AGENCJA BEZPIECZEŃSTWA WEWNĘTRZNEGO

KRAJOWA WŁADZA BEZPIECZEŃSTWA

Warszawa, dnia 31 grudnia 2010 r.

WYTYCZNE
W SPRAWIE POSTĘPOWANIA
Z INFORMACJAMI NIEJAWNYMI MIĘDZYNARODOWYMI

W celu wykonania art. 11 ust. 1-3 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz.1228), zwanej dalej „ustawą", która powierzyła Szefowi Agencji Bezpieczeństwa Wewnętrznego pełnienie funkcji krajowej władzy bezpieczeństwa, a więc szczególną odpowiedzialność za zapewnienie prawidłowości ochrony informacji niejawnych w stosunkach Rzeczypospolitej Polskiej z innymi państwami i organizacjami międzynarodowymi,

w celu zapewnienia jednolitości systemu ochrony informacji niejawnych międzynarodowych i jego zgodności z przepisami międzynarodowymi, zapewnienia wsparcia merytorycznego dla wszystkich jednostek organizacyjnych przetwarzających informacje niejawne międzynarodowe w postaci sprawdzonych i skutecznych metod oraz procedur zapewniających ich ochronę, a także

mając na uwadze dotychczasowy brak kompleksowego uregulowania zasad bezpieczeństwa dotyczących informacji niejawnych międzynarodowych

zaleca się stosowanie od dnia wejścia w życie ustawy, tj. 2 stycznia 2011 r., następujących reguł postępowania z takimi informacjami:

ZASADY OGÓLNE

1. Informacje niejawne międzynarodowe są to informacje pochodzące od podmiotów zagranicznych lub wytworzone w ich interesie, które – na podstawie zobowiązań przyjętych przez Rzeczpospolitą Polską - wymagają ochrony przed nieuprawnionym dostępem lub ujawnieniem na poziomie jednoznacznie wskazanym poprzez odwołanie

się do klauzul tajności obowiązujących w Rzeczpospolitej Polskiej (określona odpowiedniość klauzul). Informacją niejawną międzynarodową jest także polska informacja niejawna, jeżeli zostaje udostępniona partnerowi zagranicznemu.

2. Nadzór nad systemem ochrony informacji niejawnych, rozumiany jako upoważnienie do określania kierunków polskiej polityki bezpieczeństwa w zakresie ochrony informacji niejawnych międzynarodowych, wytycznych w sprawie wdrażania tej polityki, stwierdzania, czy zastosowane środki ochrony informacji niejawnych międzynarodowych spełniają wymagane dla nich kryteria oraz występowania w tych sprawach przed właściwymi organami organizacji międzynarodowych i innych państw sprawuje Szef ABW. W stosunku do podmiotów, o których mowa w art. 10 ust. 2 ustawy, Szef ABW wykonuje to zadanie przy udziale Szefa SKW, który reprezentuje Szefa ABW przed tymi podmiotami.
3. Określoną w przepisach międzynarodowych funkcję:
   a) National Security Authority (NSA) pełni Szef ABW,
   b) National Communications Security Authority (NCSA) pełni Szef ABW za wyjątkiem podmiotów, o których mowa w art. 10 ust. 2 ustawy, wobec których tę funkcję pełni Szef SKW,
   c) National Distribution Authority (NDA) – dla materiałów kryptograficznych (to jest kluczy kryptograficznych oraz urządzeń i narzędzi wraz z nośnikami, służących do szyfrowania informacji niejawnych, a także dokumentacji technicznej systemów kryptograficznych), wykorzystywanych w systemach teleinformatycznych przetwarzających informacje niejawne UE pełni Szef ABW; dla materiałów kryptograficznych, wykorzystywanych w systemach teleinformatycznych przetwarzających informacje niejawne NATO pełni Szef SKW.
4. Pozostałych informacji wymagających ochrony pozostających w obiegu międzynarodowym, w którym Rzeczpospolita Polska uczestniczy (np. ONZ, Porozumienie z Wassenaar itp.) nie traktuje się jako informacje niejawne międzynarodowe w rozumieniu ustawy. W przypadku, gdy ich przetwarzania nie regulują żadne przepisy prawa polskiego, Szef ABW pełni rolę doradczą i koordynującą w zakresie stosowania właściwych środków bezpieczeństwa. Zasada ta dotyczy m.in. informacji oznaczonych przez NATO lub UE jako odpowiednio UNCLASSIFIED lub LIMITÉ, które traktuje się jako przeznaczone wyłącznie do użytku służbowego.

5. Do ochrony informacji niejawnych międzynarodowych stosuje się następujące akty prawne (wraz z wydanymi do nich aktami wykonawczymi i dokumentami pomocniczymi):
   a) ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz.1228);
   b) umowa między Stronami Traktatu Północnoatlantyckiego o ochronie informacji sporządzona w Brukseli dnia 6 marca 1997 r. (Dz. U. z 2000 r. Nr 64, poz. 740);
   c) umowa między Stronami Traktatu Północnoatlantyckiego o Współpracy w dziedzinie informacji atomowych sporządzona w Paryżu dnia 18 czerwca 1964 r. (Dz. U. z 2001 r. Nr 143, poz.1594);
   d) C-M (2002) 49 – bezpieczeństwo w ramach Organizacji Traktatu Północnoatlantyckiego
   e) Traktat Akcesyjny podpisany dnia 16 kwietnia 2003 r. (Dz. U. z 2004 r. Nr 90, poz. 864, z późn. zm.);
   f) Rozporządzenie Rady Europejskiej Wspólnoty Energii Atomowej (Euratom) nr 3 z dnia 31 lipca 1958 r. (Dz. UE. L. z 1958 r. Nr 17, poz. 406);
   g) Decyzja Rady Unii Europejskiej2001/264/EC z dnia 19 marca 2001 r. w sprawie przyjęcia przepisów Rady dotyczących bezpieczeństwa (Dz. U. UE. L. z 2001 r. Nr 101, poz. 1 z późn. zm.);
   h) Decyzja Komisji Europejskiej 2001/844/EC z dnia 29 listopada 2001 r. (Dz. U. UE. L. z 2001 r. Nr. 317, poz. 1);
   i) bilateralne umowy (porozumienia, memoranda) o wzajemnej ochronie informacji niejawnych oraz inne umowy zawierające regulacje dotyczące ochrony informacji niejawnych międzynarodowych.

DOSTĘP DO INFORMACJI NIEJAWNYCH MIĘDZYNARODOWYCH

6. Dokumentami potwierdzającymi spełnianie przez polskich obywateli lub przedsiębiorców warunków bezpieczeństwa w zakresie ochrony informacji niejawnych międzynarodowych na terytorium Rzeczypospolitej Polskiej – odpowiednio w stosunku do osób lub przedsiębiorców - są: poświadczenie bezpieczeństwa i świadectwo bezpieczeństwa przemysłowego. Poświadczenia i świadectwa upoważniające do dostępu do polskich informacji niejawnych upoważniają jednocześnie do informacji niejawnych międzynarodowych, z wyjątkiem informacji niejawnych NATO i UE. Dostęp do informacji niejawnych tych organizacji

jest uwarunkowany posiadaniem odpowiedniego poświadczenia/świadectwa NATO lub UE. W zakresie informacji oznaczonych klauzulą stanowiącą odpowiednik klauzuli ”zastrzeżone” stosuje się art. 21 ust. 4 oraz art. 54 ust. 9 i 10 ustawy.

7. Poświadczenia i świadectwa, o których mowa w pkt. 6 wydają zgodnie z właściwością określoną w art. 10 ust. 2 i 3 Szef ABW i Szef SKW.
8. W przypadku konieczności potwierdzenia podmiotom zagranicznym zdolności polskich obywateli lub przedsiębiorców do ochrony informacji niejawnych międzynarodowych, Szef ABW wydaje w języku angielskim zaświadczenia, których wzór określają załączniki nr 1-5. Szef ABW potwierdza taką zdolność także w inny – przyjęty przez dane państwo lub organizację międzynarodową – sposób.
9. Zaświadczenia wydawane są na podstawie ważnego i odpowiedniego poświadczenia bezpieczeństwa lub świadectwa bezpieczeństwa przemysłowego.
10. W szczególnie uzasadnionych przypadkach zaświadczenie NATO lub UE może zostać wydane na podstawie ważnego poświadczenia bezpieczeństwa upoważniającego do dostępu do polskich informacji niejawnych o odpowiedniej klauzuli i jednocześnie wszczętego postępowania sprawdzającego dotyczącego dostępu do informacji niejawnych międzynarodowych.
11. W przypadku konieczności wydania zaświadczenia na podstawie poświadczenia lub świadectwa wydanego przez SKW lub WSI, SKW informuje o tym ABW potwierdzając jednocześnie fakt wydania takiego dokumentu wobec danej osoby lub podmiotu (data wydania oraz ważności, rodzaj i klauzula informacji, do której osoba lub przedmiot spełnia wymogi bezpieczeństwa) oraz podając okoliczności wymagających wydania zaświadczenia.
12. ABW może zwrócić się do SKW o uzupełnienie informacji niezbędnych do wydania zaświadczenia lub przesłanie dodatkowych wyjaśnień, jeżeli zachodzą wątpliwości, co do zasadności wydania zaświadczenia, w tym spełnienia warunku, o którym mowa w pkt. 9.
13. Po wydaniu zaświadczenia dotyczącego osoby lub podmiotu, o którym mowa w art. 10 ust. 2 ustawy, ABW przekazuje je do SKW w celu nadania mu dalszego biegu.

SZKOLENIA

14. Warunkiem udostępnienia informacji niejawnych międzynarodowych jest odbycie specjalistycznego szkolenia z zakresu ich ochrony. Szkolenia przeprowadza się wobec:

a) osób ubiegających się o dostęp do takich informacji;
b) osób posiadających dostęp do takich informacji – nie rzadziej niż co 5 lat.

15. Szkolenia, o których mowa w ust. 1, z zastrzeżeniem pkt. 18 przeprowadzają:
    a) ABW i SKW, każda w swoim zakresie określonym w art. 10 ust. 2 i 3 ustawy, wobec kierowników jednostek organizacyjnych, pełnomocników ochrony i kierowników kancelarii tajnych międzynarodowych oraz w szczególnie uzasadnionych przypadkach wobec innych osób;
    b) pełnomocnik ochrony wobec pozostałych osób zatrudnionych w danej jednostce organizacyjnej.
16. Szkolenie polega na przedstawieniu i omówieniu zasad ochrony informacji niejawnych z uwzględnieniem zagadnień praktycznych oraz przekazaniu osobom szkolonym materiałów w postaci aktów prawnych, wytycznych, regulaminów, instrukcji itp.
17. Szkolenie kończy się wydaniem zaświadczenia oraz odebraniem oświadczenia, w którym osoba stwierdza fakt odbycia szkolenia, świadomość odpowiedzialności za ochronę informacji niejawnych międzynarodowych oraz skutków i konsekwencji ich umyślnego i nieumyślnego ujawnienia oraz wykorzystania wbrew obowiązującym przepisom.
18. W przypadku szkolenia z zakresu ochrony informacji niejawnych NATO lub UE uwzględnia się przepisy art. 19 i 20 ustawy.
19. Materiały szkoleniowe są opracowywane lub zatwierdzane przez ABW.
20. W każdej jednostce organizacyjnej przetwarzającej informacje niejawne międzynarodowe znajduje się niezbędny zbiór przepisów bezpieczeństwa dotyczących ochrony tych informacji i jest on udostępniany na żądanie każdej osobie posiadającej do nich dostęp.
21. Nie rzadziej niż raz w roku każda osoba posiadająca dostęp do informacji niejawnych międzynarodowych zapoznaje się w skróconej formie z zasadami bezpieczeństwa dotyczącymi takich informacji i pisemnie ten fakt potwierdza.
22. Zapewnia się dokumentowanie przeprowadzonych szkoleń w taki sposób, aby możliwe było stwierdzenie kto, w jakim czasie i w jakim zakresie został przeszkolony.

UZGADNIANIE WIZYT I TRANSPORTÓW MIĘDZYNARODOWYCH

23. Szef ABW potwierdza dane zawarte we wnioskach o wizytę za granicą związaną z dostępem obywateli polskich do informacji niejawnych międzynarodowych oraz

wyraża zgodę na dostęp obywateli innych państw do informacji niejawnych międzynarodowych na terenie Rzeczypospolitej Polskiej.

24. Szef ABW wyraża zgodę na warunki międzynarodowego transportu materiałów stanowiących lub zawierających informacje niejawne międzynarodowe, jeżeli obowiązek wyrażenia takiej zgody wynika z przepisów prawa, odbywa się z pominięciem dyplomatycznych służb kurierskich lub w innym specjalnym trybie.
25. W przypadku, gdy wizyta lub transport dotyczy osób lub podmiotów, o których mowa w art. 10 ust. 2, Szef ABW wykonuje swoje obowiązki po uzyskaniu opinii SKW.

KANCELARIE TAJNE MIĘDZYNARODOWE

26. Kancelaria tajna międzynarodowa jest komórką organizacyjną, która obsługuje te informacje niejawne międzynarodowe, wobec których wymagane jest utworzenie odrębnego systemu kancelaryjnego. Kancelarie takie funkcjonują w oparciu o regulamin, którego przykład stanowi załącznik nr 6 oraz regulamin czytelni, którego przykład stanowi załącznik nr 7, zwane dalej „regulaminami".
27. Kancelaria tajna międzynarodowa może obsługiwać inne informacje niejawne międzynarodowe niż wymienione w pkt. 26.
28. System kancelarii tajnych międzynarodowych składa się z kancelarii o statusie: głównej kancelarii tajnej międzynarodowej dla sfery cywilnej, głównej kancelarii tajnej międzynarodowej dla sfery wojskowej, głównej kancelarii ATOMAL, kancelarii tajnych międzynarodowych oraz punktów kontroli informacji niejawnych międzynarodowych. Funkcjonujące w jednostkach organizacyjnych, o których mowa w art. 10 ust. 2 ustawy, Punkty Obsługi Dokumentów Zagranicznych (PODZ) zalicza się do punktów kontroli informacji niejawnych międzynarodowych.
29. W przypadku, gdy dostęp do informacji niejawnych jest sporadyczny i doraźny, nie jest konieczne ustanawianie kancelarii tajnej międzynarodowej, pod warunkiem wprowadzenia, wymaganych przez ABW, procedur zapewniających sprawowanie kontroli nad informacjami niejawnymi międzynarodowymi oraz uzyskania zgody Szefa ABW na tę formę przetwarzania informacji niejawnych międzynarodowych. Przepisu nie stosuje się, gdy taki dostęp dotyczy dokumentów oznaczonych klauzulą COSMIC TOP SECRET, TRÉS SECRET UE/ EU TOP SECRET oraz jako ATOMAL.
30. Kancelaria tajna międzynarodowa rozpoczyna i kończy działalność z dniem – odpowiednio - jej wpisu lub wykreślenia z ewidencji kancelarii tajnych

międzynarodowych. Ewidencję kancelarii tajnych międzynarodowych prowadzi ABW.

