資通安全
重點說明

臺灣證券交易所
券商輔導部

Taiwan Stock Exchange @Copyright 2023

修訂內容(1)

證券商內部控制制度標準規範—內部控制制度修正對照表草案

編號	作業項目	修正後內容	修正前內容	修正說明
CC-14000	資產分類與控制	作業程序及控制重點： (一)資訊資產應列有清冊且包含軟體、硬體、場地及資料等類別，並應加以維護。 (二)應訂有資訊分級並作標示處理之相關規範（適用網際網路下單證券商）。 (三)公司應對自行或委外開發之資通系統完成資通系統分級，資通系統等級應至少區分核心與非核心系統，每年應至少檢視一次資通系統分級妥適性。 (四)公司應對資訊資產之資料與文件的保存期限進行規範，並於保存期限到期後進行刪除與銷毀。 (五)公司應避免使用危害國家資通安全產品。 **(六)應定期盤點使用之應用程式介面(API)，並建立適當安全控管機制。**	作業程序及控制重點： (一)資訊資產應列有清冊且包含軟體、硬體、場地及資料等類別，並應加以維護。 (二)應訂有資訊分級並作標示處理之相關規範（適用網際網路下單證券商）。 (三)公司應對自行或委外開發之資通系統完成資通系統分級，資通系統等級應至少區分 (五)公司應避免使用危害國家資通安全產品。 **(新增)**	增訂檢查重點

為降低API使用風險，內控納入盤點API服務，連接應使用TOKEN等機制驗證。

Taiwan Stock Exchange @Copyright 2023

修訂內容(2)

證券商內部控制制度標準規範—內部控制制度修正對照表草案

編號	作業項目	修正後內容	修正前內容	修正說明
CC-16000	實體及環境安全	作業程序及控制重點： (一)電腦機房應設有門禁管制；機房內設置防火設施及緊急照明設備。另應將地震、水災等天然災害因素列入考量。 (二)電腦設備應有獨立之空調系統供[illegible]用，供給空調系統之電力來源應自成一[illegible] (三)機房內溫濕度應維持正常。 (四)電腦設備之電源供應系統，[illegible]電設備及發電機。 (五)不斷電系統、發電機等電源[illegible]應定期或不定期測試其堪用性 (六)電腦系統使用之空調、電源等相關設備，應有適當之備援對策。 (七)機房指派專人管理，其作業項目如下： 1.機房門口應揭示值班操作人員姓名及值班期間。	作業程序及控制重點： (一)電腦機房應設有**適當之**門禁管制**(例如：刷卡)**；機房內設置防火設施及緊急照明設備。另應將地震、水災等天然災害因素列入考量。 (二)電腦設備應有獨立之空調系統供其使用，供給空調系統之電力來源應自成一系統。 [illegible] (六)電腦系統使用之空調、電源等相關設備，應有適當之備援對策。 (七)機房指派專人管理，其作業項目如下： 1.機房門口應揭示值班操作人員姓名及值班期間。	1.避免限縮實務執行方式，爰刪除例示文字，以採原則性規範。；2.增訂檢查重點

讓門禁管制的方式不要侷限刷卡等機制

Taiwan Stock Exchange @Copyright 2023

修訂內容(3)

編號	作業項目	修正後內容	修正前內容	修正說明
CC-16000	實體環境與安全	廠商派員前來維護。 (十)廠商維護人員於維修設備時，應有相關人員會同檢修。 (十一)電腦系統維護工作，應避免停 使用者，儘可能安排在夜間、 人使用狀態下進行停機作業之 (十二)應訂定設備報廢作業程序，報 機密性、敏感性資料及授權軟 除、實施安全性覆寫或實體破壞，應確 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 第三者銷毀時，應簽訂保密合約。 (十三)公司應定期審查電腦機房門禁管制權 限。 **(十四)公司自有及租用之機房或機櫃，除公司之期貨商關係企業且設有網路區隔，始得與其共同使用同一機房或機櫃外，均不得將機房或機櫃空間分租、轉租、出借或以任何方式提供第三方使用。**	廠商派員前來維護。 (十)廠商維護人員於維修設備時，應有相關人員會同檢修。 實施安全性覆寫或實體破壞，應確 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。 (十三)公司應定期審查電腦機房門禁管制權 限。 **(新增)**	

代管及機房使用範圍僅限證券期貨相關業別共同使用

Taiwan Stock Exchange @Copyright 2023

修訂內容(4)

