中小企業營業秘密保護機制檢核表

【110.06.08版】

檢核項目	檢核指標
1.建立明確營業秘密保護管理政策	□1.1 指定營業秘密專責管理單位/人員。 □1.2 編列營業秘密保護管理機制經費。 □1.3 依員工職位職務，擬定不同的智慧財產相關約定： □1.3.1 保密約定。 □1.3.2 智慧財產權約定。 □1.3.3 競業禁止約定。(應符合勞基法第9條之1規定) □1.4 導入營業秘密管理規範： □1.4.1 檔案分級標準。 □1.4.2 檔案使用規則。 □1.4.3 紙本檔案管理。 □1.4.4 電子檔案管理。
2.新進員工管理	□2.1 簽訂保密約定： □2.1.1 職務上知悉或持有公司未公開之檔案，皆應保密。 □2.1.2 應保密之檔案，未經公司同意或授權，不得使用，交付或洩漏予第三人。 □2.2.3 員工離職後仍負有保密義務。 □2.2 約定職務上創作或研發成果之智慧財產權歸屬。 □2.3 簽訂競業禁止約定： □2.3.1 離職後之競業禁止期間未超過2年。 □2.3.2 競業禁止期間補償金未低於勞工離職時月平均工資50%。 □2.3.3 競業禁止之範圍，應限於與公司從事相同或類似業務，並具競爭關係者。 □2.4 新進員工之查核： □2.4.1 確認新進員工是否違反與前公司簽訂之競業禁止約定，並了解其於前公司負責之工作內容。 □2.4.2 新進員工應切結保證未攜帶前公司營業秘密進入公司使用。 □2.5 告知工作內容及應遵守之營業秘密管理規範。 □2.6 依員工工作內容，設定員工使用公司資訊設備之權限。
3.紙本檔案管理	□3.1 公司內部及外部紙本檔案，應標註機密等級。 □3.2 紙本檔案陳核後，單位主管得變更機密等級。 □3.3 分級保存： 依檔案機密等級，將機密紙本檔案由專責管理人員，或由員工自行保存於隔離空間。

檢核項目	檢核指標
	□3.4 建立造冊管理機制： 專責管理人員應建立機密紙本檔案編號造冊機制，統一管理或供各單位員工遵守實施。 □3.5 閱覽、使用機密紙本檔案之管理： □3.5.1 員工應依權限申請閱覽、使用機密檔案。 □3.5.2 專責管理人員應登記並確認員工身分及其權限後，提供機密紙本檔案。 □3.5.3 機密紙本檔案歸還時，專責管理人員應記錄歸還者身分及時間。 □3.6 建立機密紙本檔案銷毀 SOP： 定期檢視已逾保密期限或符合銷毀條件之機密紙本檔案，並按 SOP 進行銷毀。
4.電子檔案管理	□4.1 建置完善資訊設備及使用監控機制： □4.1.1 公司雲端硬碟及內部資訊系統、伺服器、及電腦等資訊設備應設置防火牆、安裝防毒軟體，並更新至最新版本。 □4.1.2 針對公司內部資訊設備之軟體安裝及連接外部裝置(如可攜式 USB、外接式硬碟)情形，設置監控機制。 □4.2 設置專責人員負責規劃、執行機密電子檔案管理機制。 □4.3 員工新增使用之電子檔案，應標註機密等級，機密檔案編號，予以納管。 □4.4 依機密等級，分級分類儲存。(如儲存於公司伺服器、雲端或個人電腦) □4.5 存取、使用機密電子檔案之管理： □4.5.1 視電子檔案機密等級與保密需要，於存取或傳輸電子檔案時，設置密碼控管。 □4.5.2 對機密電子檔案存取及複製、列印、對外傳輸等使用之情形，建置 log 紀錄及檢視機制。 □4.5.3 建立電子郵件管制程序，對郵件內容或附件含有機密檔案關鍵字或競爭公司名稱之偵測預警。 □4.6 建立機密電子檔案刪除 SOP： 定期檢視已逾保密期限或符合銷毀條件之機密電子檔案，並按 SOP 進行刪除。
5.稽核與處分	□5.1 建立稽核預警 SOP： 由專責人員定期或不定期抽檢管理成效，並將下列紀錄陳報公司營業秘密管理高層長官：

