

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。

● 資通安全適用範圍與對象

適用本公司員工及約聘雇人員，範圍包含同仁及接觸公司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「資通安全管理辦法」，以建立與實施資訊安全管理制度，其權責劃分如下：

- (1) 資安專責主管負責集團資安策略、機敏資訊分級及管理規範與政策擬定。
- (2) MIS 部門主管，負責 IT 相關的資訊安全監控。
- (3) 文管人員負責技術文件資料保存安全。
- (4) 行政人員負責實體與環境安全
- (5) 人資負責人員安全權責、訓練與獎懲。

● 資訊安全策政

- (1) 確保公司研發及業務資料之機密性、完整性及可用性，防止非法使用。
- (2) 確保公司所提供資訊服務之完整性與可用性，並提供全公司同仁便利和穩定的資訊服務。
- (3) 確保本公司所提供軟硬體資源之可用性，合法及正確地使用。

● 資訊安全策政之管理方案及控制措施

- (1) 對外進及出的電子郵件備份：對外郵件完整歸檔，以備日後存取，降低營運風險。另有完整的安全性權限管控，以確保隱私性及資料使用的合法性，而且有可追蹤的存取記錄。
- (2) 防毒及網路安全威脅防護：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) 加強 SAP、PLM、BPM 及雲端應用，軟硬體整合帶動公司營收利潤。
- (4) 防疫期間增加雲視頻與遠端連線，提供員工團隊合作即時通訊的平台，延續原本溝通的效率與生產力，防疫期間企業營運不中斷。
- (5) 落實資安意識，推廣集團所有員工，以達到人人均為資安為目的，同仁需接受資訊安全教育訓練，包括資訊安全之基本觀念、公司資訊安全政策、資訊安全控制措施等。並說明違反資訊安全政策時可能會招致處罰、法律責任與公司營運所面臨之衝擊。

111 年度公司參與自辦或派外教育訓練資訊如下：

課程名稱	上課日期	訓練方式	時數	受訓人數
資訊安全與個資保護	112.12.14	外訓	6	9