

Zakres działań wymagający wdrożenia wynikający z analizy przepisów prawnych w obszarze zabezpieczenia i bezpiecznej realizacji zadań obronnych i ochrony informacji niejawnych

I. Obszar spraw obronnych, zarządzania kryzysowego, ochrony ludności i ochrony informacji niejawnych

1. PWM wykonuje zadania obronne w ramach obowiązku obrony nałożonych przez Ministra Kultury i Dziedzictwa narodowego (podstawa: Zarządzeniem Ministra Kultury i Dziedzictwa Narodowego z dnia 06 października 2023 r. w sprawie organizacji i sposobu wykonywania zadań w ramach obowiązku obrony).
2. Zgodnie z § 6 ust. 1 pkt. 2 Zarządzenia MKiDN z dnia 06 października 2023 r. realizacja zadań następuje w obszarach planowania operacyjnego i programowania obronnego.
3. Zgodnie z § 6 ust. 2 pkt. 9 Zarządzenia MKiDN z dnia 06 października 2023 r. w związku z niejawnym charakterem, zadań wynikających z dokumentacji dotyczącej planowania operacyjnego i programowania obronnego, kierownicy jednostek organizacyjnych zobowiązani są do zapewnienia należytej ochrony oraz sposobu przetwarzania tych informacji, zgodnie z ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2023 r. poz. 756, 1030 i 1532) oraz przepisami wykonawczymi wydanymi na jej podstawie, w szczególności przez zapewnienie miejsca do przechowywania i przetwarzania informacji niejawnych, stosownego do klauzuli przetwarzanej dokumentacji.
4. Zgodnie z § 3. ust.1 w ramach systemu bezpieczeństwa fizycznego informacji niejawnych stosuje się środki bezpieczeństwa fizycznego w celu zapewnienia poufności, integralności i dostępności tych informacji (podstawa: Rozporządzenie Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych).
5. Zgodnie z § 4. ust. 2 Rozporządzenia Rady Ministrów z dnia 29 maja 2012 r. środki bezpieczeństwa fizycznego stosuje się we wszystkich pomieszczeniach i obszarach, w których są przetwarzane informacje niejawne.
6. Zgodnie z § 4. ust. 3 Rozporządzenia Rady Ministrów z dnia 29 maja 2012 r. system środków bezpieczeństwa fizycznego obejmuje stosowanie rozwiązań organizacyjnych, wyposażenia i urządzeń służących ochronie informacji niejawnych oraz elektronicznych systemów pomocniczych wspomagających ochronę informacji niejawnych. Stosuje się odpowiednią kombinację następujących środków bezpieczeństwa fizycznego:
 - ❖ bariery fizyczne – środki chroniące granice miejsca, w którym są przetwarzane informacje, w szczególności ogrodzenia, ścieżki, bramy, drzwi i okna;
 - ❖ szafy i zamki – stosowane do przechowywania informacji niejawnych lub zabezpieczających informacje przed nieuprawnionym dostępem;
 - ❖ system kontroli dostępu – obejmujący elektroniczny system pomocniczy lub rozwiązanie organizacyjne, stosowany w celu zagwarantowania uzyskiwania dostępu do pomieszczenia lub obszaru, w którym są przetwarzane informacje, wyłączony przez osoby posiadające odpowiednie uprawnienia;
 - ❖ system sygnalizacji włamania i napadu – elektroniczny system pomocniczy stosowany w celu realizacji procedur ochrony informacji niejawnych oraz podwyższenia poziomu bezpieczeństwa, który zapewniają bariery fizyczne, a w pomieszczeniach i budynkach zastępujący lub wspierający personel bezpieczeństwa;
 - ❖ system dozoru wizyjnego – elektroniczny system pomocniczy stosowany w celu bieżącego monitorowania ochronnego lub sprawdzania incydentów bezpieczeństwa i sygnałów alarmowych przez personel bezpieczeństwa.

