302

DECYZJA Nr 362/MON
MINISTRA OBRONY NARODOWEJ

z dnia 28 września 2011 r.

w sprawie wprowadzenia do użytku „Wytycznych Ministra Obrony Narodowej w sprawie określenia zasad postępowania z materiałami zawierającymi informacje niejawne oznaczone klauzulą „poufne" i „zastrzeżone""

Na podstawie § 2 pkt 6 i 14 rozporządzenia Rady Ministrów z dnia 9 lipca 1996 r. w sprawie szczegółowego zakresu działania Ministra Obrony Narodowej (Dz. U. Nr 94, poz. 426), w celu uregulowania i ujednolicenia zasad postępowania z materiałami zawierającymi informacje niejawne oznaczone klauzulą „poufne" i „zastrzeżone" w jednostkach organizacyjnych resortu obrony narodowej, ustala się, co następuje:

1. Wprowadza się do użytku „Wytyczne Ministra Obrony Narodowej w sprawie określenia zasad postępowania z materiałami zawierającymi informacje niejawne oznaczone klauzulą „poufne" i „zastrzeżone"" w jednostkach organizacyjnych resortu obrony narodowej, stanowiące załącznik do decyzji.

2. Decyzja wchodzi w życie z dniem ogłoszenia.

Minister Obrony Narodowej: *T. Siemoniak*

Załącznik do decyzji Nr 362/MON
Ministra Obrony Narodowej
z dnia 28 września 2011 r. (poz. 302)

WYTYCZNE
w sprawie określenia zasad postępowania z materiałami zawierającymi informacje niejawne oznaczone klauzulą „poufne" i „zastrzeżone" w jednostkach organizacyjnych resortu obrony narodowej

Rozdział I

Przepisy ogólne

1. Zgodnie z art. 43 ust. 3 i 5 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228), zwanej dalej „ustawą", kierownicy jednostek organizacyjnych zatwierdzają następujące dokumenty opracowane przez pełnomocników ochrony:
1) instrukcję dotyczącą sposobu i trybu przetwarzania informacji niejawnych o klauzuli „poufne" w podległych komórkach organizacyjnych;
2) instrukcję dotyczącą sposobu i trybu przetwarzania informacji niejawnych o klauzuli „zastrzeżone" w podległych komórkach organizacyjnych oraz zakres i warunki stosowania środków bezpieczeństwa fizycznego w celu ich ochrony.

2. Przy opracowaniu dokumentów, o których mowa w pkt 1, należy uwzględnić zasady w zakresie postępowania z materiałami zawierającymi informacje niejawne oznaczone klauzulą „poufne" i „zastrzeżone", które nie mogą naruszać przepisów ustawy i innych norm prawa.

3. Minimalne warunki dotyczące przetwarzania informacji niejawnych oznaczone klauzulą „poufne" i „zastrzeżone" określa załącznik do wytycznych.

4. Zakres stosowania środków bezpieczeństwa fizycznego uzależnia się od poziomu zagrożeń związanych z nieuprawnionym dostępem do informacji niejawnych lub ich utratą, o którym mowa w art. 43 ust. 4 ustawy.

Rozdział II

Wymagania dotyczące materiałów niejawnych oznaczonych klauzulą „poufne"

5. System obiegu dokumentów ma zapewnić możliwość ustalenia w każdych okolicznościach, gdzie znajduje się materiał o klauzuli „poufne" pozostający w dyspozycji jednostki/komórki organizacyjnej oraz, kto z tym materiałem się zapoznał. Żaden materiał o klauzuli „poufne" nie może zostać przekazany poza komórkę/jednostkę organizacyjną bez udziału kancelarii tajnej lub innej komórki odpowiedzialnej za ewidencjonowanie, gromadzenie i obieg materiałów niejawnych.

6. Przyjmowanie/wydawanie materiałów niejawnych oznaczonych klauzulą „poufne" odbywa się za pokwitowaniem w odpowiednim urządzeniu ewidencyjnym.

7. Zgoda kierownika jednostki organizacyjnej lub upoważnionej przez niego osoby dysponującej dokumentem wymagana jest na wykonanie jego kopii, odpisu, wyciągu, tłumaczenia lub wypisu (skanowania dokumentu do pliku elektronicznego), o ile wytwórca dokumentu nie wprowadził ograniczeń dotyczących kopiowania, sporządzania odpisów, wypisów, wyciągów i tłumaczeń tego materiału. Wszystkie kopie podlegają ewidencji w odpowiednim urządzeniu ewidencyjnym. Skany dokumentów nie podlegają ewidencji, fakt skanowania jest dokumentowany na oryginale dokumentu z podaniem numeru ewidencyjnego informatycznego nośnika danych. W przypadku zapisywania skanu w lokalizacji sieciowej należy podać numeru ewidencyjny dysku twardego stacji roboczej użytkownika wprowadzającego te dane.