檢核項目	檢核指標
	□5.1.1 機密檔案閱覽、存取、使用紀錄。 □5.1.2 公司雲端硬碟、內部資訊設備之軟體安裝及連接外部裝置之監控記錄。 □5.1.3 員工電子郵件偵測預警紀錄。 □5.2 建立營業秘密管理規範改善 SOP： 抽檢發現營業秘密管理有缺失時，陳報營業秘密管理高層長官，啟動改善 SOP。 □5.3 建立違規處理 SOP： □5.3.1 抽檢發現員工違規情事，應依 SOP 通報權責人員處理。 □5.3.2 視員工違反公司營業秘密管理規範之情節，評估採取內部處分或通報檢調提出告訴。 □5.3.3 採取內部處分，應詳實記錄違規事實及處分內容，並編製案例宣導。
6.員工在職期間管理	□6.1職務調動員工陳報及聲明義務： □6.1.1 員工陳報自行保存之機密檔案，並交還原任職單位。 □6.1.2 職務調動員工提出調職切結，保證自行保存之機密檔案，已全數交還、交接，且複本皆已銷毀、刪除。 □6.2 公司針對職務調動員工之管理： □6.2.1 視員工新工作內容及可能接觸之機密檔案，評估是否重新簽訂保密、智慧財產權及競業禁止約定。 □6.2.2 告知員工新工作內容，及應遵守之營業秘密管理規範。 □6.2.3 依新工作內容，調整員工存取、使用機密檔案之權限。
7.員工離職處理	□7.1 建置回溯盤點離職員工閱覽、存取及使用機密檔案之機制。 □7.2 經盤點發現員工閱覽、存取或使用機密檔案異常情況，應進行調查 SOP。 □7.3 與員工進行離職面談，告知離職員工應刪除、銷毀自行保存之機密檔案，並作成離職切結(書面或電子)。 □7.4 員工離職後，應即刪除離職員工登入公司資訊設備、電子信箱之帳密及使用權限。 □7.5 追蹤員工是否違反競業約定，於競爭公司任職。
8.營業秘密教育	□8.1 定期訓練及考試：

檢核項目	檢核指標
訓練	□8.1.1 定期舉辦員工營業秘密管理規範訓練課程。 □8.1.2 針對營業秘密管理規範訓練課程，舉辦訓練考試，且要求全體員工須滿分通過。 □8.1.3 妥善保存營業秘密教育訓練紀錄。 □8.2 不定期宣導： 於適當之場合，提醒員工注意保密事項，並設置保密文宣。
9.委外廠商、協力廠商及外聘人員管理	□9.1 與委外廠商、協力廠商及外聘人員簽訂保密約定： □9.1.1 應保密之檔案，未經公司有權限之人同意或授權，不得使用，交付或洩漏予第三人。 □9.1.2 是否得針對機密檔案所含技術予以改良。 □9.1.3 技術改良後所得智慧財產權歸屬之約定。 □9.2 依公司營業秘密管理規範，選擇得揭露與提供委外廠商、協力廠商，或外聘人員管理使用之機密檔案。 □9.3 建立對外提供機密檔案之管理清單、定期檢視機制。 □9.4 建立委外廠商、協力廠商或外聘人員保密管理措施之檢視機制。 □9.5 建立委外、協力或外聘契約終止或解約時，營業秘密處理 SOP，尤其應要求下列事項： □9.5.1繳回機密檔案。 □9.5.2使用機密檔案及相關成果之說明。 □9.5.3告知並要求銷毀、刪除機密檔案複本聲明。
10.營業密秘保護外部互動	□10.1 適時參與營業秘密保護研討會及宣導活動。 □10.2 與法務部調查局或內政部保二總隊等司法警察建立聯絡窗口。

運用檢核表之備註參考：

一、公司保密、智慧財產權及競業禁止約定；公司檔案分級標準、使用規則及管理等營業秘密管理規範，可視公司業務需求，擬定公司通用規範，或各單位部門各自訂定不同規範。

二、機密檔案分級標準建議至少分為以下3級，並註明得揭露與提供委外廠商、協力廠商使用之機密檔案：

第1級機密：企業最核心機密

第2級機密：洩漏將造成企業重大損害之機密

第3級機密：洩漏將造成企業相當程度損害之機密

三、與新進員工或職務調動之員工簽訂保密、智慧財產權歸屬及競業禁止約定等事宜，可視公司職務分工，由人資單位或員工單位主管辦理。

四、公司稽核、預警 SOP、營業秘密管理規範改善 SOP 及違規處理 SOP 等相關

事項，可視公司職務分工，由人資單位、營業秘密專責管理單位、資訊單位或員工單位主管辦理。