資通安全風險管理

1. 資通安全政策：

公司的資訊安全政策，是以「一、建立符合法規與客戶需求之資訊安全管理規範；二、透過全員認知，達成資訊安全人人有責的共識；三、保護公司、廠商與客戶資訊的機密性、完整性與可用性；四、提供安全的生產環境，確保公司業務之永續營運」為指導準則。並以防毒、防駭、防漏三大資安防護主軸為目標，建立防火牆、入侵偵測、防毒系統及諸多內控系統，以提升公司在防禦外部攻擊以及確保內部機密資訊防護的能力。

建立完整的資訊安全管理系統，從系統面、技術面、程序面降低企業資安威脅，建立符合客戶需求的資訊安全保護環境，並不斷地進行「計劃 - 實施 - 查核 - 行動」循環以持續改善。

「計劃階段」著重資安風險管理，為了強化資訊安全，本年度參考 CNS27001 資訊安全管理標準作業，新訂「資通安全政策及作業」並預計揭露於公司網站，使資訊系統皆能在標準的管理規範下運作，降低因人為疏失所造成的安全漏洞及生產異常，也透過年度的複審作業，不斷持續改善。

「執行階段」建構多層資安防護機制，持續導入新資安風險控管技術，以智慧化 / 自動化機制提升各類資安事件之偵測及回應處理程序的效率，並強化資訊安全及網路安全保護流程，以維護公司重要資產的防護。

「查核階段」定期監控資安管理指標成效，及上述管理系統每年第三方複審稽核，及公司內部資安稽核，以確保持續提升資安管理及防禦能力。

「行動階段」檢討與持續改善，當員工及承商違反資安相關規範及程序時，依據規定進行懲處，並持續進行資安專責人員外部相關教育及內部資安教育訓練以提升資安意識。

2. 資通安全組織架構：

(1) 本公司於 112 年設置「**資通安全推動小組**」，每年至少開會一次，推動資通安全持續精進。

(2) 「**資通安全推動小組**」由總經理擔任召集人，全公司參與。分為管理委員會和安全推行小組：

管理委員會：

召集人：總經理，核准各項資通安全制定。

委　員：各部門主管，執行各項資通安全作業推動，回饋可行性評估及改善建議。

安全推行小組：

電腦中心：因應新資通安全威脅，制定及推動相關資通安全建置。

稽 核 室：查核各項資通安全建置落實情況。

行 政 部：資通安全推廣教育訓練，相關人員出席檢核。

(3) 113 年度已召開一次管審會議。遇重大資安事件，則隨時召開會議，製定相關因應作業及落實管理辦法。

3. 資通安全具體管理方案：

為達資安政策與目標，建立全面性的資安防護，推行的管理事項及具體管理方案如下：

(1). 提升資安防禦能力：定期進行資安系統脆弱度分析及滲透測試，並加以補強與修護，以降低資安風險。建立網路安全事件應變計畫，依事件嚴重度等級進行影響和損失評估，採取對應的通報及復原行動。

(2). 精進資安管理程序：不斷強化資安防禦能力外，在管理程序及意識認知上也須並重。依據NIST（National Institute of Standards and Technology）標準建立企業資安框架，設置對應的度量指標。員工應遵守資安規定(如嚴格管制行動儲存裝置)、遵循 SOP 作業，並不斷地進行「計劃 - 實施 - 查核 - 行動」循環以持續改善。

(3). 增進網路、端點及應用安全：提升端點設備的異常偵測及防護能力，包含應用程式白名單（Application Whitelisting）機制與端點偵測與回應（EDR, Endpoint Detection and Response） 機制。整體資訊系統網路安全區域優化，增加重要主機特權帳號登入多因子認證防護。

(4). 風險控制：與國際資安大廠合作，透過其專業服務進行整體資安體檢，以公正第三方驗證之客觀結果，作為進階資安強化的依據。保護公司於發生網路攻擊時，能將潛在損失降至最小的範圍。

(5). 教育訓練：進行全員資安教育訓練與不定期社交工程釣魚郵件測試，以提升資安意識，使資安的運作在高階主管與各部門的支持下，落實到每一位員工身上。