⼀、資訊安全管理架構

1. 本公司資訊安全管理單位為資訊部，負責規劃、執行及推動資訊安全管理相關工作，並加強全體同仁資訊安全意識。

2. 本公司資訊安全查核單位為稽核室，稽核時若發現缺失，即要求受查單位提出相關改善計畫，且定期追蹤改善成效，以降低資訊安全風險。

3. 本公司已於109/11/6 董事會會前向所有董事簡報，主題為「羅昇資訊安全因應說明」。

二、資訊安全管理政策

本公司資安防護重點分為兩方面

1. 雲端管理：將傳統老舊的工作負載從資料中心移轉至雲端。於「升級」的過程中，考慮要在雲端內採用何種 IT 工具及資安防護讓營運流暢。

2. 端點防護：要建立偵測(Detect) 、防護(Protect) 和回應(Response) 等資安全面功能。

三、資訊安全管理措施

1. 建置次世代防火牆以智慧型防護機制主動偵測各種網路與應用層攻擊並具備一般防火牆被動黑白名單防護/流量管控/即時監控等傳統功能。

2. 採用反垃圾郵件軟體配合防火牆作防護，針對每一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。

3. 安裝企業防毒軟體並開啟系統的自動更新來防堵漏洞被外部攻擊，此外，重要檔案及內部主機及區域皆進行權限控管，避免被惡意程式操控危害重要的主機及竄改重要的檔案。

4. 遇到重大危害及毀損，則會啟動異地備援機制，伺服器端可以最快的速度讓服務上線及營運，而客戶端存在此機制，可讓員工遭受重大破壞後，以最快的速度重新作業。