柒、電腦作業與資訊提供：CC-10000

目　　錄

一、 資訊處理部門之功能及職責劃分：CC-10100

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
CC-10100	資訊處理部門之功能及職責劃分	一、作業程序： (一). 資訊單位之組織及功能 1. 資訊單位為非隸屬使用者單位之獨立單位，統籌全公司資訊管理有關事項，負責公司資訊系統之規劃、推行、維護、管理及支援作業。 2. 資訊系統之資料來源及使用則為各使用單位，資訊單位人員不負責資訊系統之資料來源、核准及使用。 3. 資訊服務單位人員及系統使用者權限定義： (1) 系統管理員（經理及職務代理人）：檢視系統環境，確認程式於正式工作區之使用狀況。 (2) 程式設計師：負責程式開發及維護。 (3) 系統使用者：將資料輸入資訊系統、查詢及表單列印功能。 (二). 資訊單位人員工作執掌說明 1. 資訊作業制度之訂定與維護。 2. 統籌作業系統及應用系統之規劃、開發事宜。 3. 使用者帳號密碼管理作業。 4. 使用者權限設定作業。 5. 資料輸出／入管制作業。 6. 系統復原之規劃與執行。 7. 電腦軟／硬體設備之管理作業。 8. 系統監控作業。 9. 事件通報及處理作業。	法令規章： 1.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 10 條 2.台期（稽）字第 09300034210 號 3.台財證字第 0930115938 號函 使用表單： 無

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
		10.委外廠商評估、聯繫及監控作業。 (三). 使用單位權責 1. 確保業務作業流程與電腦處理流程一致。 2. 應對實際作業環境之資料負全責，即正確操作電腦系統以確保資料之正確性及完整性。 3. 提出電腦化需求。 4. 對上述需求提供進一步資料及詳細說明。 5. 準備相關測試個案及測試資料。 6. 進行系統測試。 7. 配合修改與電腦化後之相關作業控制制度、控管重點。 8. 提出系統維護需求。 9. 協助評估各項電腦系統作業之績效。 10.監控委外廠商所提供之服務。 (四). 資訊單位人員之聘用與教育訓練 1. 資訊人員之聘用、工作及任務指派應依其職務需求，審慎評估人員之適任性。 2. 若資訊人員能力或經驗不足時，應以內部訓練方式或尋求外部訓練課程培訓資訊人員，以加強其專業能力。 二、控制重點： (一). 資訊單位之組織及功能 1. 資訊處理單位之組織功能應基於職能適當分工，訂定權責分工及職務說明，並	

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
		規劃適當之職務代理人。 2. 資訊處理單位內各單位職掌設計，應避免不同單位權責重疊現象。 (二). 資訊單位人員工作執掌說明 1. 資訊處理單位與業務單位之權責應明確劃分。 2. 資訊作業人員應填具保密切結書；離職時應取消其識別碼，並收繳其通行證、卡及相關證件。 (三). 資訊單位人員之聘用與教育訓練 1. 應定期（每年至少一次）對全公司員工辦理資訊安全宣導講習（例如：防毒、資料備份、使用合法軟體及電子郵件使用規定等），並留存紀錄。	

二、 系統開發及程式修改之控制作業：CC-10200

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
CC-10200	系統開發及程式修改之控制作業	一、作業程序： (一). 系統開發控制作業 1. 系統開發由使用單位填寫系統開發/程式修改申請單提出需求。 2. 系統開發申請需經相關權責主管核准。 3. 經資訊單位評估使用單位實際作業需求，確認可行且有開發新系統必要時，由資訊單位以簽呈方式提出，於簽呈中闡述系統開發之初步評估結果。 4. 依核決權限表之規定送請相關主管會簽。 5. 判定是否由資訊單位自行開發或外購軟體由委外廠商執行系統開發作業。 (1) 新系統開發應將設備容量規格考慮在內，以避免容量不足而導致電腦當機或系統無法執行之情形發生。 (2) 經權責主管核准以外購方式或委外開發取得之系統，由資訊單位視需要與使用單位討論，確認實際需求後作成系統規格，交由採購單位依公司之採購及付款循環之相關作業辦理公開招標或直接進行採購。 (3) 資訊單位應評估使用單位實際作業需求，確認可行且有開發新系統必要，簽呈送請相關主管會簽，判定是否執行系統開發作業。 6. 成立專案小組自行開發 (1) 經評估規模較小或資訊單位內部人力資源足以勝任之系統開發需求，簽呈由權責主管核准後，由資訊單位自行編成開發專案小組進行開發。 (2) 由系統開發人員與申請單位進行討論瞭解細部需求，除應留存各階段會議記錄外，並須編製系統規格需求說明書由申請單位確認。 7. 程式設計人員於系統開發環境中執行系統開發作業，並對其程式進行自我測	**法令規章：** 1.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 10 條 2.台期稽字第 09600018150 號 3.金管證期七字第 0950160204 號函 4.台期（稽）字第 09300034210 號 5.台財證字第 0930115938 號函 **使用表單：** 1.系統開發/程式修改申請單

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
		試，確定程式邏輯性之合理及其運用、驗證系統功能是否符合申請單位之需求規格，且於程式中加上註解，並保留相關測試文件。 8. 系統開發完成由資訊單位會同申請單位於測試環境進行測試，應將測試結果記錄於系統開發/程式修改申請單，並檢附相關報表及畫面。若測試失敗，使用單位及專案開發小組應進行討論，並由專案開發小組進行評估及更正。 9. 系統經申請單位驗收後執行系統上線作業，由系統負責人進行上線變更申請程序並填寫系統上線申請單。 10. 系統上線申請單需經資訊單位直屬主管簽核並確認預定上線日期。 11. 由經資訊單位直屬主管授權之執行人員負責將系統上線至系統正式環境，並建立軟體版本更新之控制機制。 12. 上線完成後，將系統開發/程式修改申請單、系統規格需求說明書及系統上線申請單交由資訊單位應用系統管理人員確認編號歸檔後留存。 13. 資訊系統委外開發時，應於事前審慎評估可能的潛在安全風險，並與廠商簽訂適當的資訊安全協定，以課予相關的安全管理責任。 14. 合約內容包含委外時程表、完成時間、維護方式、付款方式、版權、軟硬體需求、交付文件、相關賠償方式及規定所有必要之安全要求等，委外作業合約內容應完備嚴密。 15. 應於委外資訊系統規劃之需求分析階段，即將安全需求納入；新發展的資訊系統或是現有系統功能之強化，應明定資訊安全需求，並將安全需求納入系統功能。 16. 委外作業之開發、設計、程式撰寫、測試及驗收等各階段須依合約規定程序進	2. 系統規格需求說明書 3. 系統上線申請單

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
		行，並備妥各階段之相關文件。 (1) 委外人員進行系統開發、測試時，如需存取公司內部資料，風險應予評鑑，並由資訊人員實施適當安全控管措施。 17.委外開發系統程式撰寫完成後，委外廠商需自行測試無誤後再交付資訊單位主管，由資訊組人員協同申請單位共同測試，確定程式邏輯性之合理及其運用、驗證系統功能是否符合申請單位之需求規格。 18.委外系統上線作業前，應確實執行適當的測試計畫，以驗證系統功能符合既定的安全標準。 (二). 程式修改控制作業 1. 已上線之系統，若有程式修改之需求，應由使用單位填寫系統開發/程式修改申請單提出需求。 (1) 變更作業之控制程序，應確保系統安全控制程序不會被破壞，且任何的系統變更作業，皆應獲得資訊單位主管的同意。 (2) 使用單位若有緊急修護系統之需求時，仍須依規定由各級權責主管核准後方由資訊單位辦理。 (3) 為維護作業之正常運作，除非必要，應儘量避免不必要之修改。 (4) 修改程式應建立正式的變更控制程序，並嚴格執行，以降低可能的安全風險。 2. 資訊單位評估程式修改需求之可行性與必要性，決定由資訊單位自行修改或需由委外廠商修改。 (1) 若決議由委外廠商修改者，應遵循系統開發之委外作業，由委外廠商執行程式修改作業，並於各階段提供及保存相關表單及測試文件。	

