1.						
2.						
3.						
4.						
5.						
6.						
7.						

Przewodniczący:

Członkowie:

.....

Przyjmujący:

Wykonano w 3 egzemplarzach

Egz. nr 1 i 2 – Archiwum MSZ

Egz. nr 3 – a/a sekretariat/PODN-Z/PODN-Pf/PODN-T/KT/KTM*

*- niewłaściwe skreślić

Załącznik nr 4 do protokołu przeglądu materiałów niejawnych nr

.....
(nazwa komórki organizacyjnej/placówki)

Egz. nr.....

AKCEPTUJĘ:

.....
(podpis dyrektora/kierownika
placówki zdającej akta)

**SPIS ZDAWCZO ODBIORCZY NR
MATERIAŁÓW NIEJAWNYCH KAT. „B” za rok**

L.p.	Numer ewidencyjny	Nazwa materiału	Teczka	Wiązka	Uwagi	Adnotacje Archiwum
8.						
9.						
10.						
11.						
12.						
13.						
14.						

Przewodniczący:

Członkowie:

.....

Przyjmujący:

Wykonano w 3 egzemplarzach, dnia

Egz. nr 1 i 2 – Archiwum MSZ

Egz. nr 3 – a/a sekretariat/PODN-Z/PODN-Pf/PODN-T/KT/KTM*

*- niewłaściwe skreślić

Załącznik nr 6 do protokołu przeglądu materiałów niejawnych nr

.....
dnia.....
(nazwa komórki organizacyjnej/placówki)

.....,

Egz. pojedynczy

ZAPOZNAŁEM SIĘ

.....
(podpis dyrektora/kierownika placówki)

**OŚWIADCZENIE
POTWIERDZAJĄCE FAKT ZNISZCZENIA MATERIAŁÓW NIEJAWNYCH**

Powołana przez, decyzją nr z dnia
(stanowisko, nazwa komórki organizacyjnej/placówki zagranicznej)

komisja w składzie:

przewodniczący:
członkowie:
.....

dokonała w dniu fizycznego zniszczenia materiałów niejawnych wymienionych w spisie materiałów niejawnych przeznaczonych do zniszczenia - poz. od.... do....., stanowiącym załącznik nr 1 do zatwierdzonego przez protokołu przeglądu materiałów niejawnych nr..... . Materiały niejawne zostały zniszczone w warunkach uniemożliwiających osobom nieupoważnionym wgląd do nich lub ich przejęcie, w odpowiednich urządzeniach, w sposób uniemożliwiający odczytanie lub odtworzenie treści zniszczonej informacji.

Przewodniczący:

Członkowie:
.....

Wykonano w egzemplarzu pojedynczym - a/a sekretariat/PODN-Z/PODN-Pf/PODN-T/KT/KTM*

*- *niewłaściwie skreślić*

Załącznik nr 5 do protokołu protokół przeglądu materiałów niejawnych nr

.....
(nazwa komórki organizacyjnej/ placówki zagranicznej)

....., dnia.....

Egz. pojedynczy

AKCEPTUJĘ

.....
(imię i nazwisko, podpis dyrektora/
kierownika placówki)

SPIS

materiałów niejawnych, wytworzonych

w,
(nazwa komórki organizacyjnej/placówki zagranicznej)

w odniesieniu do których dokonano przeglądu

w aspekcie utrzymania, zmiany lub zniesienia klauzuli tajności

W oparciu o analizę treści informacji, którym nadano klauzulę tajności, oraz przesłanek ochrony określonych w art. 5 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. nr 182, poz. 1228) komisja zakwalifikowała do:

a) **utrzymania klauzuli tajności** nw. dokumentów niejawnych:

1. (sygnatura literowo-cyfrowo, data podpisania dokumentu, nazwa dokumentu lub czego dotyczy)
2.
3.

b) **obniżenia klauzuli tajności** nw. dokumentów niejawnych:

1. (sygnatura literowo-cyfrowo, data podpisania dokumentu, nazwa dokumentu lub czego dotyczy, proponowana klauzula tajności)
2.
3.

c) **zniesienia klauzuli tajności** nw. dokumentów niejawnych:

1. (sygnatura literowo-cyfrowo, data podpisania dokumentu, nazwa dokumentu lub czego dotyczy)
2.
3.

Przewodniczący:

Członkowie:

.....

Wykonano w egzemplarzu pojedynczym- – a/a sekretariat/PODN-Z/PODN-Pf/PODN-T/KT/KTM*

*- niewłaściwe skreślić

**Załącznik nr 7
do zarządzenia Nr 14
Ministra Spraw Zagranicznych
z dnia 25 lipca 2013 r.**

.....
(nazwa placówki zagranicznej)

.....
(miejsce, data)

Egz. nr

ZATWIERDZAM

.....
(imię i nazwisko kierownika placówki)

.....
(podpis)

**SPRAWOZDANIE
o ochronie informacji niejawnych za rok**

Komisja powołana przez, decyzją nr z dnia w składzie:
przewodniczący:
członkowie:
.....
.....

dokonała w dniach sprawdzenia stanu ochrony informacji niejawnych,
w szczególności:

- I. stanu zabezpieczenia PODN-Z/PODN-Pf/PODN-T* oraz przechowywanych materiałów niejawnych;
- II. sposobu prowadzenia dzienników ewidencji oraz zgodności stanu faktycznego materiałów niejawnych z ich stanem ewidencyjnym;
- III. przestrzegania przepisów dotyczących przetwarzania oraz obiegu informacji niejawnych.

