弘凱光電股份有限公司

資通安全管理辦法

一、 目的：

本辦法依據《電腦化資訊系統管理循環》之《資通安全檢查之控制》規定，為建立安全及可信賴的電子交換環境，以確保資料、系統、設備及網路的安全，資訊的適當安置及資訊安全實務作業的可行性與有效性。

二、 範圍：

本公司及其所屬子公司，有關資通安全管理事務均應依本辦法執行之。

三、 定義：

1. 資訊設備：為資訊之輸出、入時所使用之硬體設備，如個人電腦、印表機、掃瞄器、螢幕、電腦用不斷電系統等相關設備。

2. 資訊文件：使用資訊設備所產生之電子文件。

3. 儲存設備(媒體)：用於儲存電子文件資料之各種讀寫設備之總稱。如光碟片、磁帶機、移動式儲存裝置等等謂之。

四、 權責：

(一)資通主管負責統籌規劃及監督。

(二)資通安全日常作業事務，由資訊單位負責實施。

(三)涉及資通安全的應變與管理，由資通主管核決，並直接向總經理報告。

(四)各單位主管須負責督導所屬員工之資通作業安全，防範不法及不當行為。

五、 資通安全政策制定：

(一)本公司所訂定之資通安全管理政策，以書面、電子或其他方式告知本公司所屬各單位員工、連線作業之相關單位及提供資通服務之廠商共同遵行。

(二)本辦法實施後，資通單位每年得評估一次其適切性，以反映政府法令、技術及業務等最新發展現況，確保資通安全實務作業之有效性。

六、 資通安全組織：

(一)資通安全政策之研究,由資通主管統籌辦理,必要時籌組資安小組共同商議。

(二)資通安全日常作業事務之執行，由資通單位負責辦理。

(三)資通安全稽核工作之執行，由稽核單位負責辦理。

(四)資通安全系統建置方案，由資通單位研擬提報，資通主管審議通過並提報總經理核可後，依本公司採購程序辦理。

七、 資通安全管理作業規定

（一）人員安全管理及教育訓練

1. 資通主管對資通相關職務之工作人員，應加強品德操守之監督考核。
2. 資通主管對負責重要資訊系統之管理、維護、設計及操作之人員，應妥適分工，分散責任，並視需要建立人力備援制度。
3. 資通單位應視實際需要辦理資通安全教育訓練及宣導,建立員工資通安全認知,以提升公司資通安全水準。

（二）電腦主機安全管理

1. 公司主要伺服器應安置於電腦機房或專用機櫃內，由資通單位專責管理，並管制非相關人員隨意進出或開啟。
2. 非資通單位人員或維修人員，不得自行拆卸電腦機殼及更換內部零組件（設備儀器類應由權責單位管制)。
3. 電腦設備維護內容，應與廠商訂有書面維護合約，完成維護時應留存維護紀錄並由資通單位派人會同廠商維護人員共同檢查。
4. 非經資通主管授權同意，不得變更、調整電腦主機軟硬體裝置。
5. 非經資通主管授權同意，不得將主機設備移出機房。
6. 電腦伺服器周圍環境不得攜入或存放磁性、放射性、易燃性及易爆性物品，並嚴禁嬉戲、吸菸及飲用食物。
7. 電腦伺服器專用電源插座，不得使用於電腦以外之設備，以免耗用不斷電系統電源，造成跳電當機，影響電腦正常運作。

（三）資料安全管理

1. 員工依規定填寫「資訊權限申請單」並經核准後，資通單位始可設定所需之帳號與密碼。
2. 若資訊系統具有強制變更密碼功能者，即應予設定使用，其變更頻率不低於每半年一次。
3. 若資訊系統不具有強制變更密碼功能者，應以通知方式要求使用者自行變更，其變更頻率不低於每年一次。
4. 離職人員時應列入人員離職之必要手續，並立即停用其使用資訊資源權限。
5. 資通人員離職後，對於其所管理之資訊系統及網管設備，應立即變更管理者密碼。
6. 各單位之重要資料如需委外建檔者，不論在公司內外執行，應與委外廠商簽訂適當之安全管制合約，防止資料被竊取、竄改、販售、洩漏及不當備份等情形發

生。

（四）系統開發維護安全管理

1. 自行開發或委外發展系統，須在系統開發初期階段，即將資通安全納入考量；系統之維護、更新、上線執行及版本異動作業，應予安全管制，避免不當軟體、暗門及電腦病毒等危害系統安全。
2. 委託廠商建置及維護重要軟硬體設施時，應在資通部門人員監督及陪同下始得為之。
3. 對委外廠商之系統建置及維護人員,僅能於系統開發及維護期間核發臨時帳號,並依其所需執行之工作設定其權限，任務完成時應立即停用其帳號。
4. 系統程式開發應在測試區測試及驗收，確認無誤後始可更新至正式區且新程式必須備註修改日期及修改人員。
5. 系統開發人員應每月提供「程式修改月報」給資通主管審核。

