希華晶體科技股份有限公司
資訊安全作業管理辦法

一、目的：建立公司資訊作業管理之各項作業方式，使各部門電腦資訊作業能正常運作，以確保資訊系統之正確執行。

二、適用範圍：本辦法適用於本公司『電腦管理資訊系統』及相關作業之管理。

三、名詞定義：無。

四、作業辦法：

4.1 組織、職責及教育訓練：

4.1.1 資訊單位

A. 經營管理資訊系統規劃、設置及維護。
B. 資訊軟、硬體及相關週邊設備之評估、建議、請購、安裝、測試及維護。
C. 資訊作業制度辦法之制、修訂。
D. 參與各項作業資訊化之系統分析、設計及測試。
E. 資訊系統及資料安全維護。
F. 資訊使用者教育訓練之協助。
G. 其他有關資訊系統相關業務之處理。

4.1.2 資通安全推動組織及人力、物力與財力資源

A. 成立資通安全小組負責資通安全相關業務之推動、協調、監督及審查資通安全管理事 項,設置專責主管1人及專責人員至少1人,小組成員及工作職掌填應寫「資通安全 小組成員及職掌表」(附件十八)呈 總經理核准，人員異動或增減時亦同。
B. 資通安全主管負責資通安全小組任務之推動、協調、監督及審查。
C. 資通安全專責人員協助資通安全主管推動及執行資通安全工作。
D. 資通安全主管應考量資通安全政策及目標,據以規劃建置、執行、維持及持續改善資通安全相關工作，並適時檢討所需之人力、物力與財力資源。

4.1.3 職責劃分

A. 資訊單位負責資訊系統之軟、硬體管理、故障排除與資訊安全及系統維護。
B. 使用單位負責例行資訊作業管理及系統需求之提出。
C. 資訊作業使用權限由各使用單位提出,經資訊單位確認後設定使用。

D. 電腦操作人員離職時，單位主管應對其所保管之資訊相關文件及磁片、磁帶、帳號、
電腦硬體暨週邊設備等安排辦理移交，依「離免停退、職務移交管理辦法」辦理。

4.1.4 資訊安全宣導與教育訓練

A. 每年定期以公告、電子郵件或其他適當方式對使用資訊系統之人員進行資訊安全宣導，
以提升使用者安全意識，降低資安風險。

B. 資訊安全專責主管及專責人員，每年應接受適當之資訊安全專業課程訓練或資通安全
職能訓練。

4.1.5 資訊人員之任用由資訊單位負責遴選，任用後之考核、昇遷悉依公司「工作規則」辦理。

4.2 資訊安全政策制定及評估：

4.2.1 資通安全政策及目標

A. 訂定資通安全政策及目標呈 總經理核准，並每年檢討其適切性。

B. 資通安全政策應透過教育訓練、內部會議、張貼公告或其他方式向所有人員進行宣導，
並每年檢視其重要性是否有效傳達員工。

4.2.2 資訊安全評估對象

A. 資訊設施及系統提供者。
B. 使用者。
C. 管理者、系統維護者。
D. 其他有關人員。

4.2.3 由內部稽核人員不定期抽查，檢查人員是否遵守「員工任用管理辦法」中之「資訊作業規定」。

4.2.4 員工如違反資訊安全相關規定，依「工作規則」作業辦法處理。

4.2.5 新購資訊產品（如電腦軟體、硬體、通信及管理措施等），應將安全性列入評估，以免影響既有的資訊安全措施。

4.2.6 資料保存依「品質記錄管理作業辦法」實施辦理。

4.2.7 電子資料或設備之銷毀

設備故障或報廢時，應做適當處置(例如：硬碟需格式化或物理性破壞、光碟片破壞性銷毀...等)，以確保公司資訊不外流。

4.2.8 機密文件銷毀

各單位機密性文件銷毀，由保管單位依需求銷毀日執行銷毀。

4.3 電腦系統安全管理：

4.3.1 由各單位依其作業訂定操作說明書或以書面、電子或其他方式載明之，以確保員工能正確及安全操作使用電腦系統，便於工作移轉交接、維護的依據。

4.3.2 如果遭遇非預期的電腦系統作業技術問題時，由需求部門提出並通知資訊單位支援。

4.3.3 資訊系統發展及測試作業應將正式區及測試區分開處理，降低可能的風險，以減少作業軟體或資料遭意外竄改，或是未經授權存取的機率。

4.3.4 電腦主機系統之效能、磁碟使用率、記憶體容量、檔案儲存，印表機、其他輸出設備及通信系統之使用狀況等，由資訊單位人員隨時注意及觀察分析系統的作業容量，以避免容量不足而導致電腦當機。

