經濟部智慧財產局
INTELLECTUAL PROPERTY OFFICE

「營業秘密法」簡介

營業秘密立法目的

維護產業倫理與競爭秩序

調和社會公共利益

什麼是營業秘密？

Definition

營業秘密，係指方法、技術、製程、配方、程式、設計或其他可用於生產、銷售或經營之資訊，而符合下列要件

非一般涉及該類資訊之人所知者

因其秘密性而具有經濟價值者

所有人已採取合理之保密措施者

營業秘密的要件

三要件

非一般涉及該類資訊之人所知

具有實際或潛在之經濟價值

所有人已採取合理之保密措施

營業秘密的三要件

秘密性

- 秘密性之判斷，係採業界標準，除一般公眾所不知者外，**相關專業領域中之人亦不知悉**。

營業秘密的三要件

經濟性

- 所謂經濟性者，指可用於**生產**、**製造**、**經營**、**銷售**之資訊，亦即可以**產出經濟利益**或**商業價值**之資訊
- **經由投注人力、財力，經過篩選整理之資訊**，且**非可自其他公開領域取得**者，例如**客戶之個人風格、消費偏好**等，**足認係具有經濟價值**之營業秘密

營業秘密的三要件

合理保密措施

- 主觀上有保護之意願
- 客觀上有保密的積極作為

- **所有人按其人力、財力，依社會通常所可能之方法或技術，將不被公眾知悉之情報資訊，依業務需要分類、分級而由不同授權職務等級者知悉**
- 判斷是否已達合理保密措施之程度：
  - **具體個案**中，**視該營業秘密之種類、事業實際經營及社會通念而定**
  - **審查時**，不採嚴格之保密程度，解釋上**已達任何人以正當方法無法輕易探知之程度**，即可認定具備合理之保密措施
  - 合理保密措施必須「有效」，惟不須達「滴水不漏」之程度

營業秘密的三要件

合理保密措施

- 主觀上有保護之意願
- 客觀上有保密的積極作為

- 合理保密措施之例：
  - 可能接觸該營業秘密之員工簽署**保密合約**
  - 於**文件上標明「機密」或「限閱」**等註記
  - 將機密文件分類分級，對**接觸**該營業秘密者加以**管制**
  - **資料予以上鎖、設定密碼**
  - 保全措施（如**限制訪客**接近存放機密處所）

營業秘密權利歸屬

職務上研究開發

- 原則上歸雇用人所有，但契約另有約定者，從其約定
- 受雇人於非職務上研究或開發之營業秘密，歸受雇人所有。但其營業秘密 係利用雇用人之資源或經驗者，雇用人得於支付合理報酬後，於該事業使用其營業秘密

出資聘請

- 依契約約定，契約未約定者，歸受聘人所有，但出資人得於業務上使用其營業秘密

共同研究開發

- 數人共同研究或開發之營業秘密，其應有部分依契約之約定；無約定者， 推定為均等

侵害營業秘密之民事責任

侵害營業秘密之行為態樣：

以竊盜、擅自重製、違反保密義務等不正當方法取得營業秘密

知悉或因重大過失而不知其為前款之營業秘密，而取得、使用或洩漏

取得營業秘密後，知悉或因重大過失而不知其為第一款之營業秘密， 而使用或洩漏

因法律行為取得營業秘密，而以不正當方法使用或洩漏

依法令有守營業秘密之義務，而使用或無故洩漏

侵害營業秘密之民事責任

侵害營業秘密之責任：

- 排除或防止侵害請求權
- 負損害賠償責任
- 計算損賠金額之方式

侵害營業秘密之刑事責任

侵害營業秘密之行為態樣

- 以竊取、侵占、詐術、脅迫、擅自重製或其他不正方法而取得，以及取得後之使用或洩漏
- 未經授權或逾越授權範圍而重製、使用或洩漏
- 經告知應刪除、銷毀，而不為刪除、銷毀或隱匿該營業秘密
- 惡意轉得人之取得、使用或洩漏

