致和證券股份有限公司

內部控制制度聲明書　　日期：111年01月26日

本公司民國110年度之內部控制制度，依據自行評估的結果，謹聲明如下：

一、本公司確知建立、實施和維護內部控制制度係本公司董事會及經理人之責任，本公司業已建立此一制度。其目的係在對營運之效果及效率(含獲利、績效及保障資產安全等)、報導具可靠性、及時性、透明性及符合相關規範暨相關法令規章之遵循等目標的達成，提供合理的確保。

二、內部控制制度有其先天限制，不論設計如何完善，有效之內部控制制度亦僅能對上述三項目標之達成提供合理的確保；而且，由於環境、情況之改變，內部控制制度之有效性可能隨之改變。惟本公司之內部控制制度設有自我監督之機制，缺失一經辨認，本公司即採取更正之行動。

三、本公司係依據「證券暨期貨市場各服務事業建立內部控制制度處理準則」（以下簡稱「處理準則」）規定之內部控制制度有效性之判斷項目，判斷內部控制制度之設計及執行是否有效。該「處理準則」所採用之內部控制制度判斷項目，係為依管理控制之過程，將內部控制制度劃分為五個組成要素：1.控制環境，2.風險評估，3.控制作業，4.資訊與溝通，及5.監督作業。每個組成要素又包括若干項目。前述項目請參見「處理準則」之規定。

四、本公司業已採用上述內部控制制度判斷項目，評估內部控制制度之設計及執行的有效性。

五、本公司基於前項評估結果，認為本公司於民國110年12月31日的內部控制制度（含對子公司之監督與管理、資訊安全整體執行情形），包括瞭解營運之效果及效率目標達成之程度、報導係屬可靠、及時、透明及符合相關規範暨相關法令規章之遵循有關的內部控制制度等之設計及執行，除附件所列事項外，係屬有效，其能合理確保上述目標之達成。

六、本聲明書將成為本公司年報及公開說明書之主要內容，並對外公開。上述公開之內容如有虛偽、隱匿等不法情事，將涉及證券交易法第二十條、第三十二條、第一百七十一條及第一百七十四條等之法律責任。

七、本聲明書業經本公司民國111年01月26日董事會通過，出席董事10人中，有0人持反對意見，餘均同意本聲明書之內容，併此聲明。

致和證券股份有限公司

董　事　長：許文科　簽章

總　經　理：　　簽章

稽核主管：吳慧娟　簽章

資訊安全長或負責資訊安全之最高主管：　簽章

致和證券內部控制制度應加強事項及改善計畫

（基準日：110年12月31日）

應加強事項	改善措施	預定完成改善時間
櫃買中心就該110年8月30日至9月6日對本公司進行例行查核，發現下開缺失注意改善：		
一、核心系統(如：證券交易系統後台、帳務中台及雷影中台等)雖有區分營運環境及測試環境，惟未設置適當之區隔機制。	針對核心系統雖有區分營運環境及測試環境，惟未設置適當之區隔機制，已於南北2區中心各新增一台路由路，南部測試環境主機改為192.9.201.x,北部改為192.108.201.x網段，將正式環境及測試環境採實體區隔。	已改善。
二、部分系統(如：交易系統後台、三竹行動、帳務中台、精誠WEB及嘉實AP)之最高權限帳號之密碼長度為6碼，核已違反公司自訂之系統最高權限管理辦法第4條「新系統之最高權限密碼登錄，密碼應設為8碼以上，其中應包括文數字的穿插」之規定。	針對部分系統之最高權限帳號之密碼長度為6碼之情事，已將系統之高權限帳號(交易系統後台、三竹行動、帳務中台、精誠WEB及嘉實AP)之密碼調整為8碼，以符合公司自訂「系統最高權限管理辦法」第4條規定。	已改善。
三、未依規定申請資訊廠商透過遠端遙控軟體連線方式進行維護，且使用具管理者權限之應用系統帳號執行程式更新版本暨維護作業時，未留存維護作業紀錄及「公司應建立系統最高權限帳號管理辦法(含作業系統及應用系統)，如需使用最高權限帳號時須取得權責主管同意，並留存相關紀錄」之規定。	針對未依規定申請資訊廠商透過遠端遙控軟體連線方式進行維護，且使用具管理者權限之應用系統帳號執行程式更新版本暨維護作業時，未留存維護作業紀錄及「公司應建立系統最高權限帳號管理辦法(含作業系統及應用系統)，如需使用最高權限帳號時須取得權責主管同意，並留存相關紀錄」之規定，修訂本公司「遠端連線管理辦理」，新增遠端連線相關申請書，由廠商工程師提出遠端連線時申請，補正最近	已改善。