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
		3. 程式設計人員於修改程式前，須與申請單位進行討論瞭解細部需求，依申請單位之需求提出系統規格需求說明書，並留存各階段會議記錄。 4. 系統規格需求說明書需由申請單位確認。 5. 與申請單位確認需求後，程式設計人員於系統開發環境中執行程式修改，並對其程式進行自我測試，確定程式邏輯性之合理及其運用、驗證系統功能是否符合申請單位之需求規格，且於修改之程式加上註解，並保留相關測試文件。 6. 程式修改完成由資訊單位會同申請單位於測試環境進行測試，應將測試結果記錄於系統開發/程式修改申請單，並檢附相關報表及畫面。 7. 系統經申請單位驗收後執行系統上線作業，由系統負責人進行上線變更申請程序並填寫系統上線申請單。 8. 系統上線申請單經資訊單位主管簽核並確認預定上線日期。 9. 由經資訊單位主管授權之執行人員負責將系統上線至系統正式環境，並建立軟體更新的版本控制機制。 10. 上線完成後，將系統開發/程式修改申請單、系統規格需求說明書及系統上線申請單交由資訊組應用系統管理組人員確認編號歸檔後留存。 **二、控制重點：** (一). 系統開發控制作業 1. 資訊單位應評估使用單位實際作業需求，確認可行且有開發新系統必要，簽呈送請相關主管會簽，判定是否執行系統開發作業。 2. 資訊單位辦理委外開發之採購作業時，應根據使用者需求邀集相關單位共同規	

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
		劃解決方案，實際查詢廠商的成功案例，評選有能力按需求完成系統開發工作的最佳廠商。 3. 合約內容包含委外時程表、完成時間、維護方式、付款方式、版權、軟硬體需求、交付文件、相關賠償方式及規定所有必要之安全要求等，委外作業合約內容應完備嚴密。資訊單位人員應根據合約內容控管該委外案件之執行。 (二). 程式修改控制作業 1. 資訊單位權責主管應核准系統開發/程式修改申請單，以確認程式修改需求係經相關權責人員充分考量程式變更的必要性及其風險。 2. 系統開發人員應編製系統規格需求說明書，與使用單位進行討論瞭解細部需求，除應留存各階段會議紀錄外，並須由使用單位確認。 3. 資訊人員應建置有獨立之開發及測試環境，以維護正式環境之資料。系統開發及程式修改作業皆應於開發及測試環境執行。 4. 資訊單位應會同申請單位於測試環境測試開發或修改完成之系統或程式，將測試結果記錄於系統開發/程式修改申請單，並檢附相關報表及畫面。 5. 系統負責人進行上線變更申請程序並填寫系統上線申請單，經資訊單位主管簽核並確認預定上線日期，由經資訊單位主管授權之執行人員負責將系統上線至系統正式環境。 6. 系統上線至系統正式環境，資訊人員應建立軟體更新的版本控制機制。 7. 上線完成後，資訊單位應用系統管理組人員應將系統開發/程式修改申請單、系統規格需求說明書及系統上線申請單編號歸檔後留存。	

三、 編製系統文書之控制作業：CC-10300

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
CC-10300	編製系統文書之控制作業	一、作業程序： (一). 新資訊系統之開發，技術部系統管理人員或委外廠商應至少編寫系統文件，包含：系統規格書、系統文件、使用者操作說明書、系統測試記錄、驗收文件等。 (二). 資訊單位系統管理人員編寫、維護系統程式時，應於程式中適當註解，並依程式異動內容，適時修改相關系統文件。 (三). 資訊系統於開發、維護完成後，資訊單位人員得協助使用單位編製作業手冊，以做為日後使用者操作之標準。 (四). 各項系統文件與使用手冊，應設專人保管，避免未授權之存取；保管人員離職時，主管應指派交接之保管人員。 (五). 系統文書之出借或發送，應填寫電腦軟體／書籍借用記錄表經資訊單位之權責主管允許並授權後，由保管人員負責執行。 (六). 若確定舊版本之系統文件、使用手冊已無須再使用，保管人應於資訊單位主管核准後將其報廢。 (七). 自行開發系統軟體，或購買套裝軟體程式，資訊單位均應編製或轉交使用者操作說明書予使用單位；其他之系統文件等則統一由資訊單位專責人員保管，若有借閱需求時則需填寫電腦軟體／書籍借用記錄表。 二、控制重點： (一). 新資訊系統之開發，資訊單位人員或委外廠商應編寫完整之系統文件，包含：系統規格書、系統文件、使用者操作說明書、系統測試記錄、驗收文件等。 (二). 資訊單位人員編寫、維護系統程式時，應於程式中適當註解，並依程式異動內容，	**法令規章：** 1. 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 10 條 2. 台期（稽）字第 09300034210 號 3. 台財證字第 0930115938 號函 **使用表單：** 1. 系統文件 2. 電腦軟體／書籍借用記錄表 3. 系統規格書 4. 使用者操作說明書 5. 系統測試紀錄

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
		適時修改與更新相關系統文件，並記錄更新人員、範圍、時間以及版本，資訊單位權責主管應定期檢視系統文書之編製與管理作業。 (三). 各項系統文件與使用手冊，應設專人保管，避免未授權之存取；系統文書之出借或發送，應填寫電腦軟體／書籍借用記錄表並經資訊單位之權責主管允許及授權後，由保管人員負責執行。 (四). 保管人員離職時，主管應指派交接之保管人員。 (五). 若確定舊版本之系統文件、使用手冊已無須再使用，保管人應於資訊單位主管核准後將其報廢。	6.驗收文件

四、 程式及資料存取之控制作業：CC-10400

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
CC-10400	程式及資料存取之控制作業	一、作業程序： (一). 程式及資料之存取控制作業（含作業及應用系統） 1. 使用者帳號新增或權限異動，申請人員應以帳號密碼新增/異動申請單提出申請，經申請單位主管同意後，轉交資訊單位主管審核，指派相關資訊人員進行新增帳號密碼作業；完成後，應與申請人驗收確認後並將帳號密碼新增/異動申請單歸檔備查。 2. 使用者於離職前，或因職務調動需異動帳號時，應以離職/遷調程序單，通知資訊單位，並填寫帳號密碼新增/異動申請單交由資訊單位辦理帳號刪除事宜；完成後，資訊單位應將帳號密碼新增/異動申請單以連續編號歸檔備查。 3. 公司外部人員（包含維護廠商）使用之帳號不宜與公司內部一般使用者共用，並得以契約作為存取系統之規範；此類帳號之使用應妥善監控，並於非使用時期取消其存取權限。 4. 使用者帳號及權限應由相關主管與系統負責人，定期依使用者職責及職能分工原則覆核，並檢查及取消閒置帳號。 5. 若將設定權限之作業委外執行，應將上述相關控制要點訂定於合約中，並定期監控委外廠商之作業是否合於作業規範。 6. 若為公司內部網路系統、作業系統使用者權限之設定，應依其業務職責以及職能分工原則設定權限，每位系統使用者皆應擁有個別之使用者帳號，並使用密碼設定，以確保資料存取之安全。 7. 使用者帳號、密碼原則（包含錯誤登入次數、密碼最短長度、複雜性以及變更週期等），應依各系統之用途與功能加以設定。	法令規章： 1.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 10 條 2.台期（稽）字第 09300034210 號 3.台財證字第 0930115938 號函 **使用表單：** 1.帳號密碼新增/異動申請單 2.離職/遷調程序單 3.電腦工作日誌 4.資訊委外合約 5.稽核日誌

