



**SŁUŻBA KONTRWYWIADU WOJSKOWEGO
BIURO ŁĄCZNOŚCI I INFORMATYKI**

02-007 Warszawa, ul. Oczuki 1, tel. (22) 684-13-33, fax. (22) 684-17-71

**WYTYCZNE
SŁUŻBY KONTRWYWIADU WOJSKOWEGO
W SPRAWIE POWOŁYWANIA I ODWOŁYWANIA
KANCELARII KRYPTOGRAFICZNYCH**

Na podstawie art. 5 ust. 1 pkt 3 i 5 ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz. U. Nr 104, poz. 709, z późn. zm.) oraz w celu wykonania art. 10 ust. 1 oraz art. 11 ust. 2 i 3 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228), która powierza Służbie Kontrwywiadu Wojskowego nadzór nad funkcjonowaniem systemu ochrony informacji niejawnych w jednostkach organizacyjnych pozostających w jej właściwości, a Szefowi Służby Kontrwywiadu Wojskowego także nadzór nad systemem ochrony informacji niejawnych w stosunkach Rzeczypospolitej Polskiej z innymi państwami lub organizacjami międzynarodowymi i wydawania dokumentów upoważniających do dostępu do informacji niejawnych Organizacji Traktatu Północnoatlantyckiego, Unii Europejskiej lub innych organizacji międzynarodowych, w związku z koniecznością zapewnienia merytorycznego wsparcia dla jednostek organizacyjnych pozostających we właściwości Służby Kontrwywiadu Wojskowego, zaleca się stosowanie poniższych reguł postępowania w zakresie powoływania i odwoływania kancelarii kryptograficznych:

WARSZAWA, DNIA 22 MAJA 2012 R.



Rozdział 1

Definicje

- § 1. Określenia użyte w wytycznych w sprawie powoływania i odwoływania kancelarii kryptograficznych, zwanych dalej „wytycznymi”, oznaczają:
- 1) **BŁI SKW** - Biuro Łączności i Informatyki SKW;
 - 2) **Certyfikat Upoważnienia Kryptograficznego (CUK)** – Certyfikat Upoważnienia Kryptograficznego w rozumieniu § 2 pkt 5 zarządzenia;
 - 3) **dokument kryptograficzny** - dokument kryptograficzny w rozumieniu § 2 pkt 6 zarządzenia;
 - 4) **jednostka organizacyjna** – jednostkę organizacyjną w rozumieniu § 2 pkt 13 zarządzenia;
 - 5) **kancelaria kryptograficzna** – kancelarię kryptograficzną w rozumieniu § 2 pkt 14 zarządzenia;
 - 6) **kierownik jednostki organizacyjnej** – kierownika jednostki organizacyjnej w rozumieniu § 2 pkt 15 zarządzenia;
 - 7) **kierownik kancelarii kryptograficznej** – kierownika kancelarii kryptograficznej w rozumieniu § 2 pkt 16 zarządzenia;
 - 8) **Krajowy Organ Generacji i Dystrybucji (KOGD)** – Krajowy Organ Generacji i Dystrybucji w rozumieniu § 2 pkt 18 zarządzenia;
 - 9) **materiał kryptograficzny** – materiał kryptograficzny w rozumieniu § 2 pkt 20 zarządzenia;
 - 10) **Oficer Bezpieczeństwa Systemów Łączności i Informatyki (oficer BSŁil)** – Oficera Bezpieczeństwa Systemów Łączności i Informatyki w rozumieniu § 2 pkt 21 zarządzenia;
 - 11) **Organ Bezpieczeństwa Systemów Łączności i Informatyki (OBSŁil)** – Organ Bezpieczeństwa Systemów Łączności i Informatyki w rozumieniu § 2 pkt 22 zarządzenia;
 - 12) **pełnomocnik ochrony** – pełnomocnika do spraw ochrony informacji niejawnych, o którym mowa w art. 14 ustawy o ochronie informacji niejawnych;



- 13) **personel BSŁil** – personel BSŁil w rozumieniu § 2 pkt 24 zarządzenia;
- 14) **produkt kryptograficzny** – urządzenie lub narzędzie kryptograficzne;
- 15) **RCZBSiUT** – Resortowe Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych;
- 16) **SKW** - Służba Kontrwywiadu Wojskowego;
- 17) **stacja kryptograficzna** – stację kryptograficzną w rozumieniu § 2 pkt 35 zarządzenia;
- 18) **system kryptograficzny** – system kryptograficzny w rozumieniu § 2 pkt 36 zarządzenia;
- 19) **Szef Krajowego Organu Generacji i Dystrybucji (Szef KOGD)** – Szefa Krajowego Organu Generacji i Dystrybucji w rozumieniu § 2 pkt 37 zarządzenia;
- 20) **ustawa o ochronie informacji niejawnych** - ustawę z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228);
- 21) **zastępca kierownika kancelarii kryptograficznej** – zastępcę kierownika kancelarii kryptograficznej w rozumieniu § 2 pkt 46 zarządzenia;
- 22) **zarządzenie** - zarządzenie Nr 58/MON Ministra Obrony Narodowej z dnia 22 grudnia 2011 r. w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii kryptograficznych (Dz. Urz. MON Nr 25, poz. 403);
- 23) **zaświadczenie o funkcjonowaniu kancelarii kryptograficznej** - dokument potwierdzający przygotowanie personelu oraz zdolność pomieszczenia do zapewnienia wymaganej ochrony materiałów i produktów kryptograficznych;
- 24) **ZBIN SKW** - Zarząd Bezpieczeństwa Informacji Niejawnych SKW;

Rozdział 2

Przepisy ogólne

- § 2. Za właściwą ochronę materiałów kryptograficznych odpowiada kierownik jednostki organizacyjnej.



- § 3. W jednostkach organizacyjnych, w których wykorzystuje się lub planuje się wykorzystywać materiały kryptograficzne, tworzy się Organy Bezpieczeństwa Systemów Łączności i Informatyki (OBSŁil) oraz utrzymuje się powołane lub powołuje się kancelarie kryptograficzne stacjonarne lub polowe (mobilne).
- § 4. Personel OBSŁil musi posiadać poświadczenia bezpieczeństwa nie niższe niż klauzula krajowych materiałów kryptograficznych ewidencjonowanych, przechowywanych i udostępnianych przez kancelarię kryptograficzną oraz równoważnie poświadczenia bezpieczeństwa/certyfikaty NATO lub UE, jeśli w kancelarii kryptograficznej planuje się ewidencjonowanie, przechowywanie i udostępnianie materiałów kryptograficznych pochodzących z wymiany międzynarodowej.
- § 5. Kierownik jednostki organizacyjnej odsuwa pisemnie (min. rozkazem, decyzją, zarządzeniem) od pełnienia obowiązków w kancelarii kryptograficznej personel BSŁil nie posiadający poświadczenia bezpieczeństwa, o którym mowa w § 4.
- § 6. Wymagania bezpieczeństwa fizycznego i technicznego dla pomieszczeń kancelarii kryptograficznych określa zarządzenie.
- § 7. Wymagania bezpieczeństwa fizycznego i technicznego oraz ochrony fizycznej dla polowych (mobilnych) kancelarii kryptograficznych określa **załącznik nr 1** do wytycznych.
- § 8. W przypadku eksploatacji w kancelarii kryptograficznej systemów teleinformatycznych należy stosować się do odrębnych przepisów.

