久禾光電股份有限公司
資通安全管理辦法

第一條、 目的

本公司為確保資通安全管理制度能持續有效運作，建立安全可信賴之電腦化作業環境，確保電腦資料、系統、設備及網路安全，以符合相關法令規定，並保障公司權益及永續經營。

第二條、 範圍

本公司所有正式員工、聘約員工、派遣人員等公司所聘用之人員及以外來訪客和廠商等。

第三條、 目標

1 確保本公司資訊資產之機密性，落實資料存取控制，資訊需經授權人員方可存取。
2 確保本公司資訊作業管理之完整，避免未經授權之修改。
3 確保本公司資訊作業之持續運作，符合營運服務水準。
4 確保本公司資訊作業均符合相關法令規定要求。

第四條、 內容

1 資通安全政策

本公司為落實資通安全目標，及強化本公司之資訊安全管理，並確保資料、系統及網路安全，設立「資通安全管理小組」，小組內另包含一名資安主管及一名資訊員工，負責資通安全管理制度規劃、建立、實施、維護、審查與持續改善，資安主管向董事會或管理階層報告資安的執行情況。

1.1 小組相關作業的工作要點如下：

1.1.1 管制技術：外部技術處理，資訊安全維護，資訊安全工具提供、監控及規劃，資訊安全規範遵循，負責資訊安全事件蒐集調查。

1.1.2 教育訓練：資訊安全文化形塑、新人資訊安全教育、內外資訊安全訓練與講座。

1.1.3 稽核風管：資通安全管理制度內部查核與資訊風險管控。

1.1.4 文件管制：文件資訊安全管制、分類及保存管理。

1.1.5 法律合規：資通安全管理法規遵循。

1.2 資通安全涵蓋對象：

1.2.1 管理制度。

1.2.2 作業流程。

1.2.3 人員。

1.2.4 軟體。

1.2.5 應用程式。

1.2.6 電腦作業系統。

1.2.7 硬體。

1.2.8 網路設備。

1.2.9 資料、文件、媒體的儲存。

1.2.10 實體設備

1.3 資通安全管理之範圍：

本公司資訊安全管理涵蓋十四項資訊安全管理事項，以避免如因人為疏失、蓄意或天然災害等因素，遭致不當使用、洩漏、竄改、破壞等情事，而對本公司可能帶來之風險及危害程度。其安全管理事項如下：