8. Osoba mająca dostęp do zasobów sieci o klauzuli „poufne" będzie miała dostęp do informacji publikowanych w portalach intranetowych tej sieci w określonym zakresie. O zakresie udostępnienia (dokument jest powszechnie dostępny lub udostępniany wyłącznie konkretnej grupie użytkowników) zdecyduje osoba, która jest uprawniona do podpisania dokumentu lub oznaczenia innego niż dokument materiału albo adresat materiału, o ile nie wprowadzono na materiale ograniczeń dotyczących udostępniania tego materiału.

9. Wadliwie wykonane wydruki niszczy bez dokumentowania wykonawca techniczny lub wykonawca, który sporządza dokument.

10. Instrukcja w sprawie sposobu i tryb przetwarzania informacji niejawnych o klauzuli „poufne" w podległych komórkach organizacyjnych powinna określać, co najmniej:

1) miejsce ewidencji, gromadzenia i przechowania materiałów niejawnych o klauzuli „poufne";
2) zasady przekazywania i udostępniania materiałów o klauzuli „poufne";
3) sposoby i miejsca wytwarzania, kopiowania i skanowania dokumentów niejawnych zawierających informacje o klauzuli „poufne";
4) zasady i sposoby niszczenia materiałów o klauzuli „poufne";
5) zasady ochrony informacji niejawnych o klauzuli „poufne" podczas prowadzonych narad, odpraw, konferencji, spotkań, szkoleń i rozmów itp.;
6) informację o odpowiedzialności karnej, dyscyplinarnej i służbowej za naruszenie przepisów o ochronie informacji niejawnych.

Rozdział III

Wymagania dotyczące materiałów niejawnych oznaczonych klauzulą „zastrzeżone"

11. Dokumenty o klauzuli „zastrzeżone" dzieli się na:

1) dokumenty robocze — zawierające informacje pozostające w fazie opracowywania, nie posiadające podpisu osoby uprawnionej lub upoważnionej do jej akceptacji i służą wymianie między merytorycznymi pracownikami;
2) dokumenty oficjalne — dokumenty autoryzowane (podpisane lub zatwierdzone) przez osobę uprawnioną lub upoważnioną do wykonywania tej czynności — pozostające w aktach lub/i przesyłane między komórkami/jednostkami organizacyjnymi, zawierające formalne stanowiska tych instytucji i mające skutek prawny.

12. System obiegu dokumentów ma zapewnić informację gdzie, poza komórkę/jednostkę organizacyjną, wysłano dokumenty oficjalne oznaczone klauzulą „zastrzeżone". Żaden dokument oficjalny nie może być przekazany poza komórkę/jednostkę organizacyjną bez udziału kancelarii tajnej (kancelarii elektronicznej) lub innej komórki odpowiedzialnej za ewidencjonowanie, gromadzenie i obieg materiałów niejawnych.

13. Przyjmowanie/wydawanie materiałów niejawnych oznaczonych klauzulą „zastrzeżone" następuje za pokwitowaniem w odpowiednim urządzeniu ewidencyjnym wyłącznie w przypadku dokumentów wydawanych z kancelarii tajnej/biblioteki lub innej komórki odpowiedzialnej za ewidencjonowanie, gromadzenie i obieg materiałów niejawnych. Osoba przekazująca dokument może zażądać pokwitowania jego odbioru (w urządzeniu ewidencyjnym, dzienniku wykonawcy, na oryginale lub innym egzemplarzu dokumentu).

14. Zgoda na kopiowanie dokumentu na potrzeby wykonawcy nie jest wymagana.

15. Odpowiedzialność za otrzymany materiał niejawny lub informację niejawną ponosi wykonawca, który go otrzymał. Wykonawca może, jeżeli to wynika z jego kompetencji służbowych, udostępnić robocze dokumenty niejawne osobom, z innej komórki/jednostki organizacyjnej, spełniającym ustawowe wymagania dostępu do informacji niejawnych.