31. Podstawą wpisu do ewidencji kancelarii tajnych międzynarodowych są, z zastrzeżeniem pkt. 36 i 39, zatwierdzone przez ABW: plan organizacji kancelarii, którego wzór stanowi załącznik nr 8, zwany dalej „planem", oraz regulaminy.
32. Plan i regulaminy są sporządzane przez pełnomocnika ochrony w jednostce organizacyjnej, w której zamierza się utworzyć kancelarię tajną międzynarodową, a następnie, po akceptacji kierownika jednostki organizacyjnej, przekazywane odpowiednio do ABW lub SKW.
33. W przypadku zastrzeżeń do rozwiązań technicznych lub organizacyjnych opisanych w planie lub zasad określonych w regulaminach, ABW przekazuje je do jednostki organizacyjnej, która przesłała taki plan i regulaminy, w celu ich uwzględnienia.
34. Do planu lub regulaminów uwzględniających zastrzeżenia, przepis pkt 32 i 33, stosuje się odpowiednio.
35. W przypadku kancelarii tajnej międzynarodowej w jednostce organizacyjnej, o której mowa w art. 10 ust. 2 ustawy, SKW przekazuje plan oraz projekty regulaminów do ABW wraz z rekomendacją zatwierdzenia lub zgłoszenia określonych zastrzeżeń. ABW informuje taką jednostkę organizacyjną o zatwierdzeniu planu oraz regulaminów lub zgłasza do nich zastrzeżenia za pośrednictwem SKW.
36. Podstawą wpisu do ewidencji kancelarii tajnych międzynarodowych tych komórek organizacyjnych, w których będą przetwarzane informacje niejawne o klauzuli COSMIC TOP SECRET, TRÉS SECRET UE/EU TOP SECRET oraz ATOMAL jest zakończenie z wynikiem pozytywnym procedury akredytacyjnej.
37. Do procedury akredytacyjnej, o której mowa w pkt. 36, stosuje się odpowiednio przepisy pkt. 32-35. Dodatkowo warunkiem zatwierdzenia planu jest pozytywny wynik oględzin pomieszczeń przeznaczonych dla kancelarii tajnej międzynarodowej, w tym zastosowanych rozwiązań technicznych i organizacyjnych.
38. Oględziny, o których mowa w pkt. 37, można również zastosować w odniesieniu do kancelarii tajnych międzynarodowych, które będą przetwarzać informacje niejawne o innych klauzulach w celu sprawdzenia danych zawartych w planie organizacji kancelarii tajnej.
39. W przypadku zamiaru ustanowienia kancelarii tajnej międzynarodowej w oparciu o utworzoną kancelarię tajną międzynarodową lub utworzoną kancelarię tajną, o której mowa w art. 42 ustawy, podstawą wpisu do ewidencji kancelarii tajnych

międzynarodowych jest zatwierdzony przez Szefa ABW wniosek o dokonanie wpisu. Do postępowania z wnioskiem przepisy dotyczące postępowania z planem organizacji kancelarii stosuje się odpowiednio.

40. Wykreślenie kancelarii z ewidencji kancelarii tajnych międzynarodowych następuje na wniosek jednostki organizacyjnej, w której kancelaria funkcjonuje lub w przypadku stwierdzenia w wyniku inspekcji lub postępowania wyjaśniającego, że kancelaria przestała spełniać warunki gwarantujące bezpieczeństwo informacji niejawnych międzynarodowych.
41. Kancelarie tajne międzynarodowe funkcjonujące w dniu wejścia w życie ustawy uznaje się za wpisane do ewidencji kancelarii tajnych międzynarodowych. Kancelarie, którym przyznano prawo do przetwarzania informacji niejawnych międzynarodowych do określonego terminu, uznaje się za zatwierdzone bezterminowo.
42. Procedury zmierzające do utworzenia kancelarii tajnych międzynarodowych rozpoczęte przed dniem wejścia w życie ustawy, mogą być kontynuowane na dotychczasowych zasadach.

INSPEKCJE

43. Inspekcje przeprowadzają cyklicznie, zgodnie z właściwością rzeczową określoną w ustawie, odpowiednio ABW lub SKW.
44. W przypadku jednostek organizacyjnych, w których utworzono kancelarie, o których mowa w pkt. 36 inspekcje przeprowadza się nie rzadziej niż co 2 lata. Od przeprowadzenia inspekcji można odstąpić, jeśli w przeciągu ostatnich dwóch lat w danej jednostce organizacyjnej została przeprowadzona inspekcja przez struktury bezpieczeństwa organizacji międzynarodowych lub w tym czasie nie zarejestrowano żadnego dokumentu rozliczalnego.
45. Dokument rozliczalny to materiał, który stanowi lub zawiera taką informację niejawną międzynarodową, która – zgodnie z umowami międzynarodowymi – podlega obowiązkowi ścisłego nadzoru na każdym etapie jej cyklu życiowego. W przypadku braku takich uregulowań, do określenia, czy dany dokument jest rozliczalny stosuje się odpowiednio przepisy polskie.
46. Inspekcja ma na celu sprawdzenie: zgodności liczby i kompletność dokumentów niejawnych międzynarodowych z zapisami w ewidencjach, prawidłowość zabezpieczenia tych dokumentów, ich obiegu, sposobu fizycznego zabezpieczenia, a także organizację systemu bezpieczeństwa informacji w jednostce organizacyjnej.

47. Inspekcję przeprowadza się w oparciu o formularz, którego wzór stanowi załącznik nr 9.
48. W przypadku asystowania funkcjonariusza ABW w inspekcji przeprowadzanym przez SKW albo żołnierza lub funkcjonariusza SKW w inspekcji przeprowadzanej przez ABW, osoba ta pełni rolę obserwatora i nie podejmuje żadnych czynności merytorycznych.
49. Inspekcje przeprowadza komisja powołana i właściwie upoważniona odpowiednio przez Szefa ABW lub Szefa SKW.
50. Po zakończeniu inspekcji komisja sporządza notatkę z inspekcji zawierającą ocenę stanu faktycznego, wnioski oraz ewentualne zalecenia do realizacji. Jeden egzemplarz przekazuje się kierownikowi jednostki organizacyjnej, której inspekcja dotyczyła, drugi przechowuje odpowiednio ABW lub SKW. W przypadku prowadzenia inspekcji przez SKW trzeci egzemplarz notatki z inspekcji jest przekazywany do ABW.

POSTĘPOWANIA WYJAŚNIAJĄCE

51. Postępowanie wyjaśniające zmierza do stwierdzenia, czy faktycznie doszło do naruszenia przepisów dotyczących bezpieczeństwa informacji niejawnych międzynarodowych, jakich, w jaki sposób, przez kogo oraz, czy skutkiem takiego naruszenia jest lub może być narażenie na szwank takich informacji.
52. Podstawowe postępowanie wyjaśniające prowadzone jest przez pełnomocnika ochrony w zakresie okoliczności dotyczących danej jednostki organizacyjnej. Nadzorcze postępowanie wyjaśniające prowadzi Szef ABW. W jednostkach, o których mowa w art. 10 ust. 2 ustawy, postępowanie nadzorcze prowadzone jest za pośrednictwem Szefa SKW, z tym że Szef ABW może przejąć prowadzenie takiego postępowania w części lub całości.
53. W przypadku podstawowego postępowania wyjaśniającego w sprawie naruszenia przepisów dotyczących informacji o klauzuli stanowiącej odpowiednik „zastrzeżone" pełnomocnik ochrony informuje krajową władzę bezpieczeństwa o wynikach postępowania.
54. W przypadku podstawowego postępowania wyjaśniającego w sprawie naruszenia przepisów dotyczących informacji o klauzuli stanowiącej odpowiednik „poufne" i wyższej pełnomocnik informuje krajową władzę bezpieczeństwa o naruszeniu bądź podejrzeniu naruszenia przepisów niezwłocznie.

55. W ramach nadzorczego postępowania wyjaśniającego krajowa władza bezpieczeństwa może żądać informacji o czynnościach podjętych w trakcie podstawowego postępowania wyjaśniającego, o ich wynikach oraz o działaniach planowanych. Ponadto krajowa władza bezpieczeństwa może żądać podjęcia określonych czynności wyjaśniających, a także przejmować ich wykonanie od pełnomocnika lub w nich uczestniczyć.
56. Krajowa władza bezpieczeństwa może zwracać się do innych niż prowadzących podstawowe postępowania wyjaśniające pełnomocników ochrony, jeżeli wymaga tego wyjaśnianie sprawy.
57. Krajowa władza bezpieczeństwa informuje właściwe organy bezpieczeństwa organizacji międzynarodowych lub innych państw o stwierdzeniu naruszenia przepisów dotyczących informacji niejawnych w zakresie i trybie określonym w przepisach bezpieczeństwa tych organizacji lub umowach bilateralnych.
58. W przypadku podmiotów, o których mowa w art. 10 ust. 2 ustawy, Szef SKW:
    a) realizuje zadania krajowej władzy bezpieczeństwa samodzielnie w sprawach, o których mowa w pkt. 53 i 54;
    b) realizuje zadania krajowej władzy bezpieczeństwa w sprawach, o których mowa w pkt. 55 i 56 po poinformowaniu lub na zlecenie Szefa ABW;
    c) przekazuje Szefowi ABW informacje, które uzyskał w związku z realizacją zadań, o których mowa w lit. a i b.

SYTUACJE NADZWYCZAJNE

59. Sytuacja nadzwyczajna oznacza stan zagrożenia dla bezpieczeństwa informacji niejawnych międzynarodowych (nieuprawnione ujawnienie, zniszczenie lub zagubienie informacji) wynikające z: niepokojów społecznych (demonstracje, rozruchy), katastrofy budowlanej oraz wynikające z sytuacji określonej w art. 228-230 Konstytucji RP oraz określonych w przepisach ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym a także ataku cyberterrorystycznego.
60. Sposób postępowania z informacjami niejawnymi międzynarodowymi w sytuacjach nadzwyczajnych powinien stanowić część planu ochrony jednostki organizacyjnej.
61. Zalecenia do planów ochrony jednostek organizacyjnych w zakresie postępowania z informacjami niejawnymi międzynarodowymi w sytuacjach nadzwyczajnych stanowią załącznik nr 10.

WSPÓŁDZIAŁANIE SZEFA ABW Z SZEFEM SKW

62. Współdziałanie w obszarze udzielania Szefowi ABW przez Szefa SKW informacji niezbędnych do pełnienia funkcji krajowej władzy bezpieczeństwa obejmuje:
    a) informowanie o prowadzonych procedurach i procesach określonych w przepisach dotyczących ochrony informacji niejawnych międzynarodowych;
    b) przekazywanie informacji dotyczących organizacji i stanu systemu ochrony informacji niejawnych międzynarodowych oraz działań planowanych i podejmowanych w celu zapewnienia prawidłowości jego funkcjonowania;
    c) informowanie o wpływie oraz prowadzeniu korespondencji, której treść posiada istotne znaczenie dla zapewnienia prawidłowego nadzoru nad systemem ochrony informacji niejawnych międzynarodowych;
    d) bezzwłoczne informowanie o istotnych incydentach bezpieczeństwa teleinformatycznego, w systemach TI w których przetwarzane są informacje niejawne międzynarodowe, w tym o incydentach mających znamiona ataku cyberterrorystycznego;
    e) przekazywanie danych koniecznych do wypełniania zadań informacyjnych, ewidencyjnych i analitycznych;
    f) udostępnianie sprawozdań, raportów, notatek lub innych dokumentów o tym charakterze w zakresie, w jakim:
        i) zawierają wyniki czynności nadzorczych, wyjaśniających i innych opisujących stan systemu ochrony informacji niejawnych międzynarodowych,
        ii) relacjonują udział w pracach zespołów, grup, komitetów i innych spotkań poświęconych ochronie informacji niejawnych międzynarodowych,
        iii) dotyczą innych spraw objętych zakresem współdziałania.
63. Szef ABW, we współpracy z Szefem SKW, określa częstotliwość przekazywania lub udostępniania oraz rodzaj wymaganych informacji, materiałów i dokumentów.
64. Szef SKW przekazuje lub udostępnia Szefowi ABW wymagane informacje, materiały i dokumenty niezwłocznie, o ile nie wskazano terminu ich przekazania lub udostępnienia.
65. Szef ABW udziela niezwłocznie Szefowi SKW informacji, o których mowa w pkt. 62, w zakresie niezbędnym do zapewnienia skuteczności i jednolitości systemu ochrony informacji niejawnych międzynarodowych.
66. Współdziałanie w obszarze asystowania imiennie upoważnionych funkcjonariuszy ABW podczas wykonywania czynności właściwych dla krajowej władzy

bezpieczeństwa przez SKW oraz imiennie upoważnionych żołnierzy i funkcjonariuszy SKW podczas wykonywania czynności właściwych dla krajowej władzy bezpieczeństwa przez ABW, dotyczy czynności związanych z:

a) procedurą tworzenia kancelarii tajnych międzynarodowych;
b) prowadzeniem inspekcji i audytów bezpieczeństwa teleinformatycznego w podmiotach, w których są lub będą przetwarzane informacje niejawne międzynarodowe;
c) prowadzeniem czynności wyjaśniających związanych z naruszeniem przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych międzynarodowych;
d) szkoleniami oraz innymi przedsięwzięciami edukacyjnymi i doradczymi.

67. Asystowanie, o którym mowa w pkt. 66, ma na celu zebranie informacji niezbędnych do określenia jednolitych zasad, programów oraz procedur właściwych dla krajowej władzy bezpieczeństwa, a także umożliwienie dokonania oceny zastosowanych w praktyce rozwiązań.
68. W ramach współdziałania Szefa ABW z Szefem SKW, uzgadnianie działań podejmowanych w ramach wykonywania funkcji krajowej władzy bezpieczeństwa dotyczy:
    a) interpretacji przepisów dotyczących ochrony informacji niejawnych międzynarodowych;
    b) opiniowania projektów zmian w przepisach dotyczących ochrony informacji niejawnych międzynarodowych;
    c) udzielania odpowiedzi na zapytania w sprawach związanych z ochroną informacji niejawnych międzynarodowych, kierowane przez organizacje międzynarodowe, krajowe władze bezpieczeństwa innych państw oraz inne instytucje i osoby;
    d) innych przedsięwzięć mogących mieć wpływ na wywiązywanie się Rzeczypospolitej Polskiej z zobowiązań dotyczących ochrony informacji niejawnych międzynarodowych.
69. Szef ABW, we współpracy z Szefem SKW, określa jednolite zasady oraz, jeżeli to konieczne, szczegółowy sposób postępowania w sprawach, o których mowa w pkt. 68.
70. W ramach współdziałania Szefa ABW z Szefem SKW, obowiązek określania składu delegacji reprezentujących Rzeczypospolitą Polską przed organizacjami międzynarodowymi i krajowymi władzami bezpieczeństwa innych państw oraz ustalania treści stanowisk przedstawianych przez takie delegacje, dotyczy przypadków udziału przedstawicieli Rzeczypospolitej Polskiej w:

a) posiedzeniach komitetów, grup roboczych i zespołów eksperckich dotyczących ochrony informacji niejawnych międzynarodowych;
b) negocjacjach umów międzynarodowych o ochronie informacji niejawnych;
c) spotkaniach z przedstawicielami struktur organizacji międzynarodowych odpowiedzialnych za ochronę informacji niejawnych międzynarodowych oraz przedstawicielami krajowych władz bezpieczeństwa innych państw;
d) innych przedsięwzięciach dotyczących ochrony informacji niejawnych międzynarodowych.

71. Szef ABW i Szef SKW informują się nawzajem o planowanym spotkaniu, jego tematyce (agenda) proponowanym składzie delegacji oraz treści przedstawianych przez nią stanowisk. Brak zastrzeżeń oznacza uzgodnienie tych spraw.
72. Informacje, o których mowa w pkt. 71, są przekazywane w terminie pozwalającym na wyrażenie zastrzeżeń i podjęcia próby ich usunięcia.
73. W przypadku braku uzgodnienia, o którym mowa w pkt. 71, skład delegacji oraz treść przedstawianych przez nią stanowisk określa Szef ABW.
74. Określenie składu delegacji oznacza wskazanie liczby i stanowisk osób wchodzących w jej skład.
75. W składzie delegacji krajowej władzy bezpieczeństwa na spotkania dotyczące spraw pozostających we właściwości SKW jej przedstawiciel bierze udział w charakterze eksperta. Szef SKW może wskazać w to miejsce osobę nie będącą żołnierzem lub funkcjonariuszem SKW.
76. W celu zapewnienia efektywnej organizacji i koordynacji współdziałania:
    a) powołuje się zespoły zadaniowe składające się z funkcjonariuszy ABW i żołnierzy oraz funkcjonariuszy SKW pracujące pod kierunkiem funkcjonariuszy ABW;
    b) zapewnia się organizację doraźnych kontaktów roboczych, planowych odpraw sprawozdawczych i innych spotkań;
    c) wskazuje się jednostki, komórki organizacyjne i upoważnione osoby, które współdziałają ze sobą bezpośrednio;
    d) wskazuje się stały punkt kontaktowy w postaci numeru telefonu, faxu i adresu email;
    e) tworzy się lub wskazuje system teleinformatyczny służący bezpiecznej i sprawnej wymianie informacji.
77. Korespondencja pomiędzy ABW i SKW powinna odbywać się głównie w postaci przekazu elektronicznego, w tym przy użyciu zabezpieczonej łączności. W przypadku

braku takiej możliwości przesyłki nie powinny przybierać formy wymagającej, zgodnie z odrębnymi przepisami, rejestracji. Ewentualna rejestracja powinna przebiegać w oparciu o uproszczone, podręczne urządzenia.

