



# 營業秘密保護實務教戰手冊 3.0



經濟部智慧財產局 編

中華民國 111 年 8 月

## 目錄

序言 .....	1
第一章 認識營業秘密 .....	3
壹、營業秘密為什麼重要.....	3
貳、什麼是營業秘密.....	3
第二章 企業保護營業秘密的策略步驟.....	11
壹、最高管理階層應有明確的政策聲明與支持.....	12
貳、建立營業秘密保護管理政策.....	14
參、盤點機密資訊，分級分類與標示.....	15
肆、員工管理.....	17
伍、紙本及電子檔案管理.....	19
陸、區域空間與設備的管理.....	21
柒、稽核與改善.....	23
捌、教育訓練與宣導.....	24
玖、協力廠商與產學合作的管理.....	25
拾、與公部門及司法警察建立良好互動.....	26
第三章 營業秘密發生洩密之因應 .....	27
第四章 CEO 帶領成功企業的經驗分享 .....	33
第五章 營業秘密 Q & A.....	40
附錄一：企業營業秘密資訊簡易盤點表 .....	1

# 序言

隨著國際商業活動日趨複雜，跨國企業競爭態勢愈顯激烈，為妥善保障產業倫理及市場公平競爭秩序，營業秘密有以法律強化保護之必要，保護強度日益升高亦為趨勢。

我國營業秘密法於民國 85 年 1 月 17 日制定公布，至 101 年因企業界對近年來層出不窮之營業秘密侵害案件，嚴重戕害產業競爭力一事，向政府發出修正營業秘密法、增訂刑事責任之迫切呼籲，希望透過修法手段有效遏阻營業秘密侵害案件，以強化我國產業營業秘密之保護，建立公平競爭之市場環境。隨後，經召開跨部會研商會議，邀集相關機關、專家學者及企業代表研商，由經濟部智慧財產局(以下稱智慧局)提出修正草案，並於立法院獲得高度共識，營業秘密法增訂刑事責任之修正案於 102 年 1 月 11 日立法院三讀通過，並於 102 年 1 月 30 日修正公布，2 月 1 日施行。

106 年 2 月智慧局召開「營業秘密增訂刑事責任成效檢討會議」，邀請產、官、學共同與會討論，會中產業界表示，營業秘密法雖法制面已臻完善，但司法實務之執行面則需再加強，希望營業秘密案件「速偵速審」，並建議引進「偵查保密令」制度，以減緩當事人擔心營業秘密可能於偵辦過程中再次洩露，而不願意提供相關事證資料給檢調人員釐清案情，導致影響營業秘密侵害案件偵辦效率。

為回應產業建言及需求，107 年推動修法，經協調產業界、法務部及司法院意見，獲立法院支持於 108 年 12 月 31 日三讀通過營業秘密法引進「偵查保密令」制度，並於 109 年 1 月 15 日修正公布，1 月 17 日施行。

為協助企業建構更完善營業秘密保護機制，智慧局每年與台灣營業秘密保護促進協會於北、中、南合作辦理「企業營業秘密合理保密措施研討會」，宣導企業建置營業秘密合理保密措施，分享建置合理保密措施經驗之成功典範；近年另編製「中小企業營業秘密保護機制檢核表」，設計 67 項檢核指標，讓企業可按表檢核；「中小企業合理保密措施 SOP」，整理企業保護營業秘密的 7 大策略步驟；設計生動活潑的「營業秘密保護宣導短片、懶人包」等，以協助企業完善營業秘密保護制度。

自智慧局 102 年編製「營業秘密保護實務教戰手冊」、108 年更新教戰手冊 2.0 以來，持續汲取企業之成功保密經驗，追蹤我國營業秘密之司法實務見解及發展趨勢；今年再次重新編纂本手冊，更納入 CEO 帶領成功企業的經驗分享等新視角，希望提供各界更實用之具體作為，做為企業推展營業秘密保護制度之重要參考。

# 第一章 認識營業秘密

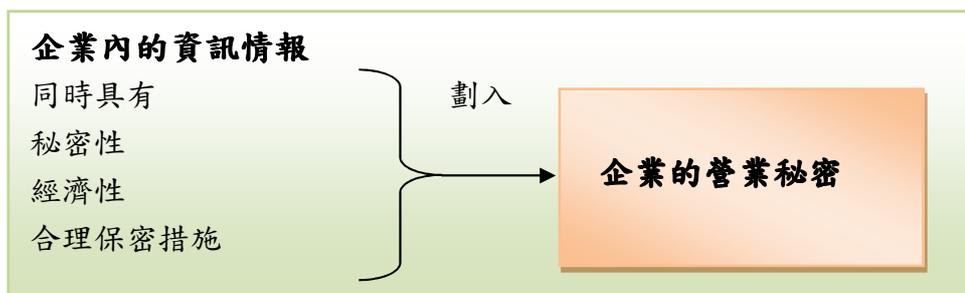
## 壹、營業秘密為什麼重要

隨著經濟全球化的發展，技術、人才等生產要素跨國的流動頻繁，企業面對激烈的競爭，應更重視對營業秘密的保護，一方面可避免重要技術被別人輕易竊取，另一方面，可確保競爭的優勢。例如：知名飲料公司可口可樂，一直就是以營業秘密來保護飲料配方不被公開，特殊口味至今尚無公司可製造出來，所以可口可樂公司可以維持長久的優勢競爭力。但是，如果可口可樂並未以營業秘密來保護飲料配方，可能就沒有今日龍頭地位與豐厚獲利，因為其他公司如果得知配方後，也能販賣一模一樣的飲料了！

因此，營業秘密非常重要，企業想要取得制勝的關鍵，維持自身競爭，就必須將營業秘密當作企業重要的資產，並加以管理保護。

## 貳、什麼是營業秘密

企業想將營業秘密當作重要資產來加以保護，首先要從眾多企業內部的資訊情報中，弄清楚什麼是自身的營業秘密，盤點出符合要件的資訊，才能劃入營業秘密的範圍。



什麼是營業秘密呢？

依營業秘密法第 2 條規定，營業秘密就是方法、技術、製程、配方、程式、設計或其他可用於生產、銷售或經營的資訊等，並且同時要符合「非一般涉及該類資訊之人所知者」（秘密性）、「因其秘密性而具有實際或潛在之經濟價值者」（經濟性）以及「所有人已採取合理之保密措施者」之三個要件<sup>1</sup>，以下就三要件分述如下：

### 一、秘密性

所謂秘密性，必須是其他人難以得知的資訊，如果在網路即可查詢到，或是業界其他人已知道的資訊，不屬於營業秘密。

「司法實務見解」

#### ● 相對秘密概念

所謂「秘密性」，屬於相對秘密概念，知悉秘密之人固不以一人為限，凡知悉者得以確定某項資訊之詳細內容及範圍，具有一定封閉性，秘密所有人在主、客觀上將該項資訊視為秘密，除一般公眾所不知者外，相關專業領域之人亦不知悉者屬之。（最高法院 107 年台上字第 2950 號）

#### ● 與發明專利應具備之絕對新穎性及進步性之要件有別

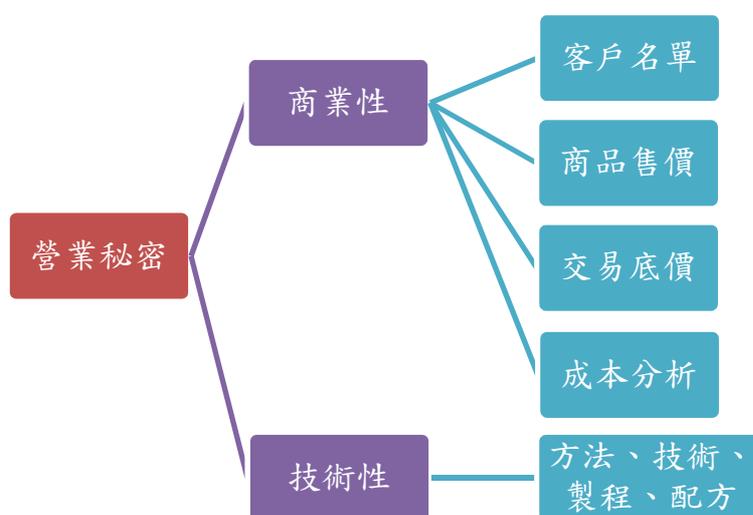
營業秘密為資訊之一種，倘非他人所公知，且無法以正當方法輕易確知，即該當「非一般涉及該類資訊之人所知」之要件，此與發明專利應具備之絕對新穎性（未構成先前技術之一部）及進步性（非該發明所屬技術領域中具有通常知識者，依申請前之技術所能輕易完成）之要件有別。（最高法院 108 年台上字第 36 號）

秘密性，與專利之「絕對新穎性」不同，營業秘密之秘密性係屬相對性概念，其所要求者僅為最低程度之新穎性，只要是「非一般涉及該類資訊之人所知者」即足當之，故一項營業秘密可能只是比一般知識、技法，多了一點技術上的先進性，或略為超過普通常識而已，且

<sup>1</sup> 營業秘密法第 2 條：「本法所稱營業秘密，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，而符合左列要件者：一、非一般涉及該類資訊之人所知者。二、因其秘密性而具有實際或潛在之經濟價值者。三、所有人已採取合理之保密措施者。」

除了少數很明顯得知的情事外，原則上不應允許將多項先前技術之技術內容加以組合，以證明某項技術資訊不具秘密性，故與專利不具進步性（基於先前技術能輕易完成）之無效抗辯亦不相同。（新竹地院108年智訴字第4號）