4.4 網路安全管理：

4.4.1 安裝防毒軟體並定期自動更新病毒碼，以確保系統不被電腦病毒感染。

4.4.2 使用網路防火牆來堵隔非法入侵。若個人因工作必要需求使用即時通訊軟體或私人網路郵箱，或是需開放／拒絕網路服務或通訊埠，應填寫「防火牆設定申請書」(附件一)送單位主管同意及 總經理核准後，交由資訊單位進行設定。

4.4.3 使用網路監控設備監控人員網路行為，以確保網路安全，調閱其紀錄資料應填寫「資料調閱申請書」(附件二)送交單位主管同意及 總經理(含)以上核准後，方可進行調閱。

4.4.4 基於網路安全之考量，整體電腦網路規劃為獨立之內部網段、非軍事區網段（DMZ）及外部網段，其間以網路防火牆區隔。

4.4.5 網路防火牆之安全控管相關設定應經常檢討，並作必要之調整，以確定發揮應有的安全控管功能。

4.4.6 辦公室以外之員工採用 VPN 方式或透過網路防火牆 SSL VPN 方式遠端網路連線作業，申請 SSL VPN 連線作業程序依 4.4.2 辦理。

4.4.7 為避免外部非法入侵，公司架設網路防火牆、電子郵件過濾系統及電腦防毒軟體，以確保資訊安全。

4.5 系統開發及程式修改控制：

4.5.1 本公司 ERP 資訊系統開發及程式修改由資訊單位自行維護，若採委外方式處理則由資訊單位統籌按下列階段實施。

A. 使用者提出系統需求。
B. 資訊單位進行可行性評估。
C. 委外公司選定。
D. 系統需求及細部規格檢討擬定。
E. 程式編號及測試。
F. 系統測試。
G. 教育訓練安排。
H. 正式上線。

4.5.2 資訊系統程式之修改由需求單位填寫「程式修改需求申請單」（附件三）提出申請，經單位主管確認並會辦相關單位意見後，送請資訊單位評估相關作業事項及意見，申請單需經資訊單位核准後方予執行。

4.5.3 修改後的程式測試由需求單位驗收及資訊單位主管複核無誤後才可使用。

4.5.4 資訊單位需將系統程式修改記錄登錄「系統程式修改明細表」（附件四）並作程式備份保存。

4.5.5 系統需求擬定應與使用單位充分參與討論。

4.6 編制系統文書之控制：

4.6.1 資訊系統主要說明書、操作手冊、訓練教材等系統文件，保存於系統中方便使用者隨時參閱，資訊單位製作備份磁帶保存，不另列印文件。

4.6.2 存放於系統中之文件隨軟體公司之版本變更作業一併更新，資訊單位亦需將備份資料更新。

4.6.3 除系統內存放之系統說明書、操作手冊、訓練教材外，資訊單位亦應針對不足部分編制相關說明文件。

4.6.4 資訊單位對資訊系統版本更新狀況應保留記錄，制訂操作文件之修廢需依『文件及資料管理辦法』辦理。

4.6.5 系統原版程式及文件由資訊單位建立「軟體明細表」(附件五）保管，軟體部分並需建立備份。

4.6.6 文件、硬體、軟體之借用，依「軟體管理辦法」處理。

4.6.7 軟體授權數控管由各單位編列預算採購。軟體的安裝由需求單位填寫「軟體安裝申請單」(附件六)經單位主管同意，並經副總級(含)以上主管核准後，交由資訊單位進行軟體異動。

4.6.8 電腦硬體設備異動由異動單位至 ERP 系統輸入資料並申請固定資產異動後，發起表單簽核流程，依表單流程完成核准同意，再交由資訊管理人員至電腦設備維護作業程式進行硬體資料之異動。