78. Szef ABW i Szef SKW, każdy zgodnie z właściwością rzeczową określoną w ustawie, prowadzą zbiory danych, zapewniając do nich wzajemny dostęp, w tym w formie transmisji danych, dotyczące:
    a) wydanych poświadczeń bezpieczeństwa, świadectw bezpieczeństwa przemysłowego i innych dokumentów uprawniających do dostępu do informacji niejawnych międzynarodowych, w tym prostych danych identyfikujących osoby i podmioty, których te dokumenty dotyczą,
    b) stanu procedur dotyczących badania zdolności osoby lub podmiotu do ochrony informacji niejawnych międzynarodowych,
    c) zatwierdzonych kancelarii tajnych międzynarodowych,
    d) wyników inspekcji i postępowań wyjaśniających,
    e) przepisów dotyczących ochrony informacji niejawnych międzynarodowych obowiązujących w jednostkach organizacyjnych, o których mowa w art. 10 ust. 2 ustawy, w tym zawartych umów i porozumień międzynarodowych dotyczących ochrony informacji niejawnych,
    f) udziału przedstawicieli RP w strukturach organizacji międzynarodowych zajmujących się bezpieczeństwem informacji (listy delegatów, sprawozdania, raporty, kalendarze spotkań itp.),
    g) akredytowanych międzynarodowych systemów teleinformatycznych,
    h) powołanych kancelarii kryptograficznych,
    i) certyfikowanych środków ochrony elektromagnetycznej, urządzeń i narzędzi kryptograficznych oraz urządzeń i narzędzi realizujących zabezpieczenia teleinformatyczne.

ZAWIERANIE UMÓW MIĘDZYNARODOWYCH

79. Szef ABW pełni wiodącą rolę w zakresie zawierania przez Rzeczpospolitą Polską umów międzynarodowych o wzajemnej ochronie informacji niejawnych a także pozostałych umów międzynarodowych regulujących zasady ochrony informacji niejawnych międzynarodowych.
80. Następujące czynności wymagają uprzedniej konsultacji z Szefem ABW:

a) przekazanie partnerom zagranicznym wiążącej deklaracji o zainteresowaniu Rzeczypospolitej Polskiej uregulowaniem zasad wzajemnej ochrony informacji niejawnych,
b) przekazanie partnerom zagranicznym projektu umowy mającej wiązać Rzeczpospolitą Polską w zakresie ochrony informacji niejawnych międzynarodowych,
c) akceptacja lub wniesienie uwag do projektu umowy mającej wiązać Rzeczpospolitą Polską w zakresie ochrony informacji niejawnych międzynarodowych przekazanej przez partnerów zagranicznych.

BEZPIECZEŃSTWO TELEINFORMATYCZNE:

81. Akredytacja systemów przetwarzających informacje niejawne międzynarodowe.
    a) Informacje niejawne międzynarodowe mogą być przetwarzane tylko w systemach, które posiadają akredytację bezpieczeństwa teleinformatycznego.
    b) Akredytacji punktów dostępowych systemów przetwarzających niejawne informacje międzynarodowe, organizowanych przez podmioty międzynarodowe, dokonuje odpowiednio, zgodnie z właściwością rzeczową, Szef ABW lub Szef SKW. Szef SKW informuje Szefa ABW o dokonanej akredytacji.
    c) Akredytacja systemów organizowanych przez polskie jednostki organizacyjne, w których dopuszczono przetwarzanie informacji niejawnych międzynarodowych, odbywa się z uwzględnieniem postanowień pkt ”b” i wymagań wynikających z umów międzynarodowych.
82. Audyt bezpieczeństwa systemów przetwarzających informacje niejawne międzynarodowe.
    a) Audyty bezpieczeństwa systemów przetwarzających informacje niejawne międzynarodowe dokonywane są przez osoby, wyznaczone przez Szefa ABW lub Szefa SKW, zgodnie z właściwością rzeczową.
    b) Audyty przeprowadzane są przed akredytacją systemu oraz w trakcie jego użytkowania, nie rzadziej niż co 18 miesięcy.
    c) W przypadku wystąpienia istotnego incydentu bezpieczeństwa teleinformatycznego audyty przeprowadzane są na zasadzie ad hoc.
    d) Audyty kończone są raportem zawierającym ocenę i wnioski. O wynikach audytu informuje się organizatora systemu. W przypadku audytów dokonywanych przez SKW, jeden egzemplarz raportu przekazywany jest do Szefa ABW.

e) W audytach prowadzonych przez SKW mogą uczestniczyć, w charakterze obserwatorów, funkcjonariusze ABW.

83. Potwierdzenie dla obrotu międzynarodowego, certyfikatu narzędzia lub urządzenia kryptograficznego, środka ochrony elektromagnetycznej lub urządzenia lub narzędzia służącego do realizacji zabezpieczenia teleinformatycznego, wydanego przez ABW lub SKW dla obrotu krajowego, realizowane jest przez Szefa ABW.
84. Zasady dystrybucji materiałów kryptograficznych
    a) Za dystrybucję, generację i bezpieczeństwo materiałów kryptograficznych służących ochronie informacji niejawnych międzynarodowych odpowiada Szef ABW we współpracy z Szefem SKW.
    b) Dystrybucja materiałów kryptograficznych zabezpieczających funkcjonowanie systemów teleinformatycznych przetwarzających informacje niejawne UE odbywa się za pośrednictwem głównej kancelarii kryptograficznej podległej Szefowi ABW. Dystrybucja tych materiałów wobec podmiotów, o których mowa w art. 11 ust. 3 ustawy odbywa się poprzez główną kancelarię kryptograficznej podległą Szefowi SKW.
    c) Dystrybucja materiałów kryptograficznych zabezpieczających funkcjonowanie systemów teleinformatycznych przetwarzających informacje niejawne NATO odbywa się za pośrednictwem głównej kancelarii kryptograficznej podległej Szefowi SKW.

Załącznik nr 1

NATIONAL SECURITY AUTHORITY
OF THE REPUBLIC OF POLAND

INTERNAL SECURITY AGENCY

NATO PERSONNEL SECURITY CLEARANCE CERTIFICATE NO. _____

1. Certification is hereby given that:

Full Name: .....

Date and Place of Birth: .....

has been granted a personnel security clearance by the Government of:

.....

in accordance with current NATO regulations, including the Security Annex to C-M (64)39 in the case of ATOMAL information, and is, therefore, declared suitable to be entrusted with information classified up to and including:

.....

2. The validity of this certificate will expire not later than: .....

Signed:

.....

Title: DIRECTOR/DEPUTY DIRECTOR OF THE DEPARTMENT FOR THE

PROTECTION OF CLASSIFIED INFORMATION, INTERNAL SECURITY AGENCY

Date:

National Security Authority of the Republic of Poland
Internal Security Agency
Rakowiecka 2 A
00 – 993 Warszawa
e-mail: nsa@abw.gov.pl
fax: +48 22 58 57 443

Załącznik nr 2

NATIONAL SECURITY AUTHORITY
OF THE REPUBLIC OF POLAND

INTERNAL SECURITY AGENCY

EU PERSONNEL SECURITY CLEARANCE CERTIFICATE NO. _____

1. Certification is hereby given that:

Full Name: .....

Date and Place of Birth: .....

has been granted a personnel security clearance and is therefore, declared suitable to be entrusted with information classified up to and including

.....

2. The validity of this certificate will expire not later than: .....

Signed:

.....

Title: DIRECTOR/DEUTY DIRECTOR OF THE DEPARTMENT FOR THE PROTECTION OF CLASSIFIED INFORMATION, INTERNAL SECURITY AGENCY

Date:

National Security Authority of the Republic of Poland
Internal Security Agency
Rakowiecka 2 A
00 – 993 Warszawa
e-mail: nsa@abw.gov.pl
fax: +48 22 58 57 443

Załącznik nr 3

NATIONAL SECURITY AUTHORITY
OF THE REPUBLIC OF POLAND

INTERNAL SECURITY AGENCY

PERSONNEL SECURITY CLEARANCE CERTIFICATE NO._____

1. Certification is hereby given that:

Full Name: .....

Date and Place of Birth: .....

has been granted a personnel security clearance and is therefore, declared suitable to be entrusted with information classified up to and including

.....

2. The validity of this certificate will expire not later than: .....

Signed:

.....

Title: DIRECTOR/DEUTY DIRECTOR OF THE DEPARTMENT FOR THE PROTECTION OF CLASSIFIED INFORMATION, INTERNAL SECURITY AGENCY

Date:

National Security Authority of the Republic of Poland
Internal Security Agency
Rakowiecka 2 A
00 – 993 Warszawa
e-mail: nsa@abw.gov.pl
fax: +48 22 58 57 443

Załącznik nr 4

NATIONAL SECURITY AUTHORITY
OF THE REPUBLIC OF POLAND

INTERNAL SECURITY AGENCY

NATO FACILITY SECURITY CLEARANCE CERTIFICATE NO. _____

1. This is to certify that:

Name of facility: .....

Address of facility: .....

has been granted NATO facility security clearance by Internal Security Agency/Counter – Intelligence Service - in accordance with the provisions of the Industrial Security Directive supporting Enclosure 'G' to the NATO Security Policy - up to and including:

.....

2. The validity of this certificate will expire not later than: .....

3. The National Security Authority of the Republic of Poland confirms that the facility:

- ☐ possesses NO storage capabilities approved for the safeguarding of NATO classified information.
- ☐ possesses storage capabilities approved for the safeguarding of classified information up to the NATO ..... level;
- ☐ possesses capabilities to generate, store and transmit in IT systems and network classified information up to the NATO ..... level.

Signed:

.....

Title: DIRECTOR/DEPUTY DIRECTOR OF THE DEPARTMENT FOR THE PROTECTION OF CLASSIFIED INFORMATION, INTERNAL SECURITY AGENCY

Date:

National Security Authority of the Republic of Poland
Internal Security Agency
Rakowiecka 2 A
00 – 993 Warszawa
e-mail: nsa@abw.gov.pl
fax: +48 22 58 57 443

Załącznik nr 5

NATIONAL SECURITY AUTHORITY
OF THE REPUBLIC OF POLAND

INTERNAL SECURITY AGENCY

EU FACILITY SECURITY CLEARANCE CERTIFICATE NO. _____

1. This is to certify that:

Name of facility: .....

Address of facility: .....

has been granted EU facility security clearance classified up to and including:

.....

2. The validity of this certificate will expire not later than: .....

3. The National Security Authority of the Republic of Poland confirms that the facility:

- ☐ possesses NO storage capabilities approved for the safeguarding of EU classified information.
- ☐ possesses storage capabilities approved for the safeguarding of classified information up to the EU ..... level;
- ☐ possesses capabilities to generate, store and transmit in IT systems and network classified information up to the EU ..... level.

Signed:

.....

Title: DIRECTOR/DEPUTY DIRECTOR OF THE DEPARTMENT FOR THE PROTECTION OF CLASSIFIED INFORMATION, INTERNAL SECURITY AGENCY

Date:

National Security Authority of the Republic of Poland
Internal Security Agency
Rakowiecka 2 A
00 – 993 Warszawa
e-mail: nsa@abw.gov.pl
fax: +48 22 58 57 443

Załącznik nr 6

ZATWIERDZAM Miejscowość, dnia .....

……
…
(imię, nazwisko, pieczęć i podpis kierownika jednostki organizacyjnej)

Regulamin
kancelarii tajnej międzynarodowej
w .....
(nazwa jednostki organizacyjnej)
obsługującej informacje niejawne……..……
(nazwa organizacji międzynarodowej, państwa, reżimu)
oznaczone ……
(wpisać poziom klauzuli, do których ma być upoważniona kancelaria)

Kancelaria Tajna Międzynarodowa w ..... (zwana dalej KTM) – działa na
(nazwa jednostki organizacyjnej)

podstawie[1]:

- „Umowy pomiędzy Stronami Traktatu Północnoatlantyckiego o ochronie informacji" (Dz. U. z 2000 r., Nr 64, poz. 740)
- artykułu 4 pkt. 3 Traktatu o Unii Europejskiej, podpisanego w Brukseli 30 kwietnia 2008 r.
- ustawy o ochronie informacji niejawnych z dnia 05 sierpnia 2010 r. (Dz. U. z 2010 r., Nr 182, poz. 1228),
- ***Inne (wpisać)*……**

KTM stosuje zasady i przepisy bezpieczeństwa:

- Organizacji Traktatu Północnoatlantyckiego, a zwłaszcza postanowienia zawarte w dokumencie C-M (2002)49,
- przepisy bezpieczeństwa Rady Unii Europejskiej oraz Komisji Europejskiej, a zwłaszcza przepisy zawarte w Decyzji Rady UE nr 2001/264/EC z 19.03.2001 oraz przepisy zawarte w Decyzji Komisji Europejskiej nr 2001/844/EC z 29.11.2001 z późn. zm.

[1] Niewłaściwe skreślić

- *Inne (wpisać) ……..*

PRZEPISY OGÓLNE

§ 1.

1. Regulamin określa zasady organizacji i funkcjonowania KTM oraz przetwarzania:
   1) materiałów ***(wpisać nazwę organizacji międzynarodowej/ych, państwa/państw, reżimu)*** opatrzonych klauzulami ***(wpisać poziom klauzul, do których ma być upoważniona kancelaria)***,
   2) materiałów pochodzących z państw członkowskich ***(wpisać nazwę organizacji międzynarodowej/ych),*** państw ***(wymienić)*** opatrzonych krajowymi odpowiednikami klauzul o których mowa w pkt. 1 przekazywanych do ***(wpisać nazwę organizacji międzynarodowej/ych, państwa/państw)*** albo RP w ramach programu, projektu lub kontraktu ***(wpisać nazwę organizacji międzynarodowej/ych, państwa/państw),***
   3) materiałów krajowych opatrzonych klauzulami (***(wpisać poziom klauzul)*** związanych ze współpracą z ***(wpisać nazwę organizacji międzynarodowej/ych, państwa/państw, reżimu)*** w sprawach określonych w pkt. 2.
2. KTM posiada status podkancelarii i podlega – w zakresie bezpieczeństwa informacji niejawnych międzynarodowych – Głównej Kancelarii Tajnej Międzynarodowej dla sfery cywilnej RP/Głównej Kancelarii Tajnej Międzynarodowej dla sfery wojskowej[2], zwanej dalej GKT.
3. Zasady udostępniania materiałów niejawnych międzynarodowych w czytelni KT są określone w oddzielnym regulaminie, zatwierdzonym przez kierownika jednostki organizacyjnej.
4. KTM nadzoruje prawidłowy obieg materiałów niejawnych międzynarodowych w ***(wpisać nazwę jednostki organizacyjnej)***

§ 2.

W rozumieniu Regulaminu:

1) dokumentem – jest każda utrwalona informacja niejawna;
2) materiałem – jest dokument lub przedmiot albo dowolna ich część, chronione jako informacja niejawna, a zwłaszcza urządzenie, wyposażenie lub broń wyprodukowane albo będące w trakcie produkcji, a także składnik użyty do ich wytworzenia;
3) przetwarzaniem informacji niejawnych międzynarodowych – są wszelkie operacje wykonywane w odniesieniu do informacji niejawnych międzynarodowych i na tych informacjach, w szczególności ich wytwarzanie, modyfikowanie, kopiowanie, klasyfikowanie, gromadzenie, przechowywanie, przekazywanie lub udostępnianie;
4) reżimem – ściśle określona grupa materiałów niejawnych międzynarodowych oraz określony tryb postępowania z tego typu materiałami np. informacje niejawne ATOMAL, BOHEMIA;
5) przesyłką – zob. § 4 Rozporządzenia Prezesa Rady Ministrów z dnia 29 września 2005 r. w

[2] Niewłaściwe skreślić

sprawie trybu i sposobu przyjmowania, przewożenia, wydawania i ochrony materiałów (Dz.U. Nr 200, poz.1650) – zwanego dalej Rozporządzeniem;

6) ustawą – ustawa o ochronie informacji niejawnych z dnia 05 sierpnia 2010 r. (Dz. U. z 2010 r., Nr 182, poz. 1228),

7) informatyczny nośnik danych – materiał lub urządzenie w rozumieniu art. 3 pkt 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. nr 64, poz. 565, z późn. zm.)