Komisja stwierdziła, że w roku:

Ad. I

1. W placówce sporządzono/zaktualizowano* w dniu dokumentację określającą poziom zagrożeń związanych z utratą poufności, integralności lub dostępności informacji niejawnych oraz dobór adekwatnych środków bezpieczeństwa fizycznego.
2. W placówce sporządzono/zaktualizowano* w dniu plan ochrony informacji niejawnych.
3. W pomieszczeniach i strefach ochronnych placówki, w których były przetwarzane informacje niejawne, stosowano odpowiednie środki bezpieczeństwa fizycznego.
(W przypadku stwierdzenia braków i nieprawidłowości w tym zakresie, należy je wyszczególnić).
4. Materiały niejawne były przetwarzane w strefie ochronnej I, strefie ochronnej II, strefie ochronnej III*. (W przypadku stwierdzenia nieprawidłowości w tym zakresie, należy je opisać).

5. W placówce przetwarzano Informacje niejawne, zgodnie z obowiązującymi procedurami, w następujących akredytowanych systemach teleinformatycznych przeznaczonych do tego celu:
(*należy wskazać rodzaje systemów TI, które były wykorzystywane do przetwarzania informacji niejawnych*).
6. Materiały niejawne były przechowywane w strefie ochronnej I, strefie ochronnej II, strefie ochronnej III*, w szafach metalowych spełniających wymagania określone w przepisach. (*W przypadku stwierdzenia braków i nieprawidłowości w tym zakresie, należy je wyszczególnić*).
7. Klucze i kody dostępu do szaf, pomieszczeń i stref ochronnych placówki, w których były przetwarzane i przechowywane materiały niejawne były udostępnione tylko uprawnionym pracownikom.
8. Dokonano/nie było potrzeby dokonania* zmiany kodów dostępu do szaf, pomieszczeń i stref ochronnych placówki, w których są przetwarzane i przechowywane materiały niejawne. Zmiany kodów dostępu dokonano w związku z (*należy wskazać przyczynę zmiany*).
9. Pomieszczenie PODN-Z/PODN-Pf/PODN-T* jest pomieszczeniem samodzielnym/ niesamodzielnym* (*w przypadku gdy pomieszczenie nie jest samodzielne należy wskazać, jakie inne funkcje pełni*).
10. Osoby realizujące w placówce zadania związane z dostępem do informacji niejawnych w ramach zakresu obowiązków na stanowisku pracy albo wykonywanych czynności zleconych, posiadały odpowiednie poświadczenia bezpieczeństwa lub upoważnienia do dostępu wyłącznie do informacji niejawnych o klauzuli „zastrzeżone” oraz aktualne zaświadczenia o odbyciu szkolenia w zakresie ochrony informacji niejawnych.
(*W przypadku stwierdzenia nieprawidłowości w tym zakresie, należy je wyszczególnić*).

Ad. II

1. W PODN-Z/PODN-Pf/PODN-T* prowadzono następujące dzienniki ewidencji:
 - 1) nr, w którym zarejestrowano ogółem
(*nazwa dziennika ewidencji*)
materiałów niejawnych, w tym oznaczonych klauzulą:
 - „zastrzeżone”
 - „poufne”
 - „tajne”
 - 2) nr, w którym zarejestrowano ogółem
(*nazwa dziennika ewidencji*)
materiałów niejawnych, w tym oznaczonych klauzulą:
 - „zastrzeżone”
 - „poufne”
 - „tajne”
 - 3) nr, w którym zarejestrowano ogółem
(*nazwa dziennika ewidencji*)
materiałów niejawnych UE, w tym oznaczonych klauzulą:
 - „restreint UE”
 - „confidentiel UE” *
 - 4) nr, w którym zarejestrowano ogółem
(*nazwa dziennika ewidencji*)
materiałów niejawnych NATO oznaczonych klauzulą „NATO restricted”.
2. Ww. dzienniki ewidencyjne były prowadzone prawidłowo, w sposób zapewniający możliwość ustalenia w każdych okolicznościach, gdzie znajduje się określony materiał niejawny. Ponadto z zapisów w ww.

dziennikach jednoznacznie wynika, który z materiałów niejawnych został protokolarnie zniszczony lub wysłany do adresata.

(W przypadku stwierdzenia nieprawidłowości w tym zakresie, należy je opisać).

3. W PODN-Z/PODN-Pf/PODN-T* przechowuje się następujące urządzenia ewidencyjne prowadzone w okresie przed wejściem w życie ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych:
 - 1) nr, rozpoczęty w roku,
(nazwa urządzenia ewidencyjnego)
zakończony..... w roku , który został rozliczony dnia/nie został rozliczony*
 - 2) nr, rozpoczęty w roku,
(nazwa urządzenia ewidencyjnego)
zakończony..... w roku , który został rozliczony dnia/nie został rozliczony*
4. W placówce wytworzono ogółem materiałów niejawnych, w tym oznaczonych klauzulą:
 - „zastrzeżone”
 - „poufne” *
 - „tajne” *
5. Do każdego materiału zawierającego informacje niejawne o klauzuli „tajne” dołączono kartę zapoznania się z dokumentem, na której odnotowano fakt każdorazowego zapoznania się z jego treścią przez osoby uprawnione.
6. Stan faktyczny materiałów niejawnych jest zgodny/nie jest zgodny* ze stanem ewidencyjnym. *(Jeżeli nie jest zgodny należy określić przyczyny nieprawidłowości oraz ew. wskazać osoby odpowiedzialne za ich powstanie).*