4.7 程式及資料之存取控制：

4.7.1 程式之修改需依規定程序辦理，資訊單位對修改內容應保留記錄。

4.7.2 程式及檔案區只允許資訊單位及資訊單位授權人員進入，一般使用者只允許執行應用程式。

4.7.3 電腦系統使用權限依工作權責劃分，由需求單位提出「TIPTOP 使用權限申請表」(附件七）經資訊單位確認後設定使用，若有跨單位需求者，則需會辦相關單位同意才可開放權限。

4.7.4 為確保電腦系統變更作業流程明確劃分權責，程式人員應定期將正式區異動之程式列表「程式修改需求清單」(附件八)，並呈交資訊主管覆核，以確保所異動之程式皆經申請及適當核准。

4.7.5 系統異常存取之稽核，資訊單位應定期覆核異常存取記錄與高權限帳號之存取記錄，並追蹤是否有企圖非法進入系統或未經授權存取或修改資料之異常狀況。

4.7.6 申請電腦系統使用帳號，由需求人員至 BPM 系統填「使用者帳號使用申請表」(附件九)，申請 PLM 系統使用權限則填寫「PLM 系統權限申請表」(附件十)，經核准後設定使用。

4.7.7 定期審查使用者帳號，對於已停用或超出六個月以上未登入之帳號，以電子郵件或其他適當方式通知本人及其直屬主管，經確認後不再使用的帳號即予以刪除。

4.8 資料輸出入之控制：

4.8.1 資料輸入時應做核對並留下可供確認的記錄。當發生錯誤時，由使用單位先行分析錯誤類別。

A. 資料本身錯誤或輸入錯誤：
由使用單位權責人員更正錯誤資料，並通知相關單位。

B. 系統異常或程式錯誤：
由使用單位填寫「系統問題反應單」(附件十一)記錄錯誤訊息，經單位主管確認後交由資訊單位分析異常原因並處理之。

4.8.2 系統資料經由使用權限設定之管制，避免機密性或敏感性資料遭不當使用。

4.8.3 機密性或敏感性資料輸出不成功需重新輸出時，原印製未完成之輸出報表應確實作廢銷毀。

4.8.4 輸出資料產生時，應依相關辦法對其使用聯數加以控制。

4.8.5 輸出資料使用後若無保存需要時，應予銷毀。

4.9 資料處理之控制：

4.9.1 日常作業資料由各使用單位依工作權責控制管理。

4.9.2 資訊單位定期檢視維護各項資訊系統、設備及帳號。

4.10 檔案及設備之安全控制：

4.10.1 設定系統密碼，除資訊單位及資訊單位授權人員外，其餘人員禁止進入程式檔案區。

4.10.2 系統程式、應用程式等資料每日執行備份並記錄「TIPTOP GP 備份管理表」(附件十二)。

4.10.3 系統資料(含作業系統或應用軟體的日誌檔)每日執行備份並記錄「資訊資料備份管理表」(附件十三)，備份磁帶輪替使用，並由資訊單位保管。

4.10.4 磁帶、磁片保存原則

A. 存放於通風、陰涼、乾燥之處，避免陽光直接照射，並遠離磁場或火源。

B. 磁片應保持直立狀況，不可摺疊或壓損。

C. 使用磁片應裝入封套，放置陰涼地點且避免潮濕。

4.10.5 系統主機應加裝 UPS 不斷電系統。

4.10.6 系統主機開關機程序遵循操作說明書內容操作。

4.10.7 系統軟、硬體以與供應商簽訂維護合約為原則，實施定期維護保養，確保系統正常運作。

4.10.8 系統軟、硬體設置區域應有空調系統及適當之消防設施。

4.10.9 電腦設備異常時，由發生單位通知資訊單位處理，並建立「系統問題反應單」。

4.10.10 病毒防護

郵件主機安裝防毒軟體，藉由軟體所提供之自動更新病毒碼與即時防護來防止電腦病毒入侵，資訊單位不定期檢查系統主機及使用者電腦作追蹤處理。

4.10.11 使用者密碼管理

A. 使用者密碼預設值與使用者帳號相同。

B. 使用者密碼長度最少 6 個字元。

C. 使用者最少每六個月應變更通行密碼。

