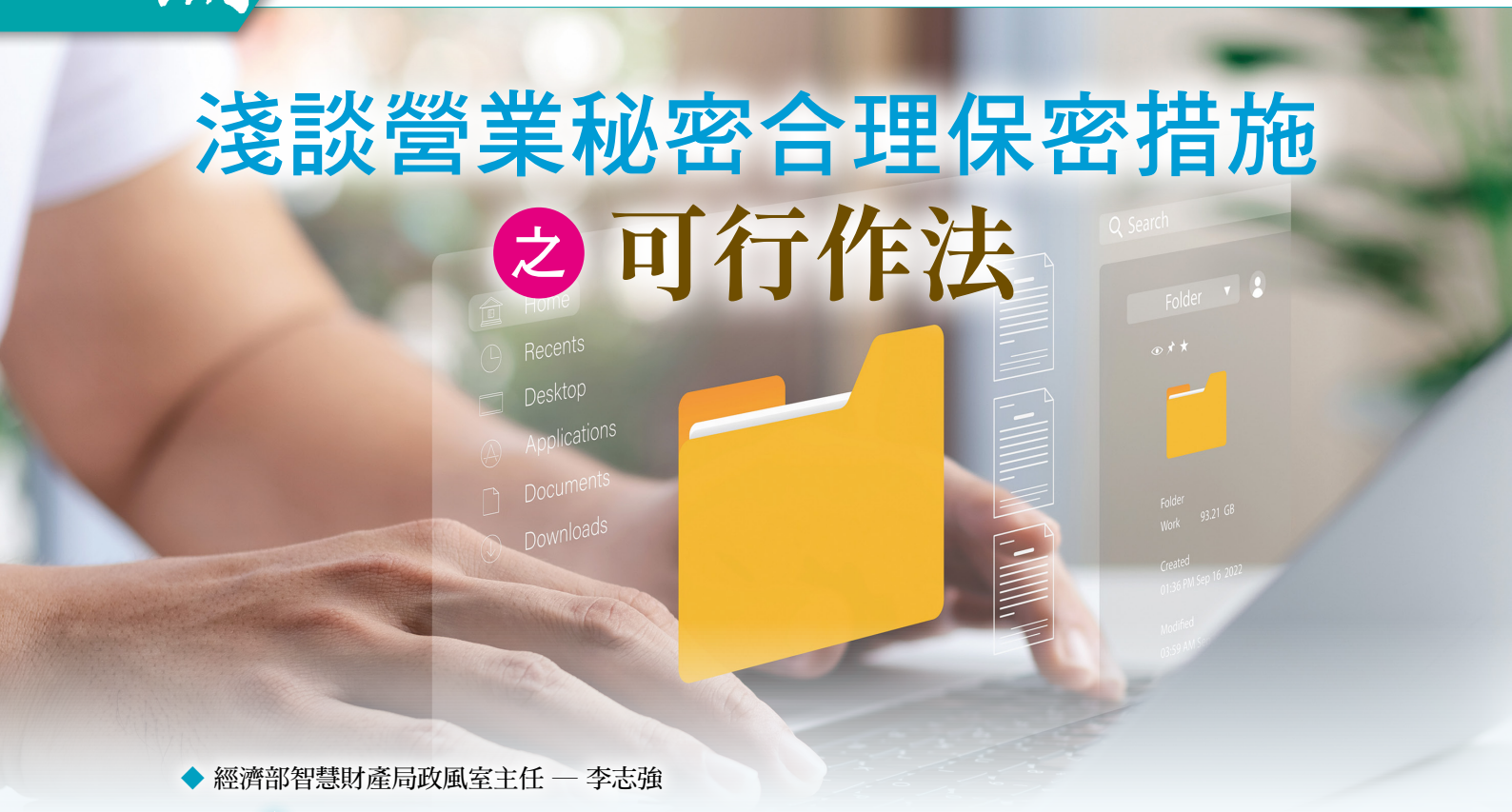
淺談營業秘密合理保密措施之可行作法



◆ 經濟部智慧財產局政風室主任 — 李志強

依《營業秘密法》規定，得作為該法保護之營業秘密，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，而具有秘密性（非一般涉及該類資訊之人所知）、經濟價值（因其秘密性而具有實際或潛在之經濟價值）、保密措施（所有人已採取合理之保密措施）3要件者，其中又以合理之保密措施為構成營業秘密與否之關鍵。