Rozdział 3

Powoływanie kancelarii kryptograficznych

- § 9. Kierownik jednostki organizacyjnej, powołując kancelarię kryptograficzną, określa maksymalną klauzulę tajności materiałów kryptograficznych, które ma rejestrować, przechowywać i udostępniać.
- § 10. Kierownik jednostki organizacyjnej w celu powołania oraz utrzymania funkcjonowania kancelarii kryptograficznej:
- 1) określa klauzule przetwarzanych materiałów kryptograficznych krajowych i międzynarodowych (NATO lub UE);
 - 2) wyznacza oficera BSŁil;



- 3) wyznacza etatowy personel kancelarii kryptograficznej, w tym kierownika kancelarii kryptograficznej, zastępcę kierownika kancelarii kryptograficznej, w zależności od potrzeb: szyfranta (szyfrantów), kuriera (kurierów) oraz dodatkowych członków personelu kancelarii. Personel kancelarii kryptograficznej może pełnić funkcje personelu kancelarii kryptograficznej stacjonarnej oraz polowej (mobilnej) w tej samej jednostce organizacyjnej;
- 4) zapewnia, aby osoby wymienione w pkt 2-3 posiadały poświadczenia bezpieczeństwa (krajowe lub międzynarodowe) właściwe do klauzuli tajności materiałów kryptograficznych, określonych w pkt 1 oraz by osoby te posiadały odpowiednie zaświadczenia potwierdzające ukończenie specjalistycznych kursów:
 - a) zaświadczenie o ukończeniu kursu *Organizatorów systemów ochrony kryptograficznej i bezpieczeństwa teleinformatycznego* dla oficera BSŁil, w jednostce organizacyjnej od szczebla związku taktycznego (brygada, pułk i równorzędnego) i jednostek nadrzędnych. W pozostałych przypadkach oficer BSŁil musi posiadać zaświadczenie ukończenia kursu *Oficerów INFOSEC (COMSEC)* lub odbyć szkolenie w *NATO CIS School (NCISS) LATINA*,
 - b) zaświadczenie o ukończeniu kursu *Oficerów INFOSEC (COMSEC)* dla osób funkcyjnych, które mogą pełnić obowiązki oficera BSŁil podczas nieobecności etatowego oficera BSŁil,
 - c) zaświadczenie o ukończeniu kursu *Personelu kancelarii kryptograficznych* dla osób funkcyjnych wchodzących w skład personelu kancelarii kryptograficznej,
 - d) zaświadczenie o ukończeniu kursu upoważniającego do obsługi urządzeń typu „S” lub „U” dla osób funkcyjnych wyznaczonych na stanowisko kierownika stacji kryptograficznej oraz zaświadczenie o ukończeniu kursu szyfranta dla osób wyznaczonych na stanowisko szyfranta,



- e) zaświadczenie o ukończeniu kursu specjalistycznego obsługi danego urzędnika kryptograficznego dla osób funkcyjnych eksploatujących urządzenie ochrony kryptograficznej,
 - f) zaświadczenie o ukończeniu *Kursu Kurierów* dla osób funkcyjnych wykonujących obowiązki kurierów materiałów kryptograficznych,
 - g) dodatkowo, w celu podnoszenia kwalifikacji, zaświadczenie o ukończeniu kursu *Działania konwoju w sytuacjach szczególnych*, prowadzonego przez placówki szkoleniowe Żandarmerii Wojskowej, dla osób funkcyjnych wykonujących obowiązki kurierów materiałów kryptograficznych;
- 5) przygotowuje i wyposaża pomieszczenie (pomieszczenia) przeznaczone na:
- a) stacjonarną kancelarię kryptograficzną, zgodnie z zarządzeniem,
 - b) polową (mobilną) kancelarię kryptograficzną, zgodnie z **załącznikiem nr 1**;
- 6) występuje do kierownika nadrzędnej jednostki organizacyjnej lub jednostki przewidzianej do zaopatrywania w materiały kryptograficzne (w przypadku braku kancelarii kryptograficznej w jednostce nadrzędnej) z wnioskiem o oddelegowanie do składu Komisji oceny stanu zabezpieczeń fizycznych i technicznych pomieszczenia/pomieszczeń przeznaczonych na kancelarię kryptograficzną oficera BSŁil (lub innego oficera ze składu OBSŁil) oraz kierownika kancelarii kryptograficznej (lub jego zastępcę);
- 7) powołuje Komisję oceny stanu zabezpieczeń fizycznych i technicznych pomieszczenia/pomieszczeń przeznaczonych na kancelarię kryptograficzną, zwaną dalej „Komisją”, w składzie:
- a) przewodniczący - osoba wyznaczona przez kierownika jednostki organizacyjnej z kierownictwa jednostki, w której powoływana jest kancelaria kryptograficzna,
 - b) zastępca przewodniczącego – oficer BSŁil nadrzędnej (zaopatrującej) jednostki organizacyjnej,



- c) pełnomocnik kierownika jednostki organizacyjnej ds. ochrony informacji niejawnych jednostki, w której powoływana jest kancelaria kryptograficzna,
 - d) oficer BSŁil jednostki organizacyjnej, w której powoływana jest kancelaria kryptograficzna,
 - e) kierownik kancelarii kryptograficznej nadrzędnej (zaopatrującej) jednostki organizacyjnej (lub jego zastępca),
 - f) kierownik kancelarii kryptograficznej jednostki organizacyjnej, w której powoływana jest kancelaria kryptograficzna,
 - g) inne, niż wymienione w lit. a-f osoby funkcyjne;
- 8) zatwierdza dokumenty:
- a) instrukcję pracy kancelarii kryptograficznej, której wzór określa zarządzenie,
 - b) regulamin czytelnicy kancelarii kryptograficznej, o ile takowa istnieje,
 - c) instrukcję postępowania z materiałami kryptograficznymi na wypadek zagrożenia dla kancelarii kryptograficznej, według wzoru określonego w **załączniku nr 2**;
- 9) występuje do Szefa KOGD z wnioskiem o powołanie, przedłużenie funkcjonowania, zmianę klauzuli tajności przechowywanych i ewidencjonowanych materiałów kryptograficznych w kancelarii kryptograficznej, którego wzór określa **załącznik nr 3**;
- 10) do wniosku, o którym mowa w pkt. 9, dołącza:
- a) zatwierdzony protokół z inspekcji zastosowanych środków ochrony fizycznej i technicznej pomieszczenia/pomieszczeń kancelarii kryptograficznej, wykonany według wzoru stanowiącego **załącznik nr 4**,
 - b) rejestr wzorów podpisów, stanowiący **załącznik nr 5**,
 - c) uzupełnienie rejestru wzorów podpisów, stanowiące **załącznik nr 6**,
 - d) szkic globalnego środowiska bezpieczeństwa,
 - e) szkic lokalnego środowiska bezpieczeństwa z wyraźnym określeniem granic stref ochronnych,



- f) zwymiarowany plan pomieszczeń kancelarii kryptograficznej, z określeniem grubości ścian, umiejscowieniem środków zabezpieczenia fizycznego i technicznego,
- g) kopię Deklaracji Zgodności Systemu Alarmowego zgodnego z Normą Obronną NO-04-A004 Obiekty wojskowe. Systemy alarmowe.

§ 11. Komisja w trakcie przeprowadzania oceny stanu zabezpieczeń fizycznych i technicznych pomieszczenia/pomieszczeń przeznaczonego na kancelarię kryptograficzną może zasięgnąć opinii:

- 1) administratora systemu alarmowego;
- 2) komendanta ochrony obiektu;
- 3) przedstawicieli wykonawcy prac w pomieszczeniu (pomieszczeniach), planowanych na kancelarię kryptograficzną.

§ 12. Komisja, z wyłączeniem osób wymienionych w §10 pkt 7 lit. g, kontroluje stan posiadania urządzeń ewidencyjnych oraz materiałów kryptograficznych na wyposażeniu kancelarii kryptograficznej.

§ 13.1. KOGD, biorąc pod uwagę kompletność, prawidłowość oraz aktualność przesłanej dokumentacji, powołuje kancelarię kryptograficzną, nadaje nowo powołanej kancelarii kryptograficznej indywidualny numer oraz wystawia **zaświadczenie o funkcjonowaniu kancelarii kryptograficznej**, którego wzór określa **załącznik nr 7**.

2. W przypadku przesłania dokumentacji niekompletnej lub niezgodnej z przepisami i wytycznymi dokumentacja ta zostaje odesłana celem uzupełnienia i poprawy.

§ 14.1. Zaświadczenie o funkcjonowaniu kancelarii kryptograficznej jest ważne przez **okres 7 lat od daty wydania**.

2. Termin ważności zaświadczeń o funkcjonowaniu kancelarii kryptograficznej wydanych przed wejściem w życie niniejszych wytycznych, przedłuża się o 4 lata, o ile przeprowadzono inspekcję zastosowanych środków ochrony fizycznej i technicznej pomieszczenia/pomieszczeń kancelarii kryptograficznej na podstawie Wytycznych Służby Kontrwywiadu Wojskowego w sprawie powoływania i odwoływania kancelarii kryptograficznych z dnia 5 maja 2011 r.



§ 15.1. Do przedłużenia funkcjonowania kancelarii kryptograficznej stosuje się odpowiednio przepisy § 9 -13;

2. W przypadku ubiegania się o przedłużenie funkcjonowania kancelarii kryptograficznej dokumenty, o których mowa w § 10 pkt 9-10, należy przesłać do KOGD co najmniej 90 dni przed upływem terminu ważności posiadanego zaświadczenia;

3. Zaświadczenie o funkcjonowaniu kancelarii kryptograficznej wydaje się na kolejny okres określony w § 14 pkt 1.

§16.1. W przypadku obniżenia klauzuli tajności przechowywanych materiałów kryptograficznych w kancelarii kryptograficznej należy przesłać:

a) wniosek określony w § 10 pkt 9;

b) rejestr wzorów podpisów oraz uzupełnienie rejestru wzorów podpisów.