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
		8. 若為一般業務應用系統使用者權限之設定，應依其業務職責以及職能分工原則設定權限，並於新增/異動時，取得應用系統負責人核准，每位系統使用者皆應擁有個別之使用者帳號，並使用密碼設定，以確保資料存取之安全。 (二).主機資源控制作業 1. 重要之系統公用程式、工具及指令應依其使用者職權限制其存取權限，僅系統管理者帳號具執行權限，係由系統管理人員持用並於負責人員調、離職時列入移交項目。 2. 一般應用系統之使用者除執行應用系統外，應無存取系統主機公用程式、工具及指令權限。 3. 系統開發及程式撰寫人員對於上線系統之程式與資料檔案應無存取權限。 4. 系統主機應設置「電腦工作日誌」，供系統操作員記載系統作業之情況，並定期由主管覆核。 5. 電腦主機之作業系統、應用系統及資料庫管理系統中應設置稽核日誌，以記錄任何可能危害系統安全事件。 6. 使用者利用網路與外界單位進行電子資料之傳輸，應釐清相關人員責任，由資訊單位人員協助訂定正式協定，並針對機密性及敏感性資料設置保護措施；此外，資料傳輸前，需經資料所有之單位主管及資訊單位主管核准。 7. 主機若為委外保管或維護，應將上述相關控制要點訂定於合約中，並定期監控委外廠商之作業是否合於作業規範。 (三).密碼及權限管控作業 1. 對於公司之重要系統，應建立適當之密碼控管原則，包含錯誤登入次數、密碼最	6.委外合約

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
		短長度、複雜性以及變更週期等。 2. 使用者第一次使用系統時，應立即更新初始密碼後方可繼續作業。 3. 密碼應以亂碼方式儲存，使用者因忘記密碼無法登入系統時，應採取嚴格確認其身分及核發程序後，方可開放其使用系統。 4. 置於危險場所或登入系統風險等級極高之終端機，於閒置時應於一定時間後自動關機或登出，避免未經授權之存取。 5. 宜使用優質密碼設定（長度超過六個字元，且具有文數字及符號），並加強宣導定期更新使用者密碼以不超過三個月為宜。 6. 檢查公司現有之網站、伺服器、網路芳鄰、路由器、交換器、作業系統及資料庫等軟硬體設備應設定使用密碼，且避免使用預設（如 administrator、root 、sa）或簡易（如 1234）之帳號密碼及未設管理者存取權限。 **二、控制重點：** (一).程式及資料之存取控制作業（含作業及應用系統） 1. 使用者權限之設定，應依其業務職責以及職能分工原則設定權限，每位系統使用者皆應擁有個別之使用者帳號，並使用密碼設定，以確保程式及資料存取之安全。 2. 授權使用者存取系統資源前，須依系統別填寫帳號密碼新增/異動申請單，經由申請單位主管核准後始予開放。 (二).主機資源控制作業 1. 機房系統作業之執行應由專人負責，於事前經系統負責人核准並由主管覆核。 2. 置於危險場所或登入系統風險等級極高之終端機，於閒置時應於一定時間後自動	

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
		關機或登出，避免未經授權之存取。 3. 重要之系統公用程式、工具及指令應依其使用者職權限制其存取權限，僅系統管理者帳號具執行權限，係由系統管理人員持用並於負責人員調、離職時列入移交項目。 4. 一般應用系統之使用者除執行應用系統外，應無存取系統主機公用程式、工具及指令權限。 5. 系統開發及程式撰寫人員對於上線系統之程式與資料檔案應無存取權限。 6. 系統主機應設置電腦工作日誌，供系統操作員記載系統作業之情狀，並定期由主管覆核。 7. 電腦主機之作業系統、應用系統及資料庫管理系統中應設置稽核日誌，以記錄任何可能危害系統安全事件。 8. 公司外部人員（包含維護廠商）之帳號應妥善監控，並於非使用時期取消其存取權限。 (三).密碼及權限管控作業 1. 對於公司之重要系統，應建立適當之密碼控管原則，包含錯誤登入次數、密碼最短長度、複雜性以及變更週期等。 2. 使用者第一次使用系統時，應立即更新初始密碼後方可繼續作業。 3. 密碼應以亂碼方式儲存，對因忘記密碼而無法登入系統之使用者重新申請核發密碼時，應採取嚴格確認其身分及核發程序後，方可開放其使用系統。 4. 使用者於離職前，或因職務調動需異動帳號時，應以帳號密碼新增/異動申請單通知資訊組人員辦理帳號刪除事宜，並將該帳號密碼新增/異動申請單編號歸檔備	

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
		查。 5. 使用者帳號及權限應由相關主管與系統負責人，定期依使用者職責及職能分工原則覆核，並檢查及取消閒置帳號。	

五、 資料輸出入之控制作業：CC-10500

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
CC-10500	資料輸出入之控制作業	一、作業程序： (一).資料輸入管理 1. 資料之輸入及修改需經適當之覆核及授權。 2. 使用單位應依照需輸入資料之性質，設計適合之電腦系統資料異動申請單；若作業流程不適合產生異動單據，使用單位應適時保存原始相關資料。 3. 原始相關資料及憑證，應由專人負責保管，並存於安全處所。 4. 各項輸入電腦系統資料異動申請單應配合原始憑證編製序號，資料輸入控制應配合序號控管，遇有漏號、單據遺失，應立即追蹤，以確保資料之完整性。 5. 資料輸入完成後，應將異動單據及原始憑證等相關資料，送交各相關單位存查。 6. 為確保資料輸入正確，在輸入之資料轉換為電腦可閱讀之形式時，須嚴加控制，自動化控制須與人工程序適當併用，其人工控制方法包括： (1)資料檢誤。 (2)資料驗證。 (3)文件數量之核對。 (4)批次控制之核對。 7. 系統應建立作業流程以確保輸入之資料係經過驗證和編輯且盡可能符合交易實質內容，程式化之輸入格式可確保資料係依正確之格式輸入正確之欄位，利用電腦自動化控制包括： (1)序號之核對。 (2)極限值之核對。 (3)範圍之核對。	**法令規章：** 1.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 10 條 2.台期（稽）字第 09300034210 號 3.台財證字第 0930115938 號函 **使用表單：** 1.電腦系統資料異動申請單 2.分發清單及簽收紀錄 3.審計軌跡報告

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
		(4)有效性之核對。 (5)合理性之核對。 (6)檢查號碼之核對。 (7)完整性之核對。 (8)重複性之核對。 (9)邏輯關係之核對。 8. 系統間資料拋轉之輸入，應設計資料完整性、正確性之自動檢查功能；若系統檢查發現錯誤，應設計自動產生相關異常警訊或報表，並由專人負責追蹤。 (二).資料輸出管理 1. 僅有經適當授權之人員始可進行資料或報表之輸出或列印作業（分為螢幕上列印、印表機列印、轉成檔案、透過網路傳送等方式）。 2. 輸出資料應分發予適當授權之人，機密性、敏感性之資料輸出設計有適當管控程序，由專人負責輸出、分送、保管，並建立分發清單及簽收紀錄。 3. 系統應產生重要資料鍵入、主檔變更及系統自動產生交易之審計軌跡報告（如交易明細報告），以供核對及調節原始輸入憑證。 4. 輸出資料若以磁性媒體保存，應定期檢查以確定必要時能以報表方式印出。 5. 各單位依照各自輸出資料之性質，訂定保存方式、保存期間、銷毀方式等適當之規範。 (三).更正例外或異常輸出項目 1. 輸出資料須與輸入資料相符，與原始憑證等相關資料核對，應定期利用人工或系統相互勾稽，包括比對筆數、序號及總和等，以確保所儲存資訊之處理程序正確	