常見企業內部之營業秘密，可以概分為「商業性營業秘密」及「技術性營業秘密」二大類型，二者因為性質不同是否符合「秘密性」條件不盡相同，以下摘錄法院判決之實務見解供參考。



### （一）商業性營業秘密

所謂「商業性營業秘密」，主要包括企業之客戶名單、經銷據點、商品售價、進貨成本、交易底價、人事管理、成本分析等與經營相關之資訊。而此等資訊是否具備秘密性，依法院之實務見解，應視該等資訊是否可以從公開管道輕易得知，或企業是否就其另投入相當之人力財力為進一步之整理、分析，而使之成為企業經營上之重要資訊而定。

「司法實務見解」

#### ● 客戶名單

倘係經投注相當之人力、財力，並經過篩選整理，始獲致客戶名單之

資訊，且該資訊非可從公開領域取得，例如：客戶之個人風格、消費偏好、歷史交易紀錄、特定行銷通路及貿易條件等，應屬營業秘密。(臺北地院 96 年勞訴字第 35 號)

若僅表明名稱、地址、連絡方式之客戶名單，可於市場上或專業領域內依一定方式查詢取得，且無涉其他類如客戶之喜好、特殊需求、相關背景、內部連絡及決策名單等經整理、分析之資訊，即難認有何秘密性及經濟價值(最高法院 99 年台上字第 2425 號)

- 公司安排業務人員行銷區域配置、產品線等資訊

附表一編號 4 之檔案內容為告訴人自成立以來，投入諸多人力、時間、物力所陸續整理編輯而成，不僅是蒐集整理公司業務員名單或個人資料而已，更進一步分析比對出每位業務人員所負責工作之國內外區域及分布比例、產品線、客戶名單等重要資訊，取得此等資訊顯然得以窺知告訴人係如何於國內外市場安排行銷人員及其各種產品行銷之區域配置與客戶比例多寡，更可得悉告訴人公司每位業務員負責行銷之客戶有誰，此為告訴人所獨有之商業機密，並無法於市場公開領域或專業市場上查知，更非一般公眾所知或告訴人競爭者可以知悉之資訊，堪認此檔案具有秘密性。(智財法院 107 年刑智上訴字第 43 號)

- 商品售價

上訴人開發業務與合作客戶簽約後，所取得之資料為企業之內部資料，並無對外公開之事實，非一般涉及該類資訊之人所能得知，內容包含客戶聯繫資訊、客戶需求之產品規格、售價、成本及銷售資料，具有實際及潛在經濟價值，且均儲存於上訴人法定代理人之個人電腦，並非上訴人所共用資訊，而非第三人可輕易使用，足認已採取合理保密措施等項目所示資訊，均具有秘密性、經濟價值及合理保密措施等營業秘密要件，即應受營業秘密之保護。(智財法院 105 年民營上更(一)字第 1 號)

- 成本分析

產品之報價或銷售價格，如不涉及成本分析，而屬替代性產品進入市場進行價格競爭時，得自市場中輕易獲取之資訊，並非營業秘密。(最高法院 102 年台上字第 235 號)

## (二)技術性營業秘密

所謂「技術性營業秘密」，係指與特定產業研發或創新技術有關之機密，包括方法、技術、製程及配方等資訊，此等技術性資訊是否具有秘密性，以及是否專屬於特定公司所有，因其他同業公司均無該等技術，故須由主張該技術性資訊為營業秘密之公司，提出具體之證據或說明。

#### 「司法實務見解」

##### ● 醫美技術

原告主張其所經營之肉毒桿菌素、玻尿酸等醫療項目，因注射之劑量、方式、療程和使用之配方及相關措施不同，而屬營業秘密。惟現今醫美市場蓬勃發展，醫美事業經營上開醫療項目者已非少數，原告未能證明其上開醫療措施較諸一般醫美事業所實施者有何優異之處，亦未證明其配方等資訊並非一般人所知者，則其空言主張有應受保護之營業秘密，殊非可採。(士林地院 100 年重勞訴字第 2 號)

##### ● 產品設計圖面及材料清單

本案標示「confidential」字樣之雷射○○○○機光學鏡組基座第○號細部設計圖及材料清單、第○號細部設計圖說及產品報價單、○○○○桿相關成本及報價、雷射○○○○機等紙本維修操作手冊及相關圖面，均為日本總公司集中控管，倘技術部工程師維修、管理部為處理客戶端詢問售價而有閱覽需求，均須向日本總公司說明事由並請示核准後，始能加以取得等情甚詳，堪認本案細部設計圖、材料清單等文件係○○公司為獲取客戶訂單，經○○公司及日本總公司投入相當人力、經費等資產研發後所取得，嗣後亦經客戶認同而應用於其等銷售之商品上，統一由日本總公司加以管理，自非屬業務可輕易取得之資訊或一般人可任意取得之資料。(臺中法院 109 年智訴字第 13 號)

##### ● 配方研發資訊

前述檔案二所揭示之技術內容，並非僅有被告所稱各化學物質之基礎功能，尚包括將特定供應商提供之化學物質商品應用於其特定研磨液產品、適用於何種（晶圓）表面材料等技術資訊，該等資訊應係告訴人○○公司於其產品研發、試誤等過程中累積經驗始能獲致之知識，而被告所提之證據或說明，不足以證明檔案二之技術內容為已經揭露之技術或業界習知之資訊，自應認定檔案二具有秘密性。(新竹地院 108 年智訴字第 4 號)

## 二、經濟性

所謂經濟性，必須是該資訊因秘密性而對企業具有實際或潛在之經濟價值而言。依司法實務之見解，企業於研發過程投入之成本、實際市場占有率或銷售額之減損，乃至可能影響競爭力，或是未來能為企業創造的產值或收益，皆屬經濟性要件評估之標的。

「司法實務見解」

### ● 帶來有形之金錢收入、經濟利益或競爭優勢

所謂經濟價值，係指某項資訊經過時間、勞力、成本之投入所獲得，在使用上不必依附於其他資訊而獨立存在，除帶來有形之金錢收入，尚包括市占率、研發能力、業界領先時間等經濟利益或競爭優勢者而言。他人擅自取得、使用或洩漏之，足以造成秘密所有人經濟利益之損失或競爭優勢之削減。(最高法院 107 年台上字第 2950 號)

### ● 投入人力、物力而為資料蒐集及整理分析

又客戶資訊之取得如係經由投注相當之人力、財力，並經過篩選整理而獲致之資訊，且非可自其他公開領域取得者，例如個別客戶之個人風格、消費偏好等，固足認係具有實際或潛在的經濟價值之營業秘密。惟若係於市場上公開之資訊，一般人均可由工商名冊任意取得，其性質僅為預期客戶名單，與所謂「營業秘密」並不相當。(最高法院 104 年台上字第 1654 號)

系爭「客戶交接清冊」、「○○業務經驗分享」資料不僅係被上訴人就其客戶資料加以蒐集而已，尚涉及被上訴人客戶承辦人員之聯絡方式、客戶特殊需求、商機評估等重要商業機密資料，並經被上訴人整理歸納及研討分析後始得資料結果，核屬被上訴人投入大量人力、物力等成本後，透過資料蒐集及整理分析，堪認具有重要經濟價值。(臺灣高等法院 104 年上易字第 1052 號)

### ● 有利企業取得訂約機會

如以競爭對手之商品交易價格資訊(報價)為基礎而同時為較低金額之報價，俾取得訂約機會，因違反營業秘密法第一條所規定維護產業倫理或競爭秩序之法目的，應認該商品交易價格資訊具有經濟價值。由○○公司支付酬勞引誘楊○○竊取系爭商品交易價格資料，並使用

該資料以取得系爭產品之訂單，因此致被上訴人之訂單流失，認定資料資料有經濟價值。(最高法院 106 年台上字第 441 號)

- **節省學習時間或減少錯誤**

持有營業秘密之企業較未持有該營業秘密之競爭者，具有競爭優勢或利益者。就競爭者而言，取得其他競爭者之營業秘密，得節省學習時間或減少錯誤，提昇生產效率，即具有財產價值，縱使試驗失敗之資訊，仍具有潛在之經濟價值。(智財法院 106 年民營上字第 1 號)

- **不因有無實際使用資訊而影響其經濟價值之判斷**

有關經濟性，即產業上利用價值部分，此「經濟性」要求較寬，僅具有潛在之經濟價值者亦屬之，不因○○公司有無實際使用而受影響。即使是○○公司多年前推出的低階產品，只要市場上仍然有需要，市場上還有公司繼續生產此種產品，該資訊仍有一定利用價值。(彰化地院 107 年智訴字第 3 號)

### 三、合理保密措施

企業必須採取合理的保密措施，使人了解企業有將該資訊當成機密加以保護的意思，例如設定網路防火牆、電腦密碼等，若企業未採取合理保密措施，讓人可輕易接觸或取得機密資訊，就不是營業秘密。

「司法實務見解」

- **分類分級及授權**

按營業秘密法第 2 條第 3 款規定「所有人已採取合理之保密措施」，應係指所有人按其人力、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、分級而由不同之授權職務等級者知悉而言，此於電腦資訊之保護，就使用者每設有授權帳號、密碼等管制措施，尤屬常見(最高法院 102 年台上字第 235 號)