2. Po przesłaniu kompletnych i prawidłowych dokumentów wymienionych w pkt. 1, wydawane jest nowe zaświadczenie o funkcjonowaniu kancelarii kryptograficznej, które obowiązuje do dnia określonego w poprzednim zaświadczeniu.

§ 17. W przypadku, gdy w okresie obowiązywania zaświadczenia o funkcjonowaniu kancelarii kryptograficznej nastąpi:

1) zmiana elementów wpływających na bezpieczeństwo fizyczne i techniczne kancelarii kryptograficznej, m.in. zmiana budowlana, zmiana dyslokacji kancelarii kryptograficznej, zmiana strefy ochronnej pomieszczeń przyległych do kancelarii kryptograficznej, należy postępować zgodnie z § 10 pkt 5-7, 9-10 oraz § 11-12;

2) zmiana osób funkcyjnych wyznaczonych na stanowiska służbowe wymienione w § 10 pkt 2-3, na osoby funkcyjne spełniające warunki określone w § 10 pkt 4 oraz jakakolwiek inna modyfikacja danych wymienionych w rejestrze wzorów podpisów lub uzupełnieniu do rejestru wzorów podpisów, należy przesłać niezwłocznie aktualne wersje wyżej wymienionych dokumentów (nie później niż w terminie 10 dni roboczych) do KOGD, RCZBSiUT (dla kancelarii zaopatrywanych poprzez RCZBSiUT), kancelarii współpracujących (zaopatrywanych);



3) potrzeba przechowywania, ewidencjonowania i udostępniania materiałów kryptograficznych o wyższej klauzuli tajności lub możliwość przechowywania, ewidencjonowania i udostępniania materiałów kryptograficznych międzynarodowych w kancelarii kryptograficznej należy postępować zgodnie z § 9 -13.

§ 18. Przed wydaniem zaświadczenia o funkcjonowaniu kancelarii kryptograficznej Szef KOGD może wyznaczyć ekspertów z SKW celem sprawdzenia zgodności przesłanej dokumentacji, o której mowa w § 10 pkt. 9-10, ze stanem faktycznym.

§ 19. KOGD przesyła zaświadczenie o funkcjonowaniu kancelarii kryptograficznej do kierownika jednostki organizacyjnej poprzez RCZBSiUT, w przypadku kancelarii jednostek organizacyjnych zaopatrywanych przez RCZBSiUT, zgodnie z hierarchią zaopatrywania kancelarii kryptograficznych.

§ 20. O odwołaniu kancelarii kryptograficznej zaopatrywanej przez RCZBSiUT, KOGD powiadamia RCZBSiUT, które to powiadamia przedmiotową kancelarię zgodnie z hierarchią zaopatrywania kancelarii kryptograficznych.

§ 21. Zaświadczenia o funkcjonowaniu kancelarii kryptograficznej oraz pisma odwołujące kancelarie kryptograficzne stanowią podstawę aktualizacji wykazu funkcjonujących kancelarii kryptograficznych. Jednostka nadrzędna (zaopatrująca) jest zobowiązana do natychmiastowego powiadamiania o zaistniałych zmianach jednostki bezpośrednio podległe (zaopatrywane).

§ 22. Po powołaniu kancelarii kryptograficznej kierownik jednostki organizacyjnej jest zobowiązany do przesyłania do kancelarii współpracujących (w tym zaopatrywanych), zgodnie z hierarchią zaopatrywania kancelarii kryptograficznych, następujących dokumentów:

- 1) rejestru wzorów podpisów;
- 2) uzupełnienia do rejestru wzorów podpisów.

§ 23. Wszystkie OBSŁiI poszczególnych szczebli dowodzenia są zobowiązane do prowadzenia i aktualizacji wykazu funkcjonujących kancelarii kryptograficznych oraz członków ich personelu.



Rozdział 4

Zawieszenie i wznowienie funkcjonowania kancelarii kryptograficznej

- § 24. W czasie obowiązywania zaświadczenia o funkcjonowaniu kancelarii kryptograficznej dopuszcza się zawieszenie pracy kancelarii kryptograficznej.
- § 25. O zawieszeniu pracy kancelarii kryptograficznej decyduje Szef KOGD na wniosek kierownika jednostki organizacyjnej. Wzór wniosku określa **załącznik nr 8**.
- § 26. Na podstawie wniosku, o którym mowa w § 25, Szef KOGD decyduje o dalszym postępowaniu z materiałami kryptograficznymi.
- § 27. Wznowienie funkcjonowania kancelarii kryptograficznej następuje po przesłaniu do KOGD, zgodnie z hierarchią zaopatrywania kancelarii kryptograficznych, wniosku o zawieszenie/wznowienie funkcjonowania kancelarii kryptograficznej wraz z aktualnym rejestrem wzorów podpisów i uzupełnieniem rejestru wzorów podpisów.
- § 28. Wznowienie pracy zawieszonych kancelarii kryptograficznych następuje po uzyskaniu zgody Szefa KOGD.

Rozdział 5

Odwoływanie kancelarii kryptograficznej

- § 29. Odwołanie kancelarii kryptograficznej następuje:
- 1) w przypadku zmiany istotnych elementów bezpieczeństwa fizycznego lub technicznego kancelarii kryptograficznej (mających wpływ na bezpieczeństwo materiałów kryptograficznych) stwierdzonych przez OBSŁiI lub inne organy i osoby funkcyjne (odpowiedzialne za ochronę informacji niejawnych);
 - 2) zaprzestania wykorzystywania materiałów kryptograficznych a w szczególności ustania przyczyn, dla których została powołana kancelaria kryptograficzna;
 - 3) na podstawie uzasadnionej decyzji Szefa KOGD;
 - 4) na wniosek organu kontrolującego za zgodą Szefa KOGD.



§ 30. Kierownik jednostki organizacyjnej w związku z odwołaniem kancelarii kryptograficznej:

- 1) powołuje skład komisji (uwzględniający przedstawiciela zaopatrującej kancelarii kryptograficznej), której zadaniem jest określenie stanu posiadania materiałów kryptograficznych oraz kwalifikacja materiałów kryptograficznych do zniszczenia;
- 2) przesyła do jednostki nadrzędnej (zaopatrującej) przygotowany raport stanu posiadania materiałów kryptograficznych celem określenia sposobu zagospodarowania lub zniszczenia materiałów kryptograficznych;
- 3) niszczy lub przekazuje materiały kryptograficzne do nadrzędnej (zaopatrującej) kancelarii kryptograficznej zgodnie ze sposobem postępowania określonym w pkt. 2;
- 4) przesyła do KOGD wnioski o odwołanie kancelarii kryptograficznej, którego wzór określa **załącznik nr 9**;
- 5) przesyła do KOGD, zgodnie z hierarchią zaopatrywania kancelarii kryptograficznych, informację o zakończeniu przedsięwzięć związanych z zamknięciem kancelarii kryptograficznej.

Rozdział 6

Przepisy przejściowe i końcowe

§ 31. Certyfikaty akredytacji bezpieczeństwa fizycznego i technicznego pomieszczeń specjalnych zachowują swoją ważność do dnia określonego w przedmiotowym certyfikacie.

§ 32. Załączniki nr 4-6 do niniejszych wytycznych oraz dokumenty przedstawione w § 10 pkt 10 lit. d, e, f powinny posiadać stosowną klauzulę tajności oraz inne oznaczenia zgodne z Rozporządzeniem Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności (Dz. U. z 2011r. Nr 288, poz. 1692).

§ 33. W przypadku odwołania kancelarii kryptograficznej lub wygaśnięcia terminu ważności zaświadczenia o funkcjonowaniu kancelarii kryptograficznej należy odesłać je do KOGD, zgodnie z hierarchią zaopatrywania kancelarii kryptograficznych, w terminie 30 dni od daty ustania przyczyn ważności przedmiotowego zaświadczenia.