8) podkancelarią – jest, w strukturze kancelarii tajnych międzynarodowych, filia Głównej Kancelarii Tajnej (GKT) utworzona w jednostce organizacyjnej, w której wykorzystywane są informacje niejawne międzynarodowe. Podkancelaria odpowiedzialna jest przetwarzanie dokumentów niejawnych międzynarodowych;

9) kancelarią tajną – jest podkancelaria;

10) zasadą „need to know" – jest zasada ograniczonego dostępu, zgodnie z którą należy określić, czy osoba, która ma stać się odbiorcą informacji, powinna uzyskać do niej dostęp, zapoznać się z nią lub też wejść w jej posiadanie w związku z wykonywaniem swoich obowiązków służbowych;

11) dekretacją – jest odręczna adnotacja właściwego przełożonego na opakowaniu przesyłki i pierwszej stronie materiału obejmująca informację o sposobie dalszego postępowania oraz imię, nazwisko, datę i podpis właściwego przełożonego;

12) pokwitowaniem – jest podanie daty, czytelnego imienia i nazwiska oraz podpis osoby odbierającej dokument na karcie zapoznania z dokumentem lub dzienniku ewidencyjnym;

13) naruszenie przepisów dotyczących bezpieczeństwa informacji niejawnych międzynarodowych – jest działanie lub zaniechanie, celowe lub przypadkowe, sprzeczne z przepisami bezpieczeństwa ***(wpisać nazwę organizacji międzynarodowej/ych, państwa/państw, reżimu)***, które doprowadziło lub mogło doprowadzić do narażenia na szwank informacji niejawnych międzynarodowych.

§ 3.

1. KTM kieruje wyznaczony przez kierownika jednostki organizacyjnej „Kierownik KTM". Kierownik jednostki organizacyjnej wyznacza także Zastępcę Kierownika, pełniącego funkcję Kierownika KTM w razie jego nieobecności.
2. Kierownik KTM podlega Pełnomocnikowi do spraw ochrony informacji niejawnych w ***(wpisać nazwę jednostki organizacyjnej)*** w zakresie określonym przepisami o ochronie informacji niejawnych.
3. Pracownicy KTM przed podjęciem czynności służbowych muszą uzyskać odpowiednie poświadczenia bezpieczeństwa oraz zostać przeszkoleni przez odpowiednio Agencję Bezpieczeństwa Wewnętrznego (ABW) lub Służbę Kontrwywiadu Wojskowego (SKW) w zakresie ochrony informacji niejawnych międzynarodowych.

§ 4.

Kierownik KTM jest w szczególności odpowiedzialny za:

1) sprawowanie nadzoru nad prawidłowym – zgodnym z regulaminem KTM – obiegiem zarejestrowanych w tej kancelarii materiałów niejawnych międzynarodowych;
2) prowadzenie bieżącej ewidencji wszystkich przychodzących oraz wychodzących materiałów niejawnych międzynarodowych z ***(wpisać nazwę jednostki organizacyjnej)***;
3) sprawowanie nadzoru nad korzystaniem z materiałów niejawnych międzynarodowych w czytelni KTM;
4) przygotowanie materiałów niejawnych międzynarodowych do brakowania oraz ich brakowanie;
5) odbieranie przesyłek zawierających materiały niejawne międzynarodowe zaadresowanych do ***(wpisać nazwę jednostki organizacyjnej)*** oraz przesyłanie takich przesyłek do innych, upoważnionych odbiorców;
6) przeprowadzenie do końca stycznia każdego roku kalendarzowego przeglądu posiadanych materiałów niejawnych międzynarodowy i przekazanie do odpowiednio ABW lub SKW sprawozdania z tego przeglądu.

§ 5.

1. Materiały niejawne międzynarodowe przechowywane są w II i I strefie ochronnej w certyfikowanych szafach metalowych.
2. Materiały o klauzuli ***(wpisać poziom klauzuli)***[3] należy dodatkowo oddzielić od informacji o innych klauzulach i przechowywać w osobnym sejfie, szafie metalowej lub jej osobno zamykanej części.
3. Sprzęt, stanowiący wyposażenie KTM i używany do przetwarzania informacji niejawnych międzynarodowych (kopiarki, faksy, urządzenia do niszczenia dokumentów, telefony oraz systemy teleinformatyczne itp.) musi być objęty ochroną fizyczną zapewniającą, że będą go używać wyłącznie osoby upoważnione.
4. Wyposażenie KTM wymienione w ust. 2, a także znajdujące się tam sejfy, szafy metalowe oraz meble biurowe, powinny być oznaczone i umieszczone w spisie inwentarza znajdującym się w tej kancelarii.

§ 6.

Dostęp do materiału niejawnego międzynarodowego bądź zawierającej go przesyłki może mieć wyłącznie osoba, która:

1) posiada odpowiednie poświadczenie bezpieczeństwa wydane przez krajową władzę bezpieczeństwa (KWB),

[3] wpisać najwyższy poziom klauzuli zgodnie z przepisami bezpieczeństwa danej organizacji międzynarodowej, państwa, reżimu.

2) została przeszkolona w zakresie ochrony informacji niejawnych międzynarodowych oraz upoważniona do dostępu do danej informacji,

3) spełnia zasadę „need-to-know”.

WYKAZY i REJESTRY

§ 7.

Wszystkie rejestry prowadzone w KTM rejestruje się w „Rejestrze dzienników, książek ewidencyjnych i teczek”, której wzór określa aneks nr 1.

§ 8.

1. KTM prowadzi aktualne wykazy, a w szczególności:
   1) wszystkich kancelarii tajnych międzynarodowych funkcjonujących w sferze cywilnej i wojskowej RP, z którymi KTM współpracuje. Wykaz kancelarii międzynarodowych funkcjonujących w sferze cywilnej i wojskowej udostępnia KWB;
   2) Głównych Kancelarii Tajnych Międzynarodowych oraz wszystkich kancelarii tajnych międzynarodowych funkcjonujących w instytucjach, agencjach i innych państwach członkowskich organizacji międzynarodowej, z którymi KTM bezpośrednio wymienia materiały niejawne na podstawie upoważnienia uzyskanego w trybie określonym w § 12 ust. 5 i 6;
   3) pracowników ***(wpisać nazwę jednostki organizacyjnej)*** posiadających poświadczenia bezpieczeństwa upoważniające do dostępu do informacji niejawnych międzynarodowych;
   4) wybrakowanych materiałów niejawnych międzynarodowych;
   5) pracowników ***(wpisać nazwę jednostki organizacyjnej)*** przeszkolonych w zakresie ochrony informacji niejawnych międzynarodowych ***(wpisać nazwę organizacji międzynarodowej/ych, państwa/państw, reżimu).***
2. KT prowadzi rejestry, a w szczególności:
   1) dziennik ewidencji - związany ze współpracą w ramach ***(wpisać nazwę organizacji międzynarodowej/ych, państwa/państw, reżimu)***, którego wzór określa aneks nr 2;
   2) książkę doręczeń przesyłek miejscowych, której wzór określa aneks nr 3;
   3) książkę osób korzystających z czytelni KTM, której wzór określa aneks nr 4;
   4) książkę interwencji technicznych, której wzór określa aneks nr 5.

§ 9.

Rejestry wymienione w § 8 powinny być przeszyte, opieczętowane, a ich karty ponumerowane.

REJESTRACJA i OBIEG MATERIAŁÓW

§ 10.

1. Do KTM bezpośrednio przekazuje się wszystkie przesyłki niejawne międzynarodowe, określone w § 1 pkt 1 - 3.
2. KTM przyjmując przesyłkę zawierającą przesyłkę lub materiał niejawny międzynarodowy:
   1) otwiera kopertę zewnętrzną oraz wewnętrzną,
   2) rejestruje w dzienniku ewidencyjnym – po uprzednim ostemplowaniu ich pieczęcią wpływu KTM.
   3) załącza kartę zapoznania się z materiałem, której wzór stanowi aneks nr 6 – z zastrzeżeniem § 15 ust. 2.

§ 11.

1. Rejestracji w KTM podlegają wszystkie materiały niejawne międzynarodowe wysyłane z ***(wpisać nazwę jednostki organizacyjnej)*** do ***(wpisać nazwę organizacji międzynarodowej, państwa członkowskiego danej organizacji międzynarodowej lub państwa)***.
2. Dokumenty wymienione w ust. 1 są opatrywane kolejnym numerem dziennika ewidencji KTM i przekazywane - z zachowaniem odpowiednich przepisów i procedur - do wysłania.

§ 12.

1. Przekazywanie materiałów niejawnych międzynarodowych pomiędzy KTM a Głównymi Kancelariami Tajnymi, kancelariami tajnymi funkcjonującymi w instytucjach międzynarodowych i państwach członkowskich organizacji międzynarodowych odbywa się za pośrednictwem GKT lub bezpośrednio za pomocą akredytowanych systemów teleinformatycznych.
2. Przekazywanie materiałów niejawnych międzynarodowych pomiędzy KTM, a uprawnionymi podmiotami sfery cywilnej i wojskowej RP, odbywa się bezpośrednio pomiędzy kancelariami.
3. Przekazywanie materiałów niejawnych międzynarodowych o klauzuli ŚCIŚLE TAJNE lub równorzędnej pomiędzy KTM, a uprawnionymi podmiotami sfery cywilnej lub wojskowej RP odbywa się poprzez Główne Kancelarie Tajne Międzynarodowe sfery cywilnej i wojskowej.
4. W celu realizacji zadań związanych z członkostwem RP w organizacji międzynarodowej, ze względu na efektywność obiegu informacji albo wyjątkowe okoliczności, Szef ABW może upoważnić KTM do wymiany:
   1) materiałów opatrzonych klauzulą ŚCIŚLE TAJNE oraz równorzędną bezpośrednio z kancelariami tajnymi sfery cywilnej i wojskowej,
   2) materiałów niejawnych międzynarodowych bezpośrednio z Głównymi Kancelariami Tajnymi Międzynarodowymi, a także kancelariami tajnymi funkcjonującymi

w instytucjach organizacji międzynarodowych i państwach członkowskich tej organizacji.

6. Upoważnienie, o którym mowa w ust. 5, wydawane jest na podstawie wniosku kierownika jednostki organizacyjnej. Egzemplarz takiego upoważnienia kierownik KTM otrzymuje za pośrednictwem odpowiednio ABW lub SKW.

UDOSTĘPNIANIE MATERIAŁÓW

§ 13.

1. Materiały niejawne międzynarodowe przechowywane w KTM, mogą być udostępniane wyłącznie osobie, która spełnia wymagania określone w § 6 oraz:
   1) jest adresatem dokumentu lub została przez adresata imiennie upoważniona do zapoznania się z dokumentem,
   2) jest prawnym następcą adresata,
2. W sytuacji, gdy osoba spoza ***(wpisać nazwę jednostki organizacyjnej)***, musi zapoznać się z materiałem niejawnym międzynarodowym przechowywanym w KTM jednostki organizacyjnej z racji obowiązków służbowych wymagane jest imienne, pisemne upoważnienie wydane przez kierownika komórki organizacyjnej, nadzorującego pracę tej osoby. Ponadto upoważnienie to musi być kontrasygnowane przez jedną z osób wymienionych w § 13 ust. 1 pkt 1 i 2 lub osobę przez nich upoważnioną. Osoba, której będą udostępnione materiały niejawne międzynarodowe musi spełniać wymagania określone w § 6.
2. Wszelkie wątpliwości związane z określeniem adresata otrzymanego materiału kierownik KTM konsultuje z kierownikiem komórki organizacyjnej, której zakres obowiązków merytorycznie odpowiada treściom zawartym w tym materiale lub osobą sprawującą nadzór merytoryczny nad realizacją zadania lub programu, do którego odnosi się materiał niejawny międzynarodowy.

§ 14.

1. Materiał niejawny międzynarodowy nie może być udostępniany poza KTM, jeżeli odbiorca nie spełnia wymogów w zakresie ochrony informacji niejawnych ***(wpisać nazwę organizacji międzynarodowej, państwa lub reżimu)***.
2. Osobami właściwymi do określenia, czy adresat spełnia wymogi w zakresie ochrony informacji niejawnych międzynarodowych oraz udostępnienia materiału niejawnego międzynarodowego, jest kierownik KTM lub jego zastępca.

§ 15.

1. Do materiałów niejawnych międzynarodowych o klauzuli TAJNE oraz równorzędnej załączana jest karta zapoznania się materiałem, której wzór stanowi załącznik nr 6 do Regulaminu.
2. Do kontroli obiegu materiałów niejawnych międzynarodowych o klauzuli POUFNE oraz równorzędnej służy dziennik ewidencji, w którym kolejni odbiorcy materiału kwitują jego

odbiór. Dopuszcza się możliwość kontroli obiegu takich materiałów poprzez kartę zapoznania się z materiałem.

3. Adresat lub osoba upoważniona poświadcza odbiór materiału, składając podpis, stosownie do klauzuli materiału: w karcie lub dzienniku ewidencji.
4. W przypadku wypożyczenia materiału poza siedzibę KTM, zgodnie z § 14, karta zapoznania się z materiałem jest przechowywana w KTM.
5. Odbiór materiału od adresata lub osoby upoważnionej do zapoznania się z materiałem odnotowuje się w jego obecności.
6. Materiały niejawne międzynarodowe przekazywane są pomiędzy pracownikami ***(wpisać nazwę jednostki organizacyjnej)*** poprzez KTM. Dopuszcza się możliwość udostępniania wypożyczonego materiału o klauzuli POUFNE lub równorzędnej przez odbiorcę innym pracownikom ***(wpisać nazwę jednostki organizacyjnej)*** z zastrzeżeniem § 6 oraz po każdorazowym uzgodnieniu warunków takiego udostępnienia z pracownikiem KTM.

§ 16.

1. Przesyłki opatrzone zapisem „Do rąk własnych" nie są otwierane. Po ich zarejestrowaniu (spisując dane z koperty), doręcza się je bezpośrednio adresatowi za pokwitowaniem. Takie oznaczenie przesyłki odnotowuje się w rubryce „uwagi" dziennika ewidencji.
2. Przesyłki pilne, telegramy bądź materiały oznaczone sygnaturą „Błyskawiczna" („Flash") doręcza się adresatom niezwłocznie. Przy pokwitowaniu tych przesyłek należy odnotować, oprócz daty, godzinę doręczenia.

TŁUMACZENIA, KOPIE, WYCIĄGI, ODPISY

§ 17.

1. Decyzje w sprawie sporządzania kopii, tłumaczeń, odpisów lub wyciągów z materiału niejawnego międzynarodowego o klauzuli TAJNE, POUFNE i równorzędnych, przechowywanych w KTM, podejmują osoby wymienione w § 13 ust. 1 pkt 1 lub 2, lub osoby przez nich upoważnione, dekretując to na materiale poprzez określenie liczby egzemplarzy do wykonania oraz ich rozdzielnika.
2. Tłumaczenia, wyciągi, odpisy lub kopie z materiałów niejawnych, o których mowa w ust. 1, wykonywane są w pomieszczeniach KTM przez osobę, która otrzymała pisemne polecenie wykonania tej czynności lub pracownika KTM.
3. Tłumaczenia, odpisy lub wyciągi z materiałów niejawnych międzynarodowych o klauzulach TAJNE i POUFNE mogą być wykonywane w strefach ochronnych zlokalizowanych w siedzibie ***(wpisać nazwę jednostki organizacyjnej).***
4. Wykonane poza siedzibą KTM tłumaczenia, kopie, odpisy lub wyciągi z pobranych z tej kancelarii materiałów niejawnych międzynarodowych mogą być zapisane wyłącznie na informatycznych nośnikach danych zarejestrowanych w KTM lub akredytowanych systemach łączności.