- **採取保密措施必須「有效」，但不要求須滴水不漏**

(一)所謂「合理之保密措施」，係指營業秘密之所有人主觀上有保護之意願，且客觀上有保密的積極作為，使人了解其有將該資訊當成秘密加以保守之意思。

- (二) 所有人所採取之保密措施必須「有效」，方能維護其資訊之秘密性，惟並不要求須達「滴水不漏」之程度，只需所有人按其人力、財力，依其資訊性質，以社會通常所可能之方法或技術，將不被該專業領域知悉之情報資訊，以不易被任意接觸之方式予以控管，而能達到保密之目的，即符合「合理保密措施」之要求，例如：對接觸該營業秘密者加以管制、於文件上標明「機密」或「限閱」等註記、對營業秘密之資料予以上鎖、設定密碼、作好保全措施（如限制訪客接近存放機密處所）等綜合判斷之。
- (三) 而是否採取合理之保密措施，不以有簽署保密協議為必要，若營業秘密之所有人客觀上已為一定之行為，使人了解其有將該資訊作為營業秘密保護之意，並將該資訊以不易被任意接觸之方式予以控管，即足當之，反之若簽署保密協議，惟任何人均得輕易接觸該等資訊，縱有保密協議之簽署，亦難謂營業秘密所有人已採取合理之保密措施。（智財法院 107 年刑智上訴字第 24 號）

● **以正當方法無法輕易探知**

判斷是否已達合理保密措施之程度，應在具體個案中，視該營業秘密之種類、事業實際經營及社會通念而定之。而審查營業秘密所有人之保密措施時，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。（智財法院 105 年民秘聲上字第 5 號）

● **依公司規模、人力、財力而採取合理保密措施**

被上訴人為資本額 500 萬元之中小型企業，員工人數僅十數人，被上訴人對於報價單之內容已限制僅少數人可接觸，對於被上訴人公司電子信箱，亦透過限制使用人員及設定密碼方式加以保護，並與員工簽訂到職切結書及離職切結書，課予員工保密義務，應認已採取合理之保密措施，縱使系爭電子信箱之密碼與公司名稱或傳真號碼有關，亦非一般人可輕易得知，又電子信箱如有定期更換密碼，固可提高安全性，惟不能因此反面推論，如未定期更換密碼，即與未設保密措施無異。（智財法院 108 年民營上易字第 1 號）

## 第二章 企業保護營業秘密的策略步驟

營業秘密是企業最重要的競爭力，企業應該有一套保護營業秘密的策略步驟，以防止洩露為目的，且從企業整體保護制度之建置開始，必須是系統性的策略，同時考量機密資訊的重要性、管理策略及營運效能衡平、投入資源等，以達營業秘密保護之目的。

另外，在營業秘密管理之政策，除了要確保自家公司的營業秘密免遭受侵害，更進一步也要避免侵害到別人的營業秘密，或自家公司研發的技術被污染，例如公司新進員工不當將前雇主之營業秘密帶入公司內部使用，若公司漠視其發生或有意促成員工攜帶前雇主之營業秘密帶槍投靠，且用於公司之產品開發、營運等相關業務，公司則有未盡監督管理責任之虞，依營業秘密法第 13 條之 4 規定，將被併科罰金，造成經營之風險。

以下將參酌日本經濟產業省「營業秘密管理指針」之內容，輔以相關文獻資料及實務案例採取之保密方法，統整歸納出企業保護營業秘密之策略步驟，希冀能提供企業適當且具體的營業秘密保護方法，藉以提升管理品質與水準，降低營業秘密遭侵害之風險。

## 壹、最高管理階層應有明確的政策聲明與支持

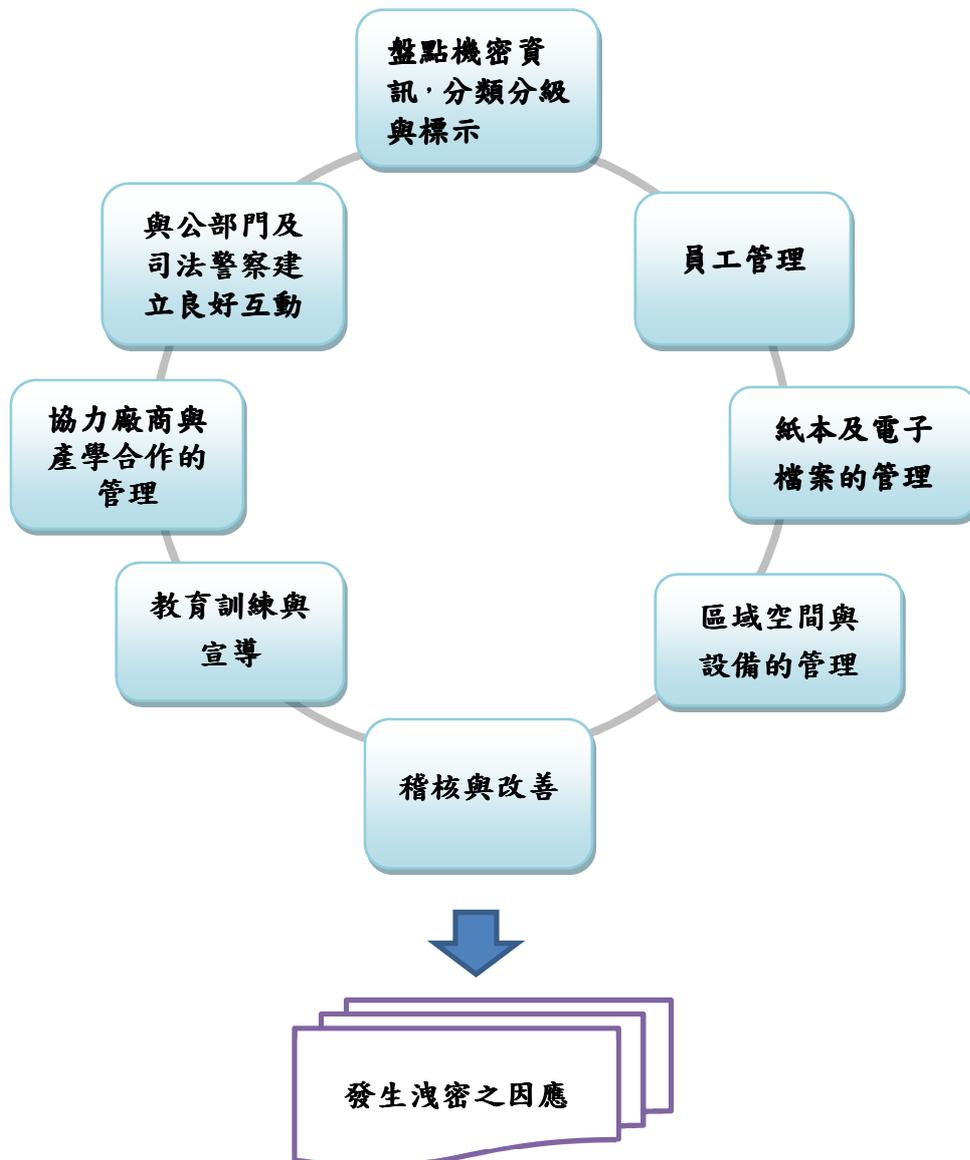
企業營業秘密管理需投入大量的時間、成本，從企業財務報表的角度切入，該時間成本的投入並無法量化成實質之收益，甚至在管理實務上，管理機制與工作效率是反比關係，管理機制愈多，工作效率可能降低，而員工因管理機制造成工作上不便，可能引發不滿而不願遵守，導致推動營業秘密保護之困難。因此，最高管理階層對營業秘密保護政策聲明與支持，對於營業秘密保護之落實與成效，具有極大之影響。於管理實例上，有科技公司在公司組織架構之設計，是獨立設置營業秘密保護專責單位，且直接向董事會報告；在管理規則之訂定，最高管理階層亦不能使用可攜式 USB，以示對政策之支持，故企業之最高管理階層於營業秘密保護之工作，建議應注意下列重點：

- 一、企業的最高管理階層對於營業秘密的管理保護，應有明確的政策聲明，表態展現建立制度的決心，參與營業秘密管理制度的制定。
- 二、設立專責單位及人員，負責統籌規劃、推動相關合理保密措施，給予人力、財力及訂立管理規定的實際支持。
- 三、企業的高層主管應以實際行動支持營業秘密管理的措施，了解營業秘密管理的適用範圍，檢視落實情形，並指示應配合調整的管理計畫，並可依照 PDCA 模式，即「Plan 計畫-Do 實施-Check 檢視-Action 修正」的步驟，加以落實營業秘密的保護。

最高管理階層應有明確的政策聲明與支持

人力  
財力  
管理規定

建立營業秘密保護管理政策



## 貳、建立營業秘密保護管理政策

為了讓員工明白公司的營業秘密保護範圍及措施，公司應訂定營業秘密管理規範，將營業秘密的範圍、如何分級分類及使用權限、人員、環境與設備等管理予以明文規定，確保員工可認識到公司對於何種機密資訊有將其作為秘密管理之意思，以及相應的保密措施為何：

- 一、導入營業秘密管理規範，訂定機密檔案範圍、分類分級標準、檔案使用規則、紙本及電子檔案管理規則等。
- 二、依機密檔案範圍之定義，將公司機密資訊與一般資訊加以區隔，並針對機密資訊設定分級分類標準。
- 三、明定公司不同部門或職務之人員可接觸或使用之機密資訊等級的權限範圍，並落實「不知道的人就不該知道，該知道的人就讓他在該知道的範圍內知道 (need to know)」原則，例如總經理僅需知悉管理資訊之商業性秘密，研發人員以知悉所負責專案之技術資訊為主，並禁止不必要的跨專案討論或交流資訊。
- 四、依員工職位職務，擬定不同的智慧財產相關約定，包含保密約定、智慧財產權約定、競業禁止約定等。
- 五、明確劃出管制區，與公司一般的區域空間加以區隔，管制進出人員、攜帶物品等；並針對公司電腦、網路、內部資料庫、電郵信箱等訂定管理措施。