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
		且合乎實際情況；若發現錯誤，應會同相關人員查明原因，須填寫「電腦系統資料異動申請單」報請權責主管核准修正後，更正資料並將申請單與相關文件妥善保存備查。 2. 更正例外或異常項目之再輸入應調節至原例外或異常項目。 **二、控制重點：** (一).資料輸入管理 1. 資料之輸入及修改需經授權，並於輸入前查驗資料輸入之正確性，依相關之原始資料輸入。 2. 原始相關資料及憑證，由各單位專人負責保管，並存於安全處所。 3. 各項輸入資料須配合原始相關資料及憑證編製序號，資料輸入控制應配合序號控管，遇有漏號或單據遺失，應立即追蹤，以確保資料之完整性。 4. 在輸入之資料轉換為電腦可閱讀之形式時，須嚴加控制，須適當併用自動化與人工之控制程序，以確保資料輸入正確。 5. 系統應建立作業流程以確保輸入之資料係經過驗證和編輯且盡可能符合交易實質內容，程式化之輸入格式可確保資料係依正確之格式輸入正確之欄位。 (二).資料輸出管理 1. 輸出資料應分發予適當授權之人，機密性及敏感性之資料輸出設計有適當管控程序，由專人負責輸出、分送及保管，並建立分發清單及簽收記錄。 2. 系統應產生重要資料鍵入、主檔變更及系統自動產生交易之審計軌跡報告（如交易明細報告），以供核對及調節原始輸入憑證。	

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
		(三).更正例外或異常輸出項目： 1. 發現資料錯誤應會同相關人員查明原因，須填寫「電腦系統資料異動申請單」報請權責主管核准修正後，更正資料並將申請單與相關文件妥善保存備查。 2. 更正例外或異常項目之再輸入應調節至原例外或異常項目。	

六、 資料處理之控制作業：CC-10600

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
CC-10600	資料處理之控制作業	一、作業程序： (一).電腦主機作業 1. 負責資料處理之電腦主機及相關設備於保固期到期後應簽訂維護合約。 2. 若出現異常情況時，先行採取排除異常之應變措施。如無法自行排除時，應立即通知維護廠商派員前來處理，並留下服務紀錄服務聯絡單。 3. 機器運轉中如發生異常狀況，應判斷是否會影響進行中之工作，如需立即停機時，立刻通知使用者暫停作業，並隨即進行修復，待修復完畢並運轉正常後，再行通知使用者重新使用。 4. 機器故障損及資料時，資訊人員應先進行資料回復作業並通知使用者自行查驗，避免影響日後資料之正確性及完整性。 5. 凡與主機相關之重大異常狀況需紀錄於機房工作記錄表，並說明異常狀況及處理方式以便於日後追蹤。 6. 資訊單位針對使用者操作說明書，將會定期檢視並更新，以確保適用於目前作業狀況。 (二).應用系統軟體 1. 系統內部作業應建立驗證資料正確性之作業程序，避免正確輸入至應用系統之資料因系統處理錯誤而產出不正確之結果。 2. 系統應針對重要資料、重要批次作業，分別設計產生自動檢核序號、處理參數的複查機制之控制。 3. 人工或系統之處理控制應能確定交易業已記錄於適當之會計期間。 4. 應用系統於處理資料時應留有資料處理異動記錄，以保持適當而完整之審核軌	法令規章： 1.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 10 條 2.台期（稽）字第 09300034210 號 3.台財證字第 0930115938 號函 **使用表單：** 1.服務聯絡單 2.機房工作紀錄表 3.維護合約 4.使用者操作說明書

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
		跡，俾供後續查核之用。 5. 系統應提供使用者作業處理中各項錯誤或作業失敗之訊息，並產生錯誤報表以利追蹤更正。 6. 使用者有變更或更新資料處理程序時，應先提出申請並經過相關權責主管核准。 7. 資訊人員應及時追蹤並更正例外或異常之訊息，並由專人覆核、更正並定期追蹤處理情形。 8. 資料媒體內外應貼有標籤，標籤上註明日期及檔案名稱。 9. 進行資料轉換前須先擬定資料轉換計畫，並進行資料備份，並比較資料轉換前後新舊系統之執行結果是否正確。 10. 如有運用外界電子資料處理中心以處理電子資料時，對於資料往返傳輸應具有上述之相關控製作業，以確保資料之完整性及安全性。 11. 資訊單位針對使用者操作說明書，將會定期檢視並更新，以確保適用於目前作業狀況。 二、控制重點： (一).電腦主機作業 1. 資料處理之相關資訊設備應由資訊人員於購入時與廠商簽訂維護合約。 2. 機器運轉中如發生異常狀況，應判斷是否會影響進行中之工作，如需立即停機時，應立刻通知使用者暫停作業，由資訊人員依據故障之訊息作初步處理，待修復完畢並運轉正常後，再行通知使用者重新使用，並將處理情形記錄於機房工作紀錄表中。如無法自行排除時，應立即通知維護廠商派員前來處理，並留下服務	

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
		紀錄。 (二).應用系統軟體 1. 應用系統應設計適當之功能、控制流程，以確保處理資料之完整性、正確性。 2. 系統應針對重要資料、重要批次作業，分別設計產生自動檢核序號、處理參數的複查機制之控制。 3. 應用系統之交易紀錄應登錄於正確之會計期間。 4. 系統應提供使用者作業處理中各項錯誤或作業失敗之訊息，並產生錯誤報表以利追蹤更正。 5. 資訊人員應及時追蹤並更正例外或異常之訊息，並由專人覆核、更正並定期追蹤處理情形。	

七、 檔案及設備之安全控制作業：CC-10700

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
CC-10700	檔案及設備之安全控制作業	一、作業程序： (一).資料檔案之安全控制 1. 應用程式及資料檔，應妥善備份；資料應依其重要性，進行日、週、月、年等不同週期之備份作業，並設定適當之存放期限，針對應永久保存之資料則應另行使用適當媒體儲存。 2. 備份之資料媒體需適當記錄於備份記錄表中，並應於備份儲存媒體貼上內外標籤以利辨識備份內容。 3. 備份資料應定期執行測試作業，適當記錄於備份資料測試紀錄表，以確保備份資料之可用性。 4. 備份資料應異地存放，媒體存放處所環境應合於電腦機房安全標準，並適當記錄於備份磁帶異地存放紀錄表。 5. 資料及文件應就其重要性妥適區分安全等級，並透過系統設定或文件管理達到安全控管之目的。 6. 系統使用單位對於檔案之使用應依照程式及資料存取控制作業辦理。 7. 為避免檔案資料或硬體設備遭病毒毀損，應建立系統自動偵測病毒之機制，並要求所有人員定期更新病毒碼。 (二).電腦設備之安全控制 1. 資訊設備於購入時，資訊單位應會同使用單位驗收，並登記於資訊設備清單列冊管理；移轉資訊設備則應填具設備移轉記錄單，經移出與移入單位經辦人員與主管簽核後送交資訊組存查。 2. 電腦設備及其存放之資料於報廢時應填具資訊設備報廢申請單，申請進行報廢程	法令規章： 1.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 10 條 2.台期（稽）字第 09300034210 號 3.台財證字第 0930115938 號函 **使用表單：** 1.備份記錄表 2.備份資料測試紀錄表 3.備份磁帶異地存放紀錄表 4.資訊設備清單 5.設備移轉記錄