§ 18.

1. Kopie, tłumaczenia, odpisy i wyciągi z materiałów niejawnych międzynarodowych wykonane w *(wpisać nazwę jednostki organizacyjnej)* rejestruje się w KTM i oznacza się zgodnie z § 12. ust. 1. Rozporządzenia Prezesa Rady Ministrów z dnia 13 sierpnia 2010 r. w sprawie sposobu oznaczania materiałów, umieszczania na nich klauzul tajności, a także zmiany nadanej klauzuli tajności (Dz. U. z 2010 r. Nr 159, poz. 1069).
2. Kopie, tłumaczenia, odpisy i wyciągi z materiałów niejawnych należy poświadczyć „za zgodność" odpowiednio przez tłumacza lub osobę wykonującą tłumaczenie, kopię, odpis lub wyciąg.
3. Kopie, tłumaczenia, odpisy i wyciągi materiałów niejawnych powinny zawierać wszystkie klauzule oraz oznaczenia materiału oryginalnego.
4. Fakt sporządzenia kopii, tłumaczenia, odpisu lub wyciągu odnotowuje się w dzienniku ewidencji przy wpisie dotyczącym oryginału.
5. Na pierwszej stronie oryginału materiału, z którego wykonano kopię, tłumaczenie, odpis lub wyciąg, odciska się pieczęć, o której mowa w § 12. ust. 3. Rozporządzenia wymienionego w ust. 1.
6. Informatyczne nośniki danych lub akredytowane systemy łączności niejawnej znajdujące się w KTM, na których zapisane są informacje niejawne międzynarodowe, powinny być zarejestrowane tej kancelarii z klauzulą równorzędną do najwyższej klauzuli informacji zapisanej na tych nośnikach.

BRAKOWANIE

§ 19.

1. W celu uniknięcia gromadzenia niepotrzebnych materiałów niejawnych międzynarodowych w pierwszym kwartale każdego roku dokonuje się ich przeglądów, celem określenia, czy mogą one być wybrakowane.
2. Kierownik KTM przygotowuje wykaz przeznaczonych do brakowania materiałów niejawnych międzynarodowych, przechowywanych w tej kancelarii. Na brakowanie tych materiałów wyrażają zgodę – w formie pisemnej - ich adresaci.
3. Kierownik *(wpisać nazwę jednostki organizacyjnej)* powołuje komisję, która przeprowadza brakowanie materiałów określonych w ust. 2 w KTM. W skład komisji powinna zostać powołana osoba spoza tej kancelarii – odpowiednio sprawdzona i upoważniona.
4. Komisji przewodniczy kierownik KTM.
5. Komisja brakuje materiały niejawne międzynarodowe w sposób uniemożliwiający ich odtworzenie.
6. Z brakowania materiałów niejawnych międzynarodowych sporządza się protokół. Protokół powinien zawierać: klauzulę materiału, oryginalną sygnaturę i oznaczenie dokumentu, datę sporządzenia materiału, sygnaturę KTM, numer egzemplarza materiału.
7. Protokół z brakowania w KTM sporządza się w dwóch egzemplarzach. Jeden egzemplarz przekazuje się odpowiednio do ABW lub SKW, drugi przechowuje w KTM.
8. Protokół z brakowania podpisują wszyscy członkowie komisji.

9. KT przechowuje karty zapoznania się z materiałem oraz dokumentację brakowania materiałów niejawnych międzynarodowych przeprowadzanych przez nią samą przynajmniej 10 lat.

TRANSPORT

§ 20.

1. Przewóz i dostarczanie odpowiednio zabezpieczonych i zapakowanych przesyłek do adresatów odbywa się za pośrednictwem, odpowiednio przeszkolonych w tym zakresie, przewoźników określonych w § 2 ust. 2 pkt 1-3 Rozporządzenia.
2. Dokumenty niejawne międzynarodowe mogą przewozić przedstawiciele nadawcy lub odbiorcy, zgodnie z uregulowaniami zawartymi w Rozporządzeniu.
3. Przedstawiciel nadawcy lub odbiorcy przewożący informacje niejawne międzynarodowe powinien być poinformowany o odpowiedzialności w zakresie bezpieczeństwa, zaopatrzony w formalne upoważnienie na piśmie, uprawniające go do przewozu tego rodzaju przesyłek.
4. Przekazywanie przewoźnikom przesyłek zawierających materiały niejawne międzynarodowe odbywa się wyłącznie w pomieszczeniach KTM.
5. Osoba kwitująca odbiór przesyłki, zobowiązana jest do sprawdzenia, czy jej zawartość jest zgodna z załączonym do niej wykazem, czy jest ona prawidłowo zabezpieczona oraz czy nie jest uszkodzona.
6. Za transportowaną przesyłkę odpowiedzialna jest osoba kwitująca jej odbiór.
7. Termin każdego transportu lub przekazania materiałów niejawnych międzynarodowych należy uprzednio ustalić pomiędzy nadawcą, odbiorcą i przewoźnikiem.
8. W obrębie obiektu ***(wpisać nazwę jednostki organizacyjnej)*** dokumenty niejawne przenosi się w sposób uniemożliwiający osobom postronnym zapoznanie się z ich treścią.

§ 21.

Przesyłki przewożone przez osoby wymienione w § 20 ust. 1 i 2 powinny być zapakowane zgodnie z § 5 Rozporządzenia. Za opakowanie zewnętrzne można uważać również zamykaną na klucz teczkę lub pojemnik.

§ 22.

W przypadku uszkodzenia przesyłki przewożonej przez przewoźników wymienionych w § 20, ust. 1, 2 postępowanie wyjaśniające przebiega zgodnie z § 16 Rozporządzenia.

§ 23.

Przepisy § 20 i § 21 stosuje się odpowiednio w przypadku dostarczania przesyłek zawierających materiały niejawne międzynarodowe do KTM z GKT lub kancelarii tajnych.

§ 24.

W razie utraty przesyłki zawierającej informacje niejawne międzynarodowe podczas transportu, przewoźnik jest zobowiązany do niezwłocznego poinformowania o tym:

1) Kierownika kancelarii tajnej, z której przesyłka została pobrana,
2) odpowiednio delegatury ABW lub SKW, jednostki wojskowej lub jednostki Policji najbliższych miejsca utraty przesyłki – w przypadku przesyłek utraconych podczas przewożenia do innych miejscowości,
3) adresata.

§ 25.

Międzynarodowy przewóz materiałów niejawnych międzynarodowych, w tym przewóz osobisty, przebiega zgodnie z przepisami określonymi w odrębnych regulacjach.

NARUSZENIE PRZEPISÓW BEZPIECZEŃSTWA DOTYCZĄCYCH INFORMACJI NIEJAWNYCH MIĘDZYNARODOWYCH

§ 26.

Kierownik KTM ma obowiązek niezwłocznego, pisemnego poinformowania pełnomocnika ochrony w ***(wpisać nazwę jednostki organizacyjnej)*** o każdym przypadku naruszenia przepisów bezpieczeństwa dotyczących informacji niejawnych międzynarodowych.

§ 27.

1. Każdy zgłoszony przypadek naruszenia przepisów bezpieczeństwa podlega postępowaniu wyjaśniającemu, które zmierza do stwierdzenia, czy faktycznie doszło do naruszenia przepisów dotyczących bezpieczeństwa informacji niejawnych międzynarodowych, w tym okoliczności wystąpienia incydentu teleinformatycznego, jakich, w jaki sposób, przez kogo, czy skutkiem takiego naruszenia jest lub może być narażenie na szwank takich informacji.
2. Podstawowe postępowanie wyjaśniające prowadzone jest przez pełnomocnika ochrony w zakresie okoliczności dotyczących ***(wpisać nazwę jednostki organizacyjnej).***
3. Nadzorcze postępowanie wyjaśniające prowadzą osoby wyznaczone przez Szefa ABW lub upoważnionego kierownika jednostki organizacyjnej ABW, a w jednostkach o których mowa w art. 10 ust. 2 ustawy za pośrednictwem Szefa SKW.

§ 28.

Postępowanie z informacjami międzynarodowymi w sferze cywilnej i wojskowej, w sytuacjach nadzwyczajnych regulują odrębne przepisy.

INSPEKCJE STANU OCHRONY INFORMACJI NIEJAWNYCH MIĘDZYNARODOWYCH

§ 29.

1. W styczniu każdego roku kierownik KTM sprawdza i porównuje stan faktyczny posiadanych materiałów niejawnych międzynarodowych z zapisami w ewidencjach kancelarii. Protokoły pokontrolne KTM powinny być przechowywane w tej kancelarii, zaś ich drugie egzemplarze niezwłocznie przekazane odpowiednio do ABW lub SKW.
2. Uprawnieni do inspekcji w zakresie prawidłowości ochrony informacji niejawnych międzynarodowych w KTM są: przedstawiciele struktur bezpieczeństwa państw/organizacji międzynarodowych, odpowiednio Agencji Bezpieczeństwa Wewnętrznego lub Służby Kontrwywiadu Wojskowego.

ZABEZPIECZENIE KLUCZY ORAZ KODÓW DO ZAMKÓW SZYFROWYCH

§ 30.

1. Wszystkie kody: do systemu alarmowego, sejfów, szaf metalowych, powinny być zmieniane:
   1) co 6 miesięcy,
   2) gdy istnieje podejrzenie ujawnienia kodu,
   3) przy każdej zmianie personelu.
2. Każda zmiana kodu powinna zostać odnotowana. Wykaz, w którym odnotowuje się zmiany kodów powinien zawierać:
   1) imię i nazwisko osoby zmieniającej kod,
   2) datę zmiany,
   3) termin następnej zmiany,
   4) podpis osoby dokonującej wpisu.
3. Wykaz, o którym mowa w ust. 2, powinien znajdować się u pełnomocnika do spraw ochrony informacji niejawnych oraz w KTM.
4. Kierownik, lub upoważniony pracownik KTM, po zakończeniu pracy, sprawdza zabezpieczenie pomieszczeń kancelarii, a następnie deponuje komplet kluczy do niej do służby dyżurnej pionu ochrony w odpowiednio zabezpieczonym i opieczętowanym pojemniku.
5. Drugie egzemplarze kluczy do pomieszczeń KTM i znajdujących się w nich sejfów i szaf metalowych oraz zestawienia kombinacji szyfrowych do ich otwarcia, znajdują się u pełnomocnika ochrony ***(wpisać nazwę jednostki organizacyjnej)*** i przechowywane są w pojemniku

oznaczonym analogicznie do najwyższej klauzuli informacji chronionej w tej kancelarii.

6. Każde uszkodzenie pieczęci na sejfach, szafach metalowych oraz inne nieprawidłowości w pomieszczeniach KTM stwierdzone przed rozpoczęciem pracy, należy natychmiast zgłosić pełnomocnikowi ochrony, który wszczyna postępowanie wyjaśniające.
7. Utratę kluczy do pomieszczeń, szaf pancernych znajdujących się w KTM zgłasza się jak w ust. 6.

POSTANOWIENIA KOŃCOWE

§ 31.

W zakresie nieuregulowanym regulaminem stosuje się przepisy[4]:

- NATO zawarte w dokumentach C-M(2002)49, AC/35-D/2000, AC/35-D/2001, AC/35-D/2002, AC/35-D/2003, AC/35-D/2004 i AC/35-D/2005,
- UE zawarte w dokumentach Decyzji Rady UE nr 2001/264/EC z 19.03.2001, Decyzji Komisji Europejskiej nr 2001/844/EC z 29.11.2001 z póż. zm.
- przepisy ustawy o ochronie informacji niejawnych z 05 sierpnia 2010 r.,
- Rozporządzenia Rady Ministrów z dnia 18 października 2005 r. w sprawie organizacji i funkcjonowania kancelarii tajnych (Dz. U. z 2005 r. Nr 208, poz. 1741),
- Rozporządzenia Prezesa Rady Ministrów z dnia 13 sierpnia 2010 r. w sprawie sposobu oznaczania materiałów, umieszczania na nich klauzul tajności, a także zmiany nadanej klauzuli tajności (Dz. U. z 2010 r. Nr 159, poz. 1069),
- Rozporządzenia Prezesa Rady Ministrów z dnia 29 września 2005 r. w sprawie trybu i sposobu przyjmowania, przewożenia, wydawania i ochrony materiałów (Dz. U. z 2005 r. Nr 200, poz.1650),
- Inne (wpisać) …….

[4] Niewłaściwe skreślić

ANEKS Nr 1

WZÓR

REJESTR DZIENNIKÓW, KSIĄŻEK EWIDENCYJNYCH I TECZEK

Oznaczenie klauzuli tajności dziennika, rejestru, książki ewidencyjnej itp.	Numer kolejny dziennika, rejestru, książki ewidencyjnej itp.	Adnotacje dot. przedłużenia okresu ochrony, zniesienia bądź zmiany klauzuli tajności	Data rejestracji dziennika, rejestru, książki ewidencyjnej itp.	Nazwa teczki, dziennika, rejestru, książki ewidencyjnej itp.	Data		Liczba stron dziennika, rejestru, książki ewidencyjnej itp.	Komórka organizacyjna, odpowiedzialna za prowadzenie dziennika, rejestru, książki ewidencyjnej itp.	Pokwitowanie odbioru dziennika, rejestru, książki ewidencyjnej itp.			Informacje uzupełniające/ Uwagi
					rozpoczęcia dziennika, rejestru, książki ewidencyjnej itp.	zakończenia dziennika, rejestru, książki ewidencyjnej itp.			imię i nazwisko	data oraz podpis osoby prowadzącej dziennik, rejestr, książkę ewidencyjną itp.	potwierdzenie zwrotu, data i podpis	
1	2	3	4	5	6	7	8	9	10	11	12	13

...../.....

...../.....

(klauzula tajności)

ANEKS Nr 2

WZÓR

DZIENNIK EWIDENCJI

Strona lewa

Oznaczenie klauzuli tajności	Numer kolejny zapisu	Adnotacje dot. przedłużenia okresu ochrony, zniesienia bądź zmiany klauzuli tajności	Data rejestracji dokumentu	Nazwa nadawcy/adresata	Numer i data dokumentu otrzymanego	Nazwa dokumentu lub czego dotyczy	Liczba egzemplarzy/ stron jednego egzemplarza	Liczba (wychodzących/przychodzących)		
								stron dokumentu lub innych jednostek miary	załączników	stron wszystkich załączników lub innych jednostek miary
1	2	3	4	5	6	7	8	9	10	11

...../.....

Strona prawa

Nr dokumentu, z którego sporządzono kopię, wyciąg, odpis, tłumaczenie, lub numer nośnika	Nazwisko osoby sporządzającej/wykonującej dokument	Imię i nazwisko osoby otrzymującej dokument, data i podpis	Potwierdzenie zwrotu dokumentu, data i podpis	Adnotacje		Informacje uzupełniające/Uwagi
				o wysłaniu dokumentu lub załącznika (poz. ks. dor. przesyłek miejscowych/poz. wykazu przesyłek nadanych/zał. do pisma nr...)	o wybrakowaniu lub archiwizacji	
12	13	14	15	16	17	18

...../.....

ANEKS Nr 3

WZÓR

KSIĄŻKA DORĘCZEŃ PRZESYŁEK MIEJSCOWYCH

Numer kolejny zapisu	Data	Adresat	Numer pisma (rodzaj przesyłki)	Potwierdzenia odbioru, podpis, pieczęć i data
1	2	3	4	5

Strona ...../.....

ANEKS nr 4

KSIĄŻKA OSÓB KORZYSTAJĄCYCH Z CZYTELNI KTM w .. ..*

L.p.	Imię i nazwisko	Nazwa komórki organizacyjnej	Data zapoznania się z dokumentem	Nr dokumentu	Podpis	Uwagi

ANEKS nr 5

KSIĄŻKA INTERWENCJI TECHNICZNYCH

Lp.	Data i godz. wizyty od - do	Przyczyna wizyty/przedsięwzięte działania	Imię i nazwisko konserwatora, nazwa firmy	Imię i nazwisko pracownika kancelarii	Uwagi

ANEKS Nr 6

WZÓR

KARTA ZAPOZNANIA SIĘ Z MATERIAŁEM NR ....

