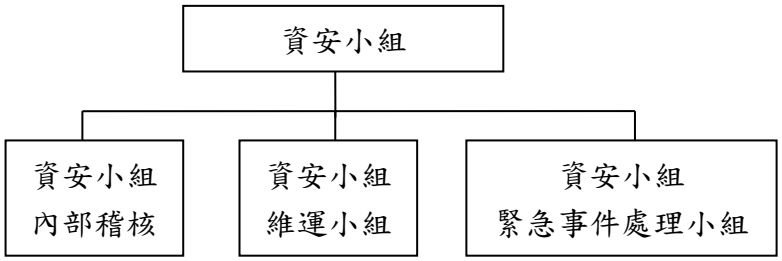
中化投資控股股份有限公司

資通安全風險管理架構、安全政策、管理方案及投入資源

（一）敘明資通安全風險管理架構、資通安全政策、具體管理方案及投入資通安全管理之資源等。

1.資通安全風險管理架構



本公司於資訊處下成立資安小組(如上組織架構圖) 及設置資安專責主管(1員)及人員(1 員)，負責審視公司及各子公司資安政策、監督資安管理運作情形，以建構出全方位的資訊安全防禦能力及同仁良好的資訊安全意識，每年定期向董事會報告資通安全管理及執行成果。在網路安全防禦措施方面，已採用多重網路安全防禦系統，位於網路前端之防火牆、入侵偵測系統、防毒作為企業資安防護基礎，在內部之主機及端點機台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。每年定期由內部稽核單位執行資通安全管理作業查核，並出具稽核報告，並定期於審計委員會及董事會做稽核結果業務報告。

2.資通安全政策

本公司的資訊安全政策涵蓋公司及各子公司，指導原則如下:

●建立符合法規與商業需求之資訊安全管理規範。

●透過持續的教育訓練，達成資訊安全人人有責的共識。

●保護本公司業務活動資訊，避免未經授權的修改，以及阻絕外界之入侵確。

●協助公司的永續經營。

並以防毒、防駭、防漏三大資安防護主軸為目標，建立防火牆、入侵偵測、防毒系統及諸多內控系統，以提升公司在防禦外部攻擊以及確保內部機密資訊防護的能力。

3.具體管理方案

●網路安全：強化網路防火牆與網路控管以防止電腦病毒跨機台及跨廠區擴散，導入先進的解決方案以偵測與處理惡意軟體，導入新技術加強資料保護，加強釣魚郵件偵測等。

●裝置安全：依電腦類型建置端點防毒措施，強化惡意軟體行為偵測。

●應用程式安全：持續強化應用程式安全控管機制，執行資通系統源碼安全措施，包含源碼存取控制與版本控管，於上線前執行安全性要求測試，包含機敏資料存取、用戶登入資訊檢核及用戶輸入輸出之檢查過濾測試，並檢討執行情形，並檢討執行情形。

●資料安全保護：資料使用及取閱嚴格權限分層授權，持續強化文件及資料加密控管及有效追蹤，導入新技術加強資料保護。

●教育訓練及宣導：透過定期教育訓練加強員工對資訊安全的觀念和郵件社交工程攻擊的警覺性，提供資訊部同仁資訊安全相關技能培訓，持續提升資安人員技能。

4.投入資通安全管理之資源：

本公司在新人訓練排定資訊系統操作和有關資通安全規範之課程不定期以時事案例透過公司內部網路對員工做資通安全宣導，為強化本公司資訊安全技術及安全防護，民國 113 年投入資通安全防護相關費用約 13,630 仟元，114 年編列投入預算約 20,000 仟元，並設置資安專責主管(1 員)及人員(1 員)，負責公司資訊安全規劃、技術導入，以維護及持續強化資訊安全。每年定期向董事會報告資通安全管理及執行。

（二）本公司最近年度及截至 113 年度止，未發生影響公司營運之重大資安事件。