編號	作業項目	修正後內容	修正前內容	修正說明
CC-17010	網路安全管理	部網路遠端連線至公司內部作業進行控管及多因子身分認證，留存相關維護紀錄並由權責主管定期覆核。 9.公司應防止未經授權設備使用內部網路。 10.應避免使用生命週期終止(End of Service， EOS/End of Life, EOL)之軟體及網路[無標題]，且於到期前擬定汰除計畫，並視情況建立補償性措施。 **11.公司應就所接收資安情資，辨識其來源之可靠性及時效性，及時進行威脅與弱點分析及研判潛在風險，並採取對應之預防或應變措施。** (二)網路設備之安全管理： 1.應建立防火牆。 2.防火牆應有專人管理。 3.防火牆進出紀錄及其備份應至少保存三年。 4.重要網站及伺服器系統(如網**際網**路下單系統等)應以防火牆與外部網際網路隔離。	部網路遠端連線至公司內部作業進行控管及多因子身分認證，留存相關維護紀錄並由權責主管定期覆核。 9.公司應防止未經授權設備使用內部網路。 10.應避免使用生命週期終止(End of Service， EOS/End of Life, EOL)之軟體及網路設備，且於到期前擬定汰除計畫，並視情況建立補償性措施。 **(新增)** (二)網路[illegible] 1.應[illegible] 2.防火牆應有專人管理。 3.防火牆進出紀錄及其備份應至少保存三年。 4.重要網站及伺服器系統(如網路下單系統等)應以防火牆與外部網際網路隔離。	

確保資安情資被有效運用

Taiwan Stock Exchange @Copyright 2023

修訂內容(5)

編號	作業項目	修正後內容	修正前內容	修正說明
CC-17010	網路安全管理	密碼卡、晶片卡、電腦、行動裝置、憑證載具等），公司應確認該設備為客戶與公司所約定持有之設備。 3.客戶提供給公司其所擁有之生物特徵(如指紋、臉部、虹膜、聲音、掌紋、靜脈、簽名等），公司應直接或間接驗證該生物特徵。 (五)身分認證與憑證管理： 1.網際網路下單證券商應訂定憑證交付程序，避免非本人取得憑證。客戶申請或更新憑證下載，必須採用多因子(如：下單憑證、綁定裝置、OTP、生物辨識及SIM 認證等)驗證方式，且與登入帳戶時使用之因子不同，確實辨認客戶身分並留存紀錄。 2.網際網路下單證券商[illegible]制。 3.公司應於伺服器端驗證客戶交易身分及使用者帳號。 4.公司對電子交易身分之申請、交付、使用、更新與驗證應訂定相關規範。 (六)電腦病毒及惡意軟體之防範： 1.應安裝防毒軟體，並及時更新程式及病毒碼。 2.應定期對資通系統及資料儲存媒體進行病毒描(含電子郵件)。 3.防毒應涵蓋個人端(含攜帶型及營業處所	密碼卡、晶片卡、電腦、行動裝置、憑證載具等），公司應確認該設備為客戶與公司所約定持有之設備。 3.客戶提供給公司其所擁有之生物特徵(如指紋、臉部、虹膜、聲音、掌紋、靜脈、簽名等），公司應直接或間接驗證該生物特徵。 (五)身分認證與憑證管理： 1.網路下單證券商應訂定憑證交付程序，避免非本人取得憑證。客戶申請或更新憑證下載，必須採用多因子(如：下單憑證、綁定裝置、OTP、生物辨識及 SIM 認證等) 使用者帳號。 4.公司對電子交易身分之申請、交付、使用、更新與驗證應訂定相關規範。 (六)電腦病毒及惡意軟體之防範： 1.應安裝防毒軟體，並及時更新程式及病毒碼。 2.應定期對資通系統及資料儲存媒體進行病毒描(含電子郵件)。 3.防毒應涵蓋個人端(含攜帶型及營業處所	

調整文字

修訂內容(6)