Ad. III

1. Informacje niejawne były udostępniane wyłącznie osobom do tego uprawnionym, zgodnie z przepisami ustawy dotyczącymi dostępu do informacji niejawnych o określonej klauzuli tajności, i tylko w zakresie niezbędnym do wykonywania przez tę osobę pracy na zajmowanym stanowisku albo wykonywania czynności zleconych.
2. Komisyjny przegląd materiałów niejawnych przetwarzanych w placówce pod kątem oceny ich dalszej przydatności oraz brakowania został przeprowadzony w dniu, zgodnie z obowiązującymi przepisami (protokół nr.....).
3. Przejęcie obowiązków w zakresie prowadzenia obsługi kancelaryjnej materiałów niejawnych dokonywane było protokolarnie oraz zgodnie z obowiązującymi procedurami. *(W przypadku stwierdzenia nieprawidłowości w tym zakresie, należy je opisać).*
4. O stwierdzonych przypadkach naruszenia przepisów o ochronie informacji niejawnych na bieżąco powiadamiany był kierownik placówki poprzez złożenie pisemnego oświadczenia o okolicznościach zdarzenia. Kierownik placówki każdorazowo powiadamiał o zdarzeniu pełnomocnika ochrony. *(W przypadku stwierdzenia braku realizacji tego wymogu, należy wskazać zdarzenia i opisać ich okoliczności).*

Ew. uwagi komisji :

Ew. uwagi kierownika placówki :

Podpisy:

przewodniczący :
członkowie:

.....

Wykonano w 2 egzemplarzach:

Egz. nr 1 – Pełnomocnik ds. Ochrony Informacji Niejawnych

Egz. nr 2 – a/a PODN-Z/PODN-Pf/PODN-T*

* - niewłaściwe skreślić

UWAGA:

W zależności od treści przedstawionych informacji, dokument powinien zostać przesłany do pełnomocnika ochrony podsystemem B-BN (jeżeli jest jawny lub został oznaczony klauzulą „zastrzeżone”), a w przypadku konieczności przesłania wersji papierowej - pocztą dyplomatyczną.

Załącznik nr 8
do zarządzenia Nr 14
Ministra Spraw Zagranicznych
z dnia 25 lipca 2013 r.

METODYKA DOBORU ŚRODKÓW BEZPIECZEŃSTWA FIZYCZNEGO

1. Środki bezpieczeństwa fizycznego zostały podzielone na 6 kategorii, z których każda dotyczy określonego aspektu bezpieczeństwa fizycznego. Poszczególnym typom każdego ze środków bezpieczeństwa fizycznego przypisano wartości liczbowe:

Kategoria	Środek bezpieczeństwa fizycznego	Liczba punktów
K1 – szafy do przechowywania informacji niejawnych	K1S1 – konstrukcja szafy (4 typy)	1-4
	K1S2 – zamek do szafy (4 typy)	1-4
K2 – pomieszczenia	K2S1 – konstrukcja pomieszczenia (4 typy)	1-4
	K2S2 – zamek do drzwi pomieszczenia (2 typy)	1 lub 4
K3 – budynki	4 typy budynków	1, 2, 3 lub 5
K4 – kontrola dostępu	K4S1 – systemy kontroli dostępu (4 typy)	1-4
	K4S2 – kontrola osób nieposiadających stałego upoważnienia do wejścia, interesantów i gości (2 typy)	1 lub 3
K5 – personel ochrony oraz systemy sygnalizacji włamania i napadu	K5S1 – personel ochrony (5 typów)	1-5
	K5S2 – systemy sygnalizacji włamania i napadu (4 typy)	1-4
K6 – granice	K6S1 – ogrodzenie (4 typy)	1-4
	K6S2 – kontrola w punktach dostępu	TAK=1 BRAK=0
	K6S3 – system kontroli osób, przedmiotów i pojazdów	TAK=1 BRAK=0
	K6S4 – system wykrywania naruszenia ogrodzenia	TAK=1 BRAK=0
	K6S5 – oświetlenie chronionego obszaru	TAK=1 BRAK=0
	K6S6 – system dozoru wizyjnego granic	TAK=1 BRAK=0

Opisy środków bezpieczeństwa fizycznego zostały zawarte w załączonej tabeli nr 1 „Klasyfikacja środków bezpieczeństwa fizycznego”.

