致和證券資訊安全政策及具體管理方案

本公司每年定期評估資訊安全政策並提報董事會通過，近期提報董事會日期為109年2月10日，且每年將前一年度資訊安全整體執行情形，由資訊安全人員與董事長、總經理、稽核主管聯名出具資訊安全整體執行情形聲明書，並提報董事會通過，於會計年度終了後三個月內將該聲明書內容揭露於公開資訊觀測站。

本公司資訊安全各項主要評估項目與具體管理方案分述如下：

（一）指定一位資訊安全人員負責執行資訊安全工作，且每年定期參加十五小時以上資訊安全專業課程訓練。

（二）每年辦理二次員工資訊安全宣導。

（三）網路系統安全評估：

(a)定期評估網路系統安全（例如：作業系統、網站伺服器、瀏覽器、防火牆及防毒版本等）。

(b)定期修補網路設備之安全漏洞。

（四）電腦病毒及惡意軟體之防範：

(a)安裝防毒軟體，並及時更新程式及病毒碼。

(b)定期對電腦系統進行病毒掃瞄

（五）定期檢查網路下單系統提供之功能。

（六）定期評估電腦系統容量，定期對系統容量進行壓力測試。

（七）每半年辦理資訊系統弱點掃描作業，針對所辨識出之潛在系統弱點，評估其相關風險或安裝修補程式。

（八）行動應用程式檢測：每年委由經財團法人全國認證基金會 （TAF）認證合格之第三方檢測實驗室進行並完成通過資安APP檢測，檢測範圍以經濟部工業局委託執行單位「行動應用資安聯盟」公布之行動應用程式基本資安檢測基準項目進行檢測。

（九）定期測試故障復原程序，針對測試缺失謀求改進。

（十）訂定資訊安全訊息通報機制，針對與資訊系統有關之資訊安全事故，採取適當矯正程序。

(十一)訂定分散式阻斷服務攻擊（DDoS）防禦與應變作業程序。

(十二)定期舉辦社交工程教育訓練及電子郵件社交工程演練，測試、宣導及強化資通安全教育，讓同仁瞭解使用電子郵件之風險，提高同仁防範社交工程攻擊之危機意識，持續演練以降低社交工程攻擊所造成之風險，進而達到保護客戶資料及重要營運資訊與服務之目的。