

**Polityka bezpieczeństwa**

# **Polityka Bezpieczeństwa Firmy**

- **Polityka Bezpieczeństwa Firmy (PBF) jest zintegrowanym zbiorem ogólnych zasad i dyrektyw wewnętrznych w zakresie bezpieczeństwa. Odzwierciedla uregulowania obejmujące Centralę i oddziały Firmy.**
- **PBF ma charakter przymusowy, czyli żaden pracownik nie może działać inaczej bez specjalnej zgody kierownika jednostki organizacyjnej Firmy.**

# **Dyrektywy Generalne**

**Realizując PBF, we współpracy ze  
służbami bezpieczeństwa państwa,  
Pełnomocnik Ochrony – Dyrektor  
Biura Ochrony Firmy - dba o interes  
Firmy w zakresie bezpieczeństwa.**

# Pełnomocnik Ochrony

- Pełnomocnik Ochrony – Dyrektor Biura Ochrony - koordynuje działania Firmy w zakresie bezpieczeństwa.
- Dyrektor Biura Ochrony Firmy kieruje pionem ochrony - wyodrębnioną wyspecjalizowaną komórką organizacyjną Firmy

# **Pełnomocnik Ochrony zapewnia**

- ochronę informacji niejawnych,**
- ochronę systemów i sieci teleinformatycznych,**
- ochronę fizyczną Firmy,**
- koordynację ochrony fizycznej jednostek organizacyjnych,**
- kontrolę ochrony informacji niejawnych,**
- przestrzeganie przepisów o ochronie informacji niejawnych,**
- okresową kontrolę ewidencji materiałów i obiegu dokumentów,**
- opracowanie planów ochrony i nadzorowanie ich realizacji,**
- szkolenie pracowników banku w zakresie ochrony informacji niejawnych.**

# **Uzgodnienia przedsięwzięć Firmy**

**Wszyscy kierownicy jednostek organizacyjnych Firmy mają obowiązek uzgodnienia z Dyrektorem Biura Ochrony, na etapie planowania realizacji oraz kontroli, wszystkich przedsięwzięć organizacyjnych i działań dotyczących bezpieczeństwa. W szczególności uzgodnieniu podlegają:**

- 1. Infrastruktura Firmy: lokalizacja budynków, warunki najmu, architektura i budowa, infrastruktura techniczna.**
- 2. Systemy teleinformatyczne: lokalizacja, sprzęt i oprogramowanie, systemy zabezpieczeń.**
- 3. Współpraca z podmiotami zewnętrznymi świadczącymi usługi na rzecz banku.**
- 4. Inne sprawy bieżące wymagające uzgodnień w zakresie bezpieczeństwa.**

# **Bezpieczeństwo informacji**

- **Reguły związane z tworzeniem informacji**
- **Ogólne zasady obiegu i przechowywania informacji**
- **Proces niszczenia informacji**

# Dane osobowe

- **Informacje zawierające dane osobowe powinny podlegać ochronie jako informacje niejawne stanowiące tajemnicę służbową oznaczone klauzulą „zastrzeżone”.**
- **Zbiory danych osobowych powinny być tworzone i przetwarzane (w rozumieniu ustawy o ochronie danych osobowych), w sposób zapewniający zachowanie ich tożsamości i odrębności.**
- **W trakcie przetwarzania danych należy w szczególności zapewnić uzyskanie dokładnych informacji na temat ich udostępnienia (komu, kiedy, w jakim zakresie, w jakim celu, w jaki sposób, przez kogo) oraz niezwłoczne i zupełne zniszczenie danych nieaktualnych lub, gdy cel, w którym były przetwarzane, został osiągnięty.**

# **Odpowiedzialność za ochronę tajemnicy państwowej**

**Zgodnie z ustawą z 22 stycznia 1999 roku o  
ochronie informacji niejawnych osobą  
odpowiedzialną za ochronę tajemnicy  
państwowej i służbowej jest kierownik  
jednostki organizacyjnej, w której  
informacje niejawne są wytwarzane,  
przetwarzane, przekazywane lub  
przechowywane.**

# Ochrona informacji niejawnych w Firmie

- **Bezpieczeństwo systemów i sieci teleinformatycznych Firmy powinno być zapewnione przed przystąpieniem do przetwarzania informacji w danym systemie lub sieci.**
- **Obowiązujące zasady w tym zakresie zawarte są w Szczególnych Wymaganiach Bezpieczeństwa Systemów i Sieci Teleinformatycznych (SWB).**
- **Integralną częścią każdego eksploatowanego lub wdrażanego systemu teleinformatycznego powinien być podsystem ochrony, a jego formalnym uzupełnieniem są Procedury Bezpiecznej Eksploatacji (PBE).**

# **Bezpieczeństwo teleinformatyczne**

- **1. Organizacja i administracja bezpieczeństwem systemów i sieci teleinformatycznych**
- **2. Bezpieczeństwo fizyczne systemów i sieci teleinformatycznych**
- **3. Bezpieczeństwo sprzętu i oprogramowania**
- **4. Bezpieczeństwo personelu**
- **5. Bezpieczeństwo dokumentów**
- **6. Bezpieczeństwo łączności teleinformatycznej**
- **7. Zabezpieczenie antywirusowe**
- **8. Plany awaryjne i zapobiegawcze (zailanie, kopie zapasowe)**
- **9. Szkolenia i ćwiczenia**

# Regulacje prawne

- Ustawa o ochronie danych osobowych z 29 sierpnia 1997
- Zgłoszenie bazy do GIODO
- Rozporządzenie MSWiA z 29 kwietnia 2004 w sprawie dokumentacji przetwarzania danych osobowych
  - **Dane osobowe:** wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej
  - **Co identyfikuje?** Cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe bądź społeczne lub nr identyfikacyjny np. PESEL
  - **Zgoda** na przetwarzanie musi być dobrowolna

# **Bezpieczeństwo osób i mienia**

- **Przedmiot bezpieczeństwa.**
- **Obowiązki osób funkcyjnych.**
- **Ochrona fizyczna**
- **Techniczne zabezpieczenie budynków**
- **System zabezpieczeń technicznych w Firmie**
- **Zabezpieczenia zewnętrzne**
- **Zabezpieczenia wewnętrzne**