資通安全管理

資通安全風險管理架構

本公司資通安全風險管理權責單位為資訊部門，下設有專責單位負責網通資訊環境安全，目前專責主管職位為總經理，下設有資安專責人員，負責對資通安全工作進行風險評估、擬定資訊環境硬體建置、電腦使用規範、資訊安全系統管理及內部訓練宣導等相關工作程序。稽核單位依稽核計畫進行督導建議，定期編製稽核報告向董事會報告。每年資訊環境亦經會計師進行資訊作業查核。

資通安全政策

為防止資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性(確保被授權之人員才可使用資訊)、完整性(確保使用之資訊正確無誤、未遭竄改)及可用性(確保被授權之人員能取得所需資訊)，本公司已制訂資通安全政策，以供全體同仁共同遵循：

1. 因應資通安全威脅情勢變化，本公司辦公室同仁(財務部、製造部、業務部、廠務部)應參與資通安全教育訓練，以提高資通安全意識。
2. 保護機敏資訊及資通系統之機密性與完整性，避免未經授權的存取與竄改。
3. 定期進行內部稽核，確保相關作業皆能確實落實。

具體管理方案

1. 本公司辦公室同仁(財務部、製造部、業務部、廠務部)每年須完成3小時資通安全教育訓練。
2. 知悉資安事件發生，能於規定的時間完成通報、應變及復原作業(每年實施一次系統復原測試計畫)。
3. 前次內部稽核發現缺失及異常事項，不得有未完成改善之情形。

投入資通安全管理之資源

為提升資通安全，本公司應提供資源，提升資通安全意識，並推動下列事項：

1. 不定期(每年至少一次)對公司員工辦理資訊安全宣導(例如：防毒、使用合法軟體及電子郵件使用規定等)，並留存紀錄。
2. 不定期檢查網站內對外提供之資訊，對具機密性、敏感性或過期之資訊內容，應立即移除或更新。
3. 有關電腦網路安全(如資訊安全政策宣導、防範網路駭客入侵事件、電腦防毒等)之事項應隨時公告。
4. 電腦應安裝防毒軟體，並設定對電腦系統進行病毒掃瞄。

最近年度因重大資通安全事件所遭受之損失、可能影響及因應措施，如無法合理估計者，應說明其無法合理估計之事實：無此情形。

光明絲織廠股份有限公司
資通安全風險管理架構圖

訂定日期：111 年 04 月 01 日