7. Zgodnie z § 4. ust. 5 Rozporządzenia Rady Ministrów z dnia 29 maja 2012 r. jeżeli istnieje zagrożenie podglądu, także przypadkowego, informacji niejawnych, zarówno w świetle dziennym, jak i w warunkach sztucznego oświetlenia, podejmuje się działania w celu wyeliminowania takiego zagrożenia.
8. Zgodnie z § 8. ust. 3 Rozporządzenia Rady Ministrów z dnia 29 maja 2012 r. przetwarzanie informacji niejawnych o klauzuli „zastrzeżone” w systemach teleinformatycznych odbywa się w pomieszczeniu lub obszarze wyposażonych w system kontroli dostępu.
9. Zgodnie z § 8. ust. 4 Rozporządzenia Rady Ministrów z dnia 29 maja 2012 r. serwery, systemy zarządzania siecią, kontrolery sieciowe i inne niewrażliwe elementy systemów teleinformatycznych umieszcza się w strefie ochronnej w przypadku przetwarzania informacji niejawnych o klauzuli „zastrzeżone”.
10. Zgodnie z art. 44 ust. 1 ustawy o ochronie informacji niejawnych z dnia 05 sierpnia 2010 r. dopuszcza się organizowanie innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za przetwarzanie materiałów niejawnych.
11. Zgodnie z art. 44 ust. 2 i art. 46 ustawy o ochronie informacji niejawnych z dnia 05 sierpnia 2010 r. przepisy art. 46 stosuje się odpowiednio w celu uniemożliwienia osobom nieuprawnionym dostępu do informacji niejawnych należy w szczególności:
 - ❖ organizować strefy ochronne;
 - ❖ wprowadzić system kontroli wstępu i wyjścia ze stref ochronnych;
 - ❖ określić uprawnienia do przebywania w strefach ochronnych;
 - ❖ stosować wyposażenie i urządzenia służące ochronie informacji niejawnych, którym przyznano certyfikaty.

Przykładowy układ pomieszczeń do przetwarzania informacji niejawnych, który powinien zapewnić zorganizowanie stref ochronnych oraz systemów elektronicznych i systemów zabezpieczenia.

Legenda:

Systemy elektroniczne które są niezbędne do prawidłowego funkcjonowania kancelarii do przetwarzania materiałów niejawnych między innymi:

- system kontroli dostępu – obejmujący elektroniczny system pomocniczy lub rozwiązanie organizacyjne, stosowany w celu zagwarantowania uzyskiwania dostępu do pomieszczenia lub obszaru, w którym są przetwarzane informacje niejawne, wyłącznie przez osoby posiadające odpowiednie uprawnienia,
- system sygnalizacji włamania i napadu – elektroniczny system pomocniczy stosowany w celu realizacji procedur ochrony informacji niejawnych oraz podwyższenia poziomu bezpieczeństwa, który zapewniają bariery fizyczne, a w pomieszczeniach i budynkach zastępujący lub wspierający personel bezpieczeństwa,
- system sygnalizacji pożaru – służący do wykrywania zagrożenia pożarowego, sygnalizowania i powiadamiania o zagrożeniu

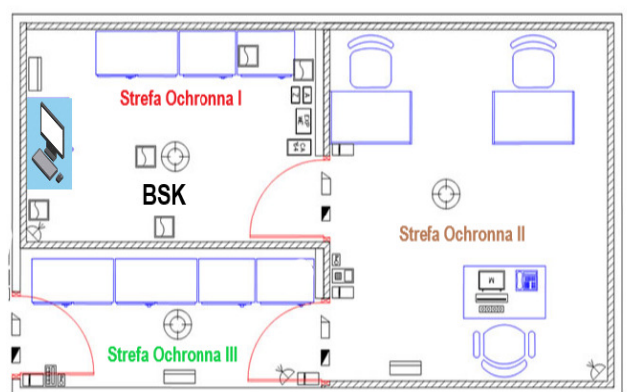
Strefy ochronne:

Strefa Ochronna I – pomieszczenie lub obszar w których informacje niejawne są przetwarzane w taki sposób, że wstęp do tego pomieszczenia lub obszaru umożliwia uzyskanie bezpośredniego dostępu do tych informacji. Wstęp możliwy jest wyłącznie ze strefy ochronnej.

Strefa Ochronna II – pomieszczenie lub obszar, w którym informacje są przetwarzane w taki sposób, że wstęp do tego pomieszczenia lub obszaru nie umożliwia uzyskania bezpośredniego dostępu do tych informacji. Wstęp możliwy jest wyłącznie ze strefy ochronnej.

Strefa Ochronna III – pomieszczenie lub obszar wymagający wyraźnego określenia granic, w obrębie których jest możliwe kontrolowanie osób.