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
		序，以避免機密資料流失。 3.為避免報廢電腦硬碟機密及敏感資料外洩，應訂定電腦設備報廢作業程序；電腦設備報廢前應將硬碟內機密性、敏感性資　料及授權軟體予以移除，實施安全性覆寫或實體破壞，確保報廢之電腦硬碟及儲存媒體儲存之資料不可還原，並留存報廢紀錄，若委託第三者銷毀時，應簽訂保密合約。 4.行動式電腦設備之攜出攜入則應填寫設備借用記錄表。 (三).通訊設備管理 1. 通信網路應加強安全防禦，以防止資料遭截取，必要時應採取加密措施。 2. 重要網站及伺服器系統，應以防火牆或同等級之防禦措施做區隔，以降低整體風險。 3. 防火牆應有專人管理，其設定應經權責主管之核准，並應以適當方式保存防火牆進出紀錄。 4. 使用外部設施管理服務前，應執行適當之風險評估，商議適當之控制措施，與廠商協議後併入合約中。 5. 若設備線路發生故障時，資訊單位應派員立即檢查，以瞭解線路故障原因，必要時通知廠商或電信單位進行維修。 (四).電腦機房之管制 1. 電腦機房應設有適當之門禁管制（例如：門鎖、刷卡或指紋機）；資訊組人員對非作業人員進出電腦機房，應請其登記於電腦機房進出管制登記表，並於資訊組人員陪同下方可進入，嚴禁未經許可人員擅入機房。 2. 資訊單位主管應定期覆核授權進出機房人員，並檢視門禁管制記錄。	單 6. 資訊設備報廢申請單 7. 設備借用記錄表 8. 電腦機房進出管制登記表

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
		3. 各項資訊設備依預定使用目的存放於電腦機房內，不應放置其他易燃或危險物品。 4. 機房內應設置獨立之空調設備以維持穩定正常之溫濕度狀態。 5. 機房內應設置高架地板，或將設備固定於合乎安全標準之架上。 6. 需備有自動火警偵測及緊急照明設備，以警示火災訊息，滅火器應置於明顯易取得之位置。 7. 應安裝自動電壓穩定裝置，以維護設備安全及系統穩定性。重要設備應裝設不斷電系統（UPS）及電源供應器以避免作業因停電而中斷。 8. 滅火器及不斷電系統等機房防護設備，應定期檢查與維護，並測試其堪用性。 9. 電腦機房使用之空調、電源等相關設備，應有適當之備援對策。 二、控制重點： (一).資料檔案之安全控制 1. 應用程式及資料檔，依其重要性執行日、週、月、年等不同週期之備份作業。 2. 備份之資料媒體需適當記錄於備份紀錄表中，並應於備份儲存媒體貼上內外標籤以利辨識備份內容。 3. 備份資料應定期執行測試作業，以確保備份資料之可用性。 4. 備份資料應異地存放，媒體存放處所環境應合於電腦機房安全標準。 (二).電腦設備之安全控制 1. 應建立系統自動偵測病毒之機制，並要求所有人員定期更新病毒碼。 2. 購入資訊設備資訊組應會同使用單位驗收，並登記於資訊設備清單列冊管理。 3. 移轉資訊設備應填具設備移轉紀錄單，經移出與移入單位經辦人員與主管簽核後	

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
		送交資訊組存查。 4. 電腦設備及其存放之資料於報廢時應填具資訊設備報廢申請單，申請進行報廢程序，以避免機密資料流失。 5. 應訂定電腦設備報廢作業程序；電腦設備報廢前應將硬碟內機密性、敏感性資料及授權軟體予以移除，實施安全性覆寫或實體破壞，確保報廢之電腦硬碟及儲存媒體儲存之資料不可還原，並留存報廢紀錄，若委託第三者銷毀時，應簽訂保密合約。 6.行動式電腦設備之攜出攜入則應填寫設備借用紀錄表。 (三).通訊設備管理 1. 通信網路應加強安全防禦，以防止資料遭截取，必要時應採取加密措施。 2. 若設備線路發生故障時，資訊組應派員立即檢查，以瞭解線路故障原因，必要時通知廠商或電信單位進行維修。 (四).電腦機房之管制 1. 電腦機房應設有適當之門禁管制；資訊單位人員對非作業人員進出電腦機房，應請其登記於「電腦主機房進出管制登記表」，並於資訊組人員陪同下方可進入，嚴禁未經許可人員擅入機房。 2. 資訊單位主管應定期覆核授權進出機房人員，並檢視門禁管制紀錄。 3. 機房內應設置獨立之空調設備、高架地板、自動電壓穩定裝置、不斷電系統（UPS）、電源供應器、自動火警偵測及緊急照明設備等機房防護設備。 4. 滅火器及不斷電系統等機房防護設備，應定期檢查與維護，並測試其堪用性。 5.機房內不應放置其他易燃或危險物品。	

八、 硬體及系統軟體之購置、使用及維護之控制作業：CC-10800

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
CC-10800	硬體及系統軟體之購置、使用及維護之控制作業	一、作業程序： (一).電腦硬體及系統軟體之購置 1. 使用單位依業務需求，欲購置電腦硬體及系統軟體時，須填寫電腦軟/硬體設備申請單經主管覆核後送交資訊單位。經資訊單位評估相容性、擴充性、業務特性及成本效益後，開立符合需求之硬體設備，並經主管核准後，依「採購內部控制」執行請購作業。 2. 資訊硬體及系統軟體統一由資訊單位負責請購，由資訊單位人員填寫請購單，經資訊單位主管覆核後送交採購單位進行採購，驗收作業則統一由資訊單位執行，確認驗收完成交付使用單位保管使用，並登記於資訊設備清單列冊管理。 3. 為確保尊重智慧財產權，落實使用合法版權軟體及兼顧公司軟體採購成本，應依據「電腦使用者軟、硬體使用辦法」執行軟體之增置、管理、經管、減損等作業。 4. 若為委外開發之系統，其版權與相關製作之文件應屬於公司資產，於開發完成後交由資訊單位歸檔。 (二).電腦硬體及系統軟體之使用 1. 使用單位對於電腦硬體及系統軟體之使用及維護應依照操作手冊之說明進行操作。 2. 使用者於應用系統使用完畢後必須離線或登出，個人電腦不使用時需關機或將螢幕上鎖。 3. 使用者借用資訊設備或系統軟體，應填寫設備借用紀錄表或電腦軟體／書籍借用紀錄表。 (三).軟、硬體設備維護	法令規章： 1.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 10 條 2.台期（稽）字第 09300034210 號 3.台財證字第 0930115938 號函 4.台期稽字第 09600018150 號 5.金管證期七字第 0950160204 號函 **使用表單：**

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
		1. 重要之系統主機與應用系統，若經資訊單位評估須由委外廠商提供維護服務者，應與委外廠商簽訂維護合約，並將資訊安全相關議題納入考量，訂定適當之資訊安全協定，規範委外廠商系統維護所接觸資料之安全管理。 2. 資訊單位各承辦人員應於合約到期前提出續約申請，經相關權責主管核准後進行採購作業。 3. 電腦設備維護如為委外處理者，委外廠商執行人員應留下服務紀錄交由資訊單位留存。 4. 主機系統維護工作，應避免停機並干擾使用者，儘可能安排在夜間、假日或無人使用狀態下進行停機作業之處理。 5. 一般事務性電腦設備於發生故障時，使用者應填寫電腦硬體設備故障送修申請單通知資訊單位派員維修，並記錄機器故障原因及維修狀況。 6. 經資訊單位人員確認硬體設備故障需送交廠商維修者，則應填寫服務聯絡單，經申請單位主管核准後由資訊單位辦理。 二、控制重點： (一).電腦硬體及系統軟體之購置 1. 使用單位須填寫電腦軟/硬體設備申請單經主管覆核後送交資訊單位。 2. 資訊單位評估相容性、擴充性、業務特性及成本效益後，開立符合需求之硬體設備。 3. 資訊單位人員填寫請購單，經資訊單位權責主管覆核後送交採購單位採購。 4. 由資訊單位執行驗收作業，確認驗收完成交付使用單位保管使用，並登記於資訊	1. 電腦軟/硬體設備申請單 2. 請購單 3. 資訊設備清單 4. 設備借用記錄表 5. 電腦軟體／書籍借用記錄表 6. 電腦硬體設備故障送修申請單 7. 服務聯絡單