16. Zniszczenie dokumentu niejawnego o klauzuli „zastrzeżone" wymaga potwierdzenia przez co najmniej jedną osobę (wykonawcę). Zasada ta nie obowiązuje, jeżeli inne przepisy regulujące postępowanie z określonymi rodzajami dokumentów nakazują komisyjne ich niszczenie. Wadliwie wykonane wydruki niszczy bez dokumentowania wykonawca techniczny (wykonawca, który sporządza dokument). Podstawę do zniszczenia lub archiwizowania dokumentu stanowić będą ustalenia wynikające z Rzeczowego wykazu akt oraz przepisów o narodowym zasobie archiwalnym i archiwach.

17. Osoba mająca dostęp do zasobów sieci o klauzuli „zastrzeżone" będzie miała dostęp do informacji publikowanych w portalach intranetowych tej sieci w określonym zakresie. O zakresie udostępnienia (dokument jest powszechnie dostępny lub udostępniany wyłącznie konkretnej grupie użytkowników) zdecyduje osoba, która jest uprawniona do podpisania dokumentu lub oznaczenia innego niż dokument materiału albo adresat materiału, o ile nie wprowadzono na materiale ograniczeń dotyczących udostępniania tego materiału.

18. „Instrukcja dotycząca sposobu i trybu przetwarzania informacji niejawnych o klauzuli „zastrzeżone" w podległych komórkach organizacyjnych oraz zakres i warunki stosowania środków bezpieczeństwa fizycznego w celu ich ochrony powinna określać, co najmniej:

1) w zakresie „Bezpieczeństwo osobowe" — warunki, które powinny spełniać osoby mające dostęp do materiałów niejawnych o klauzuli „zastrzeżone", w szczególności tryb przyznawania uprawnień osobom, które nie posiadają poświadczenia bezpieczeństwa;

2) w zakresie przetwarzania informacji niejawnych oznaczonych klauzulą „zastrzeżone", w tym:
   a) wytwarzanie — wskazanie, jakimi technikami i gdzie wytwarza się dokumenty o klauzuli „zastrzeżone",
   b) modyfikowanie — kto i na jakich zasadach może modyfikować treść informacji niejawnych zawartych w papierowych oraz elektronicznych dokumentach, a także informatycznych bazach danych,
   c) kopiowanie — zasady wykonania kopii, odpisu, wyciągu, tłumaczenia lub wypisu z dokumentu oznaczonego klauzulą „zastrzeżone", wskazanie jakimi technikami i gdzie wykonuje się kopie, uwzględniając kopie wykonywane dla potrzeb roboczych wykonawcy oraz kopie do wysłania poza jednostkę organizacyjną,
   d) klasyfikowanie — zasady nadawania i znoszenia klauzuli tajności, z uwzględnieniem kto nadaje klauzulę tajności i ją znosi, jakie czynności są wykonywane przy znoszeniu klauzuli tajności,
   e) gromadzenie i ewidencjonowanie — zasady gromadzenia i ewidencjonowania dokumentów, z uwzględnieniem jaka kancelaria lub inna komórka jest odpowiedzialna za te czynności,
   f) przechowywanie, środki bezpieczeństwa fizycznego w celu ochrony materiałów zawierających informacje niejawne oznaczone klauzulą „zastrzeżone" — miejsce i sposób przechowywania materiałów, uwzględniając ustalenia załącznika,
   g) przekazywanie — zasady przekazywania dokumentów oznaczonych klauzulą „zastrzeżone", z uwzględnieniem przekazywania tych dokumentów między wykonawcami w tej samej jednostce/komórce organizacyjnej i poza jednostkę/komórkę organizacyjną,
   h) udostępnianie — zasady udostępniania informacji oznaczonych klauzulą „zastrzeżone";
3) zasady niszczenia dokumentów oznaczonych klauzulą „zastrzeżone", uwzględniając różnice w przypadku niszczenia dokumentów „oficjalnych" i „roboczych";
4) zasady ochrony informacji niejawnych o klauzuli „zastrzeżone" podczas prowadzonych narad, odpraw, konferencji, spotkań, szkoleń i rozmów itp. — podając opis zasad wstępu na te zamierzenia, kontroli wejścia i udostępniania informacji;
5) postępowanie w przypadkach naruszenia przepisów ustawy oznaczonych klauzulą „zastrzeżone", przywołując stosowaną w jednostce organizacyjnej procedurę postępowania w tych przypadkach;
6) w zakresie „Bezpieczeństwo przemysłowe" — warunki, jakim podlegają przedsiębiorcy realizujący umowy lub zadania związane z dostępem do informacji niejawnych o klauzuli „zastrzeżone";
7) informację o odpowiedzialności karnej, dyscyplinarnej i służbowej za naruszenie przepisów o ochronie informacji niejawnych.