§ 34. W zakresie nieuregulowanym niniejszymi wytycznymi stosuje się:

- 1) w stosunku do krajowych materiałów kryptograficznych:
 - a) ustawę o ochronie informacji niejawnych;
 - b) rozporządzenie Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych (Dz. U. Nr 276, poz. 1631);
 - c) zarządzenie;
 - d) zarządzenie nr 57/MON Ministra Obrony Narodowej z dnia 16 grudnia 2011 r. w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii tajnych oraz innych niż kancelaria komórek organizacyjnych odpowiedzialnych za przetwarzanie informacji niejawnych, sposobu i trybu przetwarzania informacji niejawnych oraz doboru i stosowania środków bezpieczeństwa fizycznego (Dz. Urz. MON Nr 25, poz. 402).
- 2) w stosunku do materiałów kryptograficznych międzynarodowych:
 - a) dyrektywę AD 70-1PL;
 - b) SDIP-293/1 Instructions for the Control and Safeguarding of NATO Cryptomaterial;
 - c) SDIP-29 Facility Design Criteria and Installation of Equipment when processing NATO Classified Information;
 - d) dyrektywę AD-90-9 Procedures for the safeguarding, accounting and requesting of COMSEC material (08 December 2011);
 - e) wytyczne Szefa Agencji Bezpieczeństwa Wewnętrznego w sprawie postępowania z informacjami niejawnymi międzynarodowymi.

§ 35. W sytuacjach nieuregulowanych decyzje podejmuje Szef KOGD.

§ 36. Tracą moc wytyczne Służby Kontrwywiadu Wojskowego z dnia 5 maja 2011 r. w sprawie powoływania i odwoływania kancelarii kryptograficznych.

§ 37. Wytyczne wchodzą w życie z dniem podpisania.

ZASTĘPCA SZEFA
Służby Kontrwywiadu Wojskowego

pik Dariusz PILARZ



Załączniki do Wytycznych SKW w sprawie powoływania i odwoływania kancelarii kryptograficznych z dnia 22 maja 2012 r.

Załącznik nr 1

Wymagania ogólne na kontenery przeznaczone na polowe/mobilne kancelarie kryptograficzne

Kontenery przeznaczone na polowe/mobilne kancelarie kryptograficzne muszą posiadać pozytywną opinię wydaną przez Służbę Kontrwywiadu Wojskowego potwierdzającą spełnienie wymagań z zakresu zabezpieczenia fizycznego i technicznego.

Kontenery, powinny spełniać następujące minimalne wymagania:

1. Powinny być wykonane z płyt warstwowych, składających się z dwóch warstw blach (stopów aluminiowych lub stali) o grubości, co najmniej, 1 mm każda z nich, konstrukcyjnie ze sobą połączonych, oddzielonych od siebie, co najmniej, 50 mm warstwą twardego i niepalnego materiału izolacyjnego. Materiał ten musi charakteryzować się również niską higroskopijnością oraz dźwiękochłonnością (zgodnie z przepisami BHP).
2. W przypadku wystąpienia innych rozwiązań konstrukcyjno – technicznych mają one spełniać wymagania nie mniejsze niż opisane powyżej.
3. Płyty warstwowe na narożach powinny być zespawane i wyposażone w zaczepy transportowe umożliwiające mocowanie w czasie przewożenia różnymi środkami transportu.
4. Drzwi wejściowe powinny:
 - a) spełniać wymagania klasy odporności nie niższej niż RC2 określone w Polskiej Normie PN-EN 1627, posiadać element samozatraskowy uniemożliwiający pozostawienie pomieszczenia otwartego, samozamykacz oraz dodatkowo wyposażone w zamek mechaniczny szyfrowy, co najmniej klasy B według Polskiej Normy PN-EN 1300;



- b) być ryglowane od wewnątrz o konstrukcji uniemożliwiającej ich zablokowanie od zewnątrz (z wyłączeniem zamków);
 - c) być wyposażone w mechanizm samozamykający;
 - d) być wyposażone w urządzenie umożliwiające podgląd bezpośredniego zewnętrznego otoczenia.
5. Powinny posiadać właz ewakuacyjny otwierany od wewnątrz.
 6. Powinny posiadać otwory urządzeń wentylacyjnych i klimatyzacyjnych zabezpieczone siatką stalową o grubości nie mniejszej niż 2 mm o oczkach nie większych niż 20x20 mm, lub powierzchni nie większej niż 4 cm².
 7. Powinny być wyposażone w system alarmowy, z tym że:
 - a) powinien on sygnalizować nieuprawnione otwarcie drzwi wejściowych, włazu ewakuacyjnego i okien, ruch w pomieszczeniach oraz próby napadu,
 - b) powinien spełniać wymagania techniczne i organizacyjne określone w normie obronnej NO-04-A004 Obiekty wojskowe. Systemy alarmowe.
 8. Powinny być wyposażone w system sygnalizacji przeciwpożarowej wewnętrznej i zewnętrznej.
 9. Opcjonalnie powinny posiadać zamontowane certyfikowane (kwalifikowane) okna antywłamaniowe spełniające wymagania klasy odporności nie niższej niż RC 3 określone w Polskiej Normie PN-EN 1627.
 10. Powinny posiadać inny sprzęt (urządzenia) wymagane na podstawie odrębnych przepisów.

W kontenerach przeznaczonych na polowe (mobilne) kancelarie kryptograficzne, w których przewiduje się przyjmowanie interesantów należy wydzielić część kabiny przeznaczonej na czytelnię (miejsce do zapoznawania się z materiałami kryptograficznymi). Część kabiny należy fizycznie oddzielić poprzez zastosowanie stałej przegrody wewnętrznej. Przy zabudowie należy wziąć pod uwagę: umożliwienie personelowi kancelarii prowadzenie nadzoru nad osobą przebywającą w czytelnii oraz sterowaniem funkcji otwarcia drzwi wejściowych.



Czytelnia powinna być zorganizowana w takim miejscu, aby osoba zapoznająca się z materiałem kryptograficznym nie posiadała możliwości bezpośredniego dostępu do urządzeń do przechowywania informacji niejawnych, urządzeń do niszczenia materiałów niejawnych oraz systemów teleinformatycznych (z wyjątkiem tych, które przeznaczone są dla interesantów).

Kontenery przeznaczone na polowe/mobilne kancelarie kryptograficzne należy wyposażać w urządzenia do przechowywania materiałów kryptograficznych zgodnie z zarządzeniem, a ponadto w:

- a) urządzenia do niszczenia papierowych dokumentów niejawnych i materiałów kryptograficznych (klasy V wg norm DIN 32757);
- b) sprzęt kwaterunkowo – biurowy;
- c) sprzęt do ewakuacji;
- d) opcjonalnie w systemy teleinformatyczne;
- e) opcjonalnie inny sprzęt do niszczenia materiałów kryptograficznych.

Za organizację ochrony fizycznej polowej (mobilnej) kancelarii kryptograficznej odpowiedzialny jest pełnomocnik ds. ochrony informacji niejawnych jednostki organizacyjnej.

Polową (mobilną) kancelarię kryptograficzną organizuje się w oddzielnych samochodach, budowlach, schronach lub kontenerach, rozmieszczonych w rejonie stanowiska dowodzenia, jak najbliżej „Centrum Dowodzenia”, przy czym:

- a) obszar wokół kancelarii powinien być ogrodzony i posiadać nie więcej niż jedno strzeżone wejście;
- b) kancelaria powinna mieć zapewnioną całodobową ochronę;
- c) na czas nieobecności personelu materiały kryptograficzne powinny być przechowywane w urządzeniach do przechowywania materiałów kryptograficznych (nie dotyczy pracujących urządzeń kryptograficznych oraz nie wykorzystywanych urządzeń kryptograficznych bez wprowadzonych dokumentów kryptograficznych).



Zawartość Instrukcji postępowania z materiałami kryptograficznymi na wypadek zagrożenia dla kancelarii kryptograficznej

W instrukcji postępowania z materiałami kryptograficznymi w sytuacjach zagrożenia należy uwzględnić między innymi:

1. Miejsca lokalizacji sprzętu i środków przeciwpożarowych.
2. Procedury postępowania na wypadek zaistnienia sytuacji lub zdarzeń szczególnych (np. klęski żywiołowe, bezpośredni napad itp.).
3. Szczegółowe obowiązki personelu na zajmowanych stanowiskach służbowych (bez podawania nazwisk).
4. Niszczanie wszelkich urządzeń ewidencyjnych, materiałów kryptograficznych oraz ewidencji oprogramowania komputerowego.
5. Okresowe przeglądy przydzielonych obowiązków personelu.
6. Rozmieszczenie materiałów kryptograficznych w pomieszczeniach.
7. Miejsce przechowywania kodów dostępu (kombinacji) do zamków szyfrowych pomieszczeń i urządzeń do przechowywania informacji niejawnych.
8. Zasady dostępu do pomieszczeń kryptograficznych osób nieupoważnionych biorących udział w likwidacji zagrożeń oraz przepisy w zakresie ochrony materiałów kryptograficznych podczas takiego dostępu.
9. Wyznaczenie zasadniczego i rezerwowego miejsca składowania ewakuowanych materiałów kryptograficznych, a także zasadnicze i rezerwowe drogi ewakuacyjne.
10. Przepisy dotyczące alarmowego pakowania, ładowania i transportu materiałów kryptograficznych oraz ich zabezpieczenia podczas transportu. Ponadto, w przypadku powstania zagrożenia w czasie transportu należy uwzględnić możliwość alarmowego zniszczenia materiałów kryptograficznych.
11. Miejsce przechowywania środków do alarmowego zniszczenia materiałów kryptograficznych.
12. Załączniki:
 - a. szkic ewakuacji,
 - b. lista zapoznanych z instrukcją.