2. Pierwszym etapem procesu doboru środków bezpieczeństwa fizycznego jest odczytanie z tabeli nr 2 „Podstawowe wymagania bezpieczeństwa fizycznego” minimalnej łącznej sumy punktów wymaganych do osiągnięcia założonego poziomu ochrony informacji w wyniku zastosowania odpowiedniej kombinacji środków bezpieczeństwa fizycznego. Liczba wymaganych do uzyskania punktów zależy od najwyższej klauzuli tajności informacji niejawnych przetwarzanych w danej lokalizacji oraz poziomu zagrożeń.
3. W tabeli nr 2 „Podstawowe wymagania bezpieczeństwa fizycznego” podzielono kategorie środków bezpieczeństwa fizycznego na grupy kategorii, które muszą być obowiązkowo stosowane, oraz grupę kategorii dodatkowych. Drugi etap procesu doboru środków bezpieczeństwa obejmuje odczytanie minimalnej liczby punktów, jakie należy uzyskać w każdej z grup kategorii środków bezpieczeństwa fizycznego oznaczonych jako „obowiązkowo”. W przypadku gdy liczba punktów uzyskanych po zastosowaniu środków należących 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 grupy kategorii oznaczonych jako „dodatkowo”, które powinny zapewnić uzyskanie minimalnej łącznej sumy punktów.
4. Dobór adekwatnych środków bezpieczeństwa fizycznego 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”.
5. Trzecim etapem jest dokonanie wyboru określonych środków bezpieczeństwa fizycznego, przy którym należy posługiwać się tabelą nr 1 „Klasyfikacja środków bezpieczeństwa fizycznego”. Należy z tej tabeli odczytać liczbę punktów odpowiadającą wybranemu typowi środka bezpieczeństwa i wpisać ją w odpowiednie miejsce w tabeli nr 3 „Punktacja zastosowanych środków bezpieczeństwa fizycznego”. Niezastosowanie danego środka jest jednoznaczne z przyznaniem za niego liczby punktów „0”.

Tabela nr 1

Klasyfikacja środków bezpieczeństwa fizycznego

KATEGORIA K1		
szafy do przechowywania informacji niejawnych		
Środek bezpieczeństwa K1S1 – konstrukcja szafy		
Typ	Funkcje lub cechy	Punktacja
Typ 4	<p>Konstrukcja szafy charakteryzuje się następującymi cechami:</p> <ul style="list-style-type: none"> – korpus zewnętrzny wykonany z blachy stalowej o grubości co najmniej 3 mm; – korpus wewnętrzny wykonany z blachy stalowej o grubości co najmniej 1,5 mm; – drzwi z blachy stalowej o grubości przynajmniej 8 mm; – drzwi mocowane na zawiasach wewnętrznych, blokowane mechanizmem ryglowym na trzech krawędziach oraz stałym rygłem przyzawiasowym; – mechanizm dźwigniowy rygli w drzwiach jest zabezpieczony przed uruchomieniem dwoma zamkami typu 3 lub 4 z kategorii K1S2 (w tym obowiązkowo zamek szyfrowy); – zmiana kombinacji w zamku szyfrowym jest blokowana i uaktywniana kluczem od tyłu obudowy zamka. 	4 pkt
Typ 3	<p>Konstrukcja szafy charakteryzuje się następującymi cechami:</p> <ul style="list-style-type: none"> – korpus zewnętrzny wykonany z blachy stalowej o grubości co najmniej 3 mm; – korpus wewnętrzny wykonany z blachy stalowej o grubości co najmniej 1,5 mm; – drzwi z blachy stalowej o grubości co najmniej 3 mm; – drzwi mocowane na zawiasach wewnętrznych, blokowane mechanizmem ryglowym na trzech krawędziach oraz stałym rygłem przyzawiasowym; – mechanizm dźwigniowy rygli w drzwiach jest zabezpieczony przed uruchomieniem zamkiem szyfrowym typu 3 lub 4 z kategorii K1S2; – zmiana kombinacji w zamku szyfrowym jest blokowana i uaktywniana kluczem od tyłu obudowy zamka. 	3 pkt
Typ 2	<p>Konstrukcja szafy charakteryzuje się następującymi cechami:</p> <ul style="list-style-type: none"> – korpus i drzwi wykonane z blachy stalowej o grubości co najmniej 3 mm; – drzwi mocowane na zawiasach wewnętrznych, blokowane mechanizmem ryglowym na trzech krawędziach oraz stałym rygłem przyzawiasowym; – mechanizm dźwigniowy rygli w drzwiach jest zabezpieczony przed uruchomieniem zamkiem mechanicznym kluczowym wielozastawkowym typu 2 z kategorii K1S2, zabezpieczonym przed działaniem destrukcyjnym, w tym przed przewierceniem; 	2 pkt

	- wyjęcie klucza z zamka jest możliwe tylko w pozycji zamkniętej.	
Typ 1	Szafa charakteryzuje się umiarkowaną odpornością na nieuprawnione próby otwarcia. Jest wyposażona w zamek mechaniczny kluczowy typu 1 lub 2 z kategorii K1S2. Korpus szafy i drzwi wykonane są z blachy stalowej o grubości co najmniej 1 mm lub szafa stanowi zamykany na klucz mebel biurowy. Szafa tego typu może być wykorzystywana do przechowywania materiałów niejawnych wyłącznie o klauzuli „zastrzeżone”.	1 pkt
Środek bezpieczeństwa K1S2 – zamek do szafy		
Typ 4	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. Rodzaje zamków szyfrowych: a) zamek mechaniczny szyfrowy co najmniej trzytarczowy, o cichym przesuwie, posiadający co najmniej 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 radiologicznym. Zmiana kombinacji powinna być blokowana i uaktywniana kluczem od tyłu obudowy zamka; b) 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.	4 pkt
Typ 3	Zamek charakteryzuje się wysokim poziomem odporności na fachowe i profesjonalne działania osoby nieuprawnionej posługującej się narzędziami i umiejętnościami, dostępnymi dla profesjonalistów. Rodzaje zamków: a) zamek mechaniczny szyfrowy co najmniej trzytarczowy, o cichym przesuwie, posiadający co najmniej 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; b) zamek elektroniczny szyfrowy spełnia te same wymagania co zamek mechaniczny szyfrowy oraz nie generuje sygnałów, które mogą być	3 pkt