### 參、盤點機密資訊，分級分類與標示

由於採取保密措施需投入成本，且會對營運造成某程度的不便利，公司盤點機密資訊進行分類分級時，會與後續管理機制有連動關係，需考量產業類別、可投入的人力、成本資源等，評估如何兼顧營運效率及保密需求，依不同機密等級採取相應的管理措施：

- 一、清查盤點公司有需要保密之資訊，包含公司各種技術性或商業性的資訊，例如公司自行研發技術機密、產品配方、製作方法、他人授權或受讓之機密、公司新品開發、投資決策、行銷計畫、客戶資訊等，並釐清權利歸屬。
- 二、針對機密資訊進行分級，可依該資訊如外洩將對公司造成何影響、現階段或潛在經濟價值、技術發展先進程度等而為分級。如公司規模小，可分為非機密及機密資訊等 2 種；但公司略有規模，應至少區分為「極機密、機密」2 級：
  - 1、極機密：公司最重要的資訊，外洩將對公司有存亡危險。
  - 2、機密：公司次重要資訊，外洩將對公司造成損害。
- 三、針對機密資訊進行分類，可依公司規模、產業特性等，予以適當分類，例如區分為「商業性」或「技術性」機密檔案，或更細膩區分，如依產品生產過程，區分為「研發方向、製程順序、配方比例、溫度濕度控管、材料進貨來源、成本分析、客戶名單」等類型，將相關檔案資訊分門存放，並依機密等級做分級管理。
- 四、將機密資訊作適當切割，每個人只能知道一部分，很少人可以知道全部完整的資訊。
- 五、對於愈高等級的機密，採取愈高密度的管理機制，投入更多的

人力或成本加以保護。

- 六、 不同機密等級的資訊應有相對應的標示，紙本文件及電子檔案都要明定標示方式，例如標註限閱或機密等級。
- 七、 依不同機密等級設定須相關保管、接觸、使用的權限規定，明定不具有該等級機密資訊接觸權限的人員，不應取得該資訊。

## **肆、員工到職、在職及離職管理**

公司於日常中對於員工採取保護營業秘密措施，可依照新進員工報到、員工在職及離職等不同階段，進行動態管理：

### **一、新進員工管理**

- (一)新進員工報到時，要求員工簽訂保密協議，約定職務上知悉或持有公司未公開之檔案，均應保密，未經公司同意，不得任意使用或交付他人；且於離職後，仍負有保密義務。
- (二)與員工簽訂智慧財產權歸屬約定。
- (三)確保員工對於保密內容及相關管理措施具有認知之可能性，由部門主管或指定人員交付公司營業秘密管理規範，給新進員工簽收，說明保密內容、機密分類分級標準及使用權限等。
- (四)落實對新進員工之查核工作，包含確認新進員工是否與前公司簽訂競業禁止約定、了解其於前公司之職務內容；要求新進員工不得將前公司營業秘密攜入公司使用，並簽切結保證。

### **二、員工在職期間管理**

- (一)當員工職務調動時，請員工提出調職切結，保證先前自行保存之機密檔案，已全數交還原任職部門，複本並已刪除。
- (二)告知員工新職務內應遵守之營業秘密管理規範，重新調整員工存取、使用機密檔案之權限；並移除其存取、使用原部門相關檔案文件之權限。
- (三)依員工新職務內容可能接觸之機密檔案，評估是否重新簽訂保密或智慧財產權約定。

### **三、員工離職管理**

- (一)與員工進行離職面談，詢問員工離職原因及未來規劃，提醒員工遵守保密義務，且要刪除或歸還所持有的機密資料，不得留存備份，並作成離職切結。
- (二)從員工提出離職申請至實際離開公司之期間內，公司可啟動稽核，如發現員工有異常存取、下載公司機密檔案紀錄，或有異常加班、出入管制區域等情形，應進行調查並保存相關證據資料。
- (三)員工離職當天，要立即切斷該員工登入公司資訊系統的權限。
- (四)評估是否有需要與離職員工約定競業禁止，如有需要，要與員工另簽競業禁止條款；競業禁止條款應符合勞動基準法及其施行細則的相關規定。
- (五)追蹤員工是否有違反競業禁止約定之情事。

## 伍、紙本及電子檔案管理

營業秘密為無體的智慧財產，其載體可能為紙本或電子檔案文件，公司應針對機密資訊檔案的製作、傳遞、使用、重製、保存、銷毀等生命週期，擬定檔案管理程序，並依紙本及電子檔案而訂定不同的管理規範及使用規則，建議可採取以下的作法：

### 一、紙本檔案管理

- (一)將公司內部及外部紙本檔案，依機密資訊分級標準，標註「極機密、機密」等不同機密等級，以利識別。
- (二)對於不同機密等級之紙本檔案，明確規範其存放、閱覽、使用權限範圍。
- (三)指定專責管理人員，建立機密紙本檔案編號造冊機制。
- (四)依機密紙本檔案存放規範，將檔案交由員工或專責管理人員保存於保險櫃或特定保管區域，並應定期清查核對。
- (五)機密紙本檔案複本，應加蓋「複本」戳記，並視同原件管理。
- (六)於傳遞機密紙本檔案時，應妥善保護檔案內容，如密封等。
- (七)員工應依權限申請閱覽、使用機密檔案，專責管理人員應登記並確認員工身分及其權限，僅有具使用權限者，才可提供檔案；所有檔案之閱覽、使用、歸還等情形，均應留下紀錄。
- (八)定期檢視符合銷毀條件之機密紙本檔案，並確保銷毀文件無法被復原。

### 二、電子檔案管理

- (一)依機密資訊分級標準，將電子檔案標註不同機密等級，並設定密碼保護，必要時，並可於檔案中加入浮水印或特殊暗記。
- (二)設置專責單位或人員負責規劃、執行電子檔案管理機制。
- (三)對於不同機密等級之電子檔案，設置密碼控管，並設定不同存

取或使用權限，分級分類儲存。

- (四)對機密電子檔案之存取及複製、列印、對外傳輸等情形加以 log 記錄，並留存 log 紀錄，由專責單位或專人負責檢視追蹤。
- (五)規範員工發送電郵之檔案，均要加密處理，並加註警語，例如「本郵件涉及機密資料，禁止擅自轉傳使用」。
- (六)對存有電子機密檔案的內部資料庫、系統等，規範員工須以帳密登入；針對高度機密檔案，除非獲主管事先授權，不得開放員工閱覽或使用權限。
- (七)原則上公司內部資料庫或系統應避免遠端連線，如員工職務上有遠端連線的需要，須先獲得公司同意授權，並對員工接觸機密檔案之權限及範圍，予以規範；但針對機密等級屬「極機密」檔案，應禁止開放遠端連線。
- (八)對於遠端連線所有連結、存取機密檔案之情形，都要留下紀錄。

## 陸、區域空間與設備的管理

公司對於保存機密檔案卷宗、新製品、製造機械、模型等處所或研發部門、實驗室等區域，應強化安全警戒管理，並加強對存放機密資訊之電腦設備的控管，落實相關安全管理措施：

### 一、區域空間管理

- (一)設置管制區，與一般空間予以區隔，並可依不同專案項目，而設置個別管制區，不同的管制區僅限處理該專案人員進入。
- (二)於管制區張貼「非工作人員禁止進入」、「管制區域禁止進入」、「禁止照相」等警語，並可就不同的管制區設置不同的警示，例如「禁止擅自攜離任何物品或紙張」。
- (三)明定禁止攜入管制區物品的定義及相關管制措施，例如手機、相機，或具有攝影、錄影、錄音、資料交換功能等的電子裝置。
- (四)管制區配置保全人員或裝設監視設備，管制進出人員、時間及攜帶物品：
  - 1、針對公司內部人員：公司依不同權限等級，配發員工識別證，員工進出管制區須刷識別證。
  - 2、針對公司外部人員：訪客須事先申請及登記，經公司同意其活動的範圍及路線，並在相關人員陪同下，才能進入管制區。
- (五)針對涉及極機密資訊，在經費可允許前提下，其保管場所可加裝高科技設備，例如虹膜辨識、金屬探測等設備。

### 二、設備管理

- (一)針對公司的電腦設備或資訊系統，建立防禦機制及網路連線或使用的管理規定。
- (二)設置防火牆及防毒軟體，防堵釣魚、木馬等惡意程式。

- (三)管制員工於公司內使用 USB 或外接式硬碟等。
- (四)禁止員工在公司內部資訊設備安裝或下載軟體程式，並宣導員工不要隨意點閱不明郵件或附加檔。
- (五)員工須以個人帳號密碼，登入公司電腦設備或網路伺服器，密碼要有一定的設定強度及定期更新，並禁止員工將自己的帳密提供他人使用。
- (六)建立外部連線使用員工的認證機制，針對遠端桌面或遠端登入的網路連線建立權限管理，就遠端連線之員工、上線、離線時間等進行記錄。

## 柒、稽核與改善

營業秘密保護，首重事前預防，公司除了盤點檔案資訊，訂定分級分類標準、使用權限及管制措施外，也要建立內部稽核機制，才能及早發現以防止外洩情事，並可針對違反管制措施者，訂定處罰規定，督促員工確實執行，參考作法如下：

