營業秘密保護實務教戰手冊

2.0

‘

經濟部智慧財產局　　編

中華民國 108 年 12 月

目錄

第一章 前言

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、學共同討論，與會專家反應，營業秘密法法制面已臻完備，但司法實務之執行面發現下列兩點問題：

一、關於企業部分，對營業秘密保護之認知不足，例如未盡到採取合理保密之措施、對於營業秘密之概念不是很明確、以及擔心營業秘密於偵辦過程中二次洩露，未配合偵辦提供事證，導致營業秘密侵害案件不易偵辦。

二、關於司法人員執法部分，則遭遇偵查及審理實務之困難，特別是技術上判斷是否為營業秘密，對於不具技術專長之司法人員確實造成實際困難。

為協助企業建構更完善營業秘密保護機制，智慧局每年於北、中、南辦理「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；另於107年撰提「中小企業合理保密措施作業程序」，整理防止營業秘密外洩之重點措施，希望透過淺顯的說明，協助企業完善營業秘密保護制度，保護企業競爭力。智慧局前於102年編製「營業秘密保護實務教戰手冊」供企業參考，累積6年來之實務經驗，原手冊有與時俱進之必要，故重新編纂本手冊，提供企業更切合實務之參考，讓本手冊發揮最大之效益。

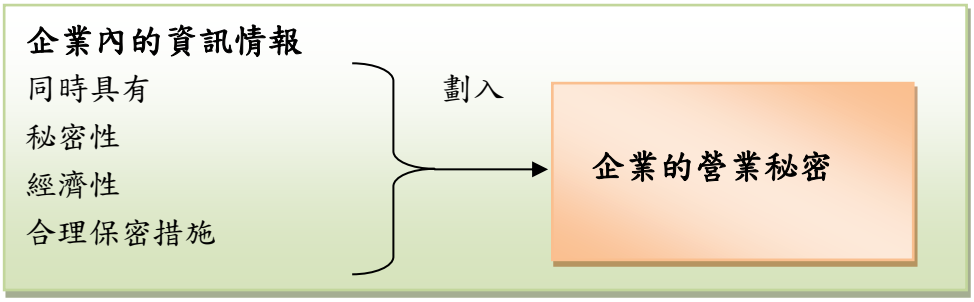
第二章 認識營業秘密

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，維持自身競爭力，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。



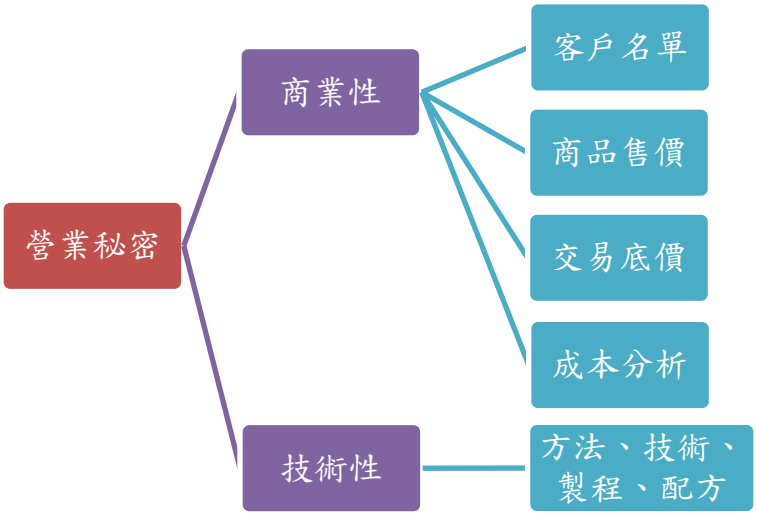
什麼是營業秘密呢?