應加強事項	改善措施	預定完成改善時間
	一次遠端連線申請紀錄及相關連線維護紀錄申請表。	
四、應用系統（含行動應用程式）程式異動，雖依規定填具「系統程式需求/測試驗收單」或「程式換版工作紀錄，且其驗收方式按上開表單紀錄係採簽核同意或就「修改測試是否符合要求」、「程式原本功能是否有被本次更新影響」及「是否同意更新至正式環境」項目勾選是否符合要求，惟未留存各該次測試項目、內容及相關測試經過紀錄。	針對應用系統（含行動應用程式）程式異動，未留存各該次測試項目、內容及相關測試經過紀錄提供最近系統程式需求/測試驗收單,含測試項目、內容及相關測試經過紀錄之情事，已對系統程式異動申請進行項目內容測試及留存相關紀錄，最近一次系統更新日期於11/23提出申請，11/26進行測試，於12/1驗收。	已改善。
五、貴公司行動裝置應用程式商店之使用帳號權限，如Apple的APP Store帳號權限，除資訊廠商三竹資訊持有APP管理帳號及開發者權限帳號外，貴公司人員亦持有多個具APP管理權限之帳號，惟前揭與APP有關之帳號權限尚未納入定期帳號權限審查範圍。	針對行動裝置應用程式商店之使用帳號權限，未納入定期帳號權限審查範圍之情事，採重新申請公司帳號並列示清冊，進行帳號與權限的管理，惟更換帳號將影響客戶之使用，故會在不能影響客戶的情況下進行更換作業，需要一段時間的轉換與審核過程，預計於111年4月底完成。	預計111年4月底完成。
六、未取得行動應用程式之程式原始碼，且未要求資訊廠商出具安全聲明文件。	針對未取得行動應用程式之程式原始碼，且未要求資訊廠商出具安全聲明文件，已將最近一次所換版本之行動應用程式（IOS版本2.0.5.0），請廠商出具Code Review 證明書，爾後若有更新行動應用程式，依規定取得行動應用程式之原始碼，或請廠商出具符合內控標準規範所條列之安全事項聲明書。	已改善。

應加強事項	改善措施	預定完成改善時間
七、未依規定對行動應用 APP 資安檢測報告執行覆核，並留存覆核紀錄。	針對未依規定對行動應用 APP 資安檢測報告執行覆核，並留存覆核紀錄之情事，已對今年所取得之行動應用 APP 資安檢測報告內容執行覆查，並留存紀錄表。	已改善。
八、所訂弱點掃描作業程序未明確規範各級風險弱點之評估及修補作業，且辦理資訊系統弱點掃描作業，僅就 WEB 網頁安全漏洞進行檢測，未包含主機作業系統及網路層面進行掃描檢測，致掃描範圍未臻完整。	針對所訂弱點掃描作業程序未明確規範各級風險弱點之評估及修補作業，且辦理資訊系統弱點掃描作業，僅就 WEB 網頁安全漏洞進行檢測，未包含主機作業系統及網路層面進行掃描檢測，致掃描範圍未臻完整，擬修訂本公司「弱點掃描作業程序」，並已洽詢廠商進行弱點掃描（簽呈-致北管簽字第39號），廠商預計於111年1月份進行作業， 預計於111年4月底完成。	預計111年4月底完成。

註:請詳列遭主管機關處警告(含)以上或罰鍰新臺幣24萬元以上之處分；另併請詳列受主管機關、證券交易所、證券櫃檯買賣中心、期貨交易所查核發現資訊安全缺失之改善情形。