- 一、建立內部稽核機制，設置負責稽核的專責單位或人員，追蹤監控機密檔案閱覽、存取、使用等紀錄、遠端連線紀錄，及偵測員工電郵之關鍵字、附檔等。
- 二、如追蹤發現有異常的資料下載、存取、列印、使用等情形，或篩選可疑員工郵件時，應即刻向營業秘密專責單位或人員提出預警通知，並保留相關證據。
- 三、由專責單位或人員定期或不定期檢視管制措施執行情形，並將檢視結果陳報公司高層。
- 四、稽核發現員工有違規情事時，如情節輕微，依處罰規定給予處分，並通報單位主管及相關權責人員，督促違規員工儘速改善，及回報改善情形；如情節重大，要注意不可打草驚蛇，並保存相關證據，提出告訴。
- 五、留存員工違規處分紀錄及追蹤改善情形，以作為公司宣示保護營業秘密的證明。
- 六、將員工違規情事及處分編製為案例進行內部宣導，讓其他員工心生警惕，避免發生類似的違規行為。
- 七、整理稽核結果、員工違規情事等，檢討公司管理措施是否需要進一步改善。

## 捌、教育訓練與宣導

公司要保護及管理營業秘密，除依靠相關技術或設備面的支援，在管理面上，公司的管制措施同時也需要依靠「人」來執行，因此，公司可透過教育訓練與宣導，提升員工對營業秘密保護的認知，以使公司管制規範被確實遵守與執行，可參考作法如下：

- 一、定期舉辦員工營業秘密管理規範訓練，並搭配考試，要求全體員工須滿分通過，如有未達滿分者，應要求補考。
- 二、教育訓練內容，應側重讓員工熟悉公司機密資訊的範圍、分級分類標準、使用權限、資安控管、處罰規定等，避免員工日後藉口不了解相關規定而不遵守。
- 三、可搭配以下方式定期及不定期提醒員工：
  - (一)利用平時開會宣導
  - (二)利用員工旅遊或文康活動等場合宣導
  - (三)於員工餐廳、梯廳、走廊電視牆播放宣導
- 四、舉辦各種有趣的營業秘密保護活動或遊戲，給予適當的獎金。
- 五、保留各種營業秘密教育訓練或宣導紀錄。

## 玖、協力廠商與產學合作的管理

在產業鏈愈趨高度專業分工的背景下，公司除了與產業鏈上、下游的廠商成為合作夥伴外，更需要重視研發之產學合作，而與外部協力廠商及學研機構的合作過程中，公司要如何保護營業秘密及預防外洩，可參考以下作法：

- 一、與協力廠商或學研機構等簽訂保密協議，約定未經公司同意或授權，不得洩漏予第三人；且雙方結束合作或解約時，仍負有保密義務。
- 二、與協力廠商或學研機構等簽訂智慧財產權歸屬約定，明定機密檔案所含技術經改良所得的智慧財產權之歸屬。
- 三、公司尋找合作的協力廠商或學研機構時，要先做好評估；授權協力廠商或學研機構運用之營業秘密盡量為「局部」，以分散風險。
- 四、要求協力廠商或學研機構有適當的保密管理措施，並稽核其執行情形。
- 五、當公司與協力廠商或學研機構結束合作或解約時，應告知並要求其繳回機密檔案、銷毀或刪除機密檔案複本等，並提醒其仍負有保密義務。

## 拾、與公部門及司法警察建立良好互動

### 一、參加公部門之訓練活動及宣導活動

公司可積極參與公部門辦理對企業之合理保密措施研討會及營業秘密保護宣導活動，除汲取其他成功企業營業秘密管理保護之經驗，亦能就公司本身在管理上所遭遇之問題提出諮詢。

### 二、建立與司法警察之連絡管道

法務部調查局及內政部警政署保安警察第二總隊設有深入企業協助之互動機制，並分享案例及舞弊之作法，對於企業防範營業秘密之侵害，以及完善營業秘密管理制度，有十分之助益，因此，公司平時與司法警察建立聯絡窗口，若有侵害發生之疑慮，可於最短時間諮詢並降低侵害、損害之擴大。

### 第三章 營業秘密發生洩密之因應

營業秘密多屬無形之資訊，營業秘密遭受侵害時，應該儘速進行危機管理，將損害降至最低，若能在營業秘密揭露於第三方知悉前，阻止其向外洩露，為侵害發生後，最理想之結果，故企業應有建置侵害發生之危機處理 SOP 流程。經參酌司法警察之經驗，以刑事告訴為核心，提出建議之因應流程如下：

#### 一、進行內部損害控管

##### (一) 確認營業秘密外洩管道

要進行內部損害控管，必須了解侵害發生之源頭，以利後續對於侵害相關之人、事、地及物等釐清，並了解侵害之方式，如 USB 存取、電子郵件夾帶或拍照等，亦有助管理策略之修正。

##### (二) 釐清接觸營業秘密人員

依過去侵害案件發生之情形，侵害營業秘密之人，多數為離職或退休員工，部分情形為離職或退休員工與在職員工之合意行為，釐清接觸之人員，以利後續蒐證、防範營業秘密外洩擴大，並可提供司法人員明確其偵辦方向及對象。

##### (三) 防範洩露營業秘密擴大

針對洩密管道進行防堵擴大事故範圍，或遏止營業秘密持續向外擴散之處理。

##### (四) 尋求專業協助

若企業內部未建置資訊專業人員，基於證據保全，對於前述事項應儘速洽請專業人員之協助，例如回復已遭格式化之硬碟或追蹤擴散之營業秘密流向等。

## 二、蒐集、保全事證

### (一)案件相關電腦保存

實務上曾有案例發生企業提出告訴後，調出涉嫌竊密之離職員工使用的電腦進行搜證，但發現電腦硬碟已被重新格式化(FORMAT)，所有證據都未被保存下來；另外，有企業依營業秘密分級管理，授權某員工有讀取特定檔案的權限，並且有讀取紀錄，但卻授權或要求員工在離職前刪除所有資料與紀錄；諸如此類都是電腦保存紀錄不夠完整之情形，對於未來舉證造成困難。另外，應避免證據污染之問題，如電腦檔案容易因存取造成時間會異動，將有損其證據能力及證據力，對於電腦檔案之取證，應尋求司法機關或專業人員之協助。

### (二)調閱監視畫面

多數企業之監視畫面資料並不會永久保存，為避監視畫面之相關佐證資料因覆蓋而遺失，應儘速調閱相關之內容，以利保存證據。

### (三)追蹤重製軌跡及文件流向

常見營業秘密受侵害之手法，為資訊檔案經重製後，以媒體或電子郵件寄出，另外，也有侵害行為以列印書面文件攜出進行，因此，追蹤營業秘密之重製軌跡與文件流向，必須包括電子檔案與書面文件，除有助於防止營業秘密擴散，亦有利於區分該事件為一般營業秘密侵害案件，或是域外使用侵害案件，使司法警察更易判斷得否依法啟動如監聽等相關之偵查方法。

### (四)要求填寫保密切結

依司法警察在營業秘密侵害案件偵查實務之分析，常見企業不易證明遭員工以不正方法取得營業秘密、或未經授權及逾

越授權取得營業秘密，因此，侵害發生後，與侵害人簽訂保密切結，並要求刪除、銷毀持有之營業秘密，以確保營業秘密不再洩露，為事後補救方法之一。尤其是對於無意圖為自己或第三人不法之利益，或損害營業秘密所有人之利益，而取得雇主之營業秘密者，該保密切結更具有警惕之效果。

### 三、確定營業秘密告訴範圍

營業秘密告訴範圍之選擇與確認，將影響案件偵查及訴訟時程，告訴範圍愈大，其所耗費偵辦及訴訟時程愈長，主要原因係營業秘密常涉有複雜或先進之技術秘密，而司法人員通常不具技術背景，對於釐清提告之標的與受侵害之標的是否同一，以及是否具備營業秘密要件等侵害事實之認定，具有相當之困難度，因此，提告受侵害之營業秘密愈多，司法人員亦需花費較多之時程，故企業所提營業秘密告訴範圍，對於侵害案件後續偵查及訴訟之時程，具有密切之連動性。

#### (一)釐清具備要件之營業秘密

於提出告訴前，應評估提出告訴之標的為營業秘密，或僅為一般機密，依營業秘密法提出告訴之機密資料，應符合秘密性、經濟性及營業秘密所有人具有合理保密措施等三要件。

#### (二)選擇適合提出告訴之營業秘密

##### 1、選擇可達成目的之營業秘密

刑事罪責之效益，可產生警惕的效果，並遏止犯罪與侵害持續擴大，與透過民事程序請求損害賠償，以損害填補為目的不同。為使提告後，達成速偵速審之效益，企業宜評估可達成目的之標的為宜；提告之營業秘密標的愈多，偵辦審理時間更長，也有更多二次外洩之風險。

##### 2、適宜提出及揭露之證據

提出告訴之營業秘密標的，因案件偵查，而有揭露於被告或其代理人之必要，且相關證據經起訴後，將成為訴訟資料之一部，因此，告訴人選擇告訴之營業秘密標的，應考量後續提出進行偵查之證據是否合宜，及是否得適度揭露予被告。

### 3、減輕舉證之負擔

提出告訴之營業秘密標的愈多，告訴人所負之舉證責任負擔愈大，司法人員相對需釐清的事項亦多，因此，提出告訴之營業秘密，需考量後續舉證之難易度及資料。

企業應在平時做好相關營業秘密管理制度，並搭配適當的紀錄留存，包含數位保存證據等，如此當發生營業秘密侵害事件時，可作為積極證據自我保護，達到迅速反擊的效果，並可減輕舉證之負擔。