1.3.1 員工安全管理及教育訓練。

1.3.2 核心業務及資訊資產價值鑑別。

1.3.3 電腦主機安全管理。

1.3.4 資料安全管理。

1.3.5 系統導入維護安全管理。

1.3.6 網路安全管理。

1.3.7 網路存取之安全控制。

1.3.8 系統與網路入侵之處理。

1.3.9 設備安全管理。

1.3.10 實體環境安全管理。

1.3.11 業務永續經營運作計劃管理。

1.3.12 資通安全應變措施。

1.3.13 備份作業。

1.3.14 設備報廢流程管理。

1.3.15 委外廠商服務管理

2 員工安全管理及教育訓練

員工依其工作職掌，給予適當的系統與資料存放取權限，定進行資訊安全教育及訓練。

2.1 工作說明及資源分配安全：

2.1.1 對於人員之新進、調派、離職或退休，進行適當之安全評估。

2.1.2 對於可存取機密性、敏感性資訊或系統之員工以及賦予系統存取特別權限之員工有妥適分工，分散權責；並實施人員通識教育訓練。

2.2 員工訓練：

2.2.1 員工必須瞭解公司之資訊安全政策。

2.2.2 依員工職務層級進行適當的資訊安全教育訓練。

2.2.3 一個月一次以E-mail方式公告資訊安全相關訊息。

2.2.4 不定期派員參與外界舉辦的相關訓練、研討會、資安展示會。

2.2.5 定期進行社交工程演練，以提升員工對資安的警覺性。

2.2.6 資安相關人員培訓計畫，應依機關時數要求，每人每年至少接受12小時以上之「資通安全專業課程訓練」或「資通安全職能訓練」。

2.2.7 內部稽核單位一年一次對資訊人員進行資通安全查核作業。

久禾光電股份有限公司
資通安全管理辦法

2.2.8　資訊部人員每年定期進行資安自我檢查作業。

3　核心業務及資訊資產價值鑑別

每年檢視公司之核心系統、軟硬體資產及應保護之機敏性資料，鑑別可能造成營運中斷事件之發生機率及影響程度，並明確訂定核心業務之復原時間目標。

3.1 核心業務敏感性及影響公司程度分類：

3.1.1　高敏感性：包含會直接影響公司整體運行重大及核心價值資產。

3.1.2　中敏感性：包含間接影響公司營運，但不會造成公司無法運作。

3.1.3　低敏感性：包含不會影響公司智慧財產、聲譽及公司營運。

3.2 根據機敏性擬定之復原時間目標：

3.2.1　高敏感性：目標回復時點一天，若遇到假日順延；目標回復時間不得超過4小時。

3.2.2　中敏感性：目標回復時小於一周，若遇到假日順延；目標回復時間不得超過三天。

3.2.3　低敏感性：目標回復大於三天；目標回復時間視情況而定。

4　電腦主機安全管理

各項電腦主機及伺服器設備均指定專人管理及維護，並設定密碼保護與定時更換，嚴禁使用非經授權及來路不明之軟硬體。

4.1 電腦設備安全：

4.1.1　作業電腦之使用、申請與相關規定，詳細作法訂定於「電腦暨網路使用管理辦法」。

4.2 電腦一般控制措施：

4.2.1　攜帶型的電腦設備訂有嚴謹的保護措施(如設密碼保護、檔案加密或專人看管)並落實執行。

4.2.2　處理敏感性資料的電腦，不使用時應加以關機、登出、設定螢幕密碼或是以其他控制措施進行保護。

5　資料安全管理

資料保存定時備份，並分機密等級管理資料檔案與權限，以防止遺失、毀壞、被偽造或竄改。

5.1 日常事務資料處理

5.1.1　每日公用資料夾之資料，應每日進行備份處理。

5.1.2　每日下班前檢測備份資料，以確保備份資料之可用性。

5.1.3　備份資料採用每週異地存放，存放於符合安全標準之場所。

5.1.4　重要資料的備份應保留三代以上(每日備份之前三日)。

5.2 儲存媒體的處理與安全

5.2.1　儲存媒體依保存規格要求，存放在安全的環境。

5.2.2　對於敏感性資訊，應採取資料加密等保護措施。

5.2.3　對於內含機密性或敏感性資料的媒體報廢，應指定專人處理。

5.2.4 儲存媒體之報廢，必須協同部門主管進行資料檢核確認後，並簽報權責主管核可後，方可進行實體報廢作業。

6 系統導入維護安全管理

新導入的資訊系統，或是現有系統功能之維護及強化，應考量資訊安全的需求與評估，並納入系統功能中。

6.1 導入系統之安全要求

6.1.1 導入新系統應依正當的授權程序辦理(如填寫「軟硬體新增需求單」提出申請)，並確實評估檢視現有作業系統妥適與否，以確保未破壞系統原有的安控措施。

6.1.2 新系統正式上線及重大變更前，應主動公告員工異動的範圍、時間以及可能的影響。

6.1.3 新系統在導入規劃分析時，應將安全需求納入考量。

6.2 導入資通安全系統的安全

6.2.1 委外開發合約中，應對著作權之歸屬訂有規範內容。

6.2.2 開發、測試與正式作業，應區隔使用不同的系統環境。

6.2.3 與廠商訂約開發資訊系統時，應簽訂履行條款與相關罰則。

7 網路安全管理

網路設備需有專人管理，隨時監測網路的狀況，並設置防火牆對內外網路進行安全管控。

7.1 適切的使用網路防火牆機制，以防禦資訊系統安全。

7.2 對網路運作環境之安全漏洞，原則上應定期進行檢測。

7.3 隨時公告有關電腦網路安全之事項。

