資通安全管理

（一）資通安全風險管理架構、資通安全政策、具體管理方案及投入資通安全管理之資源：

1.資通安全風險管理架構

為確保本公司自有及客戶夥伴之資訊資產安全，鑒於資訊安全風險評估，並保障本公司及利害關係人權益，本公司於民國111年設立工業4.0專案小組負責擬訂年度資訊安全策略，整合督導及協調年度資訊安全計劃，資訊安全檢核基準；協調相關資源及跨單位活動，統籌資訊安全事件管理，規劃資訊安全教育，擬訂及執行資訊安全稽核作業；工業4.0專案小組每月召開主管會議，檢視及決議資訊安全與資訊保護方針及政策，落實資訊安全管理措施的有效性。

2.資通安全政策

本公司制訂資訊使用辦法辦法，並參照政府法規制訂個人資料保護管理要點等等；隨時蒐集、分析最新資訊安全相關法規，以制訂或修訂相關管理辦法;定期審查所需執行的資訊安全相關作業，以確保符合安全政策。

3.具體管理方案及投入資通安全管理之資源

本公司重視資訊安全風險控制與保護，實施嚴格的管控措施，例如資料對外傳輸的管制，必須經過申請核准、郵件系統防護、列影印傳真之資料輸出管制、網路異常查核、資訊設備進出必須遵照流程提出申請核准、禁止攜入私人儲存裝置、禁止私人設備進行拍照或錄影、加強出入管制與門禁，權限需定期進行重新審閱、透過實體或線上課程給予全體同仁進行資安教育訓練，新進員工到職當日即進行新人資安教育訓練，協助了解相關資安規範，並公告資安管控及重大資安事件進行意識宣導，定期參加各類資安相關或駭客攻防的技術課程，培訓資安技術人員、實體防護強化，資安管控依年度計畫升級、新購或引進新技術。

近年來網路攻擊事件頻傳，勒索病毒尤為猖獗，影響層面廣泛，

已對企業造成莫大的損害，不得掉以輕心，本公司針對國內外重大資安事件進行深入分析探討，例如跨國金融犯罪、遠端遙控ATM、國際環球金融系統SWIFT滲透轉帳、企業詐騙、勒索、洩密等，加強內部及外部網路攻擊防護，教育訓練意識宣導，嚴格執行防火牆政策審核、主機端點防護、網路入侵偵測、防毒系統更新、主機及網路設備漏洞修補、零時差攻擊防護、釣魚郵件偵測、異常行為判定、電腦機房管理等，透過本公司資安維運的平台，定期進行系統查核與改善，導入新技術來加強資料防護；本公司秉持互惠雙贏，實事求是的經營理念，為客戶及股東創造價值，善盡社會責任。