編號	作業項目	修正後內容	修正前內容	修正說明
CC-17010	網路安全管理	器端電腦。 4.勿開啟來歷不明之電子郵件，對於電子郵件中帶有執行檔之附件，尤應特別小心開啟。 5.為防範電腦病毒擴散，影響電腦安全，公司應訂定電子郵件使用安全相關規定及建立郵件過濾機制。 6.公司應建立軟體白名單**及上網**控管機制。 7.公司應偵測釣魚網站及惡意網站連結並提醒客戶防範網路 釣魚。 8.公司應每年定期辦理社交工程演練，並對誤開啟信件或連結之人員進行教育訓練，並留存相關紀錄。 (七)網路系統功能檢查： 1.應定期檢查網路下單系統提供之功能，並留存 紀錄。 2.公司應就提供外部連線使用網測網頁與程式異動、記錄並通員處理。 (八)公司提供**客戶使用** API 服務規範 依據「證券商受理投資人使用應用程式介面(API)服務作業規範」，公司提供客戶使用應用程式介面(API)服務之相關作業，應依下列申請流程、核可標準及相關控管配套措施辦理：	器端電腦。 4.勿開啟來歷不明之電子郵件，對於電子郵件中帶有執行檔之附件，尤應特別小心 7.公司應偵測釣魚網站及惡意網站連結並提醒客戶防範網路 釣魚。 8.公司應每年定期辦理社交工程演練，並對誤開啟信件或連結之人員進行教育訓練，並留存相關紀錄。 (七)網路系統功能檢查： 1.應定期檢查網路下單系統提供之功能，並 依據「證券商受理投資人使用應用程式介面(API)服務作業規範」，公司提供客戶使用應用程式介面(API)服務之相關作業，應依下列申請流程、核可標準及相關控管配套措施辦理：	

上網管制

調整文字，範圍係為客戶使用API交易

Taiwan Stock Exchange © Copyright 2023

修訂內容(7)

編號	作業項目	修正後內容	修正前內容	修正說明
CC-17010	網路安全管理	易資料保存規範」之規定辦理。 (7)公司提供客戶使用應用程式介面(API)服務，不得違反證交法第 159 條有關全權委託禁止之規定。 (8)公司若有提供交易資訊予其開戶之客戶應依證交所「交易資訊使用管理辦法」之規定辦理。 (9)API 服務下單交易相關資料，公司應併同網際網路及語音資料，由單一窗口系統於每月前 4 個營業日申報。 (九)網際網路下單服務品質相關標準： 公司提供網際網路下單業務時，兼顧客戶服務品質，應訂定網際網路下單服務品質相關標準，並應包含下列重點： 1.交易之安全性:包括建立相關資訊安全機制，並擬定緊急應變計畫及備援措施。 2.交易之穩定及系統可用性:為維持網路交易之順暢與便捷，應定期評估系統可用性並留存紀錄，就網際網路下單客戶數、交易流量及預期將來交易量，衡量現有設備是否足以負載、是否需擴充相關軟硬體設備，以避免發生網路塞單、委託成交速度遲緩甚或當機之風險。 3.提供客戶服務：提供客戶多元之附加價值，基本服務應包括報價資訊、委託下單、帳務查詢、技術分析、即時庫存、資券配額及整戶維持率等七項。	易資料保存規範」之規定辦理。 (7)公司提供客戶使用應用程式介面(API)服務，不得違反證交法第 159 條有關全權委託禁止之規定。 (8)公司若有提供交易資訊予其開戶之客戶應依證交所「交易資訊使用管理辦法」之規定辦理。 (9)API 服務下單交易相關資料，公司應併同網際網路及語音資料，由單一窗口系統於每月前 4 個營業日申報。 (九)網際網路下單服務品質相關標準： 公司提供網際網路下單業務時，兼顧客戶服務品質，應訂定網際網路下單服務品質相關標準，並應包含下列重點： 1.交易之安全性:包括建立相關資訊安全機制，並擬定緊急應變計畫及備援措施。 2.交易之穩定及系統可用性:為維持網路交易之順暢與便捷，應定期評估系統可用性並留存紀錄，就網路下單客戶數、交易流量及預期將來交易量，衡量現有設備是否足以負載、是否需擴充相關軟硬體設備，以避免發生網路塞單、委託成交速度遲緩甚或當機之風險。 3.提供客戶服務：提供客戶多元之附加價值，基本服務應包括報價資訊、委託下單、帳務查詢、技術分析、即時庫存、資券配額及整戶維持率等七項。	

調整文字

Taiwan Stock Exchange @Copyright 2023

修訂內容(8)