D. 若登入系統錯誤超過設定次數，系統將會鎖定使用帳號而無法登入，需通知資訊單位權責人員解除鎖定後，才能重新登入系統。

4.10.12 系統備援計劃

A. 經由網路或其他媒介，定期備份重要電腦主機系統環境(含電腦作業系統及其所有應用軟體)至適當資料儲存媒體存放。

B. 當提供資訊系統服務的電腦因硬體設備或軟體原因故障時，能即時將主機系統環境的備份還原至系統備援主機，以確保資訊系統服務持續運作不中斷。

4.11 電腦週邊設備之購置、使用及維護：

4.11.1 資訊系統各項軟硬體需求由資訊單位統籌規劃，使用者參與評估後依『採購管理辦法』規定請購。

4.11.2 使用單位需求之電腦週邊設備，由使用單位提出請購。

4.11.3 資訊單位應建立「電腦週邊主要設備清單」(附件十四)，作為系統維護參考之用。

4.11.4 使用單位購入或異動硬體設備，應將購入設備規格或異動內容通知資訊單位登錄「電腦週邊主要設備清單」。

4.11.5 資產管理權責單位應定期盤點清查資產，並將盤點結果通知資訊單位更新「電腦週邊主要設備清單」。

4.11.6 資訊系統暨伺服器主機維護合約由資訊單位負責處理。

4.12 系統復原計劃制度及測試程序之控制：

4.12.1 復原準備

系統復原所需之系統軟體、應用軟體及系統資料備份磁帶由資訊單位保管。

4.12.2 復原實施

由資訊單位視狀況自行處理或請軟、硬體廠商配合處理。

4.12.3 復原測試

A. 復原實施後之作業系統測試由資訊單位執行。

B. 復原實施後之應用程式測試由使用者及資訊單位共同測試。

4.13 電腦機房管控：

4.13.1 電腦機房之伺服器維護詳閱各操作說明書。除負責機房業務有關人員外，其他未經資訊單位許可人員禁止進入電腦機房。

4.13.2 電腦機房需應規劃放置適當消防器材，以避免意外災害之發生。

4.13.3 電腦機房溫度應維持在 18℃至 25℃，相對濕度維持在 50%至 70%，當機房溫度>28℃或相對溼度>80%，則應檢查冷氣空調、除溼機器或排水設施等設備，並維護調整之。

4.13.4 上班時間由資訊單位每日進行點檢並填寫「電腦機房點檢表」(附件十五)，下班時間由守衛人員監控系統並巡視機房內相關設施，並隨時監看環控系統注意機房內溫濕變化，若發現異常現象，應即時通知相關人員處理。

4.13.5 為避免電腦機房內主機機櫃對高架地板負載過重，所導致的崩壞倒塌或物體破裂、墜落、滾落之風險，對負載過重之機櫃下方，應增加鐵片分散負荷重力，以減少意外風險的發生。

4.14 風險評估：

4.14.1 資訊單位應定期進行資訊系統安全相關風險評估，並填寫「資通安全風險評估表」(附件十六)。

4.14.2 名詞定義

A. 危害性：1~9 分，風險危害影響程度越高，評分越高。
B. 發生頻率：1~9 分，風險發生頻率程度越高，評分越高。
C. 風險等級評分 = 危害性評分 × 發生頻率評分。

風險等級	低度風險	中度風險	高度風險
評分	1~24	25~49	50~81

4.14.3 高度風險控制改善

當資通安全風險項目等級評定為高度風險時，應擬議管理面或技術面控制措施，並填寫於「資通安全風險評估表」之【降低

風險控制措施】欄位，以管制降低風險。

4.15 委外管理：

4.15.1 本公司委外辦理資通系統之建置、維運或資通服務之提供時，應考量委外廠商之專業能力與經驗、委外項目性質及資通安全需求，以選任適當的委外廠商。

4.15.2 選任委外廠商時應考量其辦理受託業務之相關程序及環境，是否具備完善之資通安全管理措施或通過第三方驗證，且是否配置經適當之資格訓練、擁有資通安全專業證照或具有類似業務經驗之資通安全專業人員。

