資通安全管理

1.資通安全管理架構

本公司已於2019年設置「資訊安全小組」,由總經理擔任召集人，下轄資訊室、財務部、綜合管理部、稽核室、銷售部及採購部等，並訂定「資訊安全政策」對本公司資訊安全進行管控，定期召開小組會議，審視資訊安全控制措施的實施與成效，定期檢討資安政策以及協調資訊安全管理業務的推動。目前資訊室已有2名專業資訊安全人員，財務部、綜合管理部、稽核室等各單位指派共7名資安代表，共同推動本公司資通安全之管理。總經理每年至少一次向董事會報告公司執行資通安全管理的政策與執行情形。

2.資通安全政策

本公司為確保資訊資產(與資訊處理之相關硬體、軟體、資訊、文件及人員等)之機密性、完整性、可用性及適法性，避免遭受內外部蓄意或意外之資安威脅，並衡量檢討本公司之業務需求，訂定本公司資安政策如下：

A.資安治理：持續精進管理制度，掌控風險及強化防範，包括強化教育訓練、資訊安全基礎架構設計等。

B.法令遵循：每年定期檢視及修訂內部作業規範以符合資安標準及各地區法令規定。

3.資通安全控制措施

A.採用反垃圾郵件軟體配合防火牆做防護，針對每封郵件與其附件及郵件中連結進行檢測及主動隔離，有效避免員工誤開惡意郵件。

B.加強公司全體員工之資訊安全意識與權責分工，並持續資訊安全運作及演練作業。

C.若遇到重大危害或毀損，將啟動異地備援機制，伺服器端可以最快速度讓服務上線及營運，降低損害的影響。

4.投入資通安全管理之資源

A.購置反垃圾郵件軟體及內網防火牆做防護，針對每封郵件與其附件及郵件中連結進行檢測及主動隔離，有效避免員工誤開惡意郵件。

B.本公司於2022年度召開2次資訊安全管理會議,檢討各單位執行資案政策之情形，並無發現有危害資安之事件。。

C.本公司於2022年度執行1次異地備援演練,加強員工對於資安風險的應變與警覺性。

D.辦理資訊安全教育訓練，課程內容包含「網路釣魚」、「訊息安全」、「瀏覽器安全」、「商業電子郵件」、「惡意軟體」等5堂課，共325人完成受訓，受訓時數為1,625小時。

5.資通安全風險及因應措施

本公司已針對營運類資產如網路設備，投保硬體設備電子保險，經「資訊安全小組」評估本公司目前只有收發郵件、瀏覽器安全及使用ERP有資通安全之風險，惟本公司已設置「資訊安全小組」負責處理有關資訊系統安全預防及危機處理相關事宜、資訊系統架構依其風險等級建立可用性之資料備份機制，每年評估對財務面、法令面、客

戶等層面之營運風險與衝擊，適時規劃設計及提升軟硬體設備資源、改善作業流程等因應措施，可大幅降低資安風險所造成的影響。2022年度本公司並無資通安全之情事發生，經「資訊安全小組」評估後，本公司資訊安全並無重大營運風險。