WNIOSEK

o powołanie kancelarii kryptograficznej *
o przedłużenie funkcjonowania kancelarii kryptograficznej nr 860048/.....*
o zmianę klauzuli tajności przechowywanych i ewidencjonowanych materiałów kryptograficznych w kancelarii kryptograficznej nr 860048/.....*

W

.....

/pełna nazwa jednostki organizacyjnej, kod pocztowy, miejscowość, ulica, budynek, pomieszczenie, kompleks
koszarowy/

z lokalizacją w

.....

/wypełniamy w przypadku, gdy adres jest inny niż jednostki organizacyjnej/

1. Uzasadnienie:

.....
.....

2. Obsługiwane klauzule tajności:.....

3. Stanowiska personelu organu bezpieczeństwa łączności i informatyki:

– Oficer BSŁil

–

–

–

–

m.p

.....

(stopień, imię, nazwisko i podpis kierownika jednostki organizacyjnej)

* - niepotrzebne skreślić



/Nazwa jednostki organizacyjnej/

miejsowość, data

ZATWIERDZAM

/stopień, imię, nazwisko, pieczęć i podpis kierownika jednostki organizacyjnej/

**PROTOKÓŁ Z INSPEKЦИИ ZASTOSOWANYCH ŚRODKÓW
OCHRONY FIZYCZNEJ I TECHNICZNEJ
POMIESZCZENIA/ POMIESZCZEŃ KANCELARII KRYPTOGRAFICZNEJ***

W.....

/pełna nazwa jednostki organizacyjnej, kod pocztowy, miejscowość, ulica, budynek, pomieszczenie, kompleks
koszarowy/

Z lokalizacją w

/wypełniamy w przypadku, gdy adres jest inny niż jednostki organizacyjnej/

Obsługiwane materiały kryptograficzne o klauzuli tajności:.....
.....

* - niepotrzebne skreślić



**Lista osób biorących udział w Inspekcji
ochrony fizycznej i technicznej
pomieszczenia/ pomieszczeń kancelarii kryptograficznej***

Lp.	stopień, imię i nazwisko	stanowisko i funkcja	Data	podpis

* - niepotrzebne skreślić

Protokół z Inspekcji zastosowanych środków ochrony fizycznej i technicznej
pomieszczeń kancelarii kryptograficznej w

.....

/pełna nazwa jednostki organizacyjnej/

sporządziła ww. komisja pod przewodnictwem

.....

.....

.....

.....

.....

.....

/stopień, imię, nazwisko przewodniczącego zespołu/komisji/pełnomocnika ochrony informacji

niejawnych jednostki organizacyjnych/pieczęć i podpis

**A. OBSZAR BEZPIECZEŃSTWA OSOBOWEGO**

Pozycja	Wyszczególnienie	Wynik (opis tak/nie lub spełnia/nie spełnia)	Opis stanu faktycznego	Różnica między stanem faktycznym a normatywnym/uwagi
A.I	Podstawa (rozkaz/ decyzja*) o wyznaczeniu / pełnieniu / wykonywaniu* obowiązków personelu BSŁil: <ul style="list-style-type: none">• Oficer BSŁil• Kierownik Kancelarii Kryptograficznej• Z-ca Kierownika Kancelarii Kryptograficznej/Kurier materiałów kryptograficznych/Szyfrant*			
A.II	Posiadanie aktualnych poświadczeń bezpieczeństwa (Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych Rozdział 5. Art. 21 ust.1.) przez personel BSŁil: <ul style="list-style-type: none">• Oficer BSŁil• Kierownik Kancelarii Kryptograficznej• Z-ca Kierownika Kancelarii Kryptograficznej/Kurier materiałów kryptograficznych/Szyfrant*			
A.III	Posiadanie aktualnych zaświadczeń stwierdzających odbycie przeszkolenia w zakresie ochrony informacji niejawnych (Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych Rozdział 4) przez personel BSŁil: <ul style="list-style-type: none">• Oficer BSŁil• Kierownik Kancelarii Kryptograficznej• Z-ca Kierownika Kancelarii Kryptograficznej/Kurier materiałów i urządzeń kryptograficznych/Szyfrant*			
A.IV	Posiadanie aktualnych Certyfikatów Upoważnienia Kryptograficznego przez personel BSŁil (nie dotyczy nowo powoływanych kancelarii kryptograficznych) <ul style="list-style-type: none">• Oficer BSŁil:• Kierownik Kancelarii Kryptograficznej• Z-ca Kierownika Kancelarii Kryptograficznej/Kurier			



Pozycja	Wyszczególnienie	Wynik (opis tak/nie lub spełnia/nie spełnia)	Opis stanu faktycznego	Różnica między stanem faktycznym a normatywnym/uwagi
	materiałów kryptograficznych/Szyfrant*			
A.V	Posiadanie aktualnych zaświadczeń odbycia przeszkolenia specjalistycznego przez personel BSŁil: <ul style="list-style-type: none"> • Oficer BSŁil • Kierownik Kancelarii Kryptograficznej • Z-ca Kierownika Kancelarii Kryptograficznej/Kurier materiałów kryptograficznych/Szyfrant* 			

UWAGI – stosować formę opisową:

Ad. A.I –

.....

Ad. A.II –

.....

Ad. A.III –

.....

Ad. A.IV –

.....

Ad. A.V –

.....

B. OBSZAR BEZPIECZEŃSTWA ORGANIZACYJNEGO

Pozycja	Wyszczególnienie	Wynik (opis tak/nie lub spełnia/nie spełnia)	Opis stanu faktycznego	Różnica między stanem faktycznym a normatywnym/uwagi
B.I	W której strefie ochronnej zlokalizowano pomieszczenie / pomieszczenia* KK: <ul style="list-style-type: none"> • I strefie ochronnej • II strefie ochronnej? 			
B.II	Z jakiej strefy ochronnej zorganizowano wyjście do pomieszczenia/ pomieszczeń* KK: <ul style="list-style-type: none"> • I strefy ochronnej • II strefy ochronnej • III strefy ochronnej? 			
B.III	Czy strefy ochronne mają wyraźnie oznaczone granice?			



B.IV	Czy wprowadzono kontrole dostępu osób wchodzących i wychodzących poruszających się między strefami ochronnymi? - Wyszczególnić jakie.			
B.V	Lokalizacja pomieszczenia / pomieszczeń* KK w oparciu o dokumentację budowlaną obiektu lub Program organizacyjno-użytkowy /co znajduje się w sąsiednich pomieszczeniach/ <ul style="list-style-type: none">• Pomieszczenia obok• Pomieszczenia powyżej• Pomieszczenia poniżej			
B.VI	Skład i organizacja pomieszczenia / pomieszczeń* KK: <ul style="list-style-type: none">• Liczba pomieszczeń• Przeznaczenie poszczególnych pomieszczeń• Sposób udostępniania dokumentów• Przyjmowanie interesantów			
B.VII	Sposób przechowywania materiałów kryptograficznych w pomieszczeniu/ pomieszczeniach* KK: <ul style="list-style-type: none">• Szafy stalowe• Szafy meblowe• Regały w pomieszczeniu magazynowym• Worki (pojemniki)			
B.VIII	Sposób zabezpieczenia kluczy użytku bieżącego, pomieszczenia/ pomieszczeń* KK oraz sejfów: <ul style="list-style-type: none">• Miejsce deponowania (sejf, dyżurka, depozytor itp.)• Sposób zabezpieczenia (depozytor itp.)• Nr rejestrów lub urządzeń ewidencyjnych			
B.IX	Sposób zabezpieczenia kluczy zapasowych do sejfów, pomieszczenia/ pomieszczeń* KK oraz haseł dostępowych do sejfów i Systemu Sygnalizacji Włamania i Napadu: <ul style="list-style-type: none">• Miejsce deponowania• Sposób zabezpieczenia• Nr rejestrów lub urządzeń ewidencyjnych pod, którymi są zarejestrowane			
B.X	Czy wykaz osób upoważnionych do pobierania kluczy i dostępu do pomieszczenia/ pomieszczeń *KK jest zgodny z obsadą etatową personelu BSłil ?			