4.15.3 監督要求委外廠商執行受託業務時，若有違反資通安全相關法令或發生資通安全事件時，應立即通知本公司並採行補救措施。

4.15.4 與委外廠商簽訂委外服務契約時，應審查確認契約中之保密條款，並要求委外廠商之業務執行人員簽署「委外廠商執行人員保密同意書」(附件十七)。

4.15.5 委外關係終止或解除時，應確認委外廠商已返還、移交、刪除或銷毀因履行委託契約而持有之資料。

4.16 資安事件通報及應變：

4.16.1 通報作業程序

A. 若發現疑似重大資通安全事件時，由發現人員依事件狀況迅速通報資安事件通報窗口，並告知直屬單位主管。

B. 資通安全小組收到通知後，依事件影響範圍及損害程度評估，研判是否為重大資通安全事件。

C. 若研判為非重大資通安全事件時，則將判定結果回覆發現人員並協助處理及解決問題。

D. 若研判為重大資通安全事件時，則依事件之影響程度通知權責單位主管。

E. 若事件處理有需要系統維護或設備保固的外部廠商之協助，應立即以事先已約定方式通知協力廠商聯絡窗口處理。

4.16.2 應變處置

A. 事前建置資訊安全系統及整體防護架構，增加防禦能力，以減少資安事件發生機率，降低資安事件損害程度。

B. 平日隨時彙集整理各項資安相關文件，在資安事件發生時可立即參考並處置，以提升應變作業效率。
C. 一旦發生重大資安事件，應於最短作業時間內控制並復原資安事件所造成的損害。
D. 資安事件緊急應變處置後，應進行討論並研擬適當之預防及矯正措施。

4.17 核心業務及營運中斷事件：

4.17.1 核心業務

核心業務	核心資通系統	機敏性資料等級（高/中/低）	系統復原時間目標（RTO）	資料復原時間點目標（RPO）
產品生產	SFT	高	6 工時	24 小時
產品銷售	ERP	高	8 工時	24 小時
客戶往來	MAIL	中	8 工時	24 小時
內部流程	BPM	低	12 工時	24 小時
人力資源	HRM	高	16 工時	24 小時

4.17.2 營運中斷事件

營運中斷事件	發生機率（高/中/低）	影響程度（大/中/小）
伺服器主機故障	低	大
資料儲存設備故障	高	大
電力供應中斷	中	大
天然災害(地震、颱風…)	低	大
聯外網路線路中斷	中	中
駭客入侵	低	中
電腦中毒	中	中
使用人員操作錯誤	中	小
使用人員蓄意破壞	低	小
其他意外事件	低	小

五、相關文件：

5.1 離免停退、職務移交管理辦法	AMD-P-026
5.2 工作規則	AMD-P-003
5.3 員工任用管理辦法	AMD-P-025
5.4 資訊作業規定	AMD-164
5.5 品質記錄管理作業辦法	TMG-P-004
5.6 文件及資料管理辦法	TMG-P-002
5.7 軟體管理辦法	TMG-P-017
5.8 採購管理辦法	PCD-P-002

六、附件：

6.1 防火牆設定申請書	TMG-056	附件一
6.2 資料調閱申請書	TMG-057	附件二
6.3 程式修改需求申請單	TMG-022	附件三
6.4 系統程式修改明細表	TMG-023	附件四
6.5 軟體明細表	TMG-021	附件五
6.6 軟體安裝申請單	TMG-058	附件六
6.7 TIPTOP 使用權限申請表	TMG-018	附件七
6.8 程式修改需求清單	TMG-052	附件八
6.9 使用者帳號使用申請表	TMG-063	附件九
6.10 PLM 系統權限申請表	TMG-061	附件十
6.11 系統問題反應單	TMG-019	附件十一
6.12 TIPTOP GP 備份管理表	TMG-062	附件十二
6.13 資訊資料備份管理表	TMG-026	附件十三
6.14 資訊週邊主要設備清單	TMG-020	附件十四
6.15 電腦機房點檢表	TMG-055	附件十五
6.16 資通安全風險評估表	TMG-064	附件十六
6.17 委外廠商執行人員保密同意書	TMG-065	附件十七
6.18 資通安全小組成員及職掌表	TMG-066	附件十八