處罰刑度

- 5年以下有期徒刑或拘役，得併科新臺幣100萬元以上1千萬元以下罰金。犯罪所得利益超過罰金最高額時，得於所得利益3倍範圍內酌量加重

不法行為態樣一

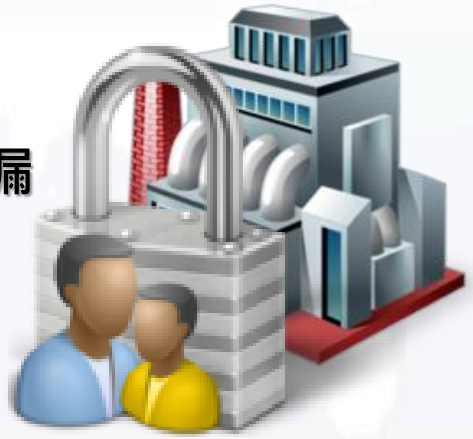
商業間諜行為：任何人

竊取、侵占、詐術、脅迫、擅自重製、其他不正方法

營業秘密

不法取得

不法使用、洩漏



不法行為態樣二

知悉或持有營業秘密者

不法行為態樣三

持有營業秘密者

營業秘密

合法取得

持有營業秘密者

經所有人告知
應刪除、銷燬

不為刪除、銷燬
或為隱匿

不法行為態樣四

惡意轉得人

不法取得
不法使用、洩漏

營業秘密

合法取得
嗣後不法重製、使用、洩漏、持有

惡意轉得人

不法取得、使用、洩漏

域外加重處罰

行為人不法取得我國人營業秘密，其意圖在國外使用者，加重處罰

1年以上10年以下有期徒刑
3百萬以上5千萬元以下罰金

所得利益超過罰金最高額時，得於所得利益2至10倍內加重

告訴相關規定

一般營業秘密罪，告訴乃論

- 告訴可分
- 對於共犯之一人告訴或撤回告訴者，其效力不及於其他共犯

域外加重，非告訴乃論

公務員犯罪加重其刑

刑事罰併同處罰

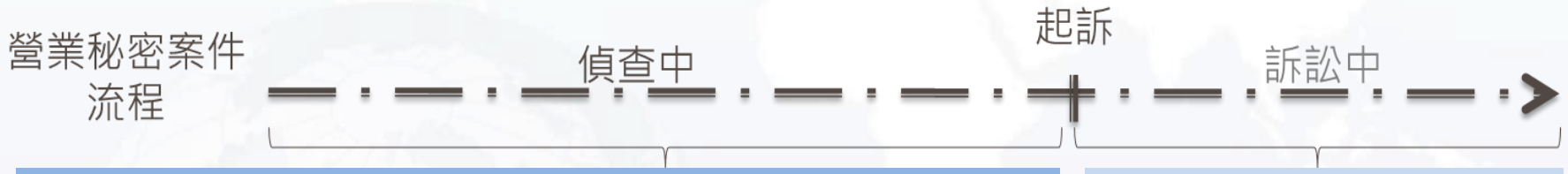
Definition

法人之代表人、代理人、受雇人或其他從業人員，因執行業務犯本法之罪者，其所屬法人及自然人雇主等對該犯罪之發生，未盡力為防止行為者，對該法人或自然人雇主處以罰金

109.1.15引進「偵查保密令」制度 (1/2)

◆106.2經濟部智慧局舉辦「營業秘密法增訂**刑事責任**4週年成效檢討會議」，產業建議：

1. 偵查應**儘速偵結**，審判應速審速結
2. 引進**偵查中**之**保密令制度**，課予**保密義務**



◆無保密令制度之實務困難

- 企業**擔心**營業秘密**外洩之風險**
- 確保**偵辦過程**中接觸偵查內容之人**保密**，實務執行**有困難**

智財案件審理法-秘密保持命令

109.1.15引進「偵查保密令」制度 (2/2)

