Warszawa, dnia 26 marca 2018 r.

Poz. 7

ZARZĄDZENIE NR 7

MINISTRA CYFRYZACJI

z dnia 23 marca 2018 r.

zmieniające zarządzenie w sprawie kancelarii tajnej

Na podstawie art. 47 ust. 3 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2018 r. poz. 412) zarządza się, co następuje:

§ 1. W zarządzeniu nr 31 Ministra Cyfryzacji z dnia 18 sierpnia 2016 r. w sprawie kancelarii tajnej (Dz. Urz. Min. Cyf. poz. 34) wprowadza się następujące zmiany:

1) tytuł zarządzenia otrzymuje brzmienie:

„w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii tajnej oraz doboru i stosowania środków bezpieczeństwa fizycznego”;

2) w § 2 pkt 3 otrzymuje brzmienie:

„3) pionie ochrony – należy przez to rozumieć pracowników Zespołu Ochrony Informacji Niejawnych Biura Dyrektora Generalnego Ministerstwa Cyfryzacji;”;

3) w § 6 ust. 3 otrzymuje brzmienie:

„3. Kierownik jednostki organizacyjnej lub pełnomocnik ochrony może wyrazić pisemną zgodę na przechowywanie materiałów o klauzuli „poufne” lub wyższej poza kancelarią, na czas niezbędny do realizacji zadań związanych z dostępem do tych materiałów, gdy zapewnione są odpowiednie do klauzuli warunki ochrony przed nieuprawnionym ujawnieniem.”;

4) § 16 otrzymuje brzmienie:

„§ 16. 1. W Ministerstwie Cyfryzacji tworzy się strefy ochronne II i III na podstawie kryteriów określonych w § 5 rozporządzenia Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz. U. z 2012 r. poz. 683 z późn. zm.).

2. Kancelarię lokalizuje się w strefie ochronnej II.”;

5) § 17 otrzymuje brzmienie:

„§ 17. 1. W kancelarii wydziela się stanowisko lub pomieszczenie, w którym osoby upoważnione mogą zapoznawać się z materiałami − czytelnię, która powinna być zorganizowana w sposób umożliwiający stały nadzór nad materiałami ze strony pracowników kancelarii. W czytelni nie instaluje się systemu nadzoru wizyjnego.

2. Pomieszczenia kancelarii wyposaża się w barierkę odgradzającą pracowników od interesantów oraz system kontroli dostępu.”;

6) po § 17 dodaje się § 17a w brzmieniu:

„§ 17a Pomieszczenia, w których przetwarzane są informacje niejawne o klauzuli „poufne” lub wyższej, spełniać muszą co najmniej następujące wymagania w zakresie stosowania środków bezpieczeństwa fizycznego:

1) oddziela się je od pozostałych pomieszczeń trwałymi ścianami i stropami, spełniającymi wymagania w zakresie klasy odporności pożarowej oraz nośności granicznej odpowiadającej co najmniej konstrukcji murowanej z cegły pełnej o grubości 100 mm;

2) wyposażone są w szafy do przechowywania informacji niejawnych:

a) spełniające co najmniej wymagania klasy odporności na włamanie S2, określone w Polskiej Normie PN-EN 14450 lub nowszej – na potrzeby przechowywania materiałów niejawnych o klauzuli „ściśle tajne” lub niższej;

b) spełniające co najmniej wymagania klasy odporności na włamanie S1, określone w Polskiej Normie PN-EN 14450 lub nowszej – na potrzeby przechowywania materiałów niejawnych o klauzuli „tajne” lub niższej;

3) przeznaczone do przechowywania materiałów o klauzuli „poufne” – na potrzeby przechowywania materiałów niejawnych o klauzuli „poufne” lub niższej;

4) konstrukcja pomieszczeń – w tym drzwi i zamków – zapewniać musi odporność na działania osoby nieuprawnionej próbującej uzyskać dostęp siłą lub za pomocą narzędzi oraz potajemne próby uzyskania nieuprawnionego dostępu;

5) okna muszą być zabezpieczone przed włamaniem oraz możliwością podglądu wnętrza z zewnątrz;

6) pomieszczenia muszą być objęte elektronicznym automatycznym systemem kontroli dostępu, wstęp do nich musi być kontrolowany przez odpowiednią barierę, która może wymagać bezpośredniego nadzoru przez personel bezpieczeństwa, a system kontroli dostępu obejmować musi wszystkie wejścia i wyjścia kontrolowanego pomieszczenia lub obszaru;

7) pomieszczenia muszą być objęte kontrolą osób nieposiadających stałego upoważnienia do wejścia na obszar jednostki organizacyjnej (interesantów);

8) pomieszczenia muszą być objęte nadzorem personelu bezpieczeństwa;

9) pomieszczenia muszą być objęte nadzorem systemu sygnalizacji napadu i włamania sygnalizującego co najmniej otwarcie drzwi, okien i innych zamknięć chronionego obszaru oraz poruszanie się w chronionym obszarze, generującym ostrzeżenia i alarmy oraz stale monitorowanym przez personel bezpieczeństwa;

10) wejścia do pomieszczeń muszą być objęte systemem dozoru wizyjnego, z rejestracją obrazu i przechowywaniem zarejestrowanego zapisu przez czas nie krótszy niż 30 dni.”.

§ 2. Zarządzenie wchodzi w życie z dniem następującym po dniu ogłoszenia.

WZ. MAREK ZAGÓRSKI

SEKRETARZ STANU

W MINISTERSTWIE CYFRYZACJI