B.XI	Czy gospodarka kluczami, kodami dostępu do sejfów, drzwi wejściowych, kodem Administratora SSW i N została ujęta w Planie Ochrony jednostki organizacyjnej (podać nazwę dokumentu oraz stronę)?			
-------------	---	--	--	--

UWAGI stosować formę opisową:

Ad. B.I –

.....
.....
.....

Ad. B.II –

.....
.....
.....

Ad. B.III –

.....
.....
.....

Ad. B.IV –

.....
.....
.....

Ad. B.V –

.....
.....
.....

Ad. B.VI –

.....
.....
.....

Ad. B.VII –

.....
.....
.....

Ad. B.VIII –

.....
.....
.....

Ad. B.IX –

.....
.....
.....

Ad. B.X –

.....
.....
.....



Ad. B.XI –

.....
.....
.....
.....

C. OBSZAR BEZPIECZEŃSTWA FIZYCZNEGO

Pozycja	Wyszczególnienie	Wynik (opis tak/nie lub spełnia/nie spełnia)	Opis stanu faktycznego	Różnica między stanem faktycznym a normatywnym/uwagi
C.I	<p>1. Czy ściany i stropy pomieszczenia/ pomieszczeń* KK spełniają wymogi przewidziane w przepisach dotyczących organizacji kancelarii:</p> <ul style="list-style-type: none">• Ściany zewnętrzne – podać grubość i materiał z czego wykonano• Ściany wewnętrzne – podać grubość i materiał z czego wykonano• Stropy – podać grubość i materiał z czego wykonano <p>2.Zabezpieczenie szybu/ kanałów wentylacyjnych w pomieszczeniu/ pomieszczeniach* KK.</p> <p>3.Wskazanie oraz przytoczenie opisu dokumentacji budowlanej/remontowej/ powykonawczej potwierdzającej spełnienie wymagań, o których mowa w punkcie 1 i 2. Kto dysponuje ww. dokumentacją.</p>			
C.II	<p>1.Drzwi wejściowe do pomieszczenia/ pomieszczeń* KK:</p> <ul style="list-style-type: none">• Typ zamontowanych drzwi (w przypadku drzwi antywłamaniowych wpisać: nr certyfikatu, świadectwa kwalifikacyjnego, deklaracji zgodności lub innego dokumentu potwierdzającego zgodność drzwi zamontowanych z wymaganiami)• Typ zamków zamontowanych w drzwiach wejściowych: nr certyfikatów, świadectw kwalifikacyjnych, deklaracji zgodności lub innego dokumentu potwierdzającego zgodność zamków z wymaganiami• Czy w ww. drzwiach zamontowano samozamykacz, elektrozworę itp.?• Czy w ww. drzwiach zamontowano wizjer? <p>2. Drzwi wewnętrzne w pomieszczeniu/ pomieszczeniach* KK:</p> <ul style="list-style-type: none">• Typ zamontowanych drzwi (w przypadku drzwi antywłamaniowych wpisać: nr certyfikatu, świadectwa			



Pozycja	Wyszczególnienie	Wynik (opis tak/nie lub spełnia/nie spełnia)	Opis stanu faktycznego	Różnica między stanem faktycznym a normatywnym/uwagi
	<p>kwalifikacyjnego, deklaracji zgodności lub innego dokumentu potwierdzającego zgodność zamontowanych drzwi z wymaganiami)</p> <ul style="list-style-type: none">• Typ zamków zamontowanych w drzwiach wejściowych wpisać: nr certyfikatów, świadectw kwalifikacyjnych, deklaracji zgodności lub innego dokumentu potwierdzających zgodność zamków z wymaganiami• Czy w ww. drzwiach zamontowano samozamykacz?			
C.III	<p>Okna w pomieszczeniu/ pomieszczeniach* KK (nie dotyczy pomieszczeń zlokalizowanych na okrętach, statkach powietrznych, pomieszczeniach zagłębionych):</p> <ul style="list-style-type: none">• Czy w pomieszczeniu / pomieszczeniach *KK są okna? (w przypadku braku okien dalszej części pkt. C III nie wypełniać)• Czy okna zabezpieczono przed podglądem z zewnątrz? (krótko scharakteryzować ww. zabezpieczenie)• Czy okna zabezpieczono przed nieuprawnionym otwarciem? (opisać sposób zabezpieczenia, np. klamki z kluczykami itp.)• Czy okna zabezpieczono kratą i/lub siatką? (opisać parametry elementów zabezpieczeń)• Czy zamontowano okna antywłamaniowe (zgodnie z zarządzeniem) ? Wpisać świadectwa kwalifikacyjne lub certyfikaty na szyby i ramy okienne			

UWAGI stosować formę opisową:

Ad. C.I 1 –

.....
.....
.....

Ad. C.I 2 –

.....
.....
.....

Ad. C.I 3 –

.....
.....
.....



.....
Ad. C.II 1 –
.....
.....
.....

.....
Ad. C.II 2 –
.....
.....
.....

.....
Ad. C.III –
.....
.....
.....

D. OBSZAR BEZPIECZEŃSTWA TECHNICZNEGO

Pozycja	Wyszczególnienie	Wynik (opis tak/nie lub spełnia/nie spełnia)	Opis stanu faktycznego	Różnica między stanem faktycznym a normatywnym/uwagi
D.I	System Sygnalizacji Pożarowej w pomieszczeniu/ pomieszczeniach* KK: <ul style="list-style-type: none">• Czy pomieszczenie/ pomieszczenia* KK jak i pomieszczenia przyległe zabezpieczono systemem sygnalizacji pożarowej?• Czy system sygnalizacji pożarowej zbudowano na bazie autonomicznego systemu czy zintegrowano z SSW iN (należy opisać)?• Typ centrali sygnalizacji pożarowej• Miejsce zainstalowania centrali sygnalizacji pożarowej (centrala musi być zainstalowana w miejscu chronionym lub pomieszczeniu służb dyżurnych/ochronnych)			
D.II	1.System Sygnalizacji Włamania i Napadu w pomieszczeniu/ pomieszczeniach* KK: <ul style="list-style-type: none">• Czy system alarmowy został zainstalowany przez instalatorów z wymaganymi uprawnieniami:<ul style="list-style-type: none">- wpisać nazwę organu, który wystawił dokument potwierdzający uprawnienia- wpisać tytuły i klauzule tajności dokumentacji powykonawczej SSWiN• Czy system alarmowy spełnia wymagania Normy Obronnej NO-04-A004 Obiekty wojskowe. Systemy alarmowe.• Wpisać deklaracje zgodności			



Pozycja	Wyszczególnienie	Wynik (opis tak/nie lub spełnia/nie spełnia)	Opis stanu faktycznego	Różnica między stanem faktycznym a normatywnym/uwagi
	<p>lub inny dokument potwierdzający zgodność zainstalowanego SSWiN z wymaganiami stosowanej normy (kto wystawił deklarację zgodności i przez kogo została podpisana)</p> <ul style="list-style-type: none">• Czy SSWiN jest okresowo konserwowany zgodnie z NO-04-A004?<ul style="list-style-type: none">- podać nr, datę oraz z kim została zawarta umowa konserwacyjna (umowa nr... z dnia ... podpisana z...)- wpisać nr książek eksploatacyjnych systemów alarmowych z aktualnymi wpisami (konserwacja, okresowe wyłączenia, testowanie, próbne alarmy czynności wykonywane przez konserwatorów i administratora SSWiN)• Czy w pomieszczeniu/ pomieszczeniach* KK zainstalowano przycisk napadowy?• Czy w pomieszczeniu/ pomieszczeniach* KK zainstalowano przycisk pomocy medycznej?• Gdzie zainstalowano Centralę Alarmową (musi być w strefie ochronnej)• Gdzie są rejestrowane zdarzenia SSWiN i czy osoby funkcyjne dokonują okresowej analizy? (Administrator SSWiN, Pełnomocnik OIN, Oficer BSłil)• Czy SSWiN posiada dodatkowe funkcje, np. opcje wejścia pod przymusem?• Czy SSWiN jednoznacznie identyfikuje użytkowników KK?• Czy SSWiN posiada funkcje dwustopniowego sterowania strefami (opisać)?• Czy zastosowane jest awaryjne (rezerwowe) zasilanie SSW iN?• Podać informację dotyczącą okresu przechowywania w pamięci centrali alarmowej zapisów komunikatów zdarzeń zarejestrowanych przez system SSWiN,			