重要觀念

營業秘密價值乃在其秘密性，營業秘密一旦被揭露，其經濟價值即將銳減甚至消失，此即所謂「一旦喪失就永遠喪失」（once lost, is lost forever），故營業秘密所有人如有保密意圖，且已採取合理之保密措施，以維護其秘密性，而將營業秘密「合理揭露」提供予特定之他人，不論係基於事業活動之信賴關係，或僱傭、銷售等契約中之保密條款，仍不失其秘密性，顯見營業秘密之秘密性，係屬相對而非絕對。換言之，營業秘密所有人若採取適當合理之保密措施，可認定該項資訊值得成為營業秘密保護客體之判斷依據；反之，若未加重視或加強就特定資訊之保護，則法律亦無加以保護之必要。

由此可見，合理保密措施係構成及保護營業秘密的重點之一，對此提出以下幾點建議：

一、小型或新創企業，因其經營模式、商業方法及技術研發等，係隨著營運而累積相關資訊，但因尚未展現經濟上

小型或新創企業在經營初期構想或研發時應重視資訊保護，儘早採取措施避免營業秘密遭攜出。

企業應盤點機密資訊、釐清權利歸屬，並依經濟價值分類分級，加以限制知情人員的授權等級。

之價值，致忽略相關資訊之保護。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，以符合秘密性與合理保密措施之要求，同時避免營業秘密遭輕易攜出。

二、企業在決定保密措施前，應先盤點所屬機密資訊，並釐清權利歸屬，另依經濟價值之重要性進行標示與分級。營業秘密所有人應衡量其人力、財力，依一般社會認知之方法或技術，將內部情報資訊依業務需要分類、分級，並由不同之授權職務等級者知悉。

三、合理保密措施必須「有效」，方能維護其資訊之秘密性，惟不要求須達「滴水不漏」程度，將相關資訊以一般社會認知不易被任意接觸之方式予以控管，亦即以正當方法無法輕易探知，能達到保密之目的即符合。

四、按司法判決實務認為，中小企業因資源、經費、員工數均有限，依公司規模採取合理之保密措施即可。

可行作法

為協助企業瞭解並落實保密作為，茲參酌經濟部智慧財產局營業秘密保護實務教戰手冊 3.0，並綜整司法實務見解分就員工管理、檔案管理、空間及設備管理等部分說明如下。

一、員工管理

企業對於員工採取保護營業秘密措施，建議可依新進員工、在職期間及離職等不同階段，分別進行動態管理。

（一）新進員工管理

1. 報到時即要求簽訂保密協議，約定職務上知悉或持有企業未對外公開之檔案均應保密，而未經同意不得任意使用或交付他人，於離職後仍負有保密義務。
2. 與員工簽訂智慧財產權歸屬約定。
3. 應由部門主管或指定人員交付營業秘密管理規範，提供新進員工簽收，說明保密內容、機密分類分級標準及使用權限等，確保員工已有認知。

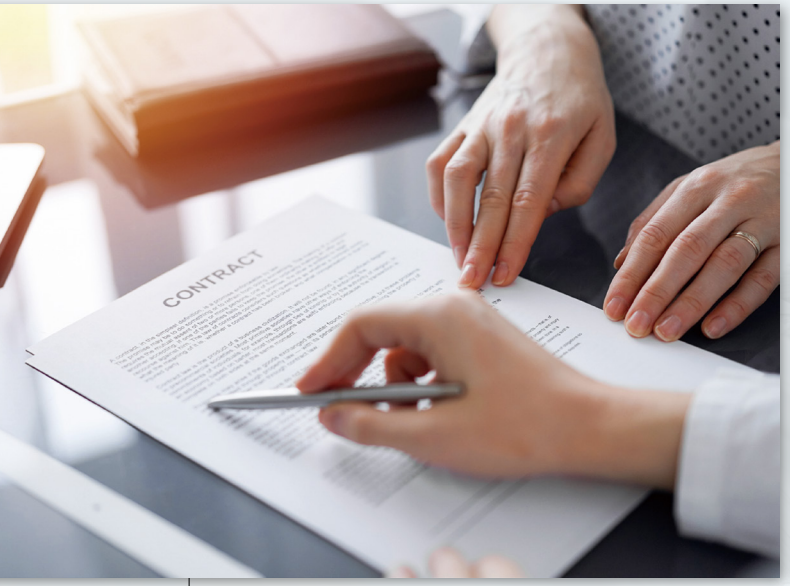
4. 落實查核工作，包括確認是否與前公司簽訂競業禁止約定，並瞭解其於前公司之職務內容；另要求不得將前公司營業秘密攜入使用，且簽切結保證書。