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
		設備清單列冊管理。 5. 資訊軟、硬體設備及作業管理委外管理之辦理。應遵循內部控制制度之採購及付款循環之規定。 (二).電腦硬體及系統軟體之使用 1. 使用單位對於電腦硬體及系統軟體之使用及維護應依照操作手冊之說明進行操作。 (三).軟、硬體設備維護 1. 資訊單位人員應定期維護重要系統主機，若經資訊單位評估須由委外廠商提供維護服務者，應與委外廠商簽訂維護合約。 2. 資訊單位人員應於合約到期前提出續約申請，經相關權責主管核准後進行採購作業。 3. 與委外廠商簽訂維護合約，應訂定適當之資訊安全協定，規範委外廠商系統維護所接觸資料之安全管理。 4. 主機系統維護工作，應避免停機並干擾使用者，儘可能安排在夜間、假日或無人使用狀態下進行停機作業之處理。 5. 電腦軟硬體定期維護應留下紀錄。如維護作業由委外廠商執行應確認維護程序皆依照維護合約所述進行，並留下服務紀錄。 6. 一般事務性電腦設備於發生故障時，使用者應填寫電腦硬體設備故障送修申請單通知資訊單位派員維修，並記錄機器故障原因及維修狀況 7. 經資訊單位人員確認硬體設備故障需送交廠商維修者，則應填寫服務聯絡單，經申請單位主管核准後由資訊單位辦理。	

九、 系統復原計畫制度及測試程序之控制作業：CC-10900

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
CC-10900	系統復原計畫制度及測試程序之控制作業	一、作業程序： (一).系統復原計畫之規劃 1. 應建立跨單位之系統復原計劃，研訂及維護系統災害復原程序。 2. 研擬備援及回復計畫，其內容至少包括下列項目之說明： (1)資料庫、檔案及程式之備援及回復。 (2)電腦作業系統備援及回復。 (3)電腦設備備援及設備故障回復。 (4)通訊設備及線路之備援及回復。 (5)電力系統備援及回復。 3. 與業務單位人員研討於重大異常狀況發生時，根據下列時間點： (1)開盤前機器無法啟動。 (2)盤中交易期間機器停頓。 (3)收盤後資料未核對完成前系統發生異常情形。 (4)每日日結作業時系統發生異常情形。 考慮當時系統發生的作業需求型態、影響的業務層面及相關人員應採的應變措施，訂定人工配合的備援計畫。 4. 核定之備援及回復計畫，由下列人員執行： (1)非人工備援作業由資訊單位人員為之。 (2)人工備援作業由使用該應用系統之業務單位人員為之。 5. 重大異常狀況發生時，資訊單位人員立即檢視電腦系統無法正常運作原因，判定災害等級，影響業務範圍，估計回覆作業時間，衡量當時作業狀況，通知相關人	法令規章： 1.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 10 條 2.台期（稽）字第 09300034210 號 3.台財證字第 0930115938 號函 **使用表單：** 1.系統復原計畫 2.測試紀錄表

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
		員根據備援及回復計畫所應採取之配合措施。 6. 不管是電腦系統或是電力、空調、消防系統發生異常，事後相關人員確實檢討原因，並謀求改進與對應預防措施。 7. 所訂定之重大異常狀況系統復原計畫應定期模擬演練，以使相關人員熟悉重大異常狀況發生時，系統之應變措施及復原程序。 (二).系統復原計劃之測試及演練 1. 系統復原計畫可能因事前的假設不正確、規劃不周全或設備及人員的職務調整變更，而無法發揮預期的作用，應定期測試及演練，以確保計畫的有效性，並使相關人員確實瞭解計畫的最新狀態。 2. 應擬訂測試作業的時程，定期進行測試；測試計畫可以定期測試個別計畫的方式進行，以減少測試完整計畫的需求及頻率。 3. 測試與演練過程紀錄於測試紀錄表，於事後召開檢討會議，針對測試缺失謀求改進，並留存記錄，作為計畫更新之參考依據。 4. 若將復原計畫委外施行，應與委外廠商簽定合乎上述要點之合約，並定期監控委外廠商之作業是否合於作業規範。 (三).系統復原計劃之更新 1. 系統復原計畫應配合業務、組織、系統及人員的調整變更而定期更新，以發揮計畫投資的效益及確保計畫持續有效。 2. 更新系統復原計畫後應呈報主管核准，並將相關訊息通知相關人員。	

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
		二、控制重點： (一).系統復原計畫之規劃 1. 重要主機應制定有系統故障或緊急應變措施與辦法。 2. 系統復原計畫應涵括各層級負責人員工作事項。 3. 系統復原計畫中應列示公司中重要的業務及電腦系統及其相關復原程序。 4. 系統復原計畫中應列示復原之地點及備援之電腦設備、系統軟、硬體。 (二).系統復原計劃之測試及演練 1. 公司(期貨信託事業)之交易主機應有備援措施。 2. 系統復原計畫應安排定期演練，並於內部教育訓練中執行系統復原計畫之訓練及宣導。 3. 系統復原計畫應安排定期測試，以驗證計畫是否完整。 4. 系統復原計畫定期測試應邀請各相關單位參與，並於測試後驗證與檢討。 5. 系統復原計畫應有專人負責與相關單位進行檢討。 (三).系統復原計劃之更新 1. 系統復原計畫應定期更新問題偵測及控制技術、人員組織調整變動、人員聯絡資料變動、業務流程的變動或實務作業的變更等相關事項。 2. 系統復原計畫的更新應呈報主管核准，並將相關的訊息告知相關人員。	

十、 資通安全檢查之控制作業：CC-11000

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
CC-11000	資通安全檢查之控制作業	一、作業程序： (一).資訊安全政策 1. 公司應依據相關法令規定及公司業務需求，訂定資訊安全政策、資訊作業之安全水準。 2. 制訂資訊安全政策，應包括下列事項： (1)資訊安全之定義、資訊安全之目標及資訊安全之範圍等。 (2)資訊安全政策之解釋及說明，資訊安全之原則、標準以及員工應遵守之相關規定。 (3)推行資訊安全工作之組織、權責及分工。 (4)發生資訊安全事件之緊急通報程序、處理流程、相關規定及說明。。 3. 所訂定之資訊安全政策，應經管理階層核准，並應正式發布要求所有員工共同遵守。 4. 公司訂定之資訊安全政策應定期評估，確保資訊安全實務作業之有效性。 5. 公司每年應將前一年度資訊安全整體執行情形，由資訊安全長或負責資訊安全之最高主管與董事長、總經理、稽核主管聯名出具「證券暨期貨市場各服務事業建立內部控制制度處理準則」第二十四條規定之內部控制制度聲明書，於會計年度終了後三個月內提報董事會通過，並將該聲明書內容揭露於主管機關指定之申報網站。 (二).建立資訊安全組織 1. 公司應配置適當人力資源及設備負責資訊安全制度之規劃、監控及執行資訊安全管理作業，所稱配置適當人力資源之規定如下： (1)實收資本額達新臺幣二百億元以上之公司，應設置資訊安全專責單位，該單位應配置專責主管及至少三名專責人員，專門負責資訊安全相關工作或職務，不得兼辦資訊或其他與職務有利益衝突之業務。	法令規章： 1.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10條、第36條之2 2.台期（稽）字第09300034210號 3.台財證字第0930115938號函 4.台期（稽）字第09600018150號 5.金管證期七字第0950160204號函 使用表單：

