

w zakresie działania Pełnomocnika ds. Ochrony Informacji Niejawnych:

1. Zapewnienie ochrony informacji niejawnych, w tym stosowanie środków bezpieczeństwa fizycznego.
2. Zapewnienie ochrony systemów teleinformatycznych, w których są przetwarzane informacje niejawne.
3. Zarządzanie ryzykiem bezpieczeństwa informacji niejawnych, w szczególności szacowanie ryzyka.
4. Kontrola ochrony informacji niejawnych oraz przestrzegania przepisów o ochronie tych informacji, w szczególności okresowa (co najmniej raz na trzy lata) kontrola ewidencji, materiałów i obiegu dokumentów.
5. Opracowanie i aktualizowanie, wymagającego akceptacji kierownika jednostki organizacyjnej, planu ochrony informacji niejawnych w jednostce organizacyjnej, w tym w razie wprowadzenia stanu nadzwyczajnego i nadzorowanie jego realizacji.
6. Prowadzenie szkoleń w zakresie ochrony informacji niejawnych.
7. Prowadzenie zwykłych postępowań sprawdzających oraz kontrolnych postępowań sprawdzających.
8. Prowadzenie aktualnego wykazu osób zatrudnionych lub pełniących służbę w jednostce organizacyjnej albo wykonujących czynności zlecone, które posiadają uprawnienia do dostępu do informacji niejawnych, oraz osób, którym odmówiono wydania poświadczenia bezpieczeństwa lub je cofnięto.

w zakresie działania Kancelarii Materiałów Niejawnych:

1. Przyjmowanie, ewidencjonowanie i wysyłanie materiałów niejawnych.
2. Udostępnianie materiałów niejawnych osobom do tego upoważnionym.
3. Wydawanie materiałów niejawnych osobom do tego uprawnionym, które zapewniają odpowiednie warunki do ich przechowywania.
4. Egzekwowanie zwrotu materiałów niejawnych.
5. Nadzór nad obiegiem materiałów niejawnych.
6. Kontrola przestrzegania właściwego oznakowania i wytwarzania materiałów niejawnych.
7. Archiwizowanie materiałów niejawnych.

w zakresie działania Inspektora Bezpieczeństwa Teleinformatycznego:

1. Nadzór nad ochroną systemów i sieci teleinformatycznych przetwarzających informacje niejawne w Urzędzie.

2. Nadzór nad wprowadzaniem zaleceń Służb Ochrony Państwa dotyczących bezpieczeństwa teleinformatycznego.
3. Prowadzenie dokumentacji dot. bezpieczeństwa teleinformatycznego.
4. Opracowywanie szczegółowych zaleceń dotyczących ochrony fizycznej systemów i sieci teleinformatycznych wykorzystywanych do opracowywania dokumentów niejawnych.