	wykorzystane do otwarcia zamka przez okres 20 roboczogodzin; c) zamek zasuwowy wielozapadkowy na klucz dwupiórowy, zapewniający wysoki poziom zabezpieczenia oraz odporności na wiercenie.	
Typ 2	Zamek charakteryzuje się odpornością na sprawne działania osoby nieuprawnionej, posługującej się zwykłymi, powszechnie dostępnymi środkami.	2 pkt
Typ 1	Zamek charakteryzuje się umiarkowaną odpornością na nieuprawnione próby otwarcia i może być wykorzystywany wyłącznie w szafach typu 1.	1 pkt
KATEGORIA K2 pomieszczenia		
Środek bezpieczeństwa K2S1 – Konstrukcja pomieszczenia		
Typ 4	<p>1. Konstrukcja pomieszczenia (w tym ścian, stropów, drzwi oraz okien) zapewnia wysoką odporność na próby otwarcia z wykorzystaniem wielu różnych zaawansowanych narzędzi ręcznych i zasilanych prądem oraz na próby uzyskania nieuprawnionego dostępu.</p> <p>2. Ściany i stropy zostały zbudowane ze zbrojonego betonu o grubości co najmniej 15 cm lub materiału o podobnej wytrzymałości.</p> <p>3. Drzwi do pomieszczenia są wyposażone w zamek typu 2 z kategorii K2S2. Szkielet drzwi stanowi konstrukcja stalowa, składająca się z ramy oraz dodatkowych wzmocnień pionowych lub poziomych. Wypełnieniem ramy drzwi jest stalowa kratownica wykonana z prętów o zwiększonej twardości. Szkielet drzwi jest obustronnie pokryty blachą stalową o grubości co najmniej 2 mm. W ramie drzwi, po stronie zawiasów, muszą się znaleźć bolce antywyważeniowe. Po zamknięciu drzwi wsuwają się one w specjalne wzmocnione otwory w ościeżnicy. Ościeżnice wykonuje się z kształtowników stalowych. Ościeżnice montowane są w otworze drzwiowym przy użyciu kołków rozporowych umieszczonych w otworach wywierconych w murze lub kotew połączonych na stałe z ościeżnicą.</p> <p>4. Okna pomieszczenia dodatkowo zabezpieczone są przed podglądem.</p>	4 pkt
Typ 3	<p>1. Konstrukcja pomieszczenia (w tym ścian, stropów, drzwi oraz okien) zapewnia odporność na działania osoby nieuprawnionej próbującej uzyskać dostęp za pomocą siłowego wtargnięcia lub przy wykorzystaniu różnorodnych narzędzi ręcznych.</p> <p>2. Ściany zostały zbudowane z cegły lekkiej o grubości 25 cm lub materiału o podobnej wytrzymałości.</p> <p>3. Drzwi do pomieszczenia są wyposażone w zamek typu 2 z kategorii K2S2. Szkielet drzwi jest obustronnie pokryty blachą stalową o grubości co najmniej 2 mm. Wypełnieniem ramy może być płyta MDF o grubości co najmniej 20 mm lub inny materiał o podobnej wytrzymałości. W ramie</p>	3 pkt

	<p>drzwi, po stronie zawiasów, muszą się znaleźć bolce antywyważeniowe. Ościeżnice wykonuje się z kształtowników stalowych. Ościeżnice montowane są w otworze drzwiowym przy użyciu kołków rozporowych umieszczonych w otworach wywierconych w murze lub kotew połączonych na stałe z ościeżnicą.</p> <p>4. Okna pomieszczenia dodatkowo zabezpieczone są przed podglądem.</p>	
Typ 2	<p>1. Konstrukcja pomieszczenia (w tym ścian, stropów, drzwi oraz okien) zapewnia umiarkowaną odporność na działania osoby nieuprawnionej próbującej uzyskać dostęp za pomocą siłowego wtargnięcia lub przy użyciu narzędzi ręcznych.</p> <p>2. Ściany zostały zbudowane z cegły lekkiej o grubości 15 cm lub materiału o podobnej wytrzymałości, albo z płyty gipsowej na ramie wspierającej;</p> <p>3. Drzwi do pomieszczenia są wyposażone w zamek typu 1 lub 2 z kategorii K2S2. Konstrukcja drzwi i materiały zastosowane do ich budowy odpowiadają rozwiązaniom stosowanym dla drzwi zewnętrznych.</p> <p>4. Okna pomieszczenia zabezpieczone są przed podglądem.</p> <p>5. Okna nie muszą spełniać wymagań określonych w pkt. 1 jeżeli:</p> <ul style="list-style-type: none"> - dolna krawędź okna znajduje się na wysokości przynajmniej 5,5 m nad gruntem lub elementem budynku (np. balkonem lub balustradą), - nie znajdują się na ostatnim piętrze, - w pobliżu nie znajduje się żaden element (np. rynna, drabina, drzewo) ułatwiający potencjalny dostęp do pomieszczenia. 	2 pkt
Typ 1	<p>1. Konstrukcja pomieszczenia (w tym ścian, stropów, drzwi oraz okien) zapewnia niską odporność na działania osoby nieuprawnionej próbującej uzyskać dostęp za pomocą siłowego wtargnięcia lub przy użyciu narzędzi ręcznych.</p> <p>2. Ściany zbudowane zostały z cegły lekkiej, gipsokartonu, drewna, płyt pilśniowych lub innego materiału o podobnej wytrzymałości.</p> <p>3. Drzwi do pomieszczenia są wyposażone w zamek typu 1 lub 2 z kategorii K2S2.</p>	1 pkt
Środek bezpieczeństwa K2S2 – Zamek do drzwi pomieszczenia		
Typ 2	Zamek obsługiwany przy użyciu klucza patentowego oraz wkładki kluczowej wielozapadkowej stanowiących elementy systemu klucza generalnego.	4 pkt
Typ 1	Zamek obsługiwany przy użyciu klucza oraz wkładki kluczowej wielozapadkowej niebędących elementami systemu klucza generalnego.	1 pkt
KATEGORIA K3		
Budynki		