§14-1 核發規定

- 檢察官依**職權核發**
- 對象：接觸偵查內容之人
- 禁止行為
  - 不得為訴訟外程序使用
  - 不得揭露予未受偵保令之人

§14-2 形式及生效規定

- 書面或言詞為之
- 以書面為之，送達生效；以言詞為之，自告知生效
- 偵保令應記載事項

§14-3 偵保令之撤銷、變更配套制度

- 偵查中及偵查終結未起訴者，由檢察官撤銷或變更之
- 起訴後，起訴效力所及之偵保令，由法院確認其效力

§14-4 違反偵保令之刑事責任

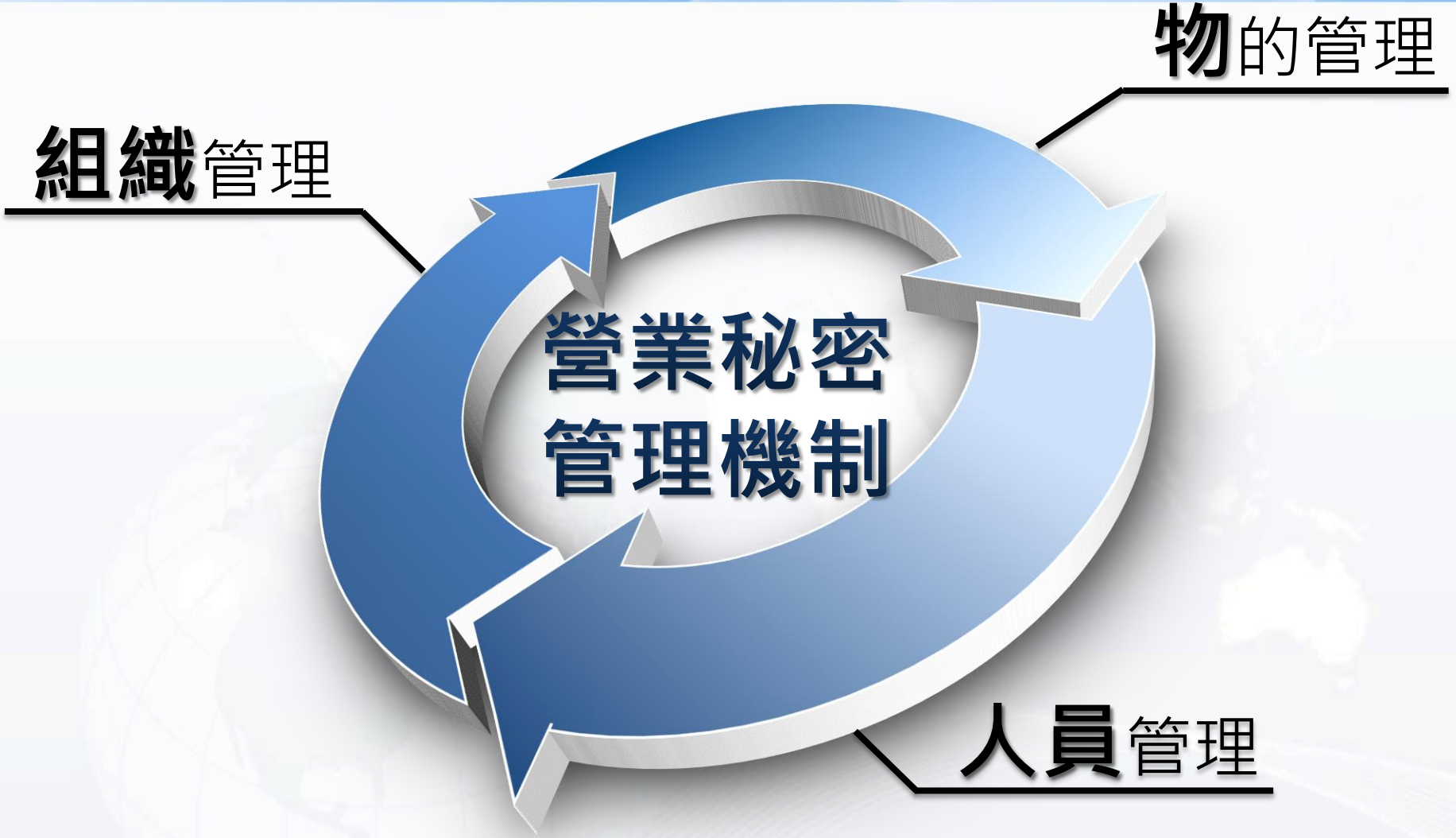
- 違反者可處**3年**以下有期徒刑或併科**100萬元**以下罰金
- 於外國、大陸地區、香港或澳門違反偵保令者，亦適用之