（二）在職期間管理

1. 當職務調動時，要求提出調職切結書，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。
2. 告知新職務內應遵守之營業秘密管理規範，重新調整存取、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。
3. 依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

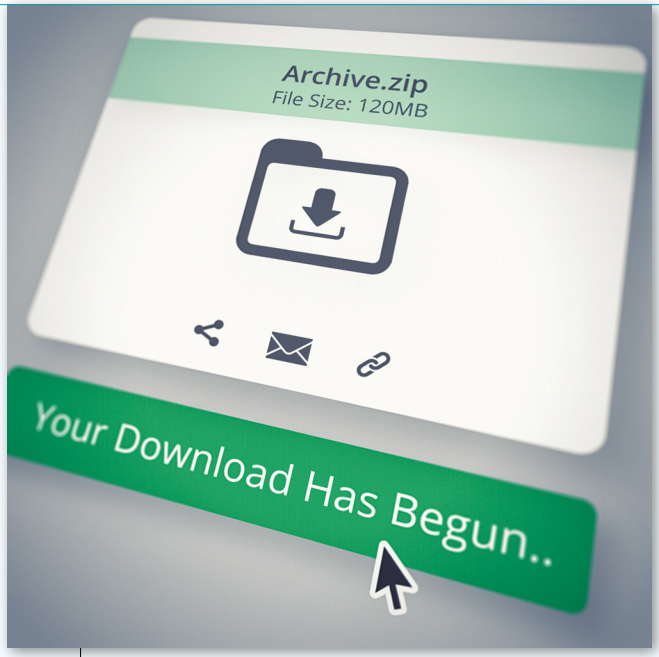
1. 進行離職面談，詢問離職原因及未來規劃，提醒遵守保密義務，且要刪除或歸還所持有的機密資料，不得留存備份，並作成離職切結書。
2. 從提出離職申請至實際離開期間內，企業可啟動稽核，如發現有異常存取、下載機密檔案紀錄，或有異常加班、出入管制區域等情形，應進行調查並保存相關證據。
3. 離職當天，立即取消該員工登入資訊系統之權限。
4. 由於簽訂競業禁止約定，* 必須給予在該競業期間內之合理補償，因此企業可評估成本，考量是否有另與離職員工簽訂之需要，若有需要，約定條款應符合《勞動基準法》（含細則）等相關規定。
5. 追蹤後續是否有違反競業禁止約定之情事。