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
		(2)實收資本額達一百億元以上，未達二百億元者，應配置資訊安全主管及至少三名資訊安全人員，除兼辦資訊職務外，不得兼辦其他與職務有利益衝突之業務；如已設置資訊安全專責單位者，得配置專責主管及二名專責人員，且專門負責資訊安全相關工作或職務，不得兼辦資訊或其他與職務有利益衝突之業務。 (3)實收資本額達四十億元以上，未達一百億元者，應配置資訊安全主管及至少二名資訊安全人員，除兼辦資訊職務外，不得兼辦其他與職務有利益衝突之業務。 (4)實收資本額未達四十億元者，應配置至少一名資訊安全人員，除兼辦資訊職務外，不得兼辦其他與職務有利益衝突之業務。 2. 公司應指定副總經理或高層主管人員，綜理資訊安全政策推動及資源調度事務，並得視需要，成立跨部門之「資訊安全推行小組」；如公司符合主管機關所訂一定條件者，應指定副總經理以上或職責相當之人兼任資訊安全長辦理上開業務。 3.公司應視資訊安全管理需要及所屬資安分級，指定專人或專責單位負責規劃與執行資訊安全工作，且資訊安全人員及主管每年應定期參加十五小時以上資訊安全專業課程訓練或職能訓練並通過評量。其他使用資訊系統之從業人員，每年應至少接受三小時以上資訊安全宣導課程。 4.公司資訊安全人力、能力及經驗，如有不足之處，得委請外界的學者專家或民間專業組織及團體，提供資訊安全顧問諮詢服務。 (三).人員安全與管理 1. 員工應依相關法令課予機密維護責任，並應填具保密切結書，以明責任。 2. 員工離職時應取消其識別碼，並收繳其通行證、卡及相關證件。 3. 應針對人員管理、業務及資訊等不同工作類別之需求，定期辦理資訊安全教育訓練	無

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
		及宣導，建立員工資訊安全認知，提升公司資訊安全水準。 4. 負責重要資訊系統之管理、維護、設計及操作之人員，應適當分工，分散權責，並視需要建立制衡機制，實施人員輪調，建立人力備援制度。 5. 應對員工的私人資訊設備作必要之安全控管，以確保系統、資料之穩定性及完整性。 6. 各級業務主管人員，應負責督導所屬員工之資訊作業安全，防範不法及不當行為。 (四).資產分類與控管 1. 應由相關權責單位統籌電腦軟硬體之分配運用及充分有效使用，並應製作所有與各資訊系統相關之重要資產清冊，並於添購或報廢時隨時更新。 2. 應建立資訊安全分級標準，包含系統文件、顯示螢幕、儲存媒體、電子訊息及檔案資料等。 3. 應制訂一套與組織採用之分類方式相符之資訊標示與處理流程。 4. 病毒偵測。 (五).內部稽核及其他 1. 執行稽查人員應通過稽核訓練。 2. 內部稽核人員依內部控制制度之電腦作業與資訊提供循環規定之週期訂定資訊安全內部稽查計畫，並確實執行該計畫。 3. 應稽查內部人員是否使用合法軟體。對於以使用人數為基礎的授權軟體是否確實履行使用人數限制。 4. 應建立軟體使用目錄並執行軟體異動登記。 5. 應指派專人負責有關個人資料保護法規、智慧財產權之蒐集、公告及實施。	

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
		二、控制重點： (一).資訊安全政策 1. 公司應依據相關法令規定及公司業務需求，訂定資訊安全政策。 2. 所訂定之資訊安全政策，應經管理階層核准，並正式發布要求所有員工共同遵守。 3. 訂定之資訊安全政策，應至少每年評估乙次，並留存相關紀錄。 4. 公司每年應將前一年度資訊安全整體執行情形，由資訊安全長或負責資訊安全之最高主管與董事長、總經理、稽核主管聯名出具「證券暨期貨市場各服務事業建立內部控制制度處理準則」第二十四條規定之內部控制制度聲明書，於會計年度終了後三個月內提報董事會通過，並將該聲明書內容揭露於主管機關指定之申報網站。 (二).建立資訊安全組織 1. 應指定副總經理或高層主管人員成立跨單位組織負責規劃、執行及推動資訊安全管理事項、風險評估、及安全分級。 2. 公司應視資訊安全管理需要及所屬資安分級，指定專人或專責單位負責規劃與執行資訊安全工作，且資訊安全專責人員及專責主管每年應定期參加十五小時以上資訊安全專業課程訓練或職能訓練並通過評量。其他使用資訊系統之從業人員，每年應至少接受三小時以上資訊安全宣導課程。 (三).人員安全與管理 1. 員工應填具保密切結書；離職時應取消其識別碼，並收繳其通行證、卡及相關證件。 2. 應依員工職務層級施予適當的資訊安全教育訓練，每年並達內部所定之訓練時數，並留存紀錄。 3. 應落實個人資訊設備之控管。	

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
		(四).資產分類與控管 1. 應製作所有與每一資訊系統相關重要資產清冊並隨時更新。 2. 應制訂一套與組織採用之分類方式相符之資訊標示與處理流程。 3. 應訂定資訊安全分級標準，並對各類資產做相對之控管。 (五).內部稽核及其他 1. 稽核人員應受過適當之稽核訓練。 2. 應依照內部控制制度之電腦作業與資訊提供循環排定內部稽核計畫，並按計畫執行查核。 3. 應建立完整之軟體使用清冊。 4. 內部稽核計畫應涵蓋合法軟體之應用及個人資料保護法等相關規定。	

十一、 向主管機關指定網站進行公開資訊申報控制作業：CC-11100

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
CC-11100	依規定向主管機關指定網站進行公開資訊申報者，其相關作業之控制作業	一、作業程序： (一).公司如屬公開發行公司者，應於內部控制制度納入「公開發行公司網路申報公開資訊應注意事項」，並據以辦理相關申報事宜。 (二).資訊單位應配合公開資訊申報作業提供負責申報單位所需之申報作業系統設備建置、網路連線、網路認證程序及系統維護等服務。 (三).財務單位設專人擔任申報作業總窗口，設置專用電腦一台，總窗口保管密碼，負責掌控所有應輸入之資訊依相關規範如期完成申報作業。 (四).公司依法令要求應申報之內容，由各相關單位分派負責人員定期準備需申報之書面資料，經單位主管覆核後簽送財務單位，於申報截止期限內執行上傳作業。 (五).資料申報方式可分為畫面申報、格式化檔案及非格式化檔案上傳 1. 畫面申報－輸入資料後，按下確定鍵，系統透過安控軟體認證檢驗身份。無誤後，即顯示申報成功之畫面。 2. 格式化檔案上傳程序： (1)申報資料上傳－選擇上傳檔名後，按下送出鍵進行檔案上傳及檢核。 (2)申報資料檢核結果查詢－完成檢核，則顯示檢核無誤。無法通過檢核，則條列式顯示紅色錯誤訊息。 (3)申報內容查詢及確認－查看上傳之尚未確認資料明細，印出網頁內容送交權責主管覆核，確認原始書面資料與網站上之資料相符後，按下確認鈕將該筆資料於公開資訊觀測站公告。 3. 非格式化檔案上傳－上傳檔案完成申報並出現檔案已完成上傳等成功訊息。在上	法令規章： 1.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 10 條 使用表單： 無

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
		傳並點選確認後若發現錯誤，在相關單位未審核前可自行刪除重傳，若審核後發現錯誤，則由相關單位退件，公司需重新傳送。 4. 使用代表公司憑證載具簽署之作業系統端若屬期貨信託事業應用系統者（例如：電子對帳單系統），留存電腦稽核紀錄（log），其保存年限比照各作業資料應保存年限。 (六).於所設網站上提供股市即時交易資訊，須經由與期交所簽約之資訊公司提供。 (七).電子憑證之申請與保管 1. 向主管機關規定之電子憑證核發機構提出申請，取得電子憑證金鑰，以維護申報資料之隱密與完整性及辨識資料傳輸來源。 2. 向相關主管機關提出申請，以取得網路應用系統申報登錄帳號及密碼。 3. 經由網際網路至申報系統下載新版安控軟體，安裝於欲用以申報之電腦設備上。 4. 電子憑證應視同本公司正式印鑑，並由負責公開資訊申報相關作業單位妥善保管該憑證及其密碼。負責上傳公開資訊之相關人員，應由權責單位主管審慎評估後授權以避免不當之資料存取。 5. 使用電子憑證ＩＣ卡、其他類型憑證晶片卡或其他憑證載具等代表公司簽署之作業（例如：期信基金資訊觀測站申報系統、公文電子交換系統等），該等憑證載具由專人負責保管並設簿登記，且應訂定相關帳號、密碼保管及使用程序，據以執行，並定期執行備份，避免磁片因日曬、受潮或磁碟機故障等因素損毀導致無法按時執行申報作業。 6. 電子憑證金鑰應確實於到期前申請展期，以免影響申報作業。 (八).密碼變更期限	