Lp.	UDOSTĘPNIENIE MATERIAŁU			ZWROT DOKUMENTU			Uwagi
	imię i nazwisko osoby, której materiał udostępniono	data	podpis	imię i nazwisko osoby, której materiał zwrócono	data	podpis	

Strona ...../.....

Załącznik nr 7

ZATWIERDZAM Miejscowość, dnia..... r.

…….
(imię, nazwisko, pieczęć i podpis
kierownika jednostki organizacyjnej)

Regulamin Czytelni
kancelarii tajnej międzynarodowej w .....
(nazwa jednostki organizacyjnej)

§ 1.

Regulamin czytelni Kancelarii Tajnej Międzynarodowej w ***(wpisać nazwę jednostki organizacyjnej),*** zwanej dalej „czytelnią", określa zasady udostępniania przechowywanych w tej kancelarii dokumentów niejawnych międzynarodowych.

§ 2.

1. Dokumenty niejawne międzynarodowe, przechowywane w Kancelarii Tajnej Międzynarodowej w ***(wpisać nazwę jednostki organizacyjnej)*** (KTM), mogą być udostępnione wyłącznie osobie, która posiada odpowiednie poświadczenie bezpieczeństwa, wydane przez krajową władzę bezpieczeństwa oraz:
   1) jest adresatem dokumentu lub została przez adresata imiennie upoważniona do zapoznania się z dokumentem,
   2) jest prawnym następcą adresata,
   3) w przypadku osoby spoza jednostki organizacyjnej adresata - musi zapoznać się z danym dokumentem z racji obowiązków służbowych. Konieczność taka musi być potwierdzona imiennym upoważnieniem wydanym przez kierownika komórki organizacyjnej, nadzorującego pracę osoby zainteresowanej, kontrasygnowanym przez jedną z osób wymienionych w pkt 1 i 2 lub osobę przez nich upoważnioną.
2. Wszelkie wątpliwości związane z określeniem adresata otrzymanego dokumentu kierownik KTM konsultuje z kierownikiem komórki organizacyjnej, której zakres obowiązków merytorycznie odpowiada treściom zawartym w tym dokumencie lub osobą sprawującą nadzór merytoryczny nad realizacją zadania lub programu, do którego odnosi się dany dokument niejawny.

§ 3.

1. W pomieszczeniach czytelni, mogą przebywać wyłącznie pracownicy KTM, a także inne osoby uprawnione.

2. Zabrania się wnoszenia do czytelni bagażu.

§ 4.

1. Korzystający z czytelni zobowiązany jest do potwierdzenia zapoznania się z dokumentem – stosownie do klauzuli - w karcie zapoznania się z dokumentem lub dzienniku korespondencji oraz w książce osób korzystających z czytelni.
2. Korzystanie z dokumentów niejawnych międzynarodowych w czytelni odbywa się w obecności pracownika KTM.
3. Korzystającym z czytelni zabrania się wynoszenia dokumentów niejawnych międzynarodowych poza jej pomieszczenie.

§ 5.

1. Zabrania się przepisywania treści dokumentów niejawnych międzynarodowych.
2. Sporządzanie notatek z dokumentów międzynarodowych możliwe jest wyłącznie na zasadach określonych przez pracownika KMT.
3. Wszelkie notatki pozostawia się w KTM. Notatki oznacza się odpowiednią klauzulą tajności.

§ 6.

Każda osoba korzystająca z czytelni zobowiązana jest do zapoznania się z regulaminem czytelni oraz pisemnego potwierdzenia tego faktu.

§ 7.

Naruszenie regulaminu czytelni, stwarzające zagrożenie dla bezpieczeństwa informacji niejawnych międzynarodowych, może stanowić podstawę do cofnięcia poświadczenia bezpieczeństwa.

Załącznik nr 8

…….. Miejscowość, data
Nazwa jednostki organizacyjnej

ZATWIERDZAM

Egz. nr ____

…….....
Szef
Agencji Bezpieczeństwa Wewnętrznego

PLAN ORGANIZACJI KANCELRII TAJNEJ MIĘDZYNARODOWEJ

W ……..……..[1]

OBSŁUGUJĄCEJ INFORMACJE NIEJAWNE…….[2]

OZNACZONE ……...[3]

CZĘŚĆ I: INFORMACJE DOTYCZĄCE JEDNOSTKI ORGANIZACYJNEJ
1. Nazwa i adres siedziby jednostki organizacyjnej, w której zamierza się utworzyć kancelarię tajną międzynarodową. **……**
2. Adres lokalizacji kancelarii tajnej międzynarodowej.[4] **……**

[1] Wpisać nazwę jednostki organizacyjnej, w której zamierza się utworzyć kancelarię tajną międzynarodową.
[2] Wpisać nazwę organizacji międzynarodowej/państwo/reżim (np. ATOMAL, BOHEMIA)
[3] Wpisać odpowiedni poziom klauzuli do których ma być upoważniona kancelaria
[4] Wypełnić w przypadku, gdy adres jest inny niż w pkt. 1 części I

3. Posiadane przez jednostkę świadectwo bezpieczeństwa przemysłowego (ŚBP) klauzula tajności[5]:

- **Stopień ŚBP i klauzula ……**
- **Data ważności/złożenia wniosku ……**
- **ŚBP wydane/postępowanie prowadzone przez: ……**

4. Status prawny budynku, w którym zamierza się utworzyć kancelarię tajną międzynarodową

4.1 Czy budynek, w którym zamierza się utworzyć kancelarię międzynarodową jest własnością jednostki organizacyjnej?

(w przypadku odpowiedzi „NIE" wypełnić ppkt. 4.4, w przypadku odpowiedzi „TAK" wypełnić ppkt. 4.2 – 4.3)

TAK ☐ **NIE** ☐

4.2 Czy jednostka organizacyjna jest jedynym właścicielem budynku?

(w przypadku zaznaczenia odpowiedzi „NIE" wpisać nazwę i siedzibę współwłaściciela/li)

TAK ☐ **NIE** ☐

……

4.3 Czy budynek lub jego część jest wynajmowana lub w inny sposób udostępniana innej jednostce organizacyjnej?

(w przypadku zaznaczenia odpowiedzi „TAK" wpisać nazwę i siedzibę jednostki/tek której/ym, budynek jest wynajmowany lub w inny sposób udostępniany, podać nr i datę umowy wynajmu/dokumentu, oraz okres, którego umowa dotyczy).

TAK ☐ **NIE** ☐

……

4.4 Nazwa, siedziba właściciela(-li) budynku, numer i data umowy lub innego dokumentu na podstawie, którego jednostka organizacyjna użytkuje budynek:

...……

5. Opis najbliższego sąsiedztwa budynku, w którym zamierza się utworzyć kancelarię tajną międzynarodową.[6]

……

[5] niepotrzebne skreślić. W przypadku posiadania ŚBP należy załączyć jego kopię.

[6] Należy wymienić i opisać przede wszystkim obiekty, które wg. opinii zatwierdzającego plan organizacji kancelarii tajnej międzynarodowej mogą wpływać na poziom bezpieczeństwa informacji niejawnych np. obiekty użyteczności publicznej, obiekty sportowe i hale widowiskowe.

6. Plan ochrony informacji niejawnych jednostki organizacyjnej:

Sporządzający ……

Zatwierdzający ……

Data sporządzenia ……

Numer ewidencyjny Planu Ochrony ……...

6.1 Czy plan ochrony informacji niejawnych odnosi się do ochrony informacji niejawnych międzynarodowych?

TAK ☐ **NIE** ☐

6.2 Czy w planie ochrony informacji niejawnych zapisane są procedury dotyczące ochrony kancelarii tajnej międzynarodowej?

TAK ☐ **NIE** ☐

6.3 Czy w planie ochrony informacji niejawnych zapisane są procedury postępowania z kluczami do kancelarii tajnej międzynarodowej?

TAK ☐ **NIE** ☐

6.4 Czy w planie ochrony informacji niejawnych zapisane są procedury zabezpieczenia wejścia/wyjścia z/do obiektu, w którym zamierza się utworzyć kancelarię tajną międzynarodową?

TAK ☐ **NIE** ☐

6.5 Czy w planie ochrony informacji niejawnych międzynarodowych jest opisany sposób w jaki służby ochrony postępują w sytuacji nadzwyczajnej?

TAK ☐ **NIE** ☐

6.6 Czy w planie ochrony informacji niejawnych zapisane są procedury dotyczące ewakuacji informacji niejawnych przechowywanych w kancelarii tajnej międzynarodowej?

TAK ☐ **NIE** ☐

CZĘŚĆ II: INFORMACJE DOTYCZĄCE III STREFY OCHRONNEJ

1. Czy w jednostce zorganizowano III strefę ochronną?
(zaznaczyć odpowiednie pole wyboru – w przypadku zaznaczenia odpowiedzi „TAK" wypełnić pkt 2-9)

TAK ☐ **NIE** ☐

2. Czy strefa ma wyraźnie oznaczoną granicę?

TAK ☐ **NIE** ☐

3. Dokładny opis granicy strefy.[7]

……

4. Czy granica strefy jest oświetlona?

TAK ☐ **NIE** ☐

5. Czy wprowadzono kontrolę osób wchodzących i wychodzących do/ze strefy?
(zaznaczyć odpowiednie pole wyboru – w przypadku zaznaczenia odpowiedzi „TAK" wypełnić pkt 6)

TAK ☐ **NIE** ☐

6. W jaki sposób realizowana jest kontrola osób wchodzących i wychodzących?[8]

……

7.Czy wprowadzono w strefie kontrolę ruchu pojazdów?

TAK ☐ **NIE** ☐

8. Organizacja ochrony strefy:
8.1 Czy ochrona strefy realizowana jest przez pracowników jednostki organizacyjnej?

TAK ☐ **NIE** ☐

8.2 Czy ochrona strefy realizowana jest przez inną jednostkę organizacyjną?
(zaznaczyć odpowiednie pole wyboru – w przypadku zaznaczenia odpowiedzi „TAK" wypełnić ppkt 8.3)

☐ ☐

[7] Podać z czego zbudowana jest granica np. ogrodzenie, mur, ściana zewnętrzna budynku oraz dokładnie opisać.
[8] Podać oraz opisać sposób realizacji kontroli np.: przepustki, identyfikatory, strażnicy.

TAK **NIE**

8.3 Nazwa firmy, numer i data koncesji posiadanej przez jednostkę organizacyjną
……

8.4.Jaki jest sposób reagowania grupy interwencyjnej?
……

8.5 Nazwa jednostki organizacyjnej, numer i data koncesji udzielonej firmie realizującej zadanie grupy interwencyjnej
……

9. Inne zabezpieczenia strefy[9].
……

CZĘŚĆ III: INFORMACJE DOTYCZĄCE II STREFY OCHRONNEJ

1. Czy ustanowiono strefę ochronną II?
(zaznaczyć odpowiednie pole wyboru – w przypadku zaznaczenia odpowiedzi „TAK" wypełnić pkt 2-10)

TAK ☐ **NIE** ☐

2. Czy strefa ochronna znajduje się przed kancelarią tajną międzynarodową?

TAK ☐ **NIE** ☐

3. Czy strefa ma wyraźnie oznaczoną granicę?

TAK ☐ **NIE** ☐

3. 1Dokładny opis granicy strefy.

……

4. Ile jest wejść do strefy?

☐

5. Czy w strefie jest obustronny system kontroli dostępu rejestrujący wejścia, wyjścia i przebywania, umożliwiający identyfikację personalną osób?
(zaznaczyć odpowiednie pole wyboru – w przypadku zaznaczenia odpowiedzi „TAK" wypełnić pkt 6)

[9] Wskazać i opisać zabezpieczenia strefy np. takie jak system telewizji dozorowej, system włamania i napadu, organy lub formacje zapewniające ochronę strefy.

TAK ☐ **NIE** ☐

6. W jaki sposób realizowana jest kontrola, o której mowa w punkcie 5?

……

……

7. Sposób organizacji ochrony strefy:

7.1 czy ochrona strefy realizowana jest pracowników jednostki organizacyjnej?

TAK ☐ **NIE** ☐

7.2 Czy ochrona strefy realizowana jest przez inną jednostkę organizacyjną?
(zaznaczyć odpowiednie pole wyboru – w przypadku zaznaczenia odpowiedzi „TAK" wypełnić ppkt. 7.3)

TAK ☐ **NIE** ☐

7.3 Nazwa firmy, numer i data koncesji posiadanej przez jednostkę organizacyjną.

……

7.4 Jaki jest sposób reagowania grupy interwencyjnej?

……

7.5 Nazwa jednostki organizacyjnej, numer i data koncesji udzielonej firmie realizującej zadanie grupy interwencyjnej

……

8. Czy w strefie zamontowano system sygnalizacji włamania i napadu?
(zaznaczyć odpowiednie pole wyboru – w przypadku zaznaczenia odpowiedzi „TAK" wypełnić ppkt. 8.1)

TAK ☐ **NIE** ☐

8.1 Podać klasę systemu włamania i napadu?

……

9. Czy w strefie zmontowano system sygnalizacji pożarowej?

TAK ☐ **NIE** ☐

10. Czy w strefie zastosowano zabezpieczenie przed podglądem i włamaniem?

TAK ☐ **NIE** ☐

11. Czy drzwi wejściowe do strefy posiadają zwiększoną odporność na włamanie?

TAK ☐ **NIE** ☐

CZĘŚĆ IV: LOKALIZACJA I ORGANIZACJA KANCELARII TAJNEJ MIĘDZYNARODOWEJ[10]

1. Czy kancelaria znajduje się w strefie ochronnej?

TAK ☐ **NIE** ☐

2. Pomieszczenia sąsiadujące z kancelarią tajną[11]:

pomieszczenia nad kancelarią …….

pomieszczenia pod kancelarią …….

pomieszczenia zlokalizowane za ścianami kancelarii

…….

3. Czy w kancelarii znajdują się niezabezpieczone przed ingerencją z zewnątrz kanały wentylacyjne, klimatyzacyjne lub inne instalacje techniczne, które mogą osłabić system bezpieczeństwa?

TAK ☐ **NIE** ☐

4. Liczba pomieszczeń planowanych na kancelarię oraz ich przeznaczenie

1. **……**
2. **……...**
3. **……**

5. Czy w pomieszczeniach kancelarii wydzielono czytelnię?
(zaznaczyć odpowiednie pole wyboru – w przypadku zaznaczenia odpowiedzi „TAK" – wypełnić ppkt 5.1 i 5.2)

TAK ☐ **NIE** ☐

5.1 Czy czytelnia jest zorganizowana w sposób umożliwiający stały nadzór ze strony pracowników kancelarii nad udostępnionym w czytelni dokumentem?

TAK ☐ **NIE** ☐

[10] Do planu organizacji kancelarii tajnej międzynarodowej należy załączyć schemat graficzny lokalizacji kancelarii tajnej

[11] Należy podać w szczególności rodzaj pomieszczenia oraz nazwę użytkownika tych pomieszczeń.

5.2 Czy osoba zapoznająca się z dokumentem ma bezpośredni dostęp do szaf, w których przechowywane są materiały niejawne?

TAK ☐ **NIE** ☐

6. Ściany i stropy kancelarii.

6.1 Czy ściany i stropy pomieszczeń kancelarii spełniają wymogi przewidziane w przepisach dotyczących organizacji kancelarii tajnych?
(zaznaczyć odpowiednie pole wyboru – w przypadku zaznaczenia odpowiedzi „TAK" – wypełnić ppkt 6.2)

TAK ☐ **NIE** ☐

6.2 Wskazanie i opis dokumentu potwierdzającego spełnienie wymogów, o których mowa w punkcie 6.1
……

7. Drzwi do kancelarii

7.1 Czy w drzwiach zamontowany jest zamek drzwiowy wielopunktowy?

TAK ☐ **NIE** ☐

7.2 Czy w drzwiach zamontowany jest zamek drzwiowy dodatkowy?

TAK ☐ **NIE** ☐

7.3 Czy drzwi posiadają zamek samozatrzaskowy?

TAK ☐ **NIE** ☐

7.3 Czy na drzwiach jest umieszczona tabliczka znamionowa z numerem certyfikatu?

TAK ☐ **NIE** ☐

7.5 Numer certyfikatu
……

7.6 Nazwa producenta drzwi
……

7.7 Klasa wyrobu, typ i numer fabryczny drzwi
……
7.8 Inne wyposażenie drzwi:[12]
……..

[12] Wpisać np. wizjer, wideofon.