Typ 4	Budynek charakteryzuje się wytrzymałą konstrukcją i następującymi cechami: a) zapewnia wysoki poziom odporności na próby włamania; b) ściany i stropy są wykonane ze zbrojonego betonu lub materiału o podobnej wytrzymałości; c) drzwi zewnętrzne są wykonane ze stali wzmocnionej lub obustronnie pokryte blachą stalową; d) rama, mocowanie i szyby okien są odporne na włamanie.	5 pkt
Typ 3	Budynek charakteryzuje się następującymi cechami: a) zapewnia średni poziom odporności na próby włamania; b) stanowi wytrzymałą konstrukcję z cegły lub pustaków, opartą na ścianach szczelinowych; c) okna i drzwi są wykonane w standardzie zapewniającym średni poziom odporności na włamanie. <u>Uwaga:</u> jako Typ 3 może również zostać sklasyfikowany budynek zbudowany z zastosowaniem nowoczesnych technologii budowlanych, z wykorzystaniem prefabrykowanych paneli lub ramy stalowej i szkła bądź podobnych materiałów.	3 pkt
Typ 2	Budynek charakteryzuje się następującymi cechami: a) zapewnia średni poziom odporności na próby włamania; b) stanowi lekką konstrukcję, zazwyczaj z pojedynczego rzędu cegieł lub lekkich bloczków; c) okna i drzwi są wykonane w standardzie odpowiadającym standardowi budynku w zakresie odporności na włamanie.	2 pkt
Typ 1	Budynek nie spełnia kryteriów określonych w typach 2-4	1 pkt
KATEGORIA K4		
kontrola dostępu		
Środek bezpieczeństwa K4S1 – Systemy kontroli dostępu		
Typ 4	Elektroniczny automatyczny system kontroli dostępu o następujących cechach: a) jest to automatyczny system zapewniający właściwy stopień ochrony, wymagający jedynie minimalnego nadzoru przez personel ochrony; b) jest stosowany w połączeniu z barierą dostępu działającą na zasadzie uniemożliwiającej otwarcie danego przejścia kontrolowanego bez uprzedniego wejścia do poprzedzającej go strefy lub jeżeli wcześniej nie nastąpiło wyjście ze strefy, do której zamierza się wejść; c) sygnały ostrzeżeń i alarmów z systemu przekazywane są do stacji monitoringu obsługiwanej przez personel ochrony;	4 pkt

	d) obejmuje wszystkie wejścia do i wyjścia z kontrolowanego pomieszczenia lub obszaru.	
Typ 3	Elektroniczny automatyczny system kontroli dostępu o następujących cechach: a) wstęp kontrolowany jest przez odpowiednią barierę, która może wymagać bezpośredniego nadzoru przez personel ochrony; b) obejmuje wszystkie wejścia do i wyjścia z kontrolowanego pomieszczenia lub obszaru.	3 pkt
Typ 2	System kontroli dostępu obejmujący wszystkie wejścia do i wyjścia z kontrolowanego obszaru, wymagający: a) obecności personelu ochrony; b) zastosowania systemu wstępu na podstawie unikalnych przepustek; w zależności od ustaleń związanych z przyznawaniem wstępu akceptowane mogą być również inne dokumenty identyfikacyjne.	2 pkt
Typ 1	System kontroli dostępu oparty na zamkniętych drzwiach pomieszczenia lub obszaru, do którego można uzyskać dostęp za pomocą kodów lub kluczy wydawanych uprawnionym osobom. System tego typu może być stosowany do zabezpieczania obszarów, w których przetwarzane są informacje niejawne do klauzuli „poufne”.	1 pkt
Środek bezpieczeństwa K4S2 – kontrola osób nieposiadających stałego upoważnienia do wejścia do budynku i poruszania się po nim (interesanci, goście)		
Eskorta	Wprowadzane osoby przez cały czas przebywają pod nadzorem uprawnionego pracownika.	3 pkt
Przepustka	Interesanci i goście mogą uzyskać prawo wstępu na dany obszar bez konieczności nadzoru uprawnionego pracownika.	1 pkt
KATEGORIA K5 personel ochrony oraz systemy sygnalizacji włamania i napadu		
Środek bezpieczeństwa K5S1 – personel ochrony		
Typ 5	Personel ochrony: a) składa się z osób zatrudnionych w jednostce organizacyjnej lub funkcjonariuszy Biura Ochrony Rządu; b) funkcjonuje w trybie całodobowym; c) dokonuje częstego patrolowania wnętrza i otoczenia budynku po losowo wybranych trasach i w nieregularnych odstępach czasu. Działania podejmowane przez personel ochrony podlegają dokumentowaniu.	5 pkt
Typ 4	Personel ochrony: a) składa się z pracowników firmy zewnętrznej; b) funkcjonuje w trybie całodobowym; c) dokonuje częstego patrolowania wnętrza i otoczenia budynku po losowo wybranych trasach i w nieregularnych odstępach czasu. Działania podejmowane przez personel ochrony podlegają	4 pkt