### 4、避免再次洩露之風險

選擇適合提出告訴且能達成目的之營業秘密，避免偵查、訴訟過程中，增加二次洩露風險。

## 四、向司法警察提出告訴

知悉被侵害事實，為避免損害擴大及營業秘密被揭露予更多人知悉，企業應儘速向司法機關提告，最遲應於知悉後6個月內提出告訴，並依下列事項配合提出告訴及偵辦，以達速偵速結之成效。

### (一)填妥釋明事項表

為了讓偵查階段建立良好基礎，使案件起訴後，法官更容易做出正確的裁定，以及注意營業秘密的秘密性維護，法務部訂定「檢察機關辦理營業秘密案件注意事項」，其所附「釋明事項表」為法務部參考美國智慧財產案件辦理手冊及檢視過往我

國營業秘密案件偵辦所遭遇之問題，經整合相關必要事項所訂定，從企業自我管理之觀點，該「釋明事項表」為企業平時自我檢視機密資訊是否符合營業秘密要件之最佳工具。

釋明事項表並非提告之必備要件，其目的係協助司法機關儘速偵速審，完整的資訊將可協助告訴人將技術語言轉化成法律語言，使司法人員能快速及精確的判斷真實，並有助於溝通，對於案件之偵辦及訴訟歷程將有十足之助益。

## (二) 事證提交司法警察

將明確之事證提交司法警察，包括協助司法警察確認營業秘密範圍，實務上，曾有告訴人不欲他人（包括司法警察）知悉其營業秘密，雖有提交事證，但不願明確指出營業秘密之範圍，造成偵查遲滯或案件無法成案之情形。

## (三) 配合偵查作為

營業秘密侵害案件與一般刑事案件不同，除法律問題，更涉及專業技術問題，若企業代表或代理人其權限或專業知識不足，於配合偵查時，無法具體回答司法人員之問題，使得調查程序需多次安排，都將延宕侵害案件偵查期程，因此，告訴人應指定權限較高之人員協助偵查程序進行，甚至應有跨法律及技術組成之團隊，配合司法人員偵查，以縮短偵查期程。

## (四) 嚴格保守秘密

告訴人參與偵查之人員，於偵查期間應避免對外透露相關內容，避免侵害人警覺而銷毀相關事證，使得司法人員取證困難。

# 五、注意司法程序中營業秘密之保護

## (一) 訴訟過程聲請秘密保持命令

依「智慧財產案件審理法」第 11 條之規定，當事人或第三

人就其持有之營業秘密，向法院釋明符合一定情形者，法院得依該當事人或第三人之聲請，對他造當事人、代理人、輔佐人或其他訴訟關係人發秘密保持命令，限制受秘密保持命令之人，就該營業秘密，不得為實施該訴訟以外之目的而使用之，或對未受秘密保持命令之人開示。違反秘密保持命令者，處三年以下有期徒刑、拘役或科或併科新臺幣十萬元以下罰金，故營業秘密所有人應適時向法院聲請秘密保持命令。

## (二) 追蹤及溝通起訴書、判決書公開之內容與範圍

依「法院組織法」第8條之規定，各級法院及分院應定期出版公報或以其他適當方式，公開裁判書，另外，高等法院以下各級法院及其分院檢察署，應於第一審裁判書公開後，公開起訴書，營業秘密所有人或告訴人對於裁判書及起訴書應公開之內容，應積極與法院或檢察署溝通，對於公開內容涉及營業秘密之部分，應適當處理，以避免營業秘密被揭露。

## 六、檢討公司營業秘密保護不足之處

### (一) 檢討營業秘密遭侵害之途徑

營業秘密發生侵害情事，代表保密機制或管理策略尚有再提升之必要，因此，進行侵害事件之原因分析，找出被侵害之途徑，以利策略修正之檢討。

### (二) 重新修正保護策略

為避免再次發生相同侵害情事，針對分析得知之洩密途徑，修正保護方法或策略，且應注意公司所能投入之資源，落實之可行性，以及管制與效能間衡平，以周全營業秘密之保護。

## 第四章 CEO 帶領成功企業的經驗分享

### 一、隱形冠軍的崛起

王泰山原本是一家生技公司的小主管，公司受到疫情影響，及管理制度不善，痛失大訂單，前景堪憂，由於王泰山本身具有資訊專長，利用閒暇時間開發出一款健康管理的 APP，為了創造自己美麗的人生，他與父母商量獲得資助 30 萬元後，提出辭職自行創業，開設了一家資訊公司，因為小資創業，預算有限，租了簡單的辦公室，招募 3 名員工，分別負責銷售、程式設計、會計等業務，公司開始營運，由於疫情宅在家，更要運動及自我健康管理之風潮，這款健康管理的 APP 迎合市場需求，一戰成名，公司知名度打開，吸引不少投資人關注，其中有大型企業看中公司的發展潛力，上門洽談投資合作，公司獲得資金的挹注，使用的消費者也持續成長，加速業務的拓展，公司營運規模與獲利不斷壯大，成功在業界拼出一片天。

王泰山能夠成功創業，關鍵除了擁有獨特的技術外，也因為目睹前公司對營業秘密保護及管理的欠缺，丟了千萬元大訂單，讓他深刻體悟，有效保護這些技術的營業秘密，公司才有生存之路，走得長遠。王泰山能帶領公司順利打下江山，迅速崛起，他的創業歷程與保護營業秘密的「533」成功經驗，值得與大家分享。

### 二、草創階段

公司草創時期，錢得花在刀口上，除了重視開發 APP 的技術，還要注意營業秘密的保護，重點在於「先求有，再求好」，配合公司業務需求及有限經費，檢視如何保護營業秘密。對公司而言，最重要的技術就是健康管理 APP，要好好保護，否則一旦被外洩，公司也要關

門大吉了，所以創業不能只靠熱情，想讓公司順利走下去，分享5項絕招：

### **(一)第1招「招募員工，要說清楚講明白」**

公司在招募新員工時，要掌握三大重點，第一，要求員工簽保密協議；第二，要求員工簽智慧財產權歸屬約定；第三，切記面試員工時，要去了解員工在前公司的職務內容、有沒有跟前公司簽保密協議或競業禁止約定。另外，要提醒員工，不可以將前公司的營業秘密帶進公司內使用。

### **(二)第2招「展現CEO保護營業秘密的決心」**

CEO在公司開會時，向員工說明公司的願景，公司雖然小，營業秘密保護制度不可少，要大家一起維護，才能保持公司競爭力，公司也會投入必要的資本來執行保護措施。要讓員工明確認知，公司開發的APP，就是公司的機密，相關開發或改良APP的技術或進度，不可以對外透漏或說明，連家人朋友也不行。

### **(三)第3招「明定營業秘密管理規範」**

公司草創期，正是建立制度最關鍵的時候，要訂定一套營業秘密管理規範，不用多，只要掌握三個重點，第一，擬定營業秘密的工作守則；第二，明確機密資訊檔案的範圍，以及使用權限，重點是盤點公司的機密，公司開發APP的技術就是重要機密，APP原始碼絕對禁止外傳；除了「技術性資訊」外，還有客戶特定需求、行銷等「商業性資訊」2類資訊都要辨識；第三，說明公司的資安規定，包含機密檔案存於公司雲端的密碼管控、使用USB的管控、需用電子郵件傳送機密文件時，要取得授權(因為公司小，所以是CEO的同意)再加密傳送等。

#### **(四)第 4 招「保密要玩真的」**

公司要讓員工清楚認知，保密措施不是形式做文章，而是玩真的，公司電腦要設防火牆及安裝防毒軟體，規定每個員工依個人帳密登入電腦，要求密碼設定有一定的強度，並定期更新；如有員工不當一回事，將密碼貼在桌上，或擅自使用別人的帳密登入電腦，一定要立即糾正禁止；在開會時，再次提醒員工，公司正在起步成長，如果讓外界拿到公司的機密，公司可能就此倒閉，因此保密措施要確實執行。

#### **(五)第 5 招「時刻保持警戒」**

公司開發的 APP 具有發展潛力，吸引投資人或企業上門洽談合作時，如果有投資人要求公司提供技術資料，以評估合作可行性，此時要切記，不可為了急於獲得資金，就把公司機密都攤開給對方看，例如，APP 的原始碼資料絕對不能提供，其他機密，可做適當遮蔽改寫，或請對方先簽保密協議再提供。

另外，也要防範公司好員工被競爭對手挖角，此時要動之以情，說明公司前景看好，未來有升職加薪的機會；如果留不住員工，記得要做離職面談，提醒員工刪除或交還機密檔案資料，讓員工知道即使跳槽，也不能帶走或擅自使用公司的機密資料，如有不法竊密，可能面臨牢獄之災。最後切記，員工離職時，立即切斷可使用公司帳密的權限。

### **三、成長階段**

隨著公司產品受市場青睞，獲得與大型企業投資合作，營運規模及業務擴大，公司部門擴編為研發部、行銷部、財務部、資訊部，員工從 3 人增加為 30 人，也有更多經費購入新的資訊設備，面對管

理層級、員工人數、機密檔案數量、類型增加，以及引進防護設備、系統等新挑戰，想讓創業的果實能夠穩定成長，除了草創期的 5 招，需要新增 3 項內功心法：

### **(一)心法 1「動態調整營業秘密管理規範」**

因應公司部門擴編，機密檔案類型及數量增加，如同小孩長大，衣服要換新的，因此，公司原本營業秘密管理規範的機密檔案分級分類標準、使用權限、資安規定要相應更新。分級可增加為「極機密、機密」等 2 級，紙本及電子檔案都要標示；分類要更細緻化，程式開發、經營策略、財務規劃、市場分析、客戶需求等類型，要分門存放。