Pozycja	Wyszczególnienie	Wynik (opis tak/nie lub spełnia/nie spełnia)	Opis stanu faktycznego	Różnica między stanem faktycznym a normatywnym/uwagi
	dotyczących KK 2. Czy wyznaczono administratora SSWiN? - podać nr i datę rozkazu/decyzji/ innego dokumentu powierzającego obowiązki - Czy użytkownicy, służby dyżurne/ ochronne oraz administrator SSWiN zostali przeszkoleni z obsługi systemu alarmowego (protokół przejęcia systemu i przeszkolenia)?			
D.III	1. System Kontroli Dostępu: <ul style="list-style-type: none">• Czy stosowany jest przy wejściu na teren jednostki organizacyjnej?• Czy stosowany jest przy wejściu do budynku, w którym zlokalizowana jest KK?• Czy stosowany jest przy wejściu do stref ochronnych?• Czy stosowany jest przy wejściu do pomieszczenia KK? 2. Jakiego rodzaju System Kontroli Dostępu stosuje się w odniesieniu do pkt. 1: <ul style="list-style-type: none">• z wykorzystaniem systemu technicznego (karta zbliżeniowa, czytniki kart itp.)• z zastosowaniem systemów elektromechanicznych (kołowroty itp.)• stosując rozwiązania organizacyjne tj. fizyczna kontrola przez warty/ służby wewnętrzne/ pracowników biur przepustek/ recepcji• inny 3. Jeśli brak to szczegółowo opisać zabezpieczenie przed niekontrolowanym wstępem osób nieupoważnionych. 4. Czy w odniesieniu do pkt. 1 istnieje obustronna kontrola wejść i wyjść? 5. Jak długo i gdzie przechowywane są rejestry z Systemu Kontroli Dostępu? 6. Czy osoby funkcyjne dokonują okresowej analizy rejestrów z Systemu Kontroli Dostępu (kto i kiedy)?			
D.IV	System Telewizji Przemysłowej CCTV: <ul style="list-style-type: none">• Czy w celu zwiększenia skuteczności ochrony pomieszczenia/ pomieszczeń* KK			



Pozycja	Wyszczególnienie	Wynik (opis tak/nie lub spełnia/nie spełnia)	Opis stanu faktycznego	Różnica między stanem faktycznym a normatywnym/uwagi
	zastosowano System Telewizji Przemysłowej CCTV? <ul style="list-style-type: none"> Gdzie zlokalizowano rejestr obrazu? Podać informację dotyczącą okresu przechowywania nagrań systemu telewizji przemysłowej CCTV; 			
D.V	1.Działanie służb ochronnych: <ul style="list-style-type: none"> Czy na terenie jednostki organizacyjnej istnieje Lokalne Centrum Nadzoru? Opis lokalizacji i systemu pracy Lokalnego Centrum Nadzoru Sposób reakcji służb dyżurnych na wywołany alarm Czas reakcji służb dyżurnych/ochronnych/grup interwencyjnych na wywołany alarm 2. Opisać i przywołać dokumenty w których opisano szczegółowo zakres działania i kompetencje: <ul style="list-style-type: none"> oficera dyżurnego dyżurnego LCN dowódcy warty wewnętrznej dowódcy grupy interwencyjnej 			
D.VI	Szkolenia: <ul style="list-style-type: none"> Kto prowadzi szkolenia służb dyżurnych/ ochronnych? Częstotliwość szkoleń służb dyżurnych/ ochronnych z zakresu procedur postępowania w sytuacjach zagrożenia Gdzie odnotowywany jest fakt szkolenia? 			

UWAGI – stosować formę opisową:

Ad. D.I –

.....

Ad. D.II 1 –

.....

Ad. D.II 2 –

.....



Ad. D.III 1 –

.....
.....
.....

Ad. D.III 2 –

.....
.....
.....

Ad. D.III 3 –

.....
.....
.....

Ad. D.III 4 –

.....
.....
.....

Ad. D.III 5 –

.....
.....
.....

Ad. D.III 6 –

.....
.....
.....

Ad. D.IV –

.....
.....
.....

Ad. D.V 1 –

.....
.....
.....

Ad. D.V 2 –

.....
.....
.....

Ad. D.VI –

.....
.....
.....

E. WYPOSAŻENIE

Pozycja	Wyszczególnienie	Wynik (opis tak/nie lub spełnia/nie spełnia)	Opis stanu faktycznego	Różnica między stanem faktycznym a normatywnym/uwagi
E.I	1.Czy pomieszczenie/pomieszczenia* KK wyposażono w urządzenia do przechowywania dokumentów niejawnych (materiałów kryptograficznych)?			



Pozycja	Wyszczególnienie	Wynik (opis tak/nie lub spełnia/nie spełnia)	Opis stanu faktycznego	Różnica między stanem faktycznym a normatywnym/uwagi
	<ul style="list-style-type: none">Klasa urządzeń/szaf stalowych - klasa A / ilość sztuk/ Numery Certyfikatów lub Zaświadczenia Kwalifikacyjne-klasa B / ilość sztuk/ Numery Certyfikatów lub Zaświadczenia Kwalifikacyjne- klasa C /ilość sztuk/ Numery Certyfikatów lub Zaświadczenia Kwalifikacyjne <ul style="list-style-type: none">Czy ww. urządzenia /szafy stalowe dodatkowo zabezpieczono:<ul style="list-style-type: none">- przytwierdzając do podłoża- instalując dodatkową czujkę SSW i N- inne <p>2. Czy urządzenia kryptograficzne deponowane są w pomieszczeniu/pomieszczeniach* magazynowych?</p> <ul style="list-style-type: none">Czy pomieszczenie / pomieszczenia* magazynowe jest/są* zlokalizowane w pomieszczeniach KK?Czy pomieszczenie / pomieszczenia* magazynowe jest/są *zlokalizowane w innej strefie ochronnej?<ul style="list-style-type: none">- opisać sposób zabezpieczenia pomieszczenia / pomieszczeń* magazynowego- strefa ochronna- drzwi (certyfikaty/ zaświadczenia kwalifikacyjne)- okna (zabezpieczenie)-SSW i N- sposób dostępu personelu do pomieszczeń magazynowych (system kontroli dostępu)			
E.II	<p>Urządzenia do niszczenia materiałów i urządzeń kryptograficznych:</p> <ul style="list-style-type: none">Czy w pomieszczeniu/ pomieszczeniach* KK zainstalowano urządzenia do niszczenia dokumentów: podać typ, nazwę, rozmiar ścinków papieru i/lub informatycznych nośników danych?Czy w pomieszczeniu/ pomieszczeniach* KK znajdują się narzędzia do niszczenia urządzeń niejawnych/ kryptograficznych (tj.zestaw dewastacyjny)<ul style="list-style-type: none">- wyszczególnić			



Pozycja	Wyszczególnienie	Wynik (opis tak/nie lub spełnia/nie spełnia)	Opis stanu faktycznego	Różnica między stanem faktycznym a normatywnym/uwagi
	<ul style="list-style-type: none"> • Czy w pomieszczeniu znajdują się urządzenia służące do ewakuacji dokumentów, materiałów, urządzeń kryptograficznych <ul style="list-style-type: none"> - pojemniki lub worki do ewakuacji dokumentów/ materiałów kryptograficznych (czy są odpowiednio opisane na czas transportu) - skrzynie do ewakuacji urządzeń (czy są odpowiednio oznakowane i opisane na czas transportu) - czy w urządzeniach przeznaczonych do ewakuacji przewidziano elementy zamknięć (kłódki certyfikowane, zamki patentowe, plomby jednorazowe) 			
E.III	Wyposażenie pomieszczenia/ pomieszczeń* KK oraz magazynowych <ul style="list-style-type: none"> - regały lub meble przeznaczone do przechowywania teczek akt, wydawnictw, urządzeń kryptograficznych - sprzęt kwaterunkowy 			

UWAGI – stosować formę opisową:

Ad. E.I 1 –

.....

Ad. E.I 2 –

.....

Ad. E.II –

.....

Ad. E.III –

.....