	dokumentowaniu.	
Typ 3	Personel ochrony: a) składa się z pracowników firmy zewnętrznej; b) funkcjonuje w trybie całodobowym; c) sprawdza zabezpieczenia budynków, ale nie ma do nich dostępu (patrole ograniczone są do kontroli otoczenia budynków i granic terenu).	3 pkt
Typ 2	Personel ochrony: a) składa się z pracowników zatrudnionych w jednostce organizacyjnej lub pracowników firmy zewnętrznej; b) przebywa w pomieszczeniu kontroli zdarzeń lub w stróżówce; c) nie przeprowadza patroli, reaguje w sytuacjach sygnalizacji alarmu i wzywa pomoc, gdy jest to wymagane.	2 pkt
Typ 1	Zadania personelu ochrony w zakresie podstawowej kontroli zabezpieczenia obiektu oraz reagowania w sytuacjach sygnalizacji alarmu wykonuje pracownik zatrudniony w jednostce organizacyjnej.	1 pkt
Środek bezpieczeństwa K5S2 — systemy sygnalizacji włamania i napadu		
Typ 4	System charakteryzuje się następującymi cechami: a) zapewnia identyfikację użytkowników włączających i wyłączających system lub jego część; b) obejmuje ochroną cały obszar i sygnalizuje: – otwarcie drzwi, okien i innych zamknięć chronionego obszaru, – penetrację drzwi, okien i innych zamknięć chronionego obszaru bez ich otwierania, – penetrację ścian i stropów, – poruszanie się w chronionym obszarze (nadzór nad określonymi miejscami, w których występuje wysokie prawdopodobieństwo wtargnięcia); c) stosowany jest wraz z systemem dozoru wizyjnego określonych obszarów z obowiązkową rejestracją w rozdzielczości nie mniejszej niż 400 linii telewizyjnych i przechowywaniem zarejestrowanego zapisu przez czas nie krótszy niż 30 dni; d) stan systemu sygnalizacji napadu i włamania oraz systemu dozoru wizyjnego (w tym generowane ostrzeżenia i alarmy) jest stale monitorowany przez personel ochrony. <u>Uwaga:</u> 4 pkt przyznaje się również w przypadku obszarów, w których całodobowo przebywają uprawnieni pracownicy.	4 pkt
Typ 3	System charakteryzuje się następującymi cechami: a) zapewnia identyfikację użytkowników włączających i wyłączających system lub jego część; b) obejmuje ochroną otwory wejściowe i określone fragmenty obszaru oraz sygnalizuje: – otwarcie drzwi, okien i innych zamknięć chronionego obszaru, – penetrację drzwi, okien i innych zamknięć chronionego obszaru bez ich otwierania, – poruszanie się w chronionym obszarze (nadzór nad określonymi	3 pkt

	<p>miejscami, w których występuje wysokie prawdopodobieństwo wtargnięcia);</p> <p>c) stan systemu (w tym generowane ostrzeżenia i alarmy) jest stale monitorowany przez personel ochrony.</p>	
Typ 2	<p>System charakteryzuje się następującymi cechami:</p> <p>a) zapewnia identyfikację użytkowników włączających i wyłączających system lub jego część;</p> <p>b) obejmuje ochroną miejsca, w których przechowywane są materiały niejawne oraz całą granicę obszaru i sygnalizuje:</p> <ul style="list-style-type: none"> - otwarcie drzwi, okien i innych zamknięć chronionego obszaru, - poruszanie się w chronionym obszarze (nadzór nad określonymi miejscami, w których występuje wysokie prawdopodobieństwo wtargnięcia); <p>c) stan systemu (w tym generowane ostrzeżenia i alarmy) jest stale monitorowany przez personel ochrony.</p>	2 pkt
Typ 1	<p>System obejmuje ochroną miejsca, w których przechowywane są materiały niejawne i sygnalizuje:</p> <ul style="list-style-type: none"> - otwarcie drzwi do chronionego obszaru, - poruszanie się w chronionym obszarze (nadzór nad wybranymi miejscami, w których występuje wysokie prawdopodobieństwo wtargnięcia). 	1 pkt
KATEGORIA K6		
granice		
Środek bezpieczeństwa K6S1 – ogrodzenie		
Typ 4	<p>Ogrodzenie charakteryzuje się następującymi cechami:</p> <p>a) zapewnia wysoki poziom odporności na próby naruszenia konstrukcji przy użyciu zaawansowanych narzędzi i maksymalnie utrudnia sforsowanie ogrodzenia;</p> <p>b) minimalna wysokość wynosi 2,5 m;</p> <p>c) górna część jest zabezpieczona z obu stron przed wspinaniem się i przechodzeniem przez ogrodzenie;</p> <p>d) zapewnia łatwe monitorowanie;</p> <p>e) między budynkami a ogrodzeniem zachowana jest wolna przestrzeń o szerokości co najmniej 15 m.</p> <p>Zabezpieczenie w postaci ogrodzenia jest wspomagane systemem dozoru wizyjnego oraz ew. systemem wykrywania naruszenia ogrodzenia.</p>	4 pkt
Typ 3	<p>Ogrodzenie charakteryzuje się następującymi cechami:</p> <p>a) zapewnia średni poziom odporności na próby naruszenia konstrukcji przy użyciu narzędzi ręcznych i utrudnia sforsowanie ogrodzenia;</p> <p>b) minimalna wysokość wynosi 2,2 m;</p> <p>c) górna część jest zabezpieczona przed wspinaniem się i przechodzeniem przez ogrodzenie;</p>	3 pkt