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[1]，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。

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、

[1] 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。」

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。(台北地院 96 勞訴字第 35 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 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 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 重勞訴字第 2 號)

- 配方研發證明

原告雖與被告約定，被告所有構思、研發或從其他員工知悉之資訊，均屬原告之機密，惟非謂凡被告之構思與研發或自其他受雇人處獲悉者，均為營業秘密，否則豈非謂受雇人間任何交流之資訊均為營業秘密？原告未證明被告提供予他公司之新配方乃利用原告資源所研發，且符合營業秘密之要件，認凡被告之構思及研發均為原告之營業秘密，尚有未洽。(台北地院 99 智字第 3 號)

- 藥水配方

諸多專利證書均提及，若僅單純將無電解鍍金技術應用於 LED 製程，而無其他有別於先前技術之技術特徵，則可謂僅是系爭專利申請前早已存在的技術思想，難稱符合秘密性之構成要件，任何人亦不能宣稱已透過專利公告之技術內容為自己之營業秘密。
上訴人稱 Epithas 製程及 TMX 系列藥水係其原已存在之製程及藥水，且原本就使用於 PCB 印刷電路板上之相關製程，上訴人並販賣該藥水，且改變其配方以用於二極體晶片，倘上訴人上開說詞可採，則堪稱為上訴人所獨具之營業秘密。然被上訴人系爭專利，並未揭示任何有關該 Epithas TMX 系列藥水之配方，自難證明被上訴人曾以不正手段竊取上訴人之營業秘密，藉以完成系爭專利之研發。(智財法院 100 民專上字第 17 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、實際市場佔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」

- 製造銷售

上訴人授權穎創公司製造系爭產品，並由宏洲公司代理，基於穎創公司、宏洲公司為營利事業，其為上訴人製造及銷售系爭產品，以謀取利潤，且穎創公司、宏洲公司嗣後亦自行製造、銷售白藜蘆醇產品，則上訴人主張上開配方具有經濟性，是否無稽，非無進一步研求之餘地。(最高法院 106 台上字第 350 號)

- 機臺程式內碼

告訴人能經由本案訴訟程序獲取聲請人公司 KG-500 機台搭載之電腦程式內碼，即可撰寫出與聲請人公司所研發之特殊功能相同之電腦程式，而侵害聲請人公司之營業利益，除削弱聲請人公司直接競爭力外，亦增加告訴人公司於同業之競爭優勢，致生聲請人公司競爭力之減損。準此，KG-500 機台電腦程式之內碼，屬極具敏感性之資料，具一定之實際或潛在經濟價值，具備經濟性之要件。(智財法院 106 刑秘聲字第 1 號)

- 研發投入

原告自成立以來，每年投入鉅額資金進行 IC 晶片之研發，始能在 IC 晶片研發及生產取得技術領先全球之地位，…且除 IC 晶片之研發與生產外，原告之成本策略、組織改組資訊、客戶及商業策略、長遠之技術藍圖及研發方向等營業秘密，也是原告在 IC 晶片設計產業獨居全球領導地位的重要原因，故原告之營業秘密具有高度經濟價值，而符合「經濟性」。(智財法院 103 民營訴字第 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」

- 合理保密措施-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 年度台上字第 235 號判決參照）

- 合理保密措施-不須滴水不漏

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。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，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 刑智上訴字第 24 號）

- 合理保密措施-以正常方法無法輕易探知

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 民秘聲上字第 5 號)

第三章 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作起，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，除了要確保企業營業秘密免遭受侵害，更進一步也要避免營業秘密遭受污染，換言之，即應避免新進員工不當將前雇主之營業秘密帶入企業內部使用，若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，且用於企業之產品開發、營運等相關業務，企業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，有併科罰金之適用，將造成企業經營風險。因此，企業保護營業秘密的策略應包括內部策略及外部策略之分別，以使企業的各類重要資訊，包括商業經營策略及技術創新等相關內容，均能獲得妥善適切之保護，協助企業進一步保障其研發成果與競爭力，以避免因營業秘密侵害之訴訟造成經營管理之風險。

