

致和證券股份有限公司資訊安全整體執行情形聲明書



謹代表致和證券股份有限公司聲明本公司於一〇八年一月一日至一〇八年十二月三十一日確實遵循「證券暨期貨市場各服務事業 建立內部控制制度處理準則」第十條第十款、第三十六條之二規定，及同業公會所定資訊安全自律規範。經審慎評估，本年度資訊安全整體執行情形，除附件所列事項外，均能確實有效執行。如有虛偽，願負法律責任。

此致

金融監督管理委員會

聲明人 董事長：

許文科

(簽章)



總經理：

潘煒華

(簽章)



稽核主管：

吳慧娟

(簽章)



負責資訊安全之最高主管：

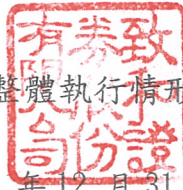
黃信元

(簽章)



中 華 民 國 109 年 2 月 10 日

致和證券股份有限公司資訊安全整體執行情形應加強事項及改善計畫



(基準日：108 年 12 月 31 日)

應加強事項	改善措施	預定完成改善時間
一、辦理資訊安全作業有下列欠妥事項： 1. 員工均可利用公司電腦網路使用社群媒體，核與所訂「雲端運算、社群媒體、行動裝置資訊安全管理辦法」第 6 條及建立證券商資通安全檢查機制第 12 點(2)a：「公司應訂定社群媒體相關資訊安全規範與運用社群媒體管理辦法」等規定不符。 2. 尚未訂定社交工程作業規範，明定辦理對象、頻率及作業程序，且迄基準日止未曾辦理社交工程演練，不利防範遭社交工程郵件入侵風險。 3. 依所訂「移動式儲存媒體使用管理辦法」第 10 點「公司個人電腦 USB 裝置預設僅開放讀取功能，若業務需求可填寫『USB 儲存媒體申請表』，經權責主管核准後開放 USB 裝置寫入功能。」，雖已訂定限制 USB 隨身碟寫入功能之規定，惟未建立控管機制，致員工未經申請核准仍可執行複製、下載等寫入功能，控管作業核欠妥當。 二、辦理業務單位資訊需求，經查有下列欠妥事項： 1. 辦理資訊系統程式之修改人員與程式換版人員為同一人，且未留存申請前後異動紀錄供主管覆核，作業不符牽制原則，且不利資訊作業之內部控制。 2. 業務部辦理高風險證券控管之異動作業，有未填具電腦作業需求單，即由資訊單位逕予修改，權責劃分不明與所訂「使用電腦化資訊	一、辦理資訊安全作業有下列欠妥事項： 1. 員工均可利用公司電腦網路使用社群媒體之情事，已訂社群媒體使用規範 2. 已訂定社交工程作業規範，明定辦理對象、頻率及作業程序，已於 108 年 11 月 1 日至 12 月 31 日對使用公司電子郵件信箱 (***)@jyhher.com.tw) 人員辦理社交工程演練。 3. 已將所有電腦之 USB 預設為唯讀，需填寫申請表後，始可開放 USB 寫入功能。 二、辦理業務單位資訊需求欠妥事項： 1. 已調整程式修改及換版人員為不同人，並提供異動記錄備查。 2. 該項業務已交由權責部門自行辦理。	已改善。 已改善。

處理作業辦法」一(三)3.C:「使用部門之職責如下:(a)負責相關應用系統內資料之輸入、修改、刪除、運用與維護作業。」之規定不符。 三、對系統使用者之管理有下列欠妥事項: 1.對證券交易系統最高權限使用者(root)帳號之使用尚未建立控管機制,未檢核作業執行內容及留存使用紀錄(log)備查,系統權限控管欠嚴謹。 2.有授予非職掌業務所需權限者,如:授予非營業單位之總經理、電資部主管及人員等6人開戶作業子系統及信用作業子系統之讀、寫權限,並包括客戶資料變更作業、信用開戶登錄等作業;授予稽核室主管及人員等3人委託買賣代理人之建檔作業權限。 四、辦理系統開發及維護委外作業,經查委外契約未約定資訊安全協定,有與對委外廠商資安稽核等條款之情事,與「建立證券商資通安全檢查機制」9、(4)系統開發及維護:「委外作業應簽訂契約,委外作業契約內容應包含資訊安全協定與對委外廠商資安稽核等條款。」之規定不符。	三、對系統使用者之管理欠妥事項: 1.已對最高權限使用建置控管機制, 2.對執行作業同步留存log記錄並限制權限功能。 四、已與委外廠商增訂資安稽核權條款。	已改善。 已改善。
---	---	-------------------------