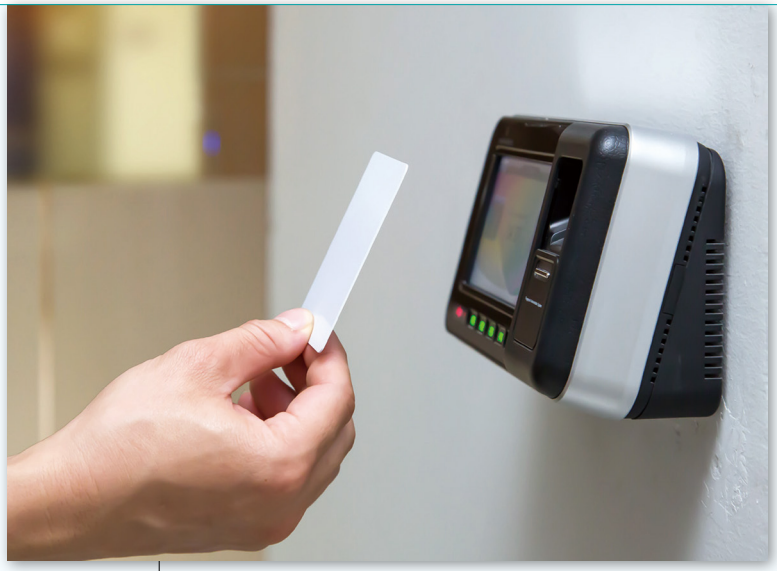
對於新進員工的管理，最好在報到時即要求簽署保密協議，且離職後仍負有保密義務。

針對在職期間的管理，若有職務調動，須告知新職務的營業秘密規範，並更新存取、使用機密檔案之權限。

* 所稱競業禁止約定，是企業與員工約定在離職一定期間內，防止員工至競爭對手任職或自行經營相同或近似之行業。



在員工離職管理方面，從提出離職申請至實際離開期間內，企業可啟動稽核機制，檢核是否有異常存取、下載機密檔案紀錄。

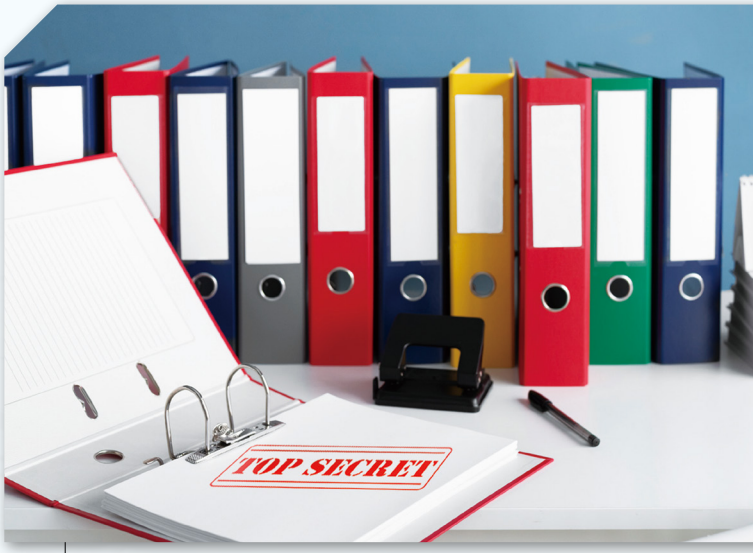


異常加班、出入管制區域等情事也屬於欲離職員工的行為稽核範圍。

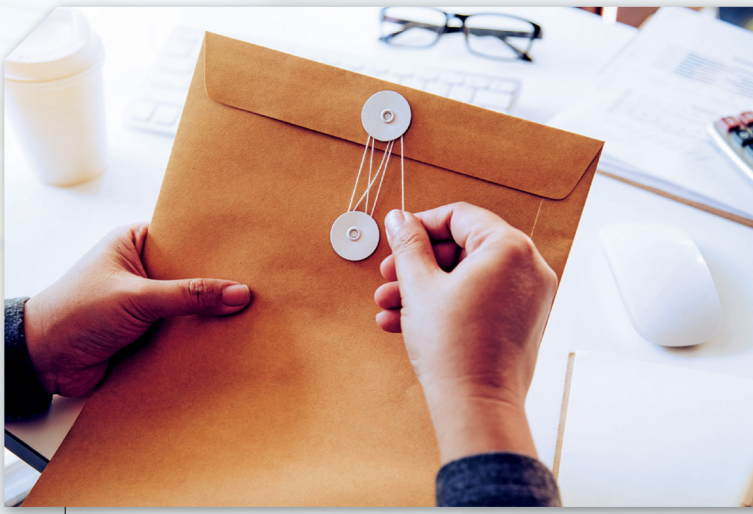
二、檔案管理

（一）紙本檔案管理

1. 內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。
2. 明確規範不同機密等級紙本檔案存放、閱覽、使用權限範圍。
3. 指定專責管理人員，建立機密紙本檔案編號造冊機制。
4. 依存放規範，將機密紙本檔案交由員工或專責管理人員保存於特定保管區域，並定期清查核對。
5. 機密紙本檔案複本應加蓋「複本」戳記，並視同原件管理。
6. 於傳遞機密紙本檔案時，應採如密封等妥善保護。
7. 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身分及權限，僅具使用權限者始可