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。

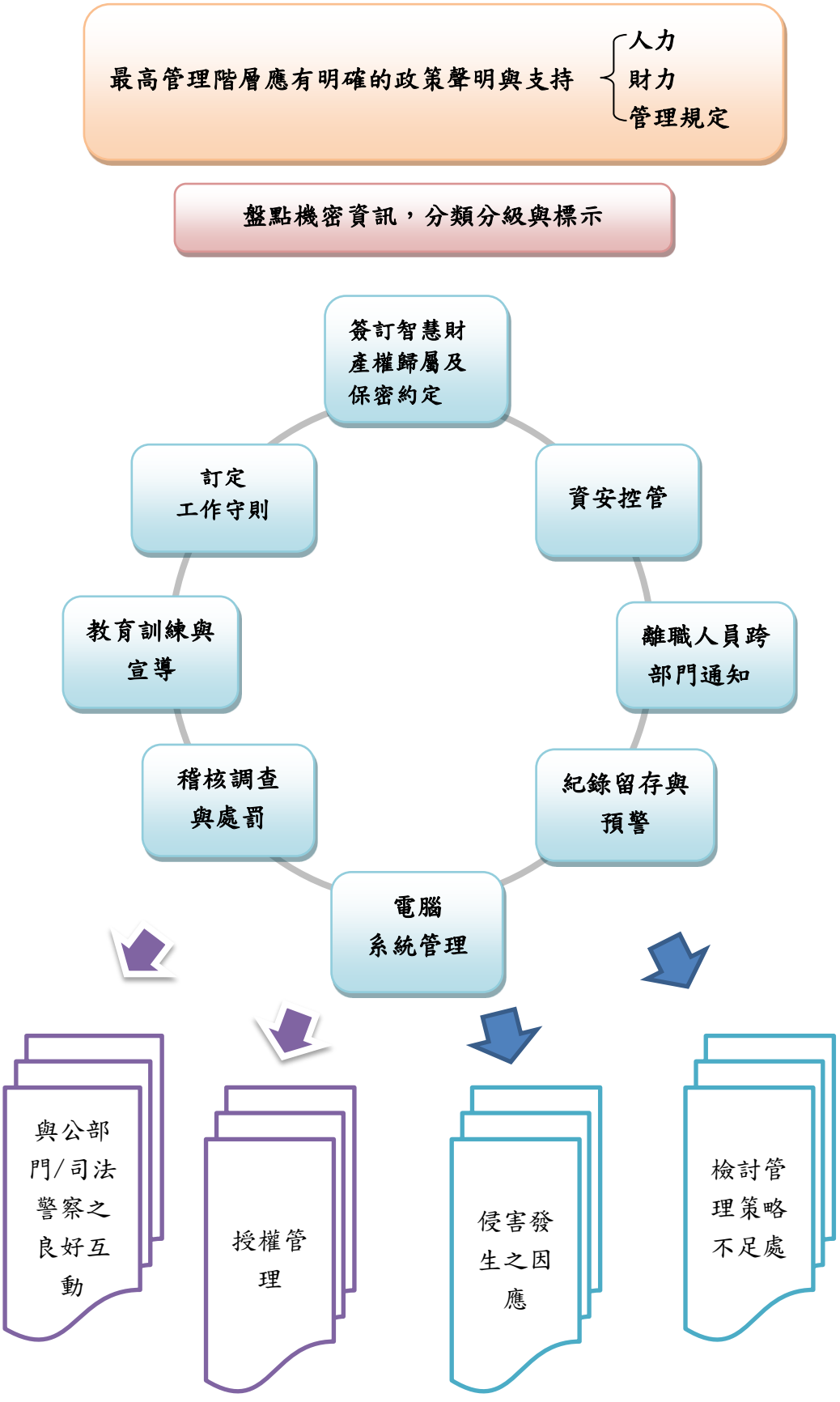
壹、最高管理階層應有明確的政策聲明與支持

企業營業秘密管理需投入大量的時間、成本,在企業財務報表上,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。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,給予人力、財力及訂立管理規定的實際支持。

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。

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
盤點機密資訊，分類分級與標示
簽訂智慧財產權歸屬及保密約定
資安控管
離職人員跨部門通知
紀錄留存與預警
電腦系統管理
稽核調查與處罰
教育訓練與宣導
訂定工作守則
與公部門/司法警察之良好互動
授權管理
侵害發生之因應
檢討管理策略不足處

貳、盤點機密資訊，分類分級與標示

一、盤點企業機密資訊：清查公司資產具有需要保密之資訊，包含有企業自行研發技術機密、他人授權或受讓之機密、企業授權他人使用之機密等，並釐清權利歸屬。

二、分級與標示：企業機密資訊依經濟價值的重要性，區分不同等級，並做標示。至少可以區分三級：第 1 級機密是企業最核心機密(例如可口可樂的配方)，第 2 級機密是會造成重大損害，第 3 級機密是會造成相當程度損害。在分級上應考量營業秘密價值及保護與工作效率之間的衡平，愈高等級的機密必採取愈高密度的管理機制，因此，妥適的分級，對於後續管理機制會有連動之關係。