Załącznik
do wytycznych

Minimalne wymagania dotyczące przetwarzania informacji niejawnych oznaczone klauzulą „Poufne" i „Zastrzeżone"

<table>
<tr><th colspan="2">Klauzula</th><th colspan="2">„POUFNE"</th><th colspan="2">„ZASTRZEŻONE"</th></tr>
<tr><th colspan="2">Warunki</th><th>Zalecane</th><th>Dopuszczalne</th><th>Zalecane</th><th>Dopuszczalne</th></tr>
<tr><td rowspan="2">1.</td><td rowspan="2">Bezpieczeństwo osobowe</td><td colspan="2">Poświadczenie bezpieczeństwa do klauzuli, co najmniej „poufne" lub pisemna zgoda kierownika jednostki organizacyjnej na udostępnienie informacji niejawnych o klauzuli „poufne" osobie, wobec której wszczęto postępowanie sprawdzające</td><td colspan="2">Poświadczenie bezpieczeństwa lub po uzyskaniu pisemnego upoważnienia przez kierownika jednostki, jeżeli osoba nie posiada poświadczenia bezpieczeństwa</td></tr>
<tr><td colspan="4">Szkolenie podstawowe w zakresie ochrony informacji niejawnych</td></tr>
<tr><td rowspan="3">2.</td><td rowspan="3">Gromadzenie, ewidencja i przekazywanie dokumentów poza jednostkę/komórkę organizacyjną</td><td>W kancelarii tajnej</td><td>W innej komórce organizacyjnej, o której mowa w art. 44 ust. 1 ustawy</td><td>W kancelarii tajnej</td><td>W innej komórce organizacyjnej, o której mowa w art. 44 ust. 1 ustawy</td></tr>
<tr><td colspan="2">W systemie poczty elektronicznej[1], zgodnie z zasadami opisanymi w zatwierdzonej dokumentacji dotyczącej szczególnych wymagań bezpieczeństwa i procedurach bezpiecznej eksploatacji lub na załączonych do pism przewodnich nośnikach danych</td><td colspan="2">W systemie poczty elektronicznej: dokumenty „oficjalne" wyłącznie poprzez kancelarię elektroniczną lub na załączonych do pism przewodnich nośnikach danych</td></tr>
<tr><td colspan="2">Nie dopuszcza się przekazywania dokumentów bezpośrednio między wykonawcami z różnych komórek/ jednostek organizacyjnych</td><td colspan="2">Dokumenty „robocze" bezpośrednio pomiędzy wykonawcami z różnych komórek/jednostek organizacyjnych lub w systemie poczty elektronicznej</td></tr>
<tr><td>3.</td><td>Wydawanie dokumentów z kancelarii tajnej/biblioteki, innej komórki odpowiedzialnej za ewidencjonowanie, gromadzenie i obieg materiałów niejawnych</td><td colspan="4">Za pokwitowaniem w odpowiednim urządzeniu ewidencyjnym</td></tr>
<tr><td>4.</td><td>Przekazywanie dokumentów między wykonawcami w tej samej jednostce/komórce</td><td colspan="2">Za pokwitowaniem w odpowiednim urządzeniu ewidencyjnym lub dzienniku wykonawcy</td><td colspan="2">Bez pokwitowania lub na żądanie osoby przekazującej dokument w odpowiednim urządzeniu ewidencyjnym, dzienniku wykonawcy, lub na oryginale (innym egzemplarzu) dokumentu</td></tr>
</table>

[1)] Narzędzia poczty elektronicznej mają zapewnić wybór klauzuli tajności wiadomości pocztowej przed wysłaniem (przed edycją) wiadomości. System poczty elektronicznej musi zapewnić rozliczalność wysyłanych wiadomości pocztowych.