外國人營業秘密之保護

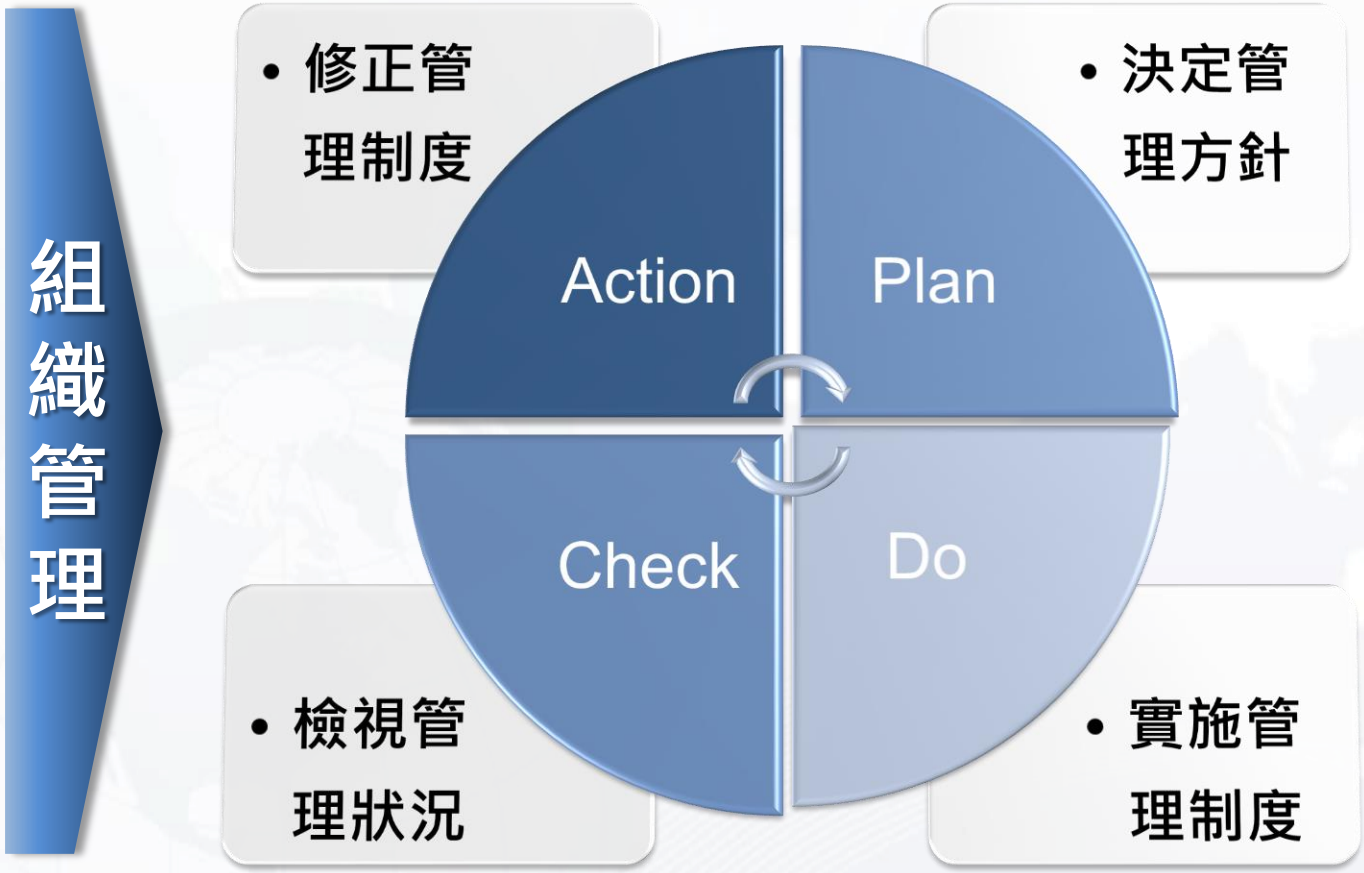
- **互惠原則** (第15條)
  - 外國人所屬之國家與中華民國如未共同參加保護營業秘密之國際條約或無相互保護營業秘密之條約、協定，或對中華民國國民之營業秘密不予保護者，其營業秘密得不予保護

- **未經認許之外國法人**，就本法規定事項得為告訴、自訴或提起民事訴訟 (第13條之5)
  - 外國法人如未經我國認許，並未取得法人資格，依司法院院字第533號解釋認為無提自訴之權，其營業秘密受侵害時，即無法循法律途徑尋求救濟，殊有礙於國際貿易之促進，且不利跨國公司來臺投資，爰參照商標法第99條、著作權法第102條、專利法第102條之規定，增訂未經認許之非本國法人得為訴訟主體

營業秘密管理機制之建立(1/11)



營業秘密管理機制之建立(2/11)



營業秘密管理機制之建立(3/11)

工作守則

確認職務範圍
注意勞動法規
不得洩密義務

教育訓練

課程研習內容
設置專責人員
善用集會場合

契約管理

簽屬保密協定
競業禁止約定

營業秘密管理機制之建立(4/11)