三、明定依機密標示等級須遵守相關保管、使用、存取的規定：明定可接觸不同機密等級資訊的人員，非因業務需要，不應取得該等級的機密資訊。為有效防護，對機密資訊甚至可以作適當切割，每個人只能知道一部分，很少人可以知道全部完整的資訊。

四、合理保密措施會對業務運作造成不便利，也需投入成本，所以企業應依據標示的機密等級，考量可投入多少的成本資源，兼顧營運效率及保密需求，再依不同機密等級，針對保管、使用、存取等權限，實施相應的管理措施。越核心的機密資訊，企業應設定更高的機密等級，投入更多的成本加以保護。

參、訂定營業秘密保護工作守則

為利員工明確了解工作中應注意之保密規定，並於任職及保密契約約定其遵守義務，企業應訂定工作守則，以利員工遵守並進行教育訓練，工作守則至少應包括下列內容：

一、企業應明定不同之職務可接觸或使用之機密等級及類型，並應區分經營者、管理者、技術人員、行政人員等職務，落實知其所應知原則（need to know），例如總經理應僅知悉管理資訊之商業秘密為主，研發人員以知悉所負責專案之技術秘密為主，禁止探知或跨部門(團隊)討論非其負責之專案項目。

二、企業應明確告知並記載員工的職務範圍，並儘可能鉅細靡遺地載明處理業務之相關程序與方式，以便讓員工確實遵守。對有撰寫工作日誌必要之員工，應明白告知相關紀錄方式、見證、保密措施及保管的權責單位等。

三、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。工作守則對全體員工均有拘束力，務必要確認所有員工都知悉其內容。

四、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。

肆、員工到職約定、在職及離職管理

一、企業聘僱員工時，應與員工簽訂智慧財產權歸屬及保密約定，告知應遵守相關保密義務，另應特定指出不得將不法取得之他人營業秘密使用於工作或研發成果。

二、企業與他人共同研發、出資聘請他人研發等，應就研發之機密技術簽訂智慧財產權歸屬約定及保密約定。

三、當員工所任職的部門或職位變動，或是參與公司重要之專案計畫，依可能涉及的研發或營運方面重要事項，要求員工另外簽訂其他保密約定。

四、員工離職前，對員工離職前存取企業營業秘密之情況，應進行清查，如有異常應進行調查。

五、當員工離職時,企業應進行面談,提醒其注意相關保密義務，以及重申已簽訂保密契約，同時要求離職員工繳回或銷毀其所保有的所有營業秘密資訊，並留下紀錄。

六、員工離職時，應即完全斷絕其可存取企業營業秘密之權限。

七、若有必要，可與離職員工簽訂競業禁止條款，簽訂競業禁止條款應符合勞動基準法之規定。

八、一般而言，保密契約的內容，建議應包括下列事項：

（一）營業秘密範圍界定

保密契約應就可特定的營業秘密項目加以規制，簽訂契約時範圍不可過於廣泛，必須注意合理性、必要性且符合公序良俗；營業秘密之內容必須是雙方都能理解，且具有客觀認知之可能性。

（二）保密義務及附隨義務

基本的保密義務包括，營業秘密不得為目的外之使用，且未被授權之人禁止揭露營業秘密，禁止複製或攜出載有營業秘密的媒體，離職時應返還營業秘密紀錄媒體等。

（三）保密期間

應儘可能設定特定資訊之保密期間，如無法設定，則須明白記載直到該資訊之秘密性喪失前，均為保密期間。

（四）違反義務時之處理

雙方可於保密契約中載明違反相關規定之罰則，例如給付違約金或請求損害賠償等。

伍、資安控管

由於營業秘密係無體的智慧財產權，故必須附著於特定的媒介上，包括有體的紙本書面文件及無體的電子化檔案，方能對外加以表達、運用、傳遞，從而產生經濟價值與效益。而這些營業秘密的具體內容，有時候可能會散見於不同的資料中，因此必須透過適當的管理與控制，以達到有效整合企業營業秘密之目的，並可明確劃分內部員工的權責及執掌範圍。據此，針對與營業秘密相關的物或資訊，進行有制度及有組織的管理，可說是建立營業秘密保護機制之首要關鍵。