BSK – Bezpieczne Stanowisko Komputerowe



Biorąc powyższe przepisy wynikające z obowiązujących aktów prawnych w celu stworzenia warunków do przetwarzania informacji niejawnych należy uwzględnić następujące warunki:

1. Konstrukcja pomieszczenia powinna charakteryzować się następującymi cechami:
 - ❖ zapewnić względną odporność na działania osoby nieuprawnionej próbującej uzyskać dostęp fizyczny lub za pomocą urządzeń elektronicznych;

- ❖ zapewnić wysoki poziom odporności na potajemne próby uzyskania nieuprawnionego dostępu;
 - ❖ zabudowa powinna być wykonana z cegły lekkiej o grubości 15 cm lub materiału o podobnej wytrzymałości albo ze spoiny oraz płyty gipsowej na ramie wspierającej;
 - ❖ drzwi i okna powinny spełniać co najmniej wymagania klasy 2 określone w Polskiej Normie PN-EN 1627;
 - ❖ drzwi winne być wyposażone w zamek spełniający co najmniej wymagania klasy 4 określone w Polskiej Normie PN-EN 12209;
 - ❖ okna nie muszą spełniać powyższych wymagań, jeżeli:
 - dolna krawędź okna znajduje się na wysokości przynajmniej 5,5 m nad gruntem lub innym elementem budynku (np. balkonem lub balustradą),
 - nie znajdują się na ostatnim piętrze,
 - w pobliżu nie znajduje się żaden element (np. rynna, drabina, drzewo) ułatwiający potencjalny dostęp i penetrację.
2. Kontrola dostępu powinna:
- ❖ posiadać elektroniczny automatyczny system kontroli dostępu o następujących cechach:
 - spełniać co najmniej wymagania systemu w klasie rozpoznania 2, a w klasie dostępu B – określone w normie PN-EN 50133-1,
 - wstęp kontrolowany jest przez odpowiednią barierę, która może wymagać bezpośredniego nadzoru uprawnionych osób,
 - obejmuje wszystkie wejścia i wyjścia kontrolowanego obszaru
3. Systemy sygnalizacji napadu i włamania powinien charakteryzować się następującymi cechami:
- ❖ spełniać co najmniej wymagania systemu stopnia 1 określone w normie PN-EN 50131-1;
 - ❖ obejmować ochroną miejsca, w których informacje niejawne są przechowywane i sygnalizuje co najmniej:
 - otwarcie drzwi do chronionego obszaru,
 - poruszanie się w chronionym obszarze (pułapkowo – nadzór nad wybranymi miejscami, w których występuje wysokie prawdopodobieństwo wykrycia).

II. Ochrona pracowników

1. Miejsce pracy pracownika recepcji/ochrony powinno uwzględniać bezpieczeństwo tych osób przed niespodziewanym wtargnięciem (atakami) oraz zapewnienie możliwości przetrwania niebezpiecznego zdarzenia i wezwania pomocy (wsparcia zewnętrznego) w przypadku wystąpienia zagrożenia:
 - ❖ bezpośredniego incydentu terrorystycznego,
 - ❖ podłożenia ładunku wybuchowego.
2. Obszar pracy pracownika recepcji/ochrony nie przewiduje bezpiecznego sortowania korespondencji wpływającej do PWM, w tym nie uwzględniają pełnej izolacji pomieszczenia oraz zapewnienia bezpieczeństwa pracownikom z pozostałych części budynku w przypadku (otrzymanie niebezpiecznej, podejrzanej przesyłki) np.:
 - ❖ wykrycia lub wystąpienia zdarzenia w postaci wycieku, wysypiania uwolnienia podejrzanej substancji (potencjalne skażenie niebezpiecznymi środkami chemicznymi lub niebezpiecznym materiałem biologicznym),
 - ❖ wykrycia potencjalnego improwizowanego niebezpiecznego urządzenia wybuchowego (materiały pirotechniczne bądź wybuchowe).
3. Brak odniesienia w dokumentacji projektowej do procedur postępowania w sytuacji wystąpienia zagrożeń wojennych np.:

- ❖ określających obszar bezpieczeństwa dla osób przebywających w obiekcie zapewniający doraźne miejsce ukrycie w budynku,
- ❖ zakresu rozwiązań projektowych oddzielających część biurowo-produkcyjną od części kawiarniano-koncertowej uniemożliwiające osobom postronnym przedostanie się i przebywanie w części biurowo-produkcyjnej w trakcie pracy księgarni, kawiarni, koncertu.