8. Czy w kancelarii są okna?
(zaznaczyć odpowiednie pole wyboru – w przypadku zaznaczenia odpowiedzi „TAK" – wypełnić ppkt 8.1 – 8.2)

TAK ☐ **NIE** ☐

8.1 czy w oknach zamontowana jest stalowa krata (zewnętrzna lub wewnętrzna)?
(zaznaczyć odpowiednie pole wyboru – w przypadku zaznaczenia odpowiedzi „TAK" – wypełnić ppkt 8.2 – 8.3)

TAK ☐ **NIE** ☐

8.2 czy zamontowane kraty są otwierane?
(zaznaczyć odpowiednie pole wyboru – w przypadku zaznaczenia odpowiedzi „TAK" – wypełnić ppkt 8.6)

TAK ☐ **NIE** ☐

8.3 czy zamknięcie zastosowane w kratach posiada certyfikat?
(zaznaczyć odpowiednie pole wyboru – w przypadku zaznaczenia odpowiedzi „TAK" – uzupełnić nr certyfikatu)

TAK ☐ **NIE** ☐

……

8.4 czy w oknie (oknach) zamontowana jest siatka z drutu stalowego lub inne zabezpieczenie posiadające odporność na włamanie nie mniejszą niż siatka?

(zaznaczyć odpowiednie pole wyboru – w przypadku zaznaczenia odpowiedzi „TAK" – wpisać poniżej rodzaj, nazwę zabezpieczenia)

TAK ☐ **NIE** ☐

……

8.5 czy okno (okna) zabezpieczono przed obserwacją z zewnątrz?
(zaznaczyć odpowiednie pole wyboru – w przypadku zaznaczenia odpowiedzi „TAK" – wpisać poniżej rodzaj zastosowanego zabezpieczenia innego)

TAK ☐ **NIE** ☐

……

9. System sygnalizacji włamania i napadu

9.1 Czy pomieszczenia kancelarii są chronione za pomocą systemu sygnalizacji włamania i napadu ?
(zaznaczyć odpowiednie pole wyboru – w przypadku zaznaczenia odpowiedzi „TAK" – wypełnić ppkt 9.2 – 9.10)

TAK ☐ **NIE** ☐

9.2 Czy system sygnalizacji włamania i napadu obejmuje wyłącznie pomieszczenia kancelarii tajnej ?

(zaznaczyć odpowiednie pole wyboru – w przypadku zaznaczenia odpowiedzi „NIE" – wypełnić ppkt 9.3)

TAK ☐ **NIE** ☐

9.3 Czy konfiguracja systemu sygnalizacji włamania i napadu zapewnia uzbrojenie/rozbrojenie części systemu obejmującego wyłącznie pomieszczenia kancelarii?

TAK ☐ **NIE** ☐

9.4 Czy system sygnalizacji włamania i napadu jednoznacznie identyfikuje użytkowników wchodzących i wychodzących do pomieszczeń kancelarii tajnej międzynarodowej?

TAK ☐ **NIE** ☐

9.5 Czy system odpowiada co najmniej klasie SA3 wg. Polskiej Normy PN 93 E-08390/14 oraz czy jednostka organizacyjna posiada deklarację zgodności na system sygnalizacji włamania i napadu?

TAK ☐ **NIE** ☐

9.6 Dane osoby lub podmiotu konserwującego system sygnalizacji włamania i napadu

(imię, nazwisko, numer i data uprawnień, organ wydający uprawnienia, nazwa podmiotu, numer i data licencji, organ wydający licencję)

……
……

9.7 Czy wyznaczono osobę odpowiedzialną za funkcjonowanie (administratora) systemu sygnalizacji włamania i napadu?

TAK ☐ **NIE** ☐

9.8 Wymienić i podać klasę elementów składowych systemu sygnalizacji włamania i napadu np. pasywnych czujek podczerwieni, czujek magnetycznych, czujek wibracyjnych.

……
……

9.9 Czy system posiada dodatkowe źródło zasilania?

TAK ☐ **NIE** ☐

9.10 Data i godzina ostatniego próbnego alarmu przeprowadzonego w pomieszczeniach kancelarii.

……

9.11 Czas reakcji służb ochrony na wywołany próbny alarm w pomieszczeniach kancelarii tajnej.

……..

9.12 Czas reakcji grupy interwencyjnej na wywołany próbny alarm w pomieszczeniach kancelarii tajnej.

……...

9.13 Czy pracownicy służby ochrony oraz grupy interwencyjnej wyposażeni byli w środki łączności?

TAK ☐ **NIE** ☐

9.14 Częstotliwość przeprowadzania próbnych alarmów w pomieszczeniach kancelarii tajnej międzynarodowej

……..

10. System sygnalizacji pożarowej

10.1 czy w kancelarii zainstalowano system sygnalizacji pożarowej
(zaznaczyć odpowiednie pole wyboru – w przypadku zaznaczenia odpowiedzi „TAK" – wypełnić ppkt 10.2)

TAK ☐ **NIE** ☐

11. System telewizji dozorowej

11.1 Czy wejście do pomieszczeń kancelarii objęte jest systemem telewizji dozorowej?
(zaznaczyć odpowiednie pole wyboru – w przypadku zaznaczenia odpowiedzi „TAK" – wypełnić ppkt 11.2)

TAK ☐ **NIE** ☐

11.2 Gdzie zlokalizowano rejestrator obrazu.

……..

12. Rejestracja i przechowywanie zdarzeń systemów zainstalowanych w kancelarii

12.1 system sygnalizacji włamania i napadu

12.1.1. czas przechowywania ☐ **dni**

12.1.2 miejsce przechowywania: ……

/podać piętro, strefę, nr pokoju oraz do kogo należy i kto ma do niego dostęp/

12.1.3 sposób przechowywania: ……..

/podać formę zapisu zdarzeń np. zapis na kasecie, cyfrowy itp./

12.2 system telewizji dozorowej

12.2.1. czas przechowywania ☐ **dni**

12.2.2 miejsce przechowywania: ……

/podać piętro, strefę, nr pokoju oraz do kogo należy i kto ma do niego dostęp/

12.2.3 sposób przechowywania: ……..

/podać formę zapisu zdarzeń np. zapis na kasecie, cyfrowy itp./

12.3 system kontroli dostępu

12.3.1. czas przechowywania ☐ **dni**

12.3.2 miejsce przechowywania: ……

/podać piętro, strefę, nr pokoju oraz do kogo należy i kto ma do niego dostęp/

12.3.3 sposób przechowywania: ……..

/podać formę zapisu zdarzeń np. zapis na kasecie, cyfrowy itp./

13. Szafy stalowe w pomieszczeniu kancelarii

Szafa nr 1 (……..)

Organizacja międzynarodowa/państwo/reżim)

tabliczka znamionowa wydana przez jednostkę certyfikującą	**tak***	**nie**
certyfikat	**tak**	**nie**
zakotwienie szafy do podłoża	**tak**	**nie**
możliwość fizycznego odseparowania dokumentów oznaczonych różnymi klauzulami tajności (osobne zamknięcie)	**tak**	**nie**

Producent: _____,
Typ: _____,
Nr fabr.: _____,
Klasa: **A B C**
Nr certyfikatu: _____,

* skreślić niewłaściwe

Szafa nr 2 (……..)
Organizacja międzynarodowa/państwo/reżim

tabliczka znamionowa	**tak**	**nie**
certyfikat	**tak**	**nie**
zakotwienie szafy do podłoża	**tak**	**nie**
możliwość fizycznego odseparowania dokumentów oznaczonych różnymi klauzulami tajności (osobne zamknięcie)	**tak**	**nie**

Producent: _____,
Typ: _____,
Nr fabr.: _____,
Klasa: **A B C**
Nr certyfikatu: _____,

14. Deponowanie kluczy i kodów szyfrowych do pomieszczeń kancelarii tajnej międzynarodowej oraz szafy (szaf) do przechowywania dokumentów niejawnych

14.1 Kto (stanowisko) ma dostęp do kluczy i kodów zapasowych do pomieszczeń kancelarii tajnej międzynarodowej?

1. ……
2. ……
3. ……

14.2 Tryb zdawania oraz miejsce deponowania kluczy i kodów bieżących oraz zapasowych do szaf i pomieszczeń kancelarii międzynarodowej

- Klucze do pomieszczenia KT:
  - bieżące –

  tryb zdawania:……....
  miejsce przechowywania:……..
  osoby, które mają dostęp do kluczy:……
  - zapasowe –

  tryb zdawania:……....
  miejsce przechowywania:……..
  stanowiska osób, które mają dostęp do kluczy:……
- Klucze do szaf w KT:
  - bieżące –

  tryb zdawania:……....
  miejsce przechowywania:……..
  stanowiska osób, które mają dostęp do kluczy:……
  - zapasowe –

  tryb zdawania:……....
  miejsce przechowywania:……..

stanowiska osób, które mają dostęp do kluczy:……

- Kody zamków szyfrowych:
  - bieżące –

tryb zdawania:……....
miejsce przechowywania:……..
stanowiska osób, które mają dostęp do kodów:……

- zapasowe –

tryb zdawania:……....
miejsce przechowywania:……..
stanowiska osób, które mają dostęp do kodów:……

15. Dodatkowe wyposażenie kancelarii

15.1 czy w kancelarii znajduje się urządzenie do niszczenia dokumentów?
(zaznaczyć odpowiednie pole wyboru – w przypadku zaznaczenia odpowiedzi „TAK" – wypełnić dane dot. urządzenia)

TAK ☐ **NIE** ☐

Producent: _____,

Klasa wg DIN 32757: **4 5 BRAK**
(skreślić niewłaściwe)

Typ: _____,

Nr fabr.: _____,

Długość / szerokość cięcia (mm): _____,

15.2 czy w kancelarii znajduje się urządzenie do kopiowania?
(zaznaczyć odpowiednie pole wyboru – w przypadku zaznaczenia odpowiedzi „TAK" – wypełnić dane dot. urządzenia)

TAK ☐ **NIE** ☐

Producent: _____,

Typ: _____,

Nr fabr.: _____,

Czy kserokopiarka jest zabezpieczona przed ujawniającą się emisją elektromagnetyczną **tak nie**
(skreślić niewłaściwe)

16. Dokumenty niezbędne do pracy kancelarii:
(należy wymienić dokumenty/przepisy organizacji międzynarodowych/państw, które dot. pracy kancelarii)

1 Zatwierdzony przez kierownika ……. Regulamin (Instrukcja) pracy kancelarii tajnej międzynarodowej i czytelni

2…….

3…….

4…….

17. Inne dokumenty oraz wykazy dotyczące kancelarii:

17.1 wykazy poświadczeń bezpieczeństwa pracowników jednostki organizacyjnej mających dostęp do informacji niejawnych międzynarodowych	**Tak**	**Nie**
17.2 wykazy szkoleń z zakresu ochrony informacji niejawnych międzynarodowych	**Tak**	**Nie**
17.3 rejestr interwencji technicznych przeprowadzonych w pomieszczeniach kancelarii	**Tak**	**Nie**
17.4 wykaz sprzętu pomieszczeń kancelarii	**Tak**	**Nie**
17.5 dokument potwierdzający wyznaczenie personelu kancelarii tajnej międzynarodowej	**Tak**	**Nie**

CZĘŚĆ V: CENTRUM MONITORINGU

1. Czy w jednostce ustanowiono centrum monitoringu?

(zaznaczyć odpowiednie pole wyboru – w przypadku zaznaczenia odpowiedzi „TAK" wypełnić pkt. 2-9)

TAK ☐ **NIE** ☐

2. Opis lokalizacji centrum.

…….

3. Opis systemu pracy centrum?

……..

4. Czy w centrum monitoringu znajduje się wyciąg z instrukcji dot. sposobu postępowania w sytuacjach nadzwyczajnych?

TAK ☐ **NIE** ☐

5. Czy pracownicy centrum są systematycznie szkoleni w zakresie procedur postępowania w sytuacjach nadzwyczajnych?

(zaznaczyć odpowiednie pole wyboru – w przypadku zaznaczenia odpowiedzi „TAK" wypełnić pkt 6-7)

TAK ☐ **NIE** ☐

6. Czy fakt odbycia szkolenia jest odnotowywany na wykazie imiennym dołączonym do wyciągu z instrukcji dot. sposobu postępowania w sytuacjach nadzwyczajnych

TAK ☐ **NIE** ☐

7. Jaka jest częstotliwość szkoleń z zakresu procedur postępowania w sytuacji nadzwyczajnej?

……...

8. Czy w centrum jest możliwość podglądu obrazu z kamer telewizji dozorowej?

TAK ☐ **NIE** ☐

9 Czy zdarzenia systemu włamania i napadu zainstalowanego w pomieszczeniach kancelarii tajnej międzynarodowej są przekazywane do centrum monitoringu i gdzie są rejestrowane?

TAK ☐ **NIE** ☐

…….

CZĘŚĆ VI: WYNIK OGLĘDZIN POMIESZCZEŃ PRZEZNACZONYCH DLA KANCELARII TAJNEJ MIĘDZYNARODOWEJ W TYM ZASTOSOWANYCH ROZWIĄZAŃ TECHNICZNYCH I ORGANIZACYJNYCH [13]

……
……
……

[13] Dotyczy wyłącznie kancelarii tajnych międzynarodowych, w których będą przetwarzane informacje niejawne o klauzuli COSMIC TOP SECRET, TRÉS SECRET UE/EU TOP SECRET oraz ATOMAL. Część VI wypełnia SKW lub ABW zgodnie z właściwością.

Plan organizacji kancelarii tajnej międzynarodowej w ……...
/nazwa jednostki organizacyjnej/

sporządził……..,
/imię, nazwisko, pieczęć i podpis
pełnomocnika ochrony informacji niejawnych w jednostce organizacyjnej/

zaakceptował …….
/imię, nazwisko, pieczęć i podpis kierownika jednostki organizacyjnej/

Załącznik nr 9

FORMULARZ INSPEKCJI ……

(kancelaria tajna międzynarodowa)

W ……..

(jednostka organizacyjna)

Zalecenia przekazane do realizacji po ostatniej inspekcji: ……

Stan realizacji zaleceń:……...

CZĘŚĆ I. Organizacja systemu bezpieczeństwa informacji niejawnych międzynarodowych

1. Dane osobowe kierownika jednostki organizacyjnej				
	TAK	**NIE**	**NIE DOTYCZY**	**UWAGI/ZALECENIA**
2. Czy kierownik jednostki organizacyjnej posiada odpowiednie uprawnienie do dostępu do informacji niejawnych międzynarodowych?				
3.Czy w jednostce organizacyjnej powołano pełnomocnika do spraw ochrony informacji niejawnych międzynarodowych?				
4.Czy określono zakres obowiązków pełnomocnika do spraw ochrony informacji niejawnych?				
5.Czy pełnomocnik do spraw ochrony informacji niejawnych podlega bezpośrednio kierownikowi jednostki organizacyjnej?				
6.Czy i kiedy pełnomocnik do spraw ochrony informacji				

niejawnych został przeszkolony z zakresu ochrony informacji międzynarodowych?				
7. Czy w jednostce organizacyjnej wyznaczono kierownika kancelarii międzynarodowej?				
8. Czy kierownik kancelarii międzynarodowej posiada odpowiednie uprawnienie do dostępu do informacji niejawnych międzynarodowych?				
9. Czy w jednostce jest plan ochrony informacji niejawnych międzynarodowych?				
10. Czy plan ochrony informacji niejawnych międzynarodowych zawiera sposób, w jaki służby ochrony postępują w sytuacji nadzwyczajnej?				
11. Czy procedury postępowania w przypadku wprowadzenia sytuacji nadzwyczajnej były sprawdzane?				
12. Czy w odniesieniu do kancelarii tajnej międzynarodowej plan ochrony informacji niejawnych zawiera: • Opis stref ochronnych, • Zastosowane środki bezpieczeństwa fizycznego, • Zasady i sposób zdawania, przechowywania i wydawania kluczy oraz ich duplikatów do pomieszczeń kancelarii tajnej międzynarodowej oraz szaf, w których przechowywane są informacje niejawne międzynarodowe oraz zasady ustalania, zmiany i deponowania haseł lub szyfrów zamków szyfrowych, • Procedury przyznawania uprawnień do wejścia, wyjścia i przebywania w strefach ochronnych i kancelarii tajnej, w tym dla pracowników obsługi				

technicznej oraz interesantów/gości, • Sposób interwencji osób odpowiedzialnych za ochronę fizyczną w przypadku wywołania alarmu w kancelarii tajnej międzynarodowej, • Procedury ewakuacji i niszczenia informacji niejawnych międzynarodowych z uwzględnieniem wystąpienia sytuacji nadzwyczajnej.				
13. Kiedy i przez kogo została przeprowadzona poprzednia inspekcja?				
14.Czy w jednostce dostępna jest notatka poinspekcyjna z poprzedniej inspekcji?				
15. Czy były zalecenia poinspekcyjne (jeśli tak, to czy je wykonano)?				
16. Czy w kancelarii tajnej znajdują się niezbędne dokumenty/przepisy dot. informacji niejawnych międzynarodowych.				
17. Czy personel kancelarii oraz osoby korzystające z dokumentów niejawnych międzynarodowych są systematycznie szkolone w zakresie procedur postępowania z informacjami niejawnymi międzynarodowymi w przypadku wystąpienia sytuacji nadzwyczajnej?				