機密檔案使用權限的規定，隨著公司垂直的管理層級、水平的部門分工增加，須重新依不同機密等級，設定使用權限範圍，例如「機密」等級以上的檔案，須經單位主管授權，始可閱覽使用；研發部的檔案，僅限該部門主管及負責專案的人員有權閱覽使用。即便是經理，業務不需要接觸資訊的員工，就不應有使用權限

此外，引進新的防護設備、系統，公司的資安規定要做相應調整，例如增設監視器及保全系統後，規定人員進出公司或辦公室，要刷員工證；設定可使用電子機密檔案系統的員工帳密。

### **(二)心法 2「強化稽核調查，開啟抓漏作戰」**

公司增設資訊部門，要建立內部稽核機制，監控員工使用電腦、機密檔案存取及列印等情形的 log 記錄，以及偵測員工電郵之關鍵字、附檔等，如發現有異常情事，或篩選出可疑電郵時，要保留證據，並通報營業秘密專責部門主管或 CEO，公

司可依員工違反情節，給予處分；另外可將員工違規情事，編製為案例進行宣導，讓其他員工心生警惕，避免出現管理漏洞。

### **(三)心法 3「形塑企業文化，讓員工內化於心，外化為行」**

相較於公司草創期只有 CEO 與 3 名員工，大家如同生命共同體，要傳達管制規範或提醒員工落實，當面就可溝通清楚，當公司員工擴充為 30 名，管理溝通層級變多，員工可能對於營業秘密保護缺少直接感受，此時更需重視透過教育訓練、考試等，將保密概念內化到員工心中，讓員工了解公司與自己是命運共同體，逐漸形塑為企業文化，讓員工不僅是因為怕被處罰而「不敢」洩密，更基於「與公司同在一條船」的信念，而「不為」洩密。

## **四、壯大階段**

隨著公司營運規模與獲利不斷壯大，公司增設副總經理、研發部、行銷業務部、智權法務部、財務部、人資部、資訊部等，除臺北的總公司，還在新竹、臺中、高雄等地設分公司，員工從 30 人增加為 300 人，且為了提升效能，部分工作開始交由外部廠商處理；此階段由於可能接觸公司營業秘密的「對象範圍」增加，除內部員工外，還有外部協力廠商，而且員工會在各部門或總公司、分公司間調動，人員流動更趨複雜，因此公司要強化「風險管理」理念，調整營業秘密管理制度，以降低洩密風險，此階段的公司想要成功「轉大人」，除了原先的 5 項絕招及 3 項內功心法的基礎下，還要再服用 3 帖靈丹妙藥，厚植根本：

### **(一)第 1 帖「重視對外部廠商的管理」**

公司業務拓展，為了提升產能，需要把部分工作交給外部

廠商處理，過程中公司要保護營業秘密不被外洩，須掌握三大重點，第一，與外部廠商簽保密協議，約定不得擅自使用或洩漏予第三人；即使中途結束合作或解約，仍負有保密義務；第二，與外部廠商簽智慧財產權歸屬協議，明定基於機密檔案之技術加以改良後的智慧財產權歸屬；第三，針對新合作的廠商，一開始授權其運用的機密資訊，應只給「局部」，不可給完整機密資訊，並要求廠商採取保密措施，如廠商確實落實保密，公司再評估是否增加授權其運用的機密資訊範圍。

## **(二)第 2 帖「員工職務異動或離職，要重視保密防護」**

當公司規模、部門擴增，員工人數高達數百人，公司很難滿足每個人想要的發展機會或晉升管道，導致可能有員工心生不滿而出走，甚至挾怨竊取公司機密投靠競爭對手，因此公司擴張後，要更重視對員工的管理與溝通，至少要掌握三大重點，第一，留住人才，避免被競爭對手挖角，除透過加薪、提供福利及訓練進修資源等，也要留意在調整員工職務前，先與員工溝通，以減緩員工的不安或不滿；第二，員工職務調動時，要重新設定使用機密檔案的權限，並依新的職務內容，評估是否重新簽訂保密或智慧財產權約定；第三，員工提出辭職時，要落實離職面談，同時啟動稽核，清查有無存取使用機密檔案、離職前假日加班等異常情形，並評估是否有需要與員工簽競業禁止約定。

## **(三)第 3 帖「營業秘密管理為競爭力管理」**

公司未來推出新的產品設計、市場行銷、戰略規劃等，最後可能發展為跨國企業，因此要保持動態的風險管理，更需創新與彈性，不能墨守成規。營業秘密的管理，要有一套機制，

要結合公司的業務推展，因應環境變動及具體情況而隨時檢視動態變化，如同練功練到最高境界，就是內功深厚，隨心隨地取用武器，讓每一位員工都是捍衛公司機密的守衛尖兵，確保公司競爭力。

## 第五章 營業秘密 Q & A

### 一、什麼樣的資訊是營業秘密呢？

屬於「營業秘密」之資訊，需符合營業秘密法第2條所規定之營業秘密三要件，亦即「秘密性」、「經濟性」及「合理保密措施」。其中，「秘密性」是指資訊為一般公眾所不知，且相關專業領域之人也不知道的；「經濟性」是指對於企業具有實際或潛在之經濟價值，例如市占率、研發能力、業界領先時間等；「合理保密措施」是指所有人主觀上有將該資訊當成秘密加以保護的意思，客觀上採取有效的保密措施，例如，簽訂保密契約、文件標示限閱或機密註記、設定密碼、存取權限等。

### 二、營業秘密應該從什麼時候開始保護？

企業之經營模式、商業方法、技術研發都會隨著營運而累積相關資訊，但是因尚未展現經濟上的價值，而忽略相關資訊的保護，這也是小型企業或新創企業較容易發生之問題，因此，即使尚未有成果或產品，於初期構想或投入資源研發時，即應開始進行保護，俟成果或產品輪廓較明顯時才進行相關保護措施，除機密資訊有可能已被輕易攜出，亦有可能無法符合秘密性與合理保密措施之要求。

### 三、企業內有那些人落實營業秘密保護之義務？

營業秘密保護是企業內每個人之義務，愈高層之主管應愈有保護之意識，並且應在企業內形塑營業秘密保護之文化，讓員工將維護營業秘密保護等同確保公司獲益、工作受到保障之意識根深蒂固，營業秘密保護文化的形成，更有助於營業秘密保護的落

實。

#### **四、營業秘密的保護是否有期限？如果公司的策略目標改變或研發技術提升，是否會使原先屬於營業秘密的技術或營運計畫等，不再受到保護？**

(一) 營業秘密的保護沒有期限，只要相關技術或商業經營的「資訊」，符合營業秘密三要件，就能一直是營業秘密而受到保護。例如可口可樂的「配方」就是一種技術資訊，從配方被研製出來，至今已超過百年，仍符合三要件，而依然是營業秘密，也正因為配方這項營業秘密，為可口可樂公司創造了豐厚的商業利潤。

(二) 公司的技術資訊或營運計畫等經營資訊，符合三要件，就是營業秘密，當公司的研發技術提升，或經營的策略目標改變時，公司應確認原有的技術或經營資訊是否仍作為營業秘密保護，如認為有必要，仍應持續有效的保密措施。

#### **五、公司的離職員工要求在職員工傳送或交付一份他先前在公司製作的資料，在職員工可以提供嗎？**

對於離職員工要求提供的資料，依照公司營業秘密管理規範之分級分類及使用權限管制，如屬不可對外提供，在職員工不可將資料提供給離職員工；如該資料並未列入不可對外提供之管制範圍，則要檢視該資料內容，是否為離職員工於「職務上完成之著作」，依著作權法規定，除公司與員工另有約定外，「職務上完成之著作」之著作財產權歸公司享有，因此，若離職員工與公司並無特別約定，除非公司同意，否則，不得提供該資料給離職員工使用；如該資料為離職員工「非職務上完成之著作」，由於著作財產權歸屬於離職員工享有，因此，離職員

工要求提供，在職員工可以提供。

**六、公司業務部門與客戶簽定的合約內容，如涉及營業秘密，可以提  
供給公司其他部門嗎？與客戶洽談時，什麼內容可說，什麼內容  
不能說呢？**

(一) 員工可否與不同部門的同事討論專案內容，或公司業務部門與客戶簽定的合約內容涉及營業秘密時，可否提供其他部門，要看專案或合約內容對應於公司營業秘密管理規範的使用權限管制，依照「need-to-know」原則，亦即「不知道的人就不該知道，該知道的人就讓他在該知道的範圍內知道」，因此，原則上專案或合約內容要限制「有需要知道的人」才可以知道。

(二) 公司人員與客戶洽談時，什麼內容可說，什麼內容不能說，應按照公司營業秘密管理規範；如洽談時，客戶要求公司先揭露部分的營業秘密資訊，以提供其評估是否進行合作，此時，公司人員應向客戶說明，公司提供給客戶的資料須依公司管理規範之規定，並報請單位主管處理，要求客戶簽訂保密協議後，再進行後續洽談。

**七、公司接到客戶委託設計製造產品，過程中涉及到相關營業秘密，  
應歸屬於公司或客戶呢？**

(一) 公司接獲客戶委託設計製造產品，如由客戶提供技術給公司製造產品，過程中未涉及技術改良，該技術自歸屬客戶所有。

(二) 如客戶下的訂購單僅提出產品規格樣式等需求，委託公司自行研發製造產品，或客戶僅提供部分技術，需結合公司在研發產品過程中作技術改良，而產出研發成果，該公司

自行研發或改良的技術應歸屬客戶或公司，應在雙方契約明定；如果契約未約定，則依個案雙方合作之關係，回歸專利法、著作權法、營業秘密法等規定，出資聘請他人研發產品，其研發創作成果之著作財產權、營業秘密等，歸屬於受聘人所有。