編號	作業項目	修正後內容	修正前內容	修正說明
CC-18000	存取控制	確認其身分及核發程序後(如聯繫客服驗證基本資料、OTP、臨櫃辦理等方式)，方可開放其使用系統。 5.除語音按鍵下單外，公司應使用優質密碼設定（長度六個字元（含）以上，且具有文數字或符號）並進行管控，及加強宣導客戶定期更新密碼以不超過三個月為宜，如客戶密碼超過一年未變更或變更密碼與前一代相同，公司應做妥善處理。公司使用者之密碼**除提供系統使用之帳號應採定期變更或適當安全控管措施（如限制人工登入、監控告警等）外，**應至少每三個月變更一次。 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。 7.為防止密碼洩漏，應採取不顯示、不印錄等措施。 8.客戶申請採電子式交易型態者，公司得以一般電子方式交付或自訂交付電子密碼條，並依下列說明辦理： (1)(2)、(3)適用於一般電子方式，(4)、(5)、(6)、(7)適用於自訂交付方式。 (1)客戶應於聲明書中聲明同意以電子方	確認其身分及核發程序後(如聯繫客服驗證基本資料、OTP、臨櫃辦理等方式)，方可開放其使用系統。 5.除語音按鍵下單外，公司應使用優質密碼設定（長度六個字元（含）以上，且具有文 管控，及加強宣導 不超過三個月為宜 未變更或變更 應做妥善處理。 使用者之密碼應至少每三個月變更一次。 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。 7.為防止密碼洩漏，應採取不顯示、不印錄等措施。 8.客戶申請採電子式交易型態者，公司得以一般電子方式交付或自訂交付電子密碼條，並依下列說明辦理： (1)(2)、(3)適用於一般電子方式，(4)、(5)、(6)、(7)適用於自訂交付方式。 (1)客戶應於聲明書中聲明同意以電子方	

加強管控

Taiwan Stock Exchange @Copyright 2023

修訂內容(9)

編號	作業項目	修正後內容	修正前內容	修正說明
CC-18000	存取控制	式交付電子密碼條。 (2)公司業務人員應確實辨認客戶身分，並確認其手機號碼及電子信箱為本人使用。 (3)傳送 OTP(One Time Password)密碼至客戶開戶留存之手機號碼，及將加密後之電子密碼條以電子方式傳送至客戶留存之電子信箱，客戶需以 OTP 密碼解密方能取得密碼，此流程相關系統紀錄應留存。 (4)應訂定交付電子式交易密碼之作業程序。 (5)應確實辨認電子式交易密碼交付對象為本人並留存相關紀錄。 (6)應訂定電子式交易密碼交付流程與安全控管機制相關內部控制制度。 (7)密碼管理應使用優質密碼設定(長度 6 個字元（含）以上，且具有文數字或符號)，並加強宣導客戶定期更新使用者密碼以不超過三個月為宜。 (四)電腦稽核紀錄管理： 1.對重要系統（如主機連線系統、網際網路下單系統等）之稽核日誌紀錄內容應包括使用者識別碼、登入之日期時間、電腦的識別資料或其網址等事項。 2.對上開重要系統之電腦稽核紀錄，應有專人定期檢視。	式交付電子密碼條。 (2)公司業務人員應確實辨認客戶身分，並確認其手機號碼及電子信箱為本人使用。 (3)傳送 OTP(One Time Password)密碼至客戶開戶留存之手機號碼，及將加密後之電子密碼條以電子方式傳送至客戶留存之電子信箱，客戶需以 OTP 密碼解密方能取得密碼，此流程相關系統紀錄應留存。 (4)應訂定交付電子式交易密碼之作業程序。 (5)應確實辨認電子式交易密碼交付對象為本人並留存相關紀錄。 交易密碼交付流程與安 關內部控制制度。 用優質密碼設定(長度 6 以上，且具有文數字或符 導客戶定期更新使用者 密碼以不超過三個月為宜。 (四)電腦稽核紀錄管理： 1.對重要系統（如主機連線系統、網路下單系統等）之稽核日誌紀錄內容應包括使用者識別碼、登入之日期時間、電腦的識別資料或其網址等事項。 2.對上開重要系統之電腦稽核紀錄，應有專人定期檢視。	

調整文字

修訂內容(10)