資安的管理往往被誤解成一套完整的資訊系統，但在資安的管理規定，除了針對記載營業秘密的各類載體外，亦包括存放相關資料的處所或區域之管理，如「紙本文件管理」、「電子檔案管理」、「置物櫃/抽屜/保險箱管理」、「電腦設備管理」及「區域空間管理」等範疇，另外針對非屬公司之載體、人員管制等皆應納入資安控管之一環。資安控管應包括下列項目：

一、人員進出的管制：企業裝設保全系統或配置保全人員，依授權許可之層級管控進出人員的身分、攜帶物品及停留時間等。

二、設定管制區域及規範

（一）明定特定管制區，禁止攜帶入管制區物品的定義與管制措施，例如：相機、手機、電腦等；違反者可要求其交出拍攝或錄製資料。

（二）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。建議可於保管場所之特定範圍內，於明顯位置張貼或設置「未經授權禁止進入」或「管制區域非請勿入」等警語標示。

（三）針對一般性的營業秘密，其保管場所必須上鎖，若有人要求進入，必須出示相關授權證明，並落實登記制度，以確認出入該場所之人的身分及停留時間。如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。

（四）針對高度機密的營業秘密，其保管場所應加裝高科技的認證系統，例如使用 IC 卡認證、虹膜辨識認證、指紋辨識認證等。

（五）如有外來人士進入公司洽公，櫃檯總機人員應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，甚至接觸保管文件資料之相關處所，以防重要機密遭盜取或外洩。

三、營業秘密電子檔的保密措施，可採取以下的作法

應設定可使用機密檔案系統之員工帳號、密碼及其權限。

（一）對不同機密等級之檔案，設定檔案的存取限制。重要機密檔案非經一定層級以上主管之授權，不得開放下載或複製之權限或功能，並應限制得接觸該電腦之員工身分，以降低重要機密外洩之風險。

（二）營業秘密應存放於隔離的電腦、伺服器。

（三）企業內部電腦網路應避免如可遠端存取，如有遠端存取之必要,對有權限人員及可存取機密資訊等級,應特別規範。

（四）禁止員工使用未經許可的電腦程式或外部裝置(例如可攜式的 USB）。

（五）資訊系統應設置防火牆及防毒軟體。

（六）系統對進出機密資訊電子檔的人員、存取資料應設定相關紀錄。

四、營業秘密書面文件的保密措施，可採取以下的作法：

（一）除以一望即知的不同等級文書卷區別，書面文件本體應於每一頁清楚標示機密或類似字樣，如直接在各文件頁面上以戳印加蓋或以浮水印標示「密」、「機密」、「極機密」、「絕對機密」等識別或依照公司所區分之機密等級標示，如此較不容易被塗銷、撕毀或抽換。若是由電子檔案印出者，應進一步標示印出之人員。

（二）書面文件與其他一般性文件應分別存放及保管，且存放於專屬保險櫃或特定保管區域，以避免混淆、缺漏或遺失。

（三）書面文件管理應有專責人員。

（四）明定書面文件的閱覽、修改等使用權限，對實際使用人員應留下紀錄。

五、離職人員跨部門通知管控

員工提出離職聲明時，無論口頭或書面，其主管應第一時間通報人事、資訊、保全、法制等相關單位，進行營業秘密資訊使用、複製、攜出等相關管控機制，並回溯盤點離職員工近期接觸營業秘密資訊之情形。

陸、電腦系統管理

一、應訂定網路連線的管理規則，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。

二、對於以電磁紀錄方式保存的營業秘密，應加入他人無法閱覽的技術限制，如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，以防容易遭人破解。當原管理者辦理離職或退休時，應立即刪除其 ID 及密碼,重設一組全新的 ID 及密碼,供其接任者使用。

三、強化對外部入侵的防禦，隨時注意是否有駭客或不肖人士企圖透過網路入侵而盜取資料，並應設置防火牆及防毒軟體，以防範電腦病毒之惡意攻擊；另針對存有營業秘密之電腦上安裝之軟體，必須進行嚴格之控管與篩選，不可任意安裝不必要的軟體，例如具有即時通訊功能的聊天軟體。