7.4 定期檢討電腦網路安全控管事項之執行。

7.5 每半年進行防火牆規則政策審核，以確保防火牆連線規則符合辦法。

8 網路存取之安全控制

使用者依其權限限制其連線作業能力，並應遵守相關安全規定；如有違反，依相關法規處理，並取消其網路資源存取權限。

8.1 依據個別應用系統的安全需求，制定安全等級或分類。

8.2 依據網路型態(Internet、Intranet、Extranet)訂定適當的存取權限管理方式。

8.3 資訊系統與網路服務，原則上儘量避免使用共同帳號。

8.4 網路服務須建立完整的使用授權程序。

8.5 依環境或業務需要，於網路防火牆作適當之設定。

8.6 依業務性質或任務分配來建置邏輯性網域的存取權限機制(如虛擬私有網路VPN)。

8.7 外部連線須建置可透過檢查來源用戶位址的機制鑑別方法，以找出連線作業的來源。

8.8 依風險評估管制使用者的連線功能。

久禾光電股份有限公司
資通安全管理辦法

8.9 設置檢測連線的來源位址與目的位址網路路由之控管措施。

9 系統與網路入侵之處理

利用防毒軟體的防護及修正防火牆的設定，以防禦網路的入侵與攻擊。

9.1 定期對電腦系統及資料儲存媒體進行病毒以及惡意程式掃瞄。

9.2 伺服器與個人電腦全面使用防毒軟體並即時更新病毒碼。

9.3 應即時公告有關電腦病毒的最新資訊。

9.4 每日檢測防火牆的病毒碼為最新狀態。

9.5 針對來路不明的外部IP設立黑名單，以防範連至公司內部。

9.6 經常性宣導對於外來及內容不確定的檔案或E-mail 在開啟使用前，要先作電腦病毒掃瞄。

9.7 軟體授權規定：禁止使用未取得授權的軟體。

10 設備安全管理

重要資訊設備應安置在適當的地點並予保護，以減少環境不安全引發的危險，及未經授權存取系統的機會。

10.1 設備之維護必須由授權之維護人員執行。

10.2 訂定設備安全管理規定(如電源之供應及備援電源等)。

10.3 資訊設備之放置應該檢視及評估火、煙、水、灰塵、震動、化學效應、電力供應、電磁幅射等加諸於設備之危害的可能性。

11 實體環境安全管理

實體環境應以事前劃定的各項資訊設施為基礎，設置必要的障礙（例如：使用身分識別卡之安全門），達成安全管控的目的。電腦機房應考量火災、水災、地震等災害的實體安全防護措施，並考量鄰近空間的可能安全威脅。

11.1 機房門禁只有資訊人員識別證進行出入。

11.2 機房進出均需填寫機房進出紀錄表，若是外部廠商或人員需要進出機房，全程需有至少一位資訊人員陪同。

11.3 於早上開始上班時間，由資訊人員進行例行性的機房設備檢查(包含系統的更新、備份機制檢查及溫濕度的紀錄)，並每日進行兩次機房的環境勘查。

12 業務永續經營運作計劃管理

為因應各種人為及天然災害造成業務運作受影響，需確實做好各項備份工作。各部門應依業務性質研擬緊急應變計畫，使各項業務得以永續運作。

12.1 事件通報：

12.1.1 發現疑似資訊安全事件時，資安事件發現人員依事件歸屬通報資訊人員，並副知其直屬主管。

12.1.2 資訊人員判定發生資訊安全事件時，應通知資安人員及主管。

12.1.3 資安人員依據資訊人員所提報之事件影響報告，需向上級主管單位通報，並依照本辦法「資通安全應變措施」項目之分級方式，若資訊安全事件級別為第三級或第四級，除透過官網更新公告方式對外公告事件發

生狀況，亦需刊登於公開資訊觀測站網站。

12.2 應變處理：

12.2.1 若為外部人為攻擊之資訊安全事件，應立即斷線與公司內網所有連線方式，並關閉受資安攻擊之設備電源，將災害降至最低。

12.2.2 檢查公司內部所有資產設備之資料，確認每台資產設備防毒更新碼以達到最新，並進行完整掃毒程序，依照本辦法「資通安全應變措施」項目之分級方式處理，確認公司內部所有資產設備之資料未受到攻擊後，再逐一開放掃毒沒問題之設備連線至公司內網。

12.2.3 受資安攻擊之設備需由資訊人員進行排除處理，處理之設備網路環境必須處於非網路連線，及與公司內部網路斷線狀態。

12.2.4 待資訊人員問題排除完成後，由資安人員檢視並測試確認至少三天未再受到資安攻擊後，方可重新連線網及公司內部網路繼續業務使用，並填寫軟體系統、硬體設備故障記錄表。

12.2.5 自然災害預防及應變作業，詳細作法訂定於「系統維護及異常管理辦法」。

13 資通安全應變措施

於發生重大資通安全事件或其他災害涉及資通安全事件時，依所載之分級方式處理。

13.1 有下列情形之一者，為第一級資通安全事件：

13.1.1 非核心業務資訊或非核心系統遭輕微竄改。

13.1.2 非核心業務之運作受影響或停頓，於可容忍中斷時間內回復正常運作，不造成機關日常作業影響。

13.2 有下列情形之一者，為第二級資通安全事件：

13.2.1 非核心業務資訊或非核心資通系統遭嚴重竄改，或未涉及公司關鍵維運之核心業務資訊或核心系統遭輕微竄改。

13.2.2 非核心業務之運作受影響或停頓，可容忍中斷時間內回復正常運作，或未涉及公司關鍵維運之核心業務或核心系統之運作受影響或停頓，於可容忍中斷時間內回復正常運作。

