資通安全管理

本公司為控管或維持公司的營運及會計等重要企業運作的功能需倚賴網路系統，網路系統可能會遭遇網路攻擊以竊取公司的機密資訊，例如客戶或其他利害關係人的專有資訊以及員工的個資。惡意的駭客亦能試圖將電腦病毒、破壞性軟體或勒索軟體導入公司網路系統，干擾公司的營運、以重新取得電腦系統控制權對本公司進行勒索或窺探機密資訊。

因應措施：

1.本公司於行政暨管理處下設置資訊部門，並任命資訊安全主管，由資訊安全主管帶領定期執行資安檢查。稽核部門每年對電腦循環進行稽核，並向審計委員會及董事會報告稽核結果。

2.本公司訂定資訊安全政策包含(1)資料備援 (2)資料儲存 (3)系統安全 (4)風險層級 (5)權限設定 (6)員工使用系統、Email 規範，並公告於企業內部網站，供全體員工查詢遵循。資訊部門定期依照資安政策執行公司資安狀態檢視，並由資訊部門主管報告予執行長。

3.不定期進行系統重大更新。如有重大資安風險即時公告並採取相對應之措施。每年開設資安課程，教育員工如何辨別不安全的電子郵件。系統受密碼保護並設置單一登入，以便於管理與維護。

4.為強化網路安全，因應網路普及帶來新的資安問題。減少病毒、蠕蟲及其他網路攻擊所造成之危害，採取多種安全防範措施並定期更新，包含防火牆、入侵偵測系統、防毒等技術，即時反應以降低各種網路攻擊所帶來之傷害。

5.資訊系統架構依其風險等級，已建立高可用性之主機備援及異地資料備份機制，以確保服務不中斷，每日檢測網路作業環境及定期備份數據，將備份數據再備份並放置在異地保管存放，加強機房各項模擬測試與緊急應變等演練以確保資訊系統之正常運作及資料保全，可降低無預警天災及人為疏失造成之系統中斷風險，確保符合預期系統復原目標時間。未來針對系統架構、擴充彈性與災害復原、資訊安全等方面選擇系統進行提升。依據風險等級，規劃設計與提升適當軟硬體設備。並評估異地資料備份之儲存空間。

6.具體管理做法如下：(a) 2022 年度資訊部門對全體員工發出至少五封宣導或通知信，提醒員工對異常信件提高警覺，並即時報請資訊人員處理。(b) 資訊部門安全主管不定時辦理資安內部培訓資安人員，並隨時與資安廠商合作安排外訓及隨時交換最新資安訊息。(c) 帳號異動及權限設定需經過核准。