四、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。

柒、紀錄留存與預警

一、針對所有員工所接觸、使用機密資訊的情形，包含電腦使用、電子郵件、檔案存取及列印等情形，將 log 紀錄留存。

二、由專責單位或專人負責分析及過濾監控 log 留存紀錄，針對機密文件可採取以下作法加以監控及追蹤：

（一）是否以複製、掃描、列印、拍攝等方式產出複本。

（二）產出複本的人員、時間點、地點。

（三）是否攜出機密文件。

三、針對機密文件的銷毀，應以無法被復原的方式處理，避免銷毀資料被還原或拼貼。

四、當監控發現有異常的資料攜出、列印、下載、存取等情形時，應即刻向營業秘密專責單位或人員提出預警通知；有受侵害的疑慮時，應蒐集、保全相關證據。

五、研發或引進技術之歷程留存相關紀錄，證明技術為自主或合法授權，產品或研發成果來自企業之投入，非不法使用他人之技術。

捌、稽核調查與處罰

一、建立企業內部的稽核機制，設置負責稽核的專責單位與處理程序，調查營業秘密管理規定與相關措施的執行狀況。

二、違反營業秘密管理規定，應有處罰規定。

三、為確保有效管理，除實施內部稽核外，必要時亦可經由外部第三方驗證稽核。

四、稽核調查結果如發現員工有違規情形，可依處罰規定給予處分，且應確實執行，避免員工存有僥倖心態，且應留存處分紀錄，以作為企業捍衛宣示營業秘密的證明。

玖、教育訓練與宣導

即便針對重要資訊或保管該等資訊之處所，已採取最嚴密、滴水不露的控管方式，如果企業內部員工不了解營業秘密管理的重要性，缺乏相關的認知意識，仍然無法達到有效管理營業秘密之目的。因此，公司平時必須並定期舉辦相關的教育訓練課程或研習活動，向員工宣導相關的法令、規定及罰則，以全面提升員工對營業秘密管理的認識。

一、推行營業秘密教育訓練，員工不論是否為營業秘密的管理者或被授權人，均應對營業秘密的價值及重要性有所認知，因此，企業必須辦理持續且有效的教育訓練研習，向員工傳授與宣導營業秘密管理的重要性、管理組織的概要、具體的管理規則及機密洩漏後之適當處理方式等內容。

二、可運用以下方式定期及不定期提醒員工，以有效傳達至企業的每個成員：

（一）定期舉辦特定的研習課程，且配合考試確認員工已了解公司營業秘密之政策及規定。

（二）應善用各類員工聚集的場合(例如晨會或工作會議)，隨時提醒員工注意營業秘密管理相關事項。

（三）利用文康活動、員工旅遊等場合宣導。

（四）於員工進出口及必經途徑設置相關文宣。

三、保留各種訓練紀錄，作為企業提出落實合理保密措施的證明。

四、企業應向有合作關係的廠商，進行設置或遵守企業合理保密措施的要求。

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

企業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，除汲取其它成功企業營業秘密管理保護之經驗，亦能就企業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,企業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。

拾壹、侵害發生之因應

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）確認竊取營業秘密管道

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、防範營業秘密洩露擴大，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，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，愈多告訴範圍，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，不以提告標的數量考量，營業秘密標的愈多，反而致生二次洩露之風險。

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，應考量後續提出輔助偵查之證據是

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 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「檢察機關辦理重大違反營業秘密法案件注意事項」，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。

拾貳、檢討保護不足之處

一、檢討營業秘密遭侵害之途徑

營業秘密發生侵害情事，代表保護或管理策略尚有再提升或缺漏之必要，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，且應注意企業所能投入之資源，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。

拾參、營業秘密授權管理

一般而言，營業秘密所有人採營業秘密保護之資訊，為保持秘密性，甚少授權他人使用，但企業有時考量生產機具之訂制、生產成本考量等因素，最後決定有授權必要性，授權前應考量下列事項：

一、評估被授權之營業秘密等級，一旦被洩露是否動搖企業根本，此類營業秘密不應授權，不宜離開企業管理監督之範圍。

二、評估被授權廠商之營業秘密管理措施，是否足以達到保密之效果，且應依營業秘密之類型不同，進行管理措施之檢核及認證，檢核通或認證過者，才得以被授權使用。

三、與被授權廠商簽訂保密契約及訂定罰則，並要求被授權廠商對接觸之相關職員，應簽保密約定、進行保密教育訓練。

四、建立稽核機制，定期及不定期檢視、考核被授權廠商之營業秘密管理措施。

第四章 營業秘密Q&A

一、什麼樣的資訊需要營業秘密保護?