13.3 有下列情形之一者，為第三級資通安全事件：

13.3.1 未涉及公司關鍵維運之核心業務資訊遭洩漏，或一般公務機密、敏感資訊或涉及關鍵基礎設施維運之核心業務資訊遭輕微洩漏。

13.3.2 未涉及公司關鍵維運之核心業務資訊或核心系統遭嚴重竄改，或一般公務機密、敏感資訊、涉及公司關鍵維運之核心業務資訊或核心系統遭輕微竄改。

13.3.3 未涉及公司關鍵維運之核心業務或核心系統之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作，或涉及公司關鍵維運之核心業務或核心系統之運作受影響或停頓，於可容忍中斷時間內回復正常運作。

13.4 有下列情形之一者，為第四級資通安全事件：

13.4.1 一般公務機密、敏感資訊或涉及公司關鍵維運之核心業務資訊遭嚴重洩漏，或極機密檔案文件遭洩漏。

13.4.2 一般公務機密、敏感資訊、涉及公司關鍵維運之核心業務資訊或核心系統遭嚴重竄改，或極機密檔案文件遭竄改。

13.4.3 涉及公司關鍵維運之核心業務或核心系統之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作。

13.5 完成資通安全事件之通報後，依下列規定時間完成該資通安全事件等級之審核，並得依審核結果變更其等級：

13.5.1 通報為第一級或第二級資通安全事件者，於接獲後八小時內。

13.5.2 通報為第三級或第四級資通安全事件者，於接獲後二小時內。

13.6 知悉資通安全事件後，應依下列規定時間完成損害控制或復原作業：

13.6.1 第一級或第二級資通安全事件，於知悉該事件後七十二小時內。

13.6.2 第三級或第四級資通安全事件，於知悉該事件後三十六小時內。

14 備份作業

應落實定期備份作業之規定，以便發生災害或是儲存媒體失效時，可迅速回復正常作業。

14.1 備份原則與作業，詳細作法訂定於「資料管理辦法」。

14.2 備份資料回存作業，詳細作法訂定於「資料管理辦法」。

15 設備報廢流程管理

規範電腦主機設備無法修復或汰舊之設備，進行報廢及銷毀方式。

15.1 報廢流程：

15.1.1 電腦設備判斷無法修復或使用時，由資訊人員拆卸可用零件(包含硬碟等設備)，其餘則做資源回收處理，並且留存報廢紀錄。

15.1.2 若因已逾使用年限、損壞或不堪使用之桌上型電腦、筆記型電腦、平板電腦及伺服器主機，得依向資訊單位提出申請銷毀，由資訊人員拆卸硬碟之資訊資產設備後，擇期進行銷毀作業。

15.1.3 報廢進行時，必要時得會同稽核人員，並對該設備加以實體破壞、或消磁、或利用工具等方式清除資料，完成後，請申請人員及所屬單位主管進行確認資訊資產已銷毀完成，並保留執行之紀錄。

16 委外廠商服務管理

進行委外規劃時，委外廠商應依資通安全管理法及相關法規定採行適當的安全控制措施，以確保資通系統達到應具備的安全防護水準。

16.1 委外廠商作業資訊安全要求：

16.1.1 委外廠商專案計畫負責人或重要成員，若必要時更換(如離職、調職等因素)，需主動告知本公司。

16.1.2 委外廠商之合作或協力廠商皆應併同遵循法律要求及本公司資通安全管理管理辦法規定。

久禾光電股份有限公司
資通安全管理辦法

16.1.3 委外廠商執行受託業務，違反資通安全相關法令或知悉資通安全事件時，應立即通知本公司及採行之補救措施。

16.1.4 委外人員進出本公司辦公區域或電腦機房區域時，均依據本辦法「實體環境安全管理」項目辦理。

16.1.5 重要系統之委外廠商應訂定緊急應變與回復標準程序，以確保本公司業務之持續運作。

16.1.6 委外廠商須配合本公司進行資安稽核。

16.1.7 委外關係終止或解除時，委外廠商返還、移交、刪除或銷毀持有資料。

第五條、 本作業辦法由資訊部擬定，經董事長通過後施行，修正時亦同。

本作業辦法生效日於中華民國113年5月2日。