Klauzula		„POUFNE”		„ZASTRZEŻONE”	
Warunki		Zalecane	Dopuszczalne	Zalecane	Dopuszczalne
	organizacyjnej	W systemie poczty elektronicznej[2], zgodnie z zasadami opisanymi w zatwierdzonej dokumentacji dotyczącej szczególnych wymagań bezpieczeństwa i procedurach bezpiecznej eksploatacji lub na załączonych do pism przewodnich nośnikach danych		W systemie poczty elektronicznej wyłącznie pliki dokumentów roboczych	
5.	Przechowywanie	Strefa ochronna oraz:			
		Szafa stalowa, co najmniej klasy A	Szafa stalowa klasy A	Szafa stalowa klasy A	Inne szafy, skrzynie, kontenery itp. zamykane na zamek uniemożliwiający ich otwarcie osobom postronnym
			lub regały przeznaczone do przechowywania teczek akt lub wydawnictw pod warunkiem zabezpieczenia pomieszczenia wg wymagań dla I strefy ochronnej		lub inne rozwiązanie pod warunkiem, że pomieszczenie jest zabezpieczone drzwiami wejściowymi z zamkiem patentowym (minimum)
6.	Przewożenie	Przy zachowaniu zasad rozporządzenia Prezesa Rady Ministrów z dnia 29 września 2005 r. w sprawie trybu i sposobu przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne (Dz. U. Nr 200, poz. 1650, z późn. zm.)			
7.	Wytwarzanie	Akredytowane systemy teleinformatyczne o klauzuli, co najmniej „Poufne”		Akredytowane systemy teleinformatyczne	
		lub inne metody (np. kreślenie, odręczne wypełnianie formularzy itp.) przy zachowaniu zasad 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. Nr 159, poz.1069)			
8.	Kopiowanie i skanowanie dokumentu do pliku	Zgoda dysponenta dokumentu na wykonanie kopii		Zgoda dysponenta dokumentu na wykonanie kopii, tylko jeżeli dokument ma być przekazany innej komórce / jednostce organizacyjnej. Dokumenty na potrzeby wewnętrzne wykonawcy – bez wymogu uzyskania zgody	
		Przy zachowaniu zasad rozporządzenia Prezesa Rady Ministrów z dnia 13 sierpnia 2010 r. w sprawie sposobu oznaczania materiałów,			

[2)] Narzędzia poczty elektronicznej mają zapewnić wybór klauzuli tajności wiadomości pocztowej przed wysłaniem (przed edycją) wiadomości. System poczty elektronicznej musi zapewnić rozliczalność wysyłanych wiadomości pocztowych.

Klauzula		„POUFNE”		„ZASTRZEŻONE”	
Warunki		Zalecane	Dopuszczalne	Zalecane	Dopuszczalne
		umieszczania na nich klauzul tajności, a także zmiany nadanej klauzuli tajności (Dz. U. Nr 159, poz.1069)			
		Ewidencjonowanie każdej kopii w Dzienniku Ewidencji Wykonanych Dokumentów			
		Analogowe urządzenia kopiujące bez wbudowanych modułów pamięci lub elektroniczne urządzenia kopiujące / wielofunkcyjne / skanery posiadające akredytację bezpieczeństwa teleinformatycznego w rozumieniu ustawy			
		Urządzenia wielofunkcyjne włączone do systemów teleinformatycznych posiadających akredytację bezpieczeństwa teleinformatycznego			
		Zabrania się wykonywania kopii (skanów) dokumentów niejawnych na urządzeniach włączonych do sieci telefonicznej (z wyjątkiem sieci przystosowanych do przekazywania informacji niejawnych) – np. faxach, lub sieci jawnych – np. urządzeniach wielofunkcyjnych połączonych z siecią Internet			
9.	Udostępnianie	Zasada wiedzy niezbędnej przy udostępnianiu informacji w dowolnej postaci przy spełnieniu warunku „bezpieczeństwo osobowe”			
		Dokumenty udostępniane na podstawie dekretacji odręcznej na dokumencie lub w elektronicznym systemie obiegu dokumentów			
		Przyjmuje się zasadę, że osoba mająca dostęp do zasobów sieci ma dostęp do wszystkich informacji publikowanych w portalach intranetowych tej sieci. O zakresie udostępnienia (dokument jest ogólnie dostępnych lub udostępniany wyłącznie konkretnej grupie użytkowników) decyduje dysponent dokumentu			
10	Niszczenie	Warunek potwierdzenia zniszczenia dokumentu, czytelnymi podpisami, przez co najmniej dwie osoby w stosownym urządzeniu ewidencyjnym		Fakt zniszczenia dokumentu niejawnego o klauzuli „zastrzeżone” wymaga potwierdzenia, przez co najmniej jedną osobę (wykonawcę) Zasada ta nie obowiązuje, jeżeli inne przepisy regulujące postępowanie z określonymi rodzajami dokumentów nakazują komisyjne ich niszczenie Podstawą do zniszczenia lub archiwizowania dokumentu są ustalenia Rzeczowego wykazu akt	
		Wadliwe wydruki bez dokumentowania zniszczenia – niszczy wykonawca techniczny			
		Niszczarka klasy IV lub wyższej wg normy DIN 32757			