CZĘŚĆ II. Bezpieczeństwo osobowe

	TAK	NIE	NIE DOTYCZY	UWAGI/ZALECENIA
1. Czy jednostka opracowała system szkoleń z zakresu ochrony informacji niejawnych międzynarodowych?				
2. Kto przeprowadza szkolenia z ochrony informacji niejawnych międzynarodowych?				
3. Jaka jest częstotliwość szkoleń?				
4. Czy fakt odbycia szkolenia przez pracowników jednostki jest udokumentowany i w jaki sposób?				
5. Czy osoby przeszkolone podpisały oświadczenie o zapoznaniu się z przepisami ochrony informacji niejawnych międzynarodowych oraz o odpowiedzialności za ochronę tych informacji?				
6. Czy personel kancelarii tajnej ma dostęp do aktualnej informacji o osobach, które były szkolone z zakresu ochrony informacji niejawnych międzynarodowych?				
7. Czy personel kancelarii tajnej ma dostęp do wykazu osób w jednostce organizacyjnej posiadających poświadczenia bezpieczeństwa?				
8. Czy osoby zapoznające się z informacjami niejawnymi międzynarodowymi posiadają odpowiednie i aktualne poświadczenie bezpieczeństwa?				
9. Czy doszło do ujawnienia, złamania zasad bezpieczeństwa informacji niejawnych międzynarodowych?				

CZĘŚĆ III. Bezpieczeństwo fizyczne kancelarii tajnej międzynarodowej

	TAK	NIE	NIE DOTYCZY	UWAGI/ZALECENIA
1. Czy zabezpieczenie kancelarii tajnej jest zgodne z planem organizacji kancelarii tajnej międzynarodowej?				
2. Czy wyposażenie kancelarii jest zgodne z planem organizacji kancelarii tajnej międzynarodowej?				
3. Czy klucze i szyfry do pomieszczeń kancelarii tajnej międzynarodowej oraz szaf są chronione przed nieuprawnionym dostępem?				
4. Czy kody do systemu sygnalizacji włamania i napadu, sejfów oraz szaf znajdujących się w kancelarii są zmieniane?				
5. Czy system sygnalizacji włamania i napadu jest konserwowany?				
6. Czy w kancelarii wywoływane są próbne alarmy w pomieszczeniach kancelarii?				
7. Jak dokumentowane są próbne alarmy?				
8. Czas i sposób reakcji na wywołany alarm w kancelarii tajnej.				

CZĘŚĆ V. Bezpieczeństwo informacji niejawnych międzynrodowych

	TAK	NIE	NIE DOTYCZY	UWAGI/ZALECENIA
1. Czy i w jaki sposób spełniona jest zasada „need to know”?				

2. Czy są osobne ewidencje dla dokumentów różnych organizacji międzynarodowych/reżimów (np. ATOMAL, BOHEMIA)/państw				
3. Czy dokonano rocznego przeglądu dokumentów zarejestrowanych w kancelarii?				
4. Czy liczba dokumentów zarejestrowanych w ewidencjach zgadza się ze stanem faktycznym?				
5. Czy w kancelarii jest dostępny protokół z rocznego przeglądu dokumentów?				
6. Ile w kancelarii zarejestrowano dokumentów rozliczanych?				
7. Czy brakowano dokumenty niejawne międzynarodowe?				
8. Czy dostępna jest dokumentacja z brakowania?				
9. Jak długo przechowywana jest dokumentacja dot. brakowania?				
10. Czy fakt wybrakowania dokumentów został odnotowany w ewidencjach?				
12. Czy wykonywano kopie, tłumaczenia, wyciągi, odpisy z dokumentów niejawnych międzynarodowych?				
13. Czy przekazywano informacje niejawne międzynarodowe innym jednostkom organizacyjnym, jeśli tak to ile, komu i jaką drogą?				

Inne/dodatkowe informacje i spostrzeżenia uzyskane podczas inspekcji.

……

……

Załącznik nr 10

ZALECENIA DO PLANÓW OCHRONY JEDNOSTEK ORGANIZACYJNYCH W ZAKRESIE POSTĘPOWANIA Z INFORMACJAMI NIEJAWNYMI MIĘDZYNARODOWYMI W SYTUACJACH NADZWYCZAJNYCH

I. OGÓLNE ZAPISY I ZALECENIA

1. Informacje niejawne międzynarodowe są rejestrowane odpowiednio w kancelarii tajnej międzynarodowej, wpisanej do Ewidencji kancelarii tajnych międzynarodowych, prowadzonej przez Agencję Bezpieczeństwa Wewnętrznego.

2. Osobami odpowiedzialnymi za przetwarzane w jednostce organizacyjnej informacje niejawne międzynarodowych są:

a) kierownik jednostki organizacyjnej – za zorganizowanie i zapewnienie funkcjonowania ochrony informacji niejawnych międzynarodowych, zatrudnienie kierownika kancelarii tajnej międzynarodowej oraz określenie zasad funkcjonowania kancelarii, akceptację planu organizacji kancelarii tajnej międzynarodowej oraz jego przekazanie odpowiednio dl ABW lub SKW;

b) pełnomocnik ds. ochrony informacji niejawnych – za bezpieczeństwo fizyczne tych informacji (tj. kontrola systemów zabezpieczeń stref ochronnych i kancelarii) oraz bezpieczeństwo osobowe (posiadanie odpowiednich poświadczeń bezpieczeństwa, szkolenia z zakresu ochrony informacji niejawnych międzynarodowych);

c) kierownik kancelarii tajnej międzynarodowej – za wdrożenie standardów bezpieczeństwa informacji niejawnych międzynarodowych oraz zgodne z zasadami bezpieczeństwa funkcjonowanie dokumentu (tj. rejestrowanie, przechowywanie, dystrybucja, obieg, przetwarzanie oraz brakowanie informacji niejawnych międzynarodowych).

3. W przypadku wystąpienia sytuacji nadzwyczajnej kierownik jednostki organizacyjnej, a w przypadkach nagłych pełnomocnik ds. ochrony informacji niejawnych, zastępca pełnomocnika lub kierownik kancelarii tajnej międzynarodowej jest odpowiedzialny za wprowadzenie poszczególnych środków ochrony informacji niejawnych międzynarodowych, a także za podejmowanie decyzji dotyczących ich ewentualnej ewakuacji.

4. Kierownik jednostki organizacyjnej, pełnomocnik lub zastępca pełnomocnika powinien na bieżąco informować ABW lub SKW o podjętych decyzjach w zakresie ochrony informacji niejawnych międzynarodowych wobec zaistnienia sytuacji nadzwyczajnej.

5. Za wszelkie czynności związane z dokumentami niejawnymi przechowanymi w kancelarii w czasie wystąpienia sytuacji nadzwyczajnej odpowiedzialny jest kierownik kancelarii tajnej, w której takie dokumenty są zarejestrowane.

II. ZALECENIA DLA PEŁNOMOCNIKA I PIONU OCHRONY DOTYCZĄCE POSTĘPOWANIA W SYTUACJACH NADZWYCZAJNYCH

ŚRODKI ZAPOBIEGAWCZE:

a) wprowadzić system bieżącej kwalifikacji dokumentów przeznaczonych do ewentualnej ewakuacji.

b) wyraźnie sprecyzować indywidualne zadania osób odpowiedzialnych za ochronę obiektu i systematycznie przypominać o zasadach postępowania w sytuacji nadzwyczajnej.

c) przeprowadzać cykliczne szkolenia dla nowo zatrudnionych osób odpowiedzialnych za ochronę obiektu w zakresie przyjętych w obiekcie procedur bezpieczeństwa.

d) przeprowadzać systematyczne przeglądy wszystkich systemów ochrony zainstalowanych w obiekcie zgodnie z przyjętymi normami odnoszącymi się do klasy systemu oraz co najmniej raz w roku przeprowadzać próbne alarmy sprawdzające gotowość służb ochrony do reakcji zgodnie z przyjętym planem ochrony obiektu.

e) na bieżąco aktualizować plany ochrony do zmieniającej się rzeczywistości – przyjęte procedury powinny odpowiadać faktycznemu stanowi rzeczy, uwzględniającemu wszystkie zaistniałe ostatnio zmiany związane z systemem bezpieczeństwa obiektu.

POSTĘPOWANIE PEŁNOMOCNIKA/PIONU OCHRONY:

- w trakcie wystąpienia sytuacji nadzwyczajnej w jednostce organizacyjnej:

a) poinformować o zaistniałej sytuacji kierownika jednostki organizacyjnej;

b) przekazać do kancelarii tajnej międzynarodowej wszystkie dokumenty niejawne znajdujące się poza tą kancelarią (dokumenty wypożyczone);

b) poinformować ABW lub SKW o zaistniałym zdarzeniu;

c) ewakuować do Głównej Kancelarii Tajnej Międzynarodowej (GKT) odpowiednio dla sfery cywilnej lub wojskowej lub miejsca zaaprobowanego przez ABW lub SKW, przechowywane dokumenty niejawne. Przekazywanie dokumentów do GKT powinno się odbywać za protokołem. Jeżeli sytuacja wymaga natychmiastowego przekazania dokumentów – protokół można sporządzić w późniejszym czasie, po ustąpieniu bezpośredniego zagrożenia. Protokół powinien zawierać sygnaturę dokumentu oraz datę jego rejestracji;

d) informacje niejawne międzynarodowe należy przewozić samochodem, w nieprzeźroczystym, niepalnym i nieprzemakalnym pojemniku lub worku przez pracownika kancelarii, z której dokumenty są przewożone, w asyście dwóch konwojentów;

e) w pierwszej kolejności należy chronić pieczęcie (w celu uniemożliwienia ich użycia w sposób nieupoważniony), dokumenty o najwyższych klauzulach tajności oraz szczególne grupy dokumentów (np. ATOMAL, BOHEMIA);

f) po zaistniałym zdarzeniu kierownik jednostki organizacyjnej powinien przesłać do ABW lub SKW informację sporządzoną przez pełnomocnika zawierającą: określenie istoty i konsekwencji stwierdzonego zagrożenia lub incydentu (w tym stan oraz ewentualne zmiany wprowadzone po usuwaniu zaistniałych szkód), opis podjętych działań, a także ocenę potencjalnego, ponownego zagrożenia;

g) po ustąpieniu zagrożenia dla obiektu, a także przylegającego do niego terenu, wszystkie ewakuowane dokumenty niejawne są zwracane do kancelarii, od której były przyjęte, na pisemny wniosek kierownika jednostki organizacyjnej lub Pełnomocnika.

- trakcie wystąpienia sytuacji nadzwyczajnej w bezpośrednim sąsiedztwie obiektu:

a) poinformować o zaistniałej sytuacji kierownika jednostki organizacyjnej;

b) przekazać do kancelarii tajnej międzynarodowej wszystkie dokumenty niejawne znajdujące się poza tą kancelarią (dokumenty wypożyczone);

c) ograniczyć udostępnianie dokumentów niejawnych wyłącznie do pomieszczeń kancelarii tajnej międzynarodowej;

d) ograniczyć liczbę osób korzystających z dokumentów i przebywających w pomieszczeniach kancelarii tajnej międzynarodowej oraz w przylegającej do niej strefie ochronnej;

e) jeśli istnieje taka możliwość (w przypadku braku zagrożenia życia lub zdrowia) przygotować dokumenty będące w bieżącym użytkowaniu do awaryjnego postępowania - spisać i wydzielić dokumenty przeznaczone do ewakuacji;

f) wzmocnić ochronę fizyczną obszaru przyległego po kancelarii tajnej międzynarodowej;

g) przeprowadzić przegląd wszystkich środków bezpieczeństwa chroniących informacje niejawne międzynarodowe;

h) sprawdzić wszystkie, dostępne środki łączności z osobami lub jednostkami organizacyjnymi nadzorującymi pracę kancelarii tajnej międzynarodowej;

i) zasięgnąć opinii ABW na temat zastosowania ewentualnych, dodatkowych środków bezpieczeństwa.

III. WYTYCZNE DLA OSÓB KORZYSTAJĄCYCH Z DOKUMENTÓW NIEJAWNYCH MIĘDZYNARODOWYCH W CZASIE WYSTĄPIENIA SYTUACJI NADZWYCZAJNYCH:

- Niezwłocznie poinformować swojego przełożonego,
- Jeśli istnieje taka możliwość (w przypadku braku zagrożenia życia lub zdrowia) przekazuje się posiadane dokumenty niejawne międzynarodowe do kancelarii tajnej międzynarodowej,
- W przypadku braku możliwości przekazania dokumentów do kancelarii należy jak najszybciej umieścić dokument w szafie metalowej, spełniającej odpowiednie wymogi bezpieczeństwa. Klucze do szafy należy zdeponować zgodnie z przyjętymi w jednostce zasadami. W przypadku braku możliwości zdeponowania kluczy należy wynieść je z budynku, a następnie przekazać Pełnomocnikowi ds. Ochrony Informacji Niejawnych,
- W sytuacji, gdy nie można zastosować żadnego z powyższych rozwiązań, dokumenty należy wynieść z budynku i przekazać Pełnomocnikowi ds. Ochrony Informacji

Niejawnych. Pełnomocnik ds. Ochrony Informacji Niejawnych zabezpiecza materiały i po ustąpieniu zagrożenia zwraca materiały do kancelarii tajnej międzynarodowej lub gdy zagrożenie nie ustępuje przekazuje je do Głównej Kancelarii Tajnej Międzynarodowej dla sfery wojskowej lub cywilnej (GKT). W przypadku gdyby transport materiałów do GKT stwarzałby duże zagrożenie dla materiałów (np. ze względu na odległość) należy je zdeponować w najbliższej kancelarii tajnej międzynarodowej lub krajowej w ABW, AW, CBA, BOR, Policji, Służby Więziennej, SWW, Straży Granicznej, Żandarmerii Wojskowej lub – w przypadku zawarcia odpowiedniej umowy - u przedsiębiorcy. Pełnomocnik informuje niezwłocznie odpowiednio ABW lub SKW o fakcie zdeponowania materiałów niejawnych międzynarodowych poza jednostką organizacyjną.

- W pierwszej kolejności należy chronić pieczęcie (w celu uniemożliwienia ich użycia w sposób nieupoważniony) oraz dokumenty o najwyższych klauzulach tajności,
- Po ustąpieniu zagrożenia wszystkie ewakuowane dokumenty należy zwrócić do kancelarii tajnej międzynarodowej,
- W przypadku wystąpienia okoliczności nadzwyczajnych w czasie trwania wizyty międzynarodowej należy przekazać dokument organizatorom spotkania.