常見保護智慧財產之方式，包括以商標、著作、專利及營業秘密等，其中專利及營業秘密交互結合運用，是企業在智財成果保護方法值得採取之方式，雖然以營業秘密保護，訂有刑事責任之規定，但企業仍應評估該類資訊是否適合，建議於評估採取營業秘密或專利保護時，可考量下列事項：

(一)標的之性質

營業秘密可區分為商業秘密及技術秘密，但專利只保護方法及物，因此，屬於商業資訊，如客戶名單、營運計畫、生產成本、商業方法等，無法申請專利，應以營業秘密保護。技術秘密如選擇以專利保護，則技術內容必須公開，日後只能獲取授權金或請求損賠，如以營業秘密保護，則可依產品價值自定價值，例如可口可樂的配方就不宜以專利保護，因為一旦公開，就失去獨家配方技術而失去競爭力。

(二)保護之期間

營業秘密只要符合具秘密性、經濟性及具有合理保密措施等三要件，營業秘密所有人可選擇永久保護，最知名的案例是可口可樂之配方。專利權之保護期間，按申請專利之類型不同，分別是發明專利權期間為20年、新型專利權期間為10年及設計專利權期間為15年。因此，由企業評估技術或產品應保護期間及方法，但營業秘密與專利保護之選擇並非互斥，企業可選擇部分以營業秘密保護，部分以專利權保護，或是研發前期及技術剛研發成功，選擇以營業秘密保護，技術成熟或一定期間後，為防止競

爭者仿製或技術領先優勢降低，可提出專利申請亦為交叉保護之方式。

(三)是否可藉由還原工程(逆向工程)仿造

採取營業秘密保護之技術，雖然無保護期間之限制，但不具有排它權利，倘有競爭者透過還原工程仿造相同的產品，並不會有違反營業秘密之問題，因此，容易 由還原工程仿造之產品或技術，應優先考慮專利權之保護。

「司法實務見解」

●還原工程

所謂還原工程，係指針對可公開取得之已知產品，經由逆向程序，逐步解析以獲得該產品之規格、功能、組成成分、製作過程或運作程序等技術資訊之方法。經由還原工程知悉其他事業之營業秘密並不構成營業秘密之侵害。系爭產品業已上市銷售，則由市場交易流通取得系爭產品，得據以知悉其電路板之電路布局，而電路板之電路布局係依據電路圖所揭示之電子元件間之連接關係、實際電路板之尺寸、層數等，所為之實際電子元件配置位置與連接線走線等之平面或立體配置，從而得據以解析而獲得該產品之電路圖，依上開說明極難謂系爭產品之電路圖或電路布局具有秘密性，要難認係營業秘密法所謂之「營業秘密」(智財法院 104 民營第 3 號判決)

(四)舉證責任

不論是專利權受侵害還是營業秘密受侵害之證明，皆需由專利權人或營業秘密所有人舉證提告，因此，進行評估時，應考量兩者在維護權利舉證的難度，如果是採專利權保護，應評估專利權受侵害時，侵權人之產品或方法是否落入申請專利範圍、是否為同一產品或技術之舉證難易、以及面對專利有效性之挑戰，如果採營業秘密保護，所有人證明符合秘密性、經濟性與具合理保密措施之難易度，且避免於司法程序中失去秘密性要件。

(五)維護費用

選擇專利權保護，需繳交申請費、審查費、證書費及每年的年費，選擇營業秘密保護，雖然無須繳交規費，但需持續在合理保密措施建置上持續投入，若未積極建置合理保密措施，除有未符合營業秘密三要件之風險，也可能易受侵害。

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、企業內有那些人有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、員工複製公司資料帶回加班，並儲存在家中個人電腦，離職後忘記刪除，是否該當營業秘密罪之要件？行銷部門離職員工之電腦中，發現研發部門之重要資訊，是否可能構成營業秘密之侵害？

（一）員工在職期間，為完成工作之目的，如經公司許可，複製公司資料回家處理，係屬正當行為，但離職時必須確認刪

除或繳回，員工如忘記刪除，由於非屬故意，因此，可能不構成犯罪，但具體個案是否構成犯罪，仍應依法院判決認定。

（二）公司研發部門持有之機密資訊，行銷部門某程度上亦有知悉之必要，才能針對產品之特性與功能加以推廣行銷，所以實務上可能會從持有資訊之多寡、範圍及時間，去判斷是否構成營業秘密之侵害行為，不會單純從是否屬於同一部門去做認定。

