

# 國票金融控股股份有限公司內部控制制度聲明書

謹代表國票金融控股股份有限公司聲明本公司於 111 年 1 月 1 日至 111 年 12 月 31 日確實遵循「金融控股公司及銀行業內部控制及稽核制度實施辦法」，建立內部控制制度，實施風險管理，並由超然獨立之稽核部門執行查核，定期陳報董事會及審計委員會。經審慎評估，本年度各單位內部控制及法規遵循情形，除附表所列事項外，均能確實有效執行。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。

謹 致

金融監督管理委員會

聲明人

董 事 長：

魏啟峰



(簽章)

總 經 理：

蘇松輝



(簽章)

總 稽 核：

侯文楚



(簽章)

總機構法令遵循主管：

吳美華



(簽章)

中 華 民 國 1 1 2 年 3 月 1 3 日

**國票金融控股股份有限公司內部控制制度應加強事項及改善計畫**  
(基準日：111 年 12 月 31 日)

應加強事項	改善措施	預定完成改善時間
<p><b>【子公司國票綜合證券公司】</b></p> <p>一、台灣證券交易所於 110 年 12 月 29 日對本公司 110 年 12 月 28 日之資通安全事件通報單進行查核，發現(一)網路下單登入未採多因子驗證。(二)資安事件延遲通報。(三)對於憑證申請及更新之驗證方式防護力不足時，未能即刻修改且無強化防護措施。(四)未能隨時檢討內部控制制度且確實執行。上述核已違反證交所 110 年 1 月 8 日臺證輔字第 1100500068 號函、110 年 11 月 30 日臺證輔字第 1100503618 號函、證交所營業細則第 18 條第 2 項之規定及證券商內部控制制度。111 年 4 月 6 日臺證輔字第 1110500866 號函，請公司注意改善，併課違約金新臺幣 43 萬元。</p>	<p>(一)111 年 3 月 31 日公司提供網路下單服務，於網路下單登入時已全面採多因子認證機制。</p> <p>(二)111 年 2 月 17 日公司已強化客戶申請憑證驗證機制(OTP 認證)，避免非本人取得憑證；每日針對本公司目前提供客戶網路下單系統之帳號登入失敗紀錄、非客戶帳號登入嘗試紀錄等異常登錄情形進行監控及分析。</p> <p>(三)資訊部於 111 年 4 月 14 日以電子郵件及 4 月 19 日「ISMS 專案」線上會議進行內控及法令宣導，嚴令同仁執行業務時，務必落實內控與法規規範，並重申要求資安人員於發生資訊系統有關之資訊安全或服務異常事件時應依『證券期貨市場資通安全事件通報應變作業注意事項』於知悉事件 30 分鐘內至通報系統，辦理事件初步通報。</p>	<p>已完成改善。</p>
<p>二、台灣證券交易所於 111 年 4 月 11 至 12 日對北投分公司進行查核，發現(一)未查證客戶同一 IP 下單原因及合理性並留存紀錄。(二)經理人與客戶有借貸款項之情事，核違反證交所營業細則第 18 條第 2 項及證券商負責人與業務人員管理規則第 18 條第 2 項第 9 款等規定。111 年 6 月 7 日臺證輔字第 1110501547 號函，請公司注意改善，併課違約金新臺幣 10 萬元。</p>	<p>(一)公司每日產製所有網際網路委託多筆買賣合計 250 萬元以上或單筆買賣 50 萬元以上明細間之相同 IP 資料，除已留存紀錄確認有精進方式可識別該相同 IP 係來自不同裝置下單者外，於次月底前完成查證作業並留存紀錄。</p> <p>(二)已於 111 年 6 月 21 日晨會及 7 月 6 日經理人會議重申加強對同仁及主管宣導相關法令遵循之教育訓練，以避免類似情事再次發生。</p>	<p>已完成改善。</p>

