資安風險及因應措施

資訊安全管理現況、資訊安全政策、資安風險及風險因應對策：

1. 資訊安全管理現況：

   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，並訂定「資訊安全政策」對本公司資訊安全進行管控，且將資訊安全檢查列入每年稽核項目中，每年定期向董事會報告。

2. 資訊安全政策：

   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. 資訊安全風險：

   本公司設置「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，應可大幅降低資安風險所造成的影響，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。考量資安險仍是新興險種，涉及資安等及檢測機構、理賠鑑識機構及不理賠條件等相關配套，後續會再評估是否購買資安險。

4. 風險因應對策：

   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。

   c. 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。

   d. 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。