編號	作業項目	修正後內容	修正前內容	修正說明
CC-19000	系統開發與維護	訂定合約，合約所含內容應包含以下內容：合約期限、服務範圍、服務交付日期、服務水準要求、服務變更規範、服務驗收之標準、資通安全事件通報及應變處理作業程序、對資訊服務供應商之稽核權條款、合約轉讓或同意分包之規範、保密義務條款、罰則與損害賠償條款、爭議處理程序、違約處理條款、合約終止規範、合約終止後之處理、保固、權利及責任。 2.公司應針對資訊委外業務項目之資通安全風險與委外作業可行性，及資訊服務供應商作業能力及集中度，由相關資訊單位共同執行風險評估，評估結果應提報適當管理層級並取得同意。 3.資訊服務供應商應提供安全性檢測證明(如行動應用程式資安檢測、源碼**掃描**、弱點掃描等)，並應確保交付之系統或程式無惡意程式及後門程式，其放置於網際網路之程式應通過源碼掃描或黑箱測試。	訂定合約，合約所含內容應包含以下內容：合約期限、服務範圍、服務交付日期、服務水準要求、服務變更規範、服務驗收之標準、資通安全事件通報及應變處理作業程序、對資訊服務供應商之稽核權條款、合約轉讓或同意分包之規範、保密義務條款、罰則與損害賠償條款、爭議處理程序、違約處理條款、合 能力及集中度，由相關資訊 共同執行風險評估，評估結果應提報適當管理層級並取得同意。 3.資訊服務供應商應提供安全性檢測證明(如行動應用程式資安檢測、源碼**檢測**、弱點掃描等)，並應確保交付之系統或程式無惡意程式及後門程式，其放置於網際網路之程式應通過源碼掃描或黑箱測試。	

調整文字，檢測改為慣用語「掃描」

修訂內容(11)

編號	作業項目	修正後內容	修正前內容	修正說明
CC-19000	系統開發與維護	外，只能由系統負責人依核定後結果執行之。 6.上線系統變更時其設計上相關之改變應及時配合更新。 7.**程式變更上線前應進行完整測試，**變更完成後須檢核與申請內容是否相符，並進行驗證以確認變更作業之**可用性及**正確性。 (十五)資通系統弱點掃描：(適用網際網路下單證券商) 1.各資通系統應定期(至少每半年一次)進行弱點掃描。 2.針對系統弱點其相關風險撰寫說明與安裝修補方式文件，並留存記錄以供參考。 (十六)程式源碼安全規範(適用網際網路下單證券商，不適用語音下單及傳統下單之證券商)： 1.程式應避免含有惡意程式等資訊安全漏洞。 2.程式應使用適當且有效之完整性驗證機制，以確保其完整性。 3.程式於引用之函式庫有更新時，應備妥對應之更新版本。	外，只能由系統負責人依核定後結果執行之。 6.上線系統變更時其設計上相關之改變應及時配合更新。 7.**系統**變更完成後須檢核與申請內容是否相符，並進行**必要**驗證以確認變更作業之正確性。 (十五)資通系統弱點掃描：(適用網際網路下單證券商) 1.各資通系統應定期(至少每半年一次)進行弱點掃描。 2.針對系統弱點其相關風險撰寫說明與安裝修補方式文件，並留存記錄以供參考。 (十六)程式源碼安全規範(適用網際網路下單證券商，不適用語音下單及傳統下單之證券商)： 1.程式應避免含有惡意程式等資訊安全漏洞。 2.程式應使用適當且有效之完整性驗證機制，以確保其完整性。 3.程式於引用之函式庫有更新時，應備妥對應之更新版本。	

考量實務及近期案例，程式上線不應只有單元測試，應就相關之功能或流程進行完整測試。

修訂內容(12)

CC-19000	系統開發與維護	(2)公司對第三方檢測員驗室所提交之檢測報告，應建立覆核機制，以確保檢測項目及內容一致，並留存覆核紀錄。 (十八)核心系統**發生錯誤時，**使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細之	(2)公司對第三方檢測員驗室所提交之檢測報告，應建立覆核機制，以確保檢測項目及內容一致，並留存覆核紀錄。 (十八)核心系統**應針對風險評估**使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細	

內容調整，系統有異常時應避免提供過多的資訊或代碼

編號	作業項目	修正後內容		說明
		錯誤訊息。 (十九)提供網際網路下單服務之核心系統上架前及系統更新時應執行「源碼掃描」安全檢測。 (二十)與資訊公司異業合作平台，不得提供或介接未經金融監督管理委員會許可之證券期貨業者所提供之證券期貨業務（如證券期貨業務有關之開戶及下單功能）。	(十九)提供網際網路下單服務之核心系統上架前及系統更新時應執行「源碼掃描」安全檢測。 (二十)與資訊公司異業合作平台，不得提供或介接未經金融監督管理委員會許可之證券期貨業者所提供之證券期貨業務（如證券期貨業務有關之開戶及下單功能）。	

Taiwan Stock Exchange @Copyright 2023

修訂內容(13)

