資通風險管理架構

- **資通安全目的**

  資通安全與營運資料保護是企業永續發展與維持核心競爭力的重要基石；為確保資訊系統之穩定性、安全性及可用性，本公司由資訊部門規劃集團資通安全風險管理，建置與維護資訊安全管理體系，建立符合法規與客戶需求之資訊安全系統，保護公司與客戶資訊的機密性、完整性與可用性，提供安全的生產環境，確保公司業務之永續營運。本公司已取得 ISO27001 資訊安全管理系統驗證，透過制度化之管理與持續改善機制，強化資訊安全治理與風險控管，確保資訊安全與防護水準符合國際標準。

- **資通安全適用範圍與對象**

  適用華晶集團及國內外子公司員工及約聘雇人員及其他具有實質控制能力之集團關係企業，範圍包含各營運據點同仁及接觸集團內部資訊之委外廠商、約聘廠商及派遣廠商，皆須遵守資訊安全政策、網際網路安全管制、電腦防毒管理、密碼原則、防火牆策略、資訊安全管理。

- **資通安全風險管理架構**

  本公司訂定「資訊安全管理辦法」，以建立與實施資訊安全管理制度，其權責劃分如下：

  (1) 資安管理委員會，負責審議資安政策、重大風險及事件應變。

  (2) 資安管理代表，統籌資安計畫執行，協調跨部門資源，推動資安政策落實。

  (3) 風險小組，執行資安風險評估、弱點管理與防護措施。

  (4) 稽核小組，負責定期執行資安稽核，檢視制度符合性與改善計畫。

  (5) 資安管理委員會：了解組織營運目標與風險，資安管理審查。

- **資訊安全策政**

  (1) 資通安全管理制度化，建立符合國際標準的資通安全管理系統，強化公司資訊環境的安全性。

  (2) 資安意識宣導，推廣資通安全政策與教育訓練，提高員工的資訊安全意識，並要求遵守相關規範。

  (3) 系統安全防護，導入先進的資訊安全技術，持續提升資通安全防護水準。

- **資訊安全策政之管理方案及控制措施**

  (1) 身分與存取控管，實施資訊系統身分存取控管，導入多因素驗證 MFA 機制以提升存取安全，密碼需符合強度要求並定期更換，權限定期審查。

  (2) 端點與惡意程式防護，電腦定期更新最新防毒碼，及建立網路防入侵機制，阻斷網路攻擊，避免電腦中毒的風險。

  (3) 網路安全防護與偵測，建置企業防火牆與分層式網路防禦架構，搭配入侵偵測與入侵預防機制（IDS/IPS），持續監控網路流量與異常行為，以強化整體網路安全防護能力。

  (4) 資安事件通報與應變，建立資安事件通報與應變流程，依事件等級逐級通報至高階管理層，並持續追蹤改善。

  (5) 教育訓練與宣導，定期舉辦資訊安全教育訓練與意識宣導，涵蓋帳號密碼安全、電腦與網路安全、社交工程防範等，提升員工資安意識並落實資訊安全管理。

  114 年度公司參與自辦或派外教育訓練資訊如下：

課程名稱	訓練方式	時數(hr)	受訓人數
資訊系統與管理守則	線上課程	0.5	404
資訊安全教育訓練	實體面授	1	27
資訊安全系統稽核員訓練	外部訓練	6	10
資安事件預防措施，資訊安全意識，資通安全指引	外部訓練	6	1