弘凱光電股份有限公司

資訊安全政策

【組織架構】

1. 資訊安全日常作業事務，由資訊單位負責實施，資訊主管負責統籌規劃及監督，涉及資訊安全的應變與管理，由資訊主管核決，並直接向總經理報告。
2. 各單位主管須負責督導所屬員工之資訊作業安全，防範不法及不當行為。

【資訊安全政策制定】

1. 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訊服務之廠商共同遵行。
2. 資訊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，確保資訊安全實務作業之有效性。

【人員安全管理及教育訓練】

1. 資訊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。
2. 資訊單位應視實際需要辦理資訊安全教育訓練及宣導，建立員工資訊安全認知，以提升公司資訊安全水準。

【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，由資訊單位專責管理，並管制非相關人員隨意進出或開啟。機房管理應訂有作業準則，並每日進行查核確認。
2. 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訊單位派人會同廠商維護人員共同檢查。
3. 電源供應依據製造廠商提供的規格設置，以防止斷電或其他電力不正常導致的傷害。

【資料安全管理】

1. 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。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。
2. 各單位之重要資料如需委外建檔者，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。

【系統開發安全管理】

1. 自行開發或委外開發系統之維護、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。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。

2. 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。

【網路安全管理】

1. 網路系統管理人員應隨時掌握最新資訊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。
2. 防火牆系統軟體，應定期檢視與評估更新版本，資訊人員每日需檢查防火牆是否有異常紀錄。

【網路存取安全控制】

1. 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妨礙網路系統的正常運作。
2. 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。

【系統與網路入侵之處理】

1. 立即切斷入侵者的連接，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。
2. 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。

【軟體使用管理】

1. 本公司使用有合法版權的軟體，並遵守相關法令及授權規定。
2. 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。

【永續運作計畫管理】

1. 資訊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. 資訊單位制定《系統復原計畫》，每半年進行演練計劃。