F. DOKUMENTACJA

Pozycja	Wyszczególnienie	Wynik (opis tak/nie lub spełnia/nie spełnia)	Opis stanu faktycznego	Różnica między stanem faktycznym a normatywnym/uwagi
F.I	1.Plan Ochrony/Plan Ochrony Informacji Niejawnych oraz inne dokumenty opisujące ochronę fizyczną oraz zakres działań: 2.Wymienić tytuł i nr ewidencyjny dokumentów: - służb dyżurnych, - ochronnych, - grup interwencyjnych (opisać)			
F.II	1.Czy opracowano Instrukcję (regulamin) pracy pomieszczenia/ pomieszczeń* KK? 2.Czy opracowano Instrukcję (regulamin) czytelní?			
F.III	Czy opracowano Procedury reagowania w sytuacjach zagrożenia dla pomieszczenia/ pomieszczeń* KK?			
F.IV	Czy KK wyposażono w odpowiednie urządzenia ewidencyjne? (opisać jakie)			
F.V	Czy KK wyposażono w odpowiednie uregulowania prawne w zakresie ochrony informacji niejawnych (opisać jakie)?			

UWAGI – stosować formę opisową:

Ad. F.I 1 –

.....
.....

Ad. F.I 2 –

.....
.....

Ad. F.II 1 –

.....
.....

Ad. F.II 2 –

.....
.....

Ad. F.III –

.....
.....

Ad. F.IV –

.....
.....

Ad. F.V –

.....
.....

* niepotrzebne skreślić



REJESTR WZORÓW PODPISÓW							
DANYCH KANCELARII KRYPTOGRAFICZNEJ							
Numer kancelarii	860048/	Z dnia		-		-	
Kancelaria podlega pod	860048/						
Kancelaria odbiera materiał kryptograficzny od	860048/						
Adres:							
Adres Kurierski	860048/						
Ulica/Budynek/Pokój							
Kod, miasto							
Kraj							
Adres do wiadomości							
Dane telefoniczno-faksowe:							
IVSN							
DSN							
Tel. jawny							
Tel. CA MON							
Tel. utajniony 1	Typ						
Tel. utajniony 2	Typ						
Fax. utajniony							
Fax. jawny							

**WZORY PODPISÓW****Oficer Bezpieczeństwa Systemów Łączności i Informatyki**

Nazwisko i imię			
Stopień		Rodz. wojsk	
Certyfikat		Data wyznaczenia	
Data zmiany			
Nr telefonu			
Podpis			

Kierownik Kancelarii Kryptograficznej / Cryptocustodian

Nazwisko i imię			
Stopień		Rodz. wojsk	
Certyfikat		Data wyznaczenia	
Data zmiany			
Podpis			

..... (**)

Nazwisko i imię			
Stopień		Rodz. wojsk	
Certyfikat		Data wyznaczenia	
Podpis			

..... (**)

Nazwisko i imię			
Stopień		Rodz. wojsk	
Certyfikat		Data wyznaczenia	
Podpis			

Potwierdzenie:

m.p.

.....
(Podpis kierownika jednostki organizacyjnej)

**- wpisać kolejno etatowy personel kancelarii kryptograficznej



UZUPEŁNIENIE DO REJESTRU WZORÓW PODPISÓW

Z dnia					
--------	--	--	--	--	--

Dane Kancelarii Kryptograficznej

Numer kancelarii	Numer Certyfikatu ABFiT / Zaświadczenia KOGD* <i>(jeśli jest)</i>	Wydany dnia / ważny do	Klauzula tajności	Uwagi
860048/.....				

Dane oficera BSłil oraz Personelu Kancelarii Kryptograficznej
(oficer BSłil, osoby zastępującej Oficera INFOSEC, itd. w kolejności jak w Załączniku 1)

Lp	Stopień, Nazwisko i Imię	Kurs specjalistyczny (nazwa, numer, data)	Poświadczenie bezpieczeństwa			NATO (UE) Personnel Security Clearance Certificate lub odpowiednie poświadczenie bezpieczeństwa		
			Numer	Klauzula tajności	Data ważności	Numer	Klauzula tajności	Data ważności
1								
2								
3								
4								

m.p.

.....
(podpis dowódcy)

* - niepotrzebne skreślić



SŁUŻBA KONTRWYWIADU WOJSKOWEGO
KRAJOWY ORGAN GENERACJI I DYSTRYBUCJI
NATIONAL DISTRIBUTION AUTHORITY

02-007 Warszawa, ul. Oczki 1, tel. (22) 684-13-33, fax. (22) 684-17-71

Z A Ś W I A D C Z E N I E

nr

o funkcjonowaniu kancelarii kryptograficznej

Numer ewidencyjny kancelarii (ang. ACCN):

Data wydania zaświadczenia:

Lokalizacja pomieszczenia:

Klauzula tajności:

krajowa:

międzynarodowa:

Nazwa i adres

posiadacza zaświadczenia:

Data ważności

zaświadczenia:

Podstawa wydania

zaświadczenia:

Zaświadczenie jest ważne wyłącznie dla wskazanej powyżej kancelarii kryptograficznej powołanej w celu zapewnienia wymaganej ochrony materiałów kryptograficznych krajowych oraz pochodzących z wymiany międzynarodowej.

Z upoważnienia Szefa SKW

DYREKTOR

**Biura Łączności i Informatyki
Służby Kontrwywiadu Wojskowego**

Oficer BSłil

Krajowego Organu Generacji i Dystrybucji

m.p.

.....

.....

Warszawa,



(na odwrocie Załącznika nr 7)

WARUNKI WAŻNOŚCI ZAŚWIADCZENIA

§ 1

Bezpieczeństwo fizyczne

Użytkownik zobowiązany jest do eksploataowania pomieszczeń kancelarii kryptograficznej zgodnie z przepisami Ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2010 r. Nr 182, poz.1228) oraz Zarządzenia Nr 58/MON Ministra Obrony Narodowej z dnia 22 grudnia 2011 r. w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii kryptograficznych (Dz. Urz. MON z 2011 r. Nr 25 poz. 403).

§ 2

Zmiany w pomieszczeniach kancelarii kryptograficznej

1. Użytkownik zobowiązany jest do utrzymania poziomu zabezpieczenia przedmiotowego pomieszczenia zgodnie z dokumentacją stanowiącą podstawę do wydania zaświadczenia.
2. Zabronione jest wprowadzanie zmian wpływających na poziom bezpieczeństwa pomieszczenia bez zgody Szefa KOGD.

§3

Nadzór

Nadzór sprawowany jest przez przedstawicieli nadrzędnych OBSŁiI w zakresie wypełniania przez Użytkowników obowiązków wynikających z posiadania zaświadczenia, prawidłowości eksploatacji pomieszczenia/pomieszczeń kancelarii kryptograficznej.

§4

Postępowanie z zaświadczeniem

Niniejsze zaświadczenie należy odesłać do KOGD, zgodnie z hierarchią zaopatrywania kancelarii kryptograficznych, w przypadku:

1. Odwołania kancelarii kryptograficznej.
2. Wygaśnięcia terminu ważności zaświadczenia.



WNIOSEK

**o zawieszenie/wznowienie* funkcjonowania kancelarii kryptograficznej
nr 860048/.....**

W

.....

/pełna nazwa jednostki organizacyjnej, kod pocztowy, miejscowość, ulica, budynek, pomieszczenie, kompleks
koszarowy/

z lokalizacją w

.....

/wypełniamy w przypadku, gdy adres jest inny niż jednostki organizacyjnej/

1. Uzasadnienie zawieszenia/wznowienia* funkcjonowania:

.....
.....
.....

2. Planowany termin zawieszenia działalności**:

m.p

.....

(stopień, imię, nazwisko i podpis kierownika jednostki organizacyjnej)

* niepotrzebne skreślić

** wypełniać tylko przy zawieszeniu działalności kancelarii kryptograficznej



WNIOSEK

o odwołanie kancelarii kryptograficznej nr 860048/.....

W

.....

/pełna nazwa jednostki organizacyjnej, kod pocztowy, miejscowość, ulica, budynek, pomieszczenie, kompleks
koszarowy/

z lokalizacją w

.....

/wypełniamy w przypadku, gdy adres jest inny niż jednostki organizacyjnej/

1. Uzasadnienie odwołania:

.....
.....
.....

2. Materiały kryptograficzne zostaną przekazane do kancelarii kryptograficznej nr 860048/.....

3. Dotychczasowe miejsce kancelarii w systemie zaopatrywania w materiały kryptograficzne:

– Kancelarie zaopatrujące:

.....
.....

– Kancelarie zaopatrywane:

.....
.....
.....

m.p

.....

(stopień, imię, nazwisko i podpis kierownika jednostki organizacyjnej)