編號	作業項目	修正後內容	修正前內容	修正說明
CC-20000	營運持續管理	時間，衡量當時作業狀況，通知相關人員根據備援及回復計畫所應採取之配合措施。 (五)不管是電腦系統或是電力、空調、消防系統發生異常，事後相關人員應確實檢討原因，並謀求改進與對應預防措施。 (六)所訂定之重大異常狀況系統復原計劃應定期模擬演練，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。 (七)公司（證券經紀商）之交易主機應有備援措施，並依所屬資安分級建置異地備援機房。 (八)公司應執行營運衝擊分析，評估核心系統可容忍中斷時間、復原時間目標（RTO）、資料復原點目標（RPO ），並擬訂營運持續計畫（含起動條件、參與人員、緊急程序、備援程序、維護時間表、教育訓練、職責說明、往來外單位之應變規劃及合約適當性等）及其必要之 安分級定期辦理業務持 演練範圍是否涉及第 參與演練。網際網路下單證券商應依經紀業務規模市占率暨自然人客戶數比率分級，訂定核心系統可容忍中斷時間。 (九)公司應訂定資訊安全訊息通報機制（例如：正式之通報程序及資安事件通報聯絡人），及針對與資通系統有關之資訊安全或	時間，衡量當時作業狀況，通知相關人員根據備援及回復計畫所應採取之配合措施。 (五)不管是電腦系統或是電力、空調、消防系統發生異常，事後相關人員應確實檢討原因，並謀求改進與對應預防措施。 (六)所訂定之重大異常狀況系統復原計劃應定期模擬演練，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。 (七)公司（證券經紀商）之交易主機應有備援措施，並依所屬資安分級建置異地備援機房。 (八)公司應執行營運衝擊分析，評估核心系統可容忍中斷時間、復原時間目標（RTO）、資料復原點目標（RPO ），並擬訂營運持續計畫（含起動條件、參與人員、緊急程序、備援程序、維護時間表、教育訓練、職責說[無標題]往來外單位之應變規劃及合約適當性等）及其必要之維護，依其所屬資安分級定期辦理業務持續運作演練，且視演練範圍是否涉及第三方，邀請相關廠商參與演練。網路下單證券商應依經紀業務規模市占率暨自然人客戶數比率分級，訂定核心系統可容忍中斷時間。 (九)公司應訂定資訊安全訊息通報機制（例如：正式之通報程序及資安事件通報聯絡人），及針對與資通系統有關之資訊安全或	

調整文字

修訂內容(14)

編號	作業項目	修正後內容	修正前內容	修正說明
CC-20000	營運持續管理	服務異常事件應依「證券期貨市場資通安全事件通報應變作業注意事項」及「證券商通報重大資安事件之範圍申報程序及其他應遵循事項」辦理，並採取適當矯正程序，留存紀錄。 (十)公司發生個人資料之竊取、竄改、毀損、滅失、或洩漏等資安事故者，應即函報證交所(或櫃檯買賣中心、券商公會)轉陳主管機關。 (十一)公司應明確訂定分散式阻斷服務攻擊(DDoS)防禦與應變作業程序，並每年進行演練。 (十二)故障復原程序應定期測試，測試後應召開檢討會議，針對測試缺失謀求改進，並留存紀錄。	服務異常事件應依「證券期貨市場資通安全事件通報應變作業注意事項」及「證券商通報重大資安事件之範圍申報程序及其他應遵循事項」辦理，並採取適當矯正程序，留存紀錄。 (十) (十一)公司應明確訂定分散式阻斷服務攻擊(DDoS)防禦與應變作業程序。 (十二)故障復原程序應定期測試，測試後應召開檢討會議，針對測試缺失謀求改進，並留存紀錄。	

為強化營運持續量能，定期演練

Taiwan Stock Exchange @Copyright 2023

重點要辦理事項說明

資安健診

- 健診缺失改善事項追蹤應由資安單位追蹤完畢後，再由稽核覆核落實情形。

持續營運

- 第四級證券商辦理持續營運演練

Taiwan Stock Exchange @Copyright 2023

重點案例說明(1/2)

強化持續營運

- 機房遇天然災害致影響交易。
- 公司重大系統整合，未考量對交易衝擊。

委外系統異常

- 驗章系統異常。
- 作業系統更新異常。

Taiwan Stock Exchange @Copyright 2023

重點案例說明(2/2)

對外介接系統異常

- 圈存系統異常，造成扣款失敗。

應用系統異常

- 資源不足。
- 程式更新版本錯誤。
- 主機設備故障。

Taiwan Stock Exchange @Copyright 2023

簡報結束
敬請指導

Taiwan Stock Exchange @Copyright 2023