應加強事項	改善措施	預定完成改善時間
	<p>(三)北投分公司自行查核人員將缺失事項完成連續十個營業日增列為查核項目，經查未有類似缺失，並作成稽核報告備查。</p> <p>(四)稽核室針對缺失事項加強輔導與查核，經查核評估業已完成改善。</p>	
<p>三、金管會檢查局於 110 年 8 月 16 日至 9 月 11 日對公司進行資訊作業專案檢查，發現(一)作業系統主機設定之密碼原則安全參數，未明訂密碼最小長度、密碼複雜度及密碼最長使用期限。(二)辦理弱點掃描及滲透測試作業，對所發現中風險及低風險等級弱點，有未評估其相關風險或安裝修補程式者及弱點掃描範圍不足等情事。(三)辦理事聯網設備之安全管理作業，有未更新預設密碼、未關閉不必要之網路連線及服務及尚未對未具備安全性更新機制之物聯網設備，建立補償性管控機制等情事。(四)對行動應用程式(APP)所需權限之必要性及合理性，未建立審核機制。(五)啟動行動應用程式 APP 時偵測行動裝置疑似遭破解未提示使用者注意風險。上述核已違反證券商管理規則第 2 條第 2 項規定。111 年 6 月 29 日金管證券字第 11003776501 號函核處糾正、金管證券罰字第 1100377650 號裁處書罰鍰新台幣 48 萬元整及公司自有資本適足比率之作業風險約當金額應增加計提 0.5 倍。</p>	<p>111 年 8 月 2 日檢送相關資料呈交易所審查，交易所於 8 月 11 日回覆本公司完成改善情形，得自次月起恢復原作業風險計提比率。</p>	<p>已完成改善。</p>

應加強事項	改善措施	預定完成改善時間
<p>【子公司樂天國際商業銀行】</p> <p>一、111年10月1日本行發生重大偶發事件「網路銀行及行動銀行登入後無法正常顯示資料」</p>	<ol style="list-style-type: none"> <li>1. 納入系統自動監控及預警機制。</li> <li>2. 修正造成異常之程式物件。</li> <li>3. 納入年度異地備援演練項目。</li> <li>4. 納入風險控制自我評估之項目。</li> <li>5. 納入自行查核專項作業。</li> </ol>	<ol style="list-style-type: none"> <li>1. 已於111年10月完成改善。</li> <li>2. 已於111年11月完成改善。</li> <li>3. 已於111年11月完成改善。</li> <li>4. 已於112年01月完成改善。</li> <li>5. 已於111年11月完成改善。</li> </ol>
<p>二、辦理可攜式儲存媒體存取係留存攜出檔案紀錄覆核機制與寄送電子郵件至外部網域電子郵件地址覆核機制有欠妥善。</p>	<ol style="list-style-type: none"> <li>1. 檢視111年6、7月DLP USB使用紀錄，如有USB使用紀錄，將由資訊安全部主管發送給各部門主管進行覆核程序。並將USB使用規定與覆核程序納入主管會議議程及全行教育訓練中。</li> <li>2. 已於111.07.06變更USB預設設定為停用，未授權人員無法使用。</li> </ol>	<ol style="list-style-type: none"> <li>1. 已於111年08月完成改善。</li> <li>2. 已於111年08月完成改善。</li> </ol>
<p>三、辦理Data Loss Prevention系統(下稱DLP)持有放行電子郵件權限帳號可自行核准自己寄出遭DLP攔阻的電子郵件。辦理DLP系統測試個資防護及附件檔案Policy設定未妥，存有例外狀況未被偵測或記錄之情形。 【111.12.13/ 檢局(銀)字第1110509229號函】</p>	<ol style="list-style-type: none"> <li>1. 資訊安全部將再次全面比對DLP系統各帳號、角色、資安事端設定與寄件者資安事端基本資料，以確保遭DLP攔阻之電子郵件無法由同一人核准放行。</li> <li>2. 資訊安全部將視全行營業情況判斷評估制訂電子郵件使用規範。</li> <li>3. 本單位將DLP相關管控機制(電子郵件、可攜式儲存媒體…等)納入自行查核計畫並辦理查核。</li> <li>4. 資訊安全部將全面檢視本行個人資料保護系統(DLP)</li> </ol>	<ol style="list-style-type: none"> <li>1. 已於111年12月已完成設定並於112年1月已完成測試。</li> <li>2. 目前已有電子郵件控管措施，以及相關申請與執行作業，部分規範訂於資訊存取控制管理作業程序內，將研擬制訂電子郵件使用規範已強化電子郵件相關安全控管，預計112年3月完成。</li> <li>3. 已於111.12.22完成112年度自行查核計畫，並將DLP相關管控機制納入自行查核項目中。</li> <li>4. 已於111.12.15完成，並與廠商確認</li> </ol>

應加強事項	改善措施	預定完成改善時間
	偵測規則，並與廠商分析系統相關限制與現實差異，再測試各規則有效性，且納入自行查核計畫，至少每年 2 次一般自行查核定期辦理。	DLP 偵測規則之正確性，並於 111.12.22 完成 112 年度自行查核計畫，將 DLP 相關管控機制納入自行查核項目中。