資訊安全風險管理

為保護本公司營業秘密、智慧財產及公司機密資訊，降低公司營運風險，並對個人資料之保護與管理，本公司已訂定各項電腦化資訊系統處理作業及個人資料保護等相關辦法，以落實內控制度與維護資訊安全政策。透過每年檢視和評估其安全規章及程序，確保其適當性和有效性。以下分項進行詳細說明：

(1)資訊安全政策

A.確保本公司資料、系統、設備及網路通訊安全，阻絕外界之入侵、破壞。

B.確保系統資訊帳戶存取權限與系統之變更均經過公司規定程序授權處理。

C.落實銷毀程序，已報廢之電腦儲存媒體應加以銷毀避免資料意外暴露外流。

D.監控資訊系統之安全狀態與活動紀錄，有效掌握並處理資訊安全事件。

E.維護資料與系統之可用性與完整性，發生災害或受破壞時，可回復正常作業。

目前本公司資訊安全維護措施完備且考量資安險仍是新興險種，且涉及資安分級和理賠鑑識等配套，因此尚在評估未來適用性之階段。

(2)資安網路架構

本公司注重資訊安全事項，必要時定期向經理人會報資安管理運作情形。公司之內部系統皆處於虛擬網路之中，外部網路受隔離無法直接進入，並已採用多重網路安全防禦系統，位於網路前端之防火牆、郵件內容安全控管系統負責過濾網路進出連線的內容，能防禦外部網路攻擊，並即時封鎖最新惡意軟體、有害之網站連結、垃圾電子郵件等威脅。位於內部之主機及端點皆由中控台佈署防毒軟體，隨時更新病毒碼與即時辨識惡意行為特徵，能即時攔截病毒木馬蠕蟲、勒索軟體、文件夾帶之惡意程式等，有效降低被駭客攻擊損害之風險。

(3)系統帳號生命週期管理與權限帳號管理

依各業務範圍、權責分別設定使用者之帳號及權限，資料之存取皆需透過簽核流程經各權責主管申請並核准後始能使用與變更。使用者一旦離開原職務，立即撤銷該使用者之帳號及權限，以防範未經授權之使用。

(4)資料存取紀錄稽核備存

能紀錄系統檔案文件存取之軌跡記錄、往來郵件等資料，進行歸檔保存。報廢程序完成之電腦均執行硬碟拆解破壞以符合法規遵循的管理制度及資安政策。

(5)資訊系統持續運作

重要系統與文件皆採取每日、每週及每月之本地備份，相關之備份資料以磁帶方式存放到異地資料中心(IDC)做為異地備份。並每年定期執行系統資料復原測試演練，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災害造成之資料損失風險。

(６)教育訓練

不定期辦理資訊安全教育訓練及宣導，建立員工資訊安全認知及尊重智慧財產權概念，保護人員及公司資訊。

本公司年度稽核項目包含資訊安全檢查，透過稽核單位查核，加強內控管理，資訊中心執行作業依本公司規定程序均能落實執行，確保資料完成性與安全性，風險評估結果尚屬良好，資訊中心執行作業依本公司規定程序均能落實執行，確保資料之完成性與安全性。