	d) zapewnia łatwe monitorowanie; e) między budynkami a ogrodzeniem zachowana jest wolna przestrzeń o szerokości co najmniej 10 m.	
Typ 2	Ogrodzenie charakteryzuje się następującymi cechami: a) zapewnia umiarkowany poziom odporności na próby naruszenia konstrukcji i utrudnia sforsowanie ogrodzenia; b) minimalna wysokość wynosi 1,8 m.	2 pkt
Typ 1	Ogrodzenie służy wyłącznie do wyznaczenia granic terenu i zapewnienia minimalnego zabezpieczenia przed intruzami.	1 pkt
Środek bezpieczeństwa K6S2 — kontrola w punktach dostępu umieszczonych w ogrodzeniu		
TAK	Bramy i furtki w ogrodzeniu objęte są kontrolą dostępu.	1 pkt
Środek bezpieczeństwa K6S3 — system kontroli osób, przedmiotów i pojazdów		
TAK	Rozwiązanie organizacyjne przy ew. wykorzystaniu elektronicznego systemu pomocniczego lub sprzętu, polegające na zapewnieniu kontroli osób, przedmiotów wnoszonych do lub wynoszonych z obiektu oraz pojazdów.	1 pkt
Środek bezpieczeństwa K6S4 — system wykrywania naruszenia ogrodzenia		
TAK	System pomocniczy w formie zamaskowanych urządzeń bądź też widocznego sprzętu, stosowany w celu zwiększenia poziomu bezpieczeństwa zapewnionego przez ogrodzenie. Stosowany w połączeniu z systemem weryfikacji alarmu (np. system dozoru wizyjnego).	1 pkt
Środek bezpieczeństwa K6S5 – oświetlenie chronionego obszaru		
TAK	Oświetlenie zapewniające widoczność wymaganą dla prowadzenia skutecznej kontroli obszaru realizowanej bezpośrednio przez personel ochrony lub pośrednio za pomocą systemu dozoru wizyjnego.	1 pkt
Środek bezpieczeństwa K6S6 – System dozoru wizyjnego granic		
TAK	System z obowiązkową rejestracją w rozdzielczości nie mniejszej niż 400 linii telewizyjnych i przechowywaniem zarejestrowanego zapisu przez czas nie krótszy niż 30 dni.	1 pkt

Tabela nr 2

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	11	13
Obowiązkowo: kategorie K4+K5**	6	7	7
Dodatkowo: kategoria K6	4	5	5
Łącznie suma punktów	20	23	25
TAJNE			
Obowiązkowo: kategorie K1+K2+K3	8	9	10
Obowiązkowo: kategorie K4+K5***	4	5	5
Dodatkowo: kategoria K6	4	5	5
Łącznie suma punktów	16	19	20
POUFNE			
Obowiązkowo: kategorie K1+K2+K3	6	8	9
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	2	2	2
Dodatkowo: kategoria K4,K5 lub K6	-	1	2
Łącznie suma punktów	2	3	4

* tylko jedna wartość może być równa 0.

** żadna z wartości nie może być mniejsza od 2.

***żadna z wartości nie może być równa 0.

Tabela nr 3

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 - zamek do drzwi pomieszczenia Liczba punktów za środek bezpieczeństwa (K2S2=4 lub 1 pkt)	
Liczba punktów za kategorię K2 stanowiąca iloczyn punktów za oba powyższe środki bezpieczeństwa (K2=K2S1xK2S2)	
KATEGORIA K3: budynki	
Liczba punktów za kategorię (K3=5,3,2 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 ochrony i systemy sygnalizacji włamania i napadu	
Środek bezpieczeństwa K5S1 - personel ochrony Liczba punktów za środek bezpieczeństwa (K5S1=5, 4, 3, 2 lub 1 pkt)	

Środek bezpieczeństwa K5S2 - systemy sygnalizacji włamania i napadu 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, 1 lub 0 pkt)	
Środek bezpieczeństwa K6S2 - kontrola w punktach dostępu Liczba punktów za środek bezpieczeństwa (K6S2= 1 lub 0 pkt)	
Środek bezpieczeństwa K6S3 - system kontroli osób, p0rzedmiotów i pojazdów 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	