（三）目前很多公司都會推行知識管理之制度，但建議公司不要將極具重要性與價值性的營業秘密納入員工分享知識管理之範疇，因為知識管理之目的是希望員工多方學習，與營業秘密必須具備秘密性，越少人知道越好之特性不符。

五、離職員工要求在職員工傳送或交付一份他先前製作之資料，是否構成營業秘密之侵害？

依營業秘密法第 13 條之 1 第 1 項第 2 款之規定，員工不得未經公司授權或逾越授權範圍，而使用或洩漏公司之營業秘密。因此，在職員工傳送資料給離職員工如果該資料為公司之營業秘密，雖為前員工之前之資料，仍會構成營業秘密之侵害。

六、員工長期在某一領域工作，因而累積許多該領域之智識技能，轉職後如果僅是自然地將所學應用在新公司的業務上，是否構成營業秘密之侵害？

（一）所謂記憶抗辯，係指係指員工於特定領域工作已久，累積了相當深厚豐富的專業知識與技能，但該等資訊都只存在於該員工腦中，其離職後並未竊取或下載任何公司文件資料，至新公司後自然地將其腦中具備的智識分享給新公司

的成員，是否亦構成營業秘密之侵害？有關此一問題，由於目前我國實務上,針對此種行為是否構成營業秘密侵害，尚未有相關司法判決。是以，茲介紹美國「必然揭露理論」(Inevitable Disclosure Doctrine)之內涵、判斷標準及適用現況，作為我國未來處理此類事件之參考。

（二）所謂「必然揭露理論」,係指美國法院於前雇主主張營業秘密有被離職員工不正洩露之威脅或危險，而聲請假處分救濟時，經由案例累積所建立之原則。美國法院適用必然揭露理論之判斷標準如下：

1.新雇主是否為前雇主之直接競爭對手。

2.新舊雇主之產品或服務相似度高低。

3.所處行業別及各該營業秘密之性質。

4.系爭營業秘密是否對新舊雇主都有很高之經濟價值。

5.離職員工或新雇主是否缺乏誠信。

6.離職員工之新工作與其舊工作是否幾乎相同。

7.離職員工是否有簽署保密條款或競業禁止約定。

8.前雇主為防止營業秘密洩漏所做的努力。

9.是否確有營業秘密侵害行為出現。

10.前雇主能否明確指認特定營業秘密之暴露風險。

（三）美國適用現況：

1.部分法院承認「必然揭露理論」,認為前雇主可主張「必然揭露理論」,以限制其離職員工受雇於競爭對手，其實質效力等同於競業禁止條款。

2.不承認「必然揭露理論」之各州，雇主唯有仰賴訂定周延之競業禁止條款，始得有效保護其營業秘密。

七、營業秘密法第 13 條之 1 第 1 項第 3 款的適用前提是否須被告知人有刪除義務？告知須告知到何種程度？如果是有合作關係的 A、B 公司，A 公司將秘密交給 B 公司，合作結束後，A 公司告知 B 公司刪除，B 公司不從，是否亦有本款之適用？

（一）第 13 條之 1 第 1 項第 3 款規定，持有營業秘密人，經營業秘密所有人告知應刪除、銷毀，被告知人負有刪除之義務。

（二）必須依照實際個案情形加以認定，才能判斷營業秘密所有人是否確實有告知對方刪除。

（三）本款不限於公司與員工間才能適用，公司之間當然也適用。

八、如員工竊取公司機密後，即轉至外國公司任職，則公司對其提起營業秘密侵害訴訟，是否有其實益？又應如何蒐證或進行相關訴訟程序，獲致勝訴判決之機會較高？

（一）在我國境內竊取營業秘密後，意圖在外國、中國大陸或港澳地區使用者，加重其刑。因此，公司當然可以對竊取營業秘密後，轉至外國公司任職之員工提起訴訟。

（二）至於如何蒐證或進行訴訟程序，才能提高勝訴之機會，仍須視個案情況而定，建議公司必須事先妥善蒐集相關事證，包括提供充分證據證明遭竊取之資訊確屬營業秘密，以及釋明員工確有不法取得、使用或洩漏公司營業秘密之行為。

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、機密或密。
(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。