資通安全管理及執行情形

1. 資通安全管理架構：

本公司為強化資訊安全管理，落實資通安全管理目標，確保資料、系統及網路之安全，特設立「資通安全管理小組」，小組內另包含一名資安主管及一名資訊員工，負責資通安全管理制度之規劃、建置、實施、維護、審查及改善，並由資安主管向董事會或管理階層報告資安的執行情況。

2. 資通安全政策：

制定「資通安全管理辦法」，確保所屬資訊資產之機密性、完整性及可用性，透過教育訓練及管理程序之落實，強化公司資通管理之及基礎架構、設備環境及系統安全。

3. 資訊安全具體管理方案及實施狀況：

具體方案	113 年度實施狀況
員工安全管理及教育訓練	1. 資安培訓計畫： 針對人員之工作職掌，給予不同之職務權限，透過適當之資安訓練，使人員充分了解公司之資安政策；不定期派員參與外界舉辦之教育訓練、研討會及資安展示會等。 2. 資安政策宣導： 一個月一次以上以 E-mail 方式公告資訊安全相關訊息。 3. 資安人員培訓： 每人每年至少接受 12 小時以上之「資通安全專業課程訓練」或「資通安全職能訓練」。
電腦主機及網路設備安全	1. 定期漏洞掃描及修補： 定期進行漏洞掃描，即時修補發現之漏洞，以確保系統安全性。 2. 強化設備設定： 確保所有設備使用安全上之設定，包括防火牆、連線政策、密碼政策及登入權限限制等。 3. 定期更新與升級： 確保所有系統設備軟體均能即時收到版本升級通知並即時更新，以修補已發現的安全漏洞。 4. 實施多層防禦： 除使用系統內建的防護軟體外，亦採購知名品牌之防毒軟體及高階硬體式防火牆，並持續進行更新使軟硬體保持最新的防護版本及病毒碼。 5. 實施存取控制： 利用公司網域帳號建立存取控制政策，避免未經授權之人員進入系統並進行資料存取。
系統與資料控管安全	1. 定義資料敏感性： 針對不同敏感程度之資料加以分類，並依敏感程度給予不同之控管規範。 2. 建立備份還原計畫： 擬定備份還原計畫，包含備份設備、備份時機、備份種類及還原流程等，以確保於災害發生或儲存媒體失效時，可迅速回復正常作業。 3. 實施流量控管監控： 擬定監控機制，定期監控網路流量狀況，及時偵測異常狀況。

	4. 定期進行內部資安盤查： 定期針對資安內部進行稽核審查，根據環境變化及法令規範，隨時精進資安管理制度，以應對瞬息萬變之資安環境。 5. 社交工程演練： 定期進行社交工程演練，以提升員工對資安的警覺性。
投入資訊安全資源	依年度預算進行防火牆及防毒軟體續約授權，並視公司需求，新購垃圾郵件系統及電子資料控管系統，另外，每年至少一次與防火牆及防毒軟體廠商配合進行系統維護作業，以提高並確保整體作業環境之安全性。