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
		1. 登入公開資訊觀測站之密碼應依主管機關規定之期限內定期變更之。 2. 初次取得之電子憑證金鑰應立即變更密碼，其後亦應定期變更之，所稱定期得於前條主管機關規定之期限內為之。 (九).公司定期或不定期稽核依個人資料保護法定義之個人資檔案管理情形。 (十).定期檢查網站內對外提供之資訊，對具機密性、敏感性之資訊內容，應立即移除。 (十一).個人資料檔案之資料，其更新、更正或註銷均應報經核准，並將更新、更正、註銷內容、作業人員及時間詳實記錄。 二、控制重點： (一).總窗口負責掌控所有應輸入之資訊依相關規範如期完成申報作業。 (二).權責主管應覆核申報之書面資料，經核對無誤後，方由總窗口執行資料確認。 (三).負責申報人員遇職務異動時，應清楚交接公開資訊申報應注意事項。 (四).應依「個人資料保護法」，妥善處理客戶資料。 (五).於所設網站上提供股市即時交易資訊，須經由與期交所簽約之資訊公司提供。 (六).使用電子憑證ＩＣ卡、其他類型憑證晶片卡或其他憑證載具等代表公司簽署之作業（例如：期信基金資訊觀測站申報系統、公文電子交換系統等），該等憑證載具應由專人負責保管並設簿登記，且應訂定相關帳號、密碼保管及使用程序，並據以執行，並定期執行備份。 (七).使用代表公司憑證載具簽署之作業系統端若屬期貨信託事業應用系統者（例如：電子對帳單系統），應留存電腦稽核紀錄（log），其保存年限比照各作業資料應保存年限。 (八).登入密碼應依主管機關規定之期限內定期變更之。	

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
		(九).初次取得之電子憑證金鑰應立即變更密碼，其後亦應定期變更之。 (十).電子憑證金鑰應確實於到期前申請展期，以免影響申報作業。 (十一).最高使用權限人員設定使用者之帳號及權限，應依各業務範圍及權責設定。 (十二).權責主管須覆核定期或不定期申報公開資訊之正確性。 (十三).公司應定期或不定期稽核依個人資料保護法定義之個人資檔案管理情形。 (十四).應定期檢查網站內對外提供之資訊，對具機密性、敏感性之資訊內容，應立即移除。 (十五).各種重要法令規章及通知應立即張貼於公布欄。 (十六).個人資料檔案之資料，其更新、更正或註銷均應報經核准，並將更新、更正、註銷內容、作業人員及時間詳實記錄。	

十二、新興科技應用：CC-11200

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
CC-11200	新興科技應用	作業程序及控制重點： 一、雲端服務：(涉及關鍵性系統、資料或服務者需符合以下要求) (一)公司為雲端服務使用者時應訂定雲端運算服務運作安全規範內含雲端提供者之遴選機制、查核措施、備援機制、服務水準(含資訊安全防護)與復原時間要求等，如有不符需求之處，需有其他補償性措施。 (二)公司為雲端服務提供者時，應訂定雲端運算服務安全控管措施，應包含法律遵循、權限控管、權責歸屬及資訊安全防護等項目。如涉及敏感性資料之傳遞，應使用超文字傳輸安全協定(HTTPS)、安全檔案傳輸協定(SFTP)等加密之網路協定。 二、社群媒體： (一)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，應包含以下內容： 1.界定可於公務用社群媒體上分享之業務相關資料。 2.界定私人與公務用社群媒體之區別與應注意事項。 (二)公司應針對開放員工使用社群媒體評估其風險程度，包含：資料外洩、社交工程、惡意程式攻擊等，並採行適當的安全控管措施。 (三)公司應訂定經營官方社群媒體資訊安全規範與管理辦法，並包含以下內容： 1.應事先了解所經營之社群媒體隱私政策，並定期檢視其隱私政策之異動及評估其風險。 2.於官方網站提供連結供使用者連至公司外之社群媒體時，應出現提示視窗告知使用者該連結非公司本身之網站。 3.對經營之社群媒體應標示期貨商名稱、聯絡方式，以區別為官方經營之社群媒體。 4.應建立帳號權限管理機制，對發布內容進行控管與監視，並針對不適當言論及異常	法令規章： 1.中華民國期貨業商業同業公會「新興科技資訊安全自律規範」 2.證券期貨市場相關公會新興科技資訊安全管控指引 使用表單： 無

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
		事件，進行通報或處置。 三、行動裝置： 公司應訂定行動裝置之資訊安全規範與管理辦法，須包含以下項目： (一)公務用行動裝置設備管理辦法： 1.公務用行動裝置管理辦法對於申請、使用、更新、繳回與審核應訂有相關規範。 2.人員異動時，應進行重新配置或清除配置程序，以確保行動裝置環境安全性。 3.對公務用之行動裝置應避免安裝非官方發布之行動應用程式，或僅安裝由公司列出通過檢測可安裝之行動應用程式。 (二)員工自攜行動裝置管理辦法，應含以下項目： 1.應要求員工自攜行動裝置使用用途。 2.應與持有人簽署員工自攜行動裝置使用協議，含：使用限制及雙方責任等。 3.應限制內部資訊設備透過員工自攜行動裝置私接存取網際網路(Internet)之行為。 (三)應訂定行動應用程式之發布規範與管理辦法，並包含下列要點： 1.應用程式發布前，應確認程式碼或程序庫符合以下安全事項： (1)通過內容安全或驗證程序，如：程式原始碼檢測或掃描，確認未含惡意程式碼與有敏感性資料。 (2)行動應用程式宜完整定義特殊符號篩選機制。 2.無法取得行動應用程式原始碼時，應要求行動應用程式提供者符合前項安全事項。 (四)應訂定行動應用程式安全控管規範與管理辦法，並包含以下項目： 1.應針對交易或帳務等敏感性資料設計行動應用程式存取驗證機制，並僅供經授權之行動應用程式使用該敏感性資料。	

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
		2.透過行動應用程式發送簡訊或其他訊息通知方式告知使用者敏感性資料時，應進行適當去識別化。 3.透過行動應用程式傳送帳號、密碼及其他敏感性資料時，應以憑證驗證或加密機制確保傳送安全。 4.透過行動應用程式儲存密碼、憑證、交易或帳務等敏感性資料時，應對儲存之資料進行雜湊(Hash)或加密控管保護。 5.透過行動應用程式處理交易或金流作業時，應留存存取日誌，且存取日誌應予以保護以防止未經授權存取。 四、物聯網： 應訂定物聯網相關資訊安全規範與管理辦法，須包含下列項目： (一)應建立物聯網設備管理清冊並至少每年更新一次，且應變更前開設備之初始密碼。 (二)物聯網設備應具備安全性更新機制且定期(每年一次)更新，如存在已知弱點無法更新時，應建立補償性管控機制。 (三)應關閉物聯網設備不必要之網路連線及服務，避免使用對外公開的網際網路位置。 (四)如與物聯網設備供應商簽定採購合約時，其內容宜包含資訊安全相關協議，明確約定相關責任(如：服務承諾、安全性更新年限、主動通報設備已知資安漏洞並提出相關應變處置方案)，確保設備不存在已知安全性漏洞。	