紙本檔案應進行不同機密等級分類，並規範不同等級紙本存放、閱覽、使用權限範圍。



如需傳遞機密文件，應採密封保護。

提供；且其閱覽、使用、歸還等情形，均應留下紀錄。

8. 定期檢視符合銷毀條件之機密紙本檔案，並確保銷毀後無法被復原。

（二）電子檔案管理

1. 依機密資訊分級標準標註不同機密等級，並設定密碼保護，必要時可加入浮水印或特殊暗記。
2. 設置專責單位或人員規劃、執行電子檔案管理機制。
3. 設立不同機密等級電子檔案之密碼控管與存取使用權限，分級分類儲存資料。
4. 機密電子檔案之存取及複製、列印、對外傳輸等 log 記錄須留存，由專責單位或專人檢視追蹤。
5. 電郵檔案均須加密處理，並加註警語，例如「本郵件涉及機密資料，禁止擅自轉傳使用」。
6. 存有電子機密檔案的內部資料庫、系統等，規範須以帳密登入；高度機密檔案，除非獲事先授權，不得開放閱覽或使用權限。
7. 內部資料庫或系統原則應避免遠端連線，如職務上有遠端連線需要，須先獲取授權，並對接觸之權限及範圍予以規範；但若屬「極機密」檔案，應禁止開放遠端連線。
8. 遠端連線所有連結、存取機密檔案紀錄，均需留存。

三、空間及設備管理

（一）空間管理

1. 視不同專案項目或實務狀況，設置個別管制區，管制區僅限處理該專案人員進入。
2. 管制區張貼「管制區域禁止進入」、「禁止拍照攝影」等警語，並可另加設置如「禁止擅自攜離任何物品或紙張」等警示。
3. 明定禁止攜入管制區物品定義，如手機、相機，或具有攝影、錄影、

內部系統應避免遠端連線，若有需求須設置權限範圍，並留存所有連結、存取機密檔案紀錄，且禁止開放極機密檔案。

錄音、資料交換等功能的電子裝置，以及管制措施。

4. 配置保全人員或監視設備，管制進出人員、時間及攜帶物品；可考慮內部人員以識別證區分權限，外部人員則須事先申請並由專人全程陪同進入。
5. 若經費許可，涉及極機密資訊之保存場域可加裝虹膜辨識、金屬探測等高科技管制設備。

（二）設備管理

1. 建立電腦設備或資訊系統之防禦機制及網路連線使用管理規定。
2. 設置防火牆及防毒軟體，防堵釣魚、木馬等惡意程式。
3. 管制員工於辦公室使用雲端或外接儲存設備。
4. 禁止在內部資訊設備安裝或下載軟體程式，並宣導勿隨意點閱不明郵件或附加檔。
5. 公務電腦設備或網路伺服器規範須以一定強度之帳密進行登入，密碼須定期更新並禁止提供他人使用。
6. 建立遠端桌面或登入等外部連線使用認證機制及權限管理，並就遠端連線之活動狀況等進行記錄。

結語

營業秘密之保密措施，強調的是合理性並非滴水不漏，鑑於近來國內發生數起惡意挖角或離職員工為提高跳槽身價而「帶槍投靠」案例，為杜絕類似竊取營業秘密情事，建議可參考上述可行作法製作檢核表，並依人力、規模及預算等，針對員工管理擇定執行重點，後續適時進行滾動式修正比照；若查有員工於任職期間或離職後有違反約定情事，應採取法律途徑，以維企業權益。

企業應配置保全與監視設備，管控進出人員與物品。

空間及設備管理中，資安控管尤其重要，可以透過建立防禦機制、設置防火牆、管制外接存儲等作法，以進行有效防護。