#### **八、公司執行專案過程中需要與外部廠商合作，可否將以前專案的部分內容，透露給合作的廠商討論？**

公司執行專案過程中，與外部廠商合作及進行討論時，可否將公司以前專案的部分內容透漏給廠商，要依公司的營業秘密管理規範之分類分級標準，按該專案資料所屬機密等級，遵守相應的管制措施。依照「need-to-know」原則，有需要知道的人只在「該知道的範圍內」知道，採取包含遮蔽專案的部分內容、簽訂保密協議等方式，此外，公司也要審慎評估合作廠商的保密機制，並要求廠商落實合理保密措施。

#### **九、公司提供報價資料、設計圖給客戶時，如何作管制，以避免被客戶拿給同行參考或利用呢？**

(一) 公司要提供報價資料、設計圖給客戶時，應依公司的營業秘密管理規範及分類分級標準，釐清報價資料、設計圖所屬之機密等級，並遵守按照該機密等級對外提供資料之管制規定。

(二) 為了避免提供資料被客戶拿給同行利用，公司可依提供資料為書面或電子檔，採取相應的管制作為。例如提供書面資料時，資料標示「機密」或「限閱」字樣，並可加上浮水印；提供電子檔資料時，資料加上浮水印或其他暗記，加註「機密、密等、公司名稱」字樣，並將資料加密，於

傳送客戶的電郵備註「本郵件及所附檔案，非經同意不得任意轉傳或提供他人」等。

**十、投資方或潛在合作者向公司詢問並取得涉及公司營業秘密的資料後，卻未與公司進行投資或研發合作，反而與第三方進行合作，是否涉及營業秘密侵害呢？**

- (一) 投資方或潛在合作者與公司洽談合作，並取得涉及公司營業秘密的資料，最後卻未與公司合作，反而與第三方合作，是否涉及營業秘密侵害，須回歸營業秘密法之規定。針對民事責任部分，指行為人因故意或過失而不法侵害他人營業秘密之情形，其侵害行為可參考營業秘密法第 10 條第 1 項規定的 5 種態樣；針對刑事責任部分，指行為人意圖為自己或第三人不法之利益，或損害營業秘密所有人之利益，而侵害他人營業秘密之行為，其侵害行為可參考營業秘密法第 13 條之 1 第 1 項規定的 4 種態樣。因此，投資方或潛在合作者是否涉及營業秘密侵害，負有營業秘密法之民、刑事責任，須依事證，並由司法機關依個案情形判斷之。
- (二) 為了避免與投資方或潛在合作者之間生意未談成，卻在洽談過程提供涉及公司營業秘密資料，公司在洽談合作時，應盡量避免揭露公司的機密資訊，如投資方或潛在合作者為了評估合作案，要公司提供相關機密資料，應由適當管理階層來決定如何提供，並評估哪些資料可提供，必要時，可請投資方或潛在合作者先簽訂保密協議，才提供資料。

**十一、公司為了防堵營業秘密被外洩，應該與哪些對象簽訂保密協議呢？應於何時簽訂較適合呢？內容為何？**

- (一) 針對公司內部員工：除了可於員工到職時要求簽訂保密協議，如員工任職部門或職務內容變動時，也可要求員工另簽保密協議；當員工提出離職，公司進行離職面談時，要提醒員工負有保密義務。
- (二) 針對公司外部的上、下游供應鏈廠商、產學合作對象，可採取以下 3 種策略步驟：
- 1、先盤點在雙方合作過程中，公司會提供哪些資訊、是否涉及營業秘密資訊。
  - 2、如公司須提供營業秘密資訊給合作對象，要先簽保密協議再提供，並且要去思考如何在「最小範圍」提供營業秘密資訊，以及用何種方式提供。
  - 3、除了公司提供給合作對象的營業秘密資訊要簽保密協議外，公司與合作對象「洽談合作」這件事，本身也需要保密，也可納入保密協議中。
- (三) 公司與員工或廠商等簽訂保密協議，內容通常會約定：員工或廠商負有保密義務，即使員工離職、公司與廠商合作終止，仍負有保密義務，不得擅自將公司機密資訊向第三方揭露或自行使用，並將屬於公司之所有檔案或文件等，歸還給公司或由其自行全數銷毀，電子檔案則應立即刪除，不得保留複本。

## **十二、公司已經與員工簽訂保密條款，是否仍需要與員工另外簽訂競業禁止條款呢？公司是否要與每位員工都簽訂競業禁止條款？**

- (一) 公司與員工簽訂保密條款，通常在要求員工不得洩漏或未經授權而使用公司的機密資訊，當僱傭關係結束或員工離

職，員工仍負有保密義務；而競業禁止條款，則是公司與員工約定在離職一定期間內，防止員工至公司競爭對手任職或自行經營與公司相同或近似之行業。基於簽訂競業禁止條款，須給予員工在該競業期間內之合理補償，因此公司可評估成本，考量是否有另簽訂競業禁止條款之需要。

- (二) 原則上，公司選擇有需要簽訂競業禁止條款的員工，要以其職務會接觸、使用公司機密資訊的員工為對象，例如研發部門負責開發公司重要技術的員工，一旦技術機密被競爭對手獲知，可能影響公司未來的競爭優勢，就有需要與該員工簽訂競業禁止條款；如員工職務內容不會接觸公司機密資訊，則無簽訂競業禁止條款之需要。

### **十三、公司對外通訊之電子郵件收發是否須進行管制，以防止營業秘密外洩？公司應該如何管制？**

- (一) 關於公司對外通訊之電郵收發，員工可能透過「發電郵」將公司機密資料寄送給競爭對手或私人信箱，另外，員工「收電郵」時，也可能點閱「釣魚郵件」，導致駭客藉機侵入公司電腦系統竊取機密資料，因此，為了防止營業秘密外洩，公司要將對外通訊的電郵收發，納入營業秘密管理機制的一環，加以管制。

- (二) 公司可以採取下列管制措施：

- 1、安裝防毒軟體，建立網路防火牆，防堵釣魚、木馬等惡意程式。
- 2、加強社交工程教育，宣導員工不要隨意點閱不明郵件或附加檔。
- 3、限制員工在公司內部資訊設備安裝或下載軟體程式。

- 4、發送電郵之檔案要加密處理，並加註「本郵件涉及機密資料，禁止擅自轉傳使用」的警語。
- 5、公司考量成本，評估是否委由外部資安公司，或公司可採購運用軟體偵測電郵關鍵字、附檔等，篩選可疑郵件進行稽核，尤其員工離職前有寄出大量檔案等情事，更需加強稽核，以防止不法外洩。

#### **十四、 疫情期間，公司開放員工在家使用筆電遠端辦公，如何管制才能防範營業秘密外洩呢？**

公司可參考以下 8 種管制策略：

- (一) 員工在家辦公地點最好在只有員工本人能進入的房間為宜，離開座位要使用螢幕保護程式。
- (二) 員工要避免利用公共或不安全的 wifi，並使用密碼保護居家 wifi。
- (三) 員工將在家辦公完成的資料電郵回傳公司，要加密處理。
- (四) 公司要建立外部連線使用員工的認證機制，針對遠端桌面或遠端登入的網路連線建立權限管理，就遠端連線之員工、上線、離線時間等進行記錄。
- (五) 限制員工遠端存取「機密資料」的權限，根據「need-to-know」原則，亦即「不知道的人就不該知道，該知道的人就讓他在該知道的範圍內知道」，僅限「有需要」使用該機密資訊的人員才有遠端存取權限，職務上沒有需要的人員，則不開放有遠端存取權限。
- (六) 針對機密等級屬「極機密」的資料，最好不要開放遠端存取。
- (七) 對於有遠端存取權限的人員所有連結、存取機密資訊之情

形，都要留下紀錄。

(八) 定期備份監控紀錄並查核有無異常情事。

## 附錄一：企業營業秘密資訊簡易盤點表

企業營業秘密盤點是整個營業秘密保護策略最重要的一環，只要企業能盤點出營業秘密之標的，以及其重要性，即能針對不同型態之營業秘密進行管理密度之規劃，因應企業規模之不同，其營業秘密資訊盤點之複雜度亦不同，為利企業對營業秘密資訊盤點能有初步之認識，本手冊提供下列簡易盤點表，以協助企業建立盤點營業秘密資訊之基礎。

部門/單位	業務內容	檔案分類	檔案形式	機密等級	經濟價值	資訊利用區域		檔案保存位置
						公司內部	公司外部	
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)

- (1) 企業內部之部門，例如研發部、製程部、採購部門或客戶服務部門等。
- (2) 關於部門所負責之業務內容，例如化學藥劑配方研發、製程改善計畫等。
- (3) 檔案分類例如研發紀錄、參考資料、會議紀錄。
- (4) 指電子檔案或紙本文件。
- (5) 依企業需要區分不同等級機密，例如極機密、機密。
- (6) 經濟價值指企業自行評估該相關資訊可能涉及之合理價值，建議予以貨幣價值量化，如高價值為新臺幣 1 億元以上、中價值為新臺幣 5 仟萬元至 1 億元、低價值為 5 仟萬以下。
- (7) 該資訊可使用之地點，如僅在公司內部，或可由公司外部連網使用。
- (8) 企業規劃保存該營業秘密資訊之位置，比如有密碼之保險櫃、不連網之特定電腦等。