契約管理

簽署保密協定

- 簽署對象
  - 在職員工 + 離職員工
- 簽署時機
  - 進公司時
  - 在職中
  - 離職時
- 簽署內容
  - 營業秘密範圍界定
  - 保密義務及附隨義務
  - 保密期間
  - 違反義務時之處理

競業禁止約定

- 競業限制內容不得超出合理範圍

營業秘密管理機制之建立(5/11)

工作守則

確認職務範圍

- 應明確告知員工之職務範圍，並載明業務處理程序及方式
- 對有撰寫工作日誌必要之員工，亦應明白告知相關記錄方式

注意勞動法規

- 企業於工作守則中規定員工之保密義務時，應注意不得違反勞動相關法規，增刪修改相關規定時亦同

不得洩密義務

- 工作守則中亦應明定，即便非屬自己業務範圍內的機密事項，員工亦負有不得將該秘密外洩之義務

營業秘密管理機制之建立(6/11)

教育訓練

課程研習內容

- 營業秘密管理的重要性
- 管理組織的概要
- 具體的管理規則
- 機密洩漏後之適當處理方式

設置專責人員

- 選定適合的教育研習負責人，專門負責規劃教育研習的課程內容、製作各式教材、挑選適當講師及評估員工學習成效，將教育責任明確化，將有助於此項業務之推展與專業化

善用集會場合

- 應善用各類員工集會場合(如晨會或工作會議)，隨時提醒員工注意營業秘密管理相關事項
- 如有營業秘密相關之新聞報導或重大時事，亦可公告週知，並藉機告知員工正確處理方式

營業秘密管理機制之建立(7/11)

1.資訊密等之區辨與標示

2.設備管制

物的管理

4.電腦系統管理

3.區域控管

營業秘密管理機制之建立(8/11)

為使接觸企業內部資訊之人，能清楚認識接觸之文件內容是否為機密，應落實加註機密等級之措施

資訊密等之區辨與標示

具體作法

- 機密文件可以依重要性及機密程度區分不同等級
  - **紙本文件**：標籤or卷宗or戳記
  - **電子檔案**：USB標籤加密
- 機密文件與其他一般性文件應分別存放及保管

營業秘密管理機制之建立(9/11)

設備管制

紙本機密文件之控管

- 將紙本機密文件存放於保險櫃中，由專門人士負責管理，管理者有輪調或更替之情況時，應確實辦理交接工作，並同時更換相關設備之密碼

電子機密檔案之控管

- 一般機密檔案→可儲存於負責員工之電腦，但應加密並定期更換密碼
- 重要機密檔案→僅開放於特定電腦開啟或操作，且非經一定層級以上主管之授權，不得開放下載之權限或功能，並應限制得接觸該電腦之員工身分

限制機密文件資料之處理

- 限制機密文件資料之存取、下載、複製、回收及銷毀，配置專責人員，職司紀錄機密文件資料或檔案卷宗存取、下載、複製、回收及銷毀之時間、流向與次數

採取不可回復之措施

- 紙本機密文件→應落實回收銷毀之機制
- 電子機密文件→採取不可回復之刪除銷毀措施

營業秘密管理機制之建立(10/11)

區域控管

場所區隔

- 保管營業秘密之場所應與一般場所 有所劃分，以茲區隔與辨識
- 可於保密場所之特定範圍內，於明顯位置張貼或設置警語標示

設置保全

- 保管場所應配置全天候輪班的保全人員，並落實出入管理登記制度
- 無足夠經費聘請保全人員，至少應裝設保全系統或監視錄影器

認證系統

- 保管場所應加裝高科技的認證系統，例如使用IC卡認證、指紋辨識認證、虹膜辨識認證等

貴賓接待

- 櫃檯總機人員應將外來洽公人士引導至貴賓接待室或會議室等待，避免其進入公司辦公核心區域

營業秘密管理機制之建立(11/11)

電腦系統管理

訂定網路連線管理規則

- 將電子郵件內容及備份資料編碼化，並以書面明確記載資料複製或備份之步驟，以便後續查驗或稽核

加密限制

- 設定電腦或檔案之登入密碼，且密碼設定的強度亦應予以要求，禁止同一或類似的密碼重複使用

強化入侵防禦

- 應設置防火牆及防毒軟體，以防範電腦病毒之惡意攻擊；存有營業秘密之電腦，不可任意安裝不必要的軟體

認證系統

- 登入電腦或網路伺服器時，要求使用IC卡認證、指紋辨識認證等認證系統，並在該系統上加入PIN輸入功能