（五）網路安全管理

1. 設置防火牆設施以防外界的不當入侵。
2. 防火牆系統軟體，應定期檢視與評估更新版本，以因應各種網路攻擊。
3. 網路系統管理人員應隨時掌握最新資通安全政策及規定的更新，以及網路設備的變動，隨時檢討及調整防火牆系統的設定，調整系統存取權限，以反應最新的狀況。
4. 防火牆設置完成時，應測試防火牆是否依設定的功能正常及安全地運作，如有缺失，應立即調整系統設定，直到符合既定的安全目標。
5. 資通人員每日需檢查防火牆是否有異常紀錄。

（六）網路存取之安全控制

1. 網路使用者應遵守網路安全規定，並確實瞭解其應負的責任；如有違反網路安全情事，應依資通安全規定，限制或撤消其網路資源存取權利。
2. 嚴禁存取網路上未經許可的檔案或企圖獲得存取的權限，且禁止在網路上散播色情及任何危害公司與國家安全之文字、圖片、影像、聲音等，並禁止以任何手段蓄意干擾或防礙網路系統的正常運作。
3. 嚴禁使用者私自將無線網路存取設備接至公司網路。
4. 嚴禁網路使用者發送電子郵件騷擾他人及發送匿名信，或偽造他人名義發送電子郵件。
5. 被授權的網路使用者，只能在授權範圍內存取網路資源。

（七）系統與網路入侵之處理

1. 立即拒絕入侵者任何存取動作以防止災害繼續擴大。當防護網被突破時，系統應設定拒絕任何存取；或入侵者已被嚴密監控，在不危害內部網路安全的前題下，得適度允許入侵者存取動作，以利追查入侵者。
2. 切斷入侵者的連接,如無法切斷則必須關閉防火牆或為達到追查入侵者的目的,可考慮讓入侵者做有條件的連接，一旦入侵者危害到內部網路安全，則必須立即切斷入侵者的連接。
3. 應全面檢討網路安全措施及修正防火牆的設定，以防禦類似的入侵與攻擊。
4. 應正式記錄入侵的情形及評估影響的層面。
5. 立即向權責主管報告入侵情形。

（八）設備安全管理

1. 設備應安置在電腦機房並予保護，以減少環境不安全引發的危險及減少未經授權存取系統的機會。
2. 設備安置應遵循的原則如下：
   i. 應檢查及評估火災、煙、水、灰塵、震動、化學效應、電力供應、電磁幅射等可能的風險。
   ii. 電腦作業區應禁止抽煙及飲用食物。
3. 電源供應
   i. 電腦設備之設置，應予保護，以防止斷電或其他電力不正常導致的傷害；電源供應依據製造廠商提供的規格設置。
   ii. 應考量安置預備電源，並使用不斷電系統。
   iii. 應謹慎使用電源延長線，以免電力無法負荷導致火災等危害安全情事。

（九）軟體使用管理

1. 公司使用有智慧財產權的軟體，應遵守相關法令及授權規定。
2. 軟體複製應考量之事項如下：
   i. 不應保有及使用未取得授權的軟體。
   ii. 應將公司智慧財產權保護政策,以書面、電子或其他方式明確通知機關員工,禁止員工在未取得智慧財產權擁有者的書面同意前，將軟體複製到機器設備內。
   iii. 除非取得授權，不應將專屬的軟體複製到公司以外的機器設備。
   iv. 須在原授權許可之外的機器上使用軟體時，應取得正式的授權或另行採購。
   v. 應建立軟體使用的註冊管理機制，並定期稽核軟體使用情形。

（十）資產分類與控管

1. 重要資訊資產應指定保管人。
2. 重要資訊資產應列冊管制並隨時更新。
3. 資通主管應不定期盤點重要資訊資產，頻率不低於每年一次。

（十一）永續運作計畫管理

1. 資通單位須定期進行資料備份，以降低各種人為或天然災害對公司營運活動之影響程度。
2. 資通單位應制定《系統復原計畫》，並每半年進行演練計劃。
3. 各單位在發生資通安全事件時，資通單位及稽核單位應介入調查，必要時聯繫檢警調單位協助偵查。

八、 內部稽核作業

（一）資通安全檢查項目，依「資通安全檢查表」查核。

（二）稽核單位應定期稽查資通安全事項辦理情形，並提出查核缺失以作為改善之依據。

（三）相關查核記錄應妥善保存至少 5 年。

（四）經資通單位及稽核單位發現有違反資通安全政策之行為，應立即通報管理階層，並依公司獎懲規定予以懲處。

九、 本辦法經總經理核准後公告實施，修正時亦同。

十、 使用單據：

（一）資訊權限申請單。

（二）程式修改月報。

（三）資通安全檢查表。

本辦法制訂於 2018 年 09 月 10 日。