存取控制

文件編號：	SC-01-008
文件版次：	V 1.1
發行日期：	2024/08/28

文件修訂履歷

V1.0	2023/11/01	新版文件。	丘建華副總經理	李文柱總經理	因應 2022 轉版，重新發行。
V1.1	2024/08/07	因應內控調整「第一章目的」。	吳允文副總經理	李文柱總經理	

目　錄

第一章 目的

為確保群益金鼎證券（以下簡稱本公司）於權限管理、密碼管理、資料輸入出管理、電腦稽核紀錄管理有效運作，以及遵循臺灣證券交易所發布「建立證券商資通安全檢查機制」之規範，特訂定本要點以維護本公司之內容管理，以達成以下目標：

第一節 存取控制

一、 為避免資訊設備遭受損壞以致影響業務之持續運作，並設置適當之防護以保護資訊資產，依據臺灣證券交易所發布《建立證券商資通安全檢查機制》訂定及落實相關要點，含權限管理、密碼管理以及申請異動程序。

二、 相關帳號申請異動程序則依據《SO-MG-006_資訊設備帳號及管理權限程序》，故以此特訂定本要點以規定執行作業時應遵循之事項。

第二節 個人資料外洩防護機制

一、 建置個資防護系統架構，以強化可攜式媒體（如 USB）存取、電子郵件外寄郵件內容與附加檔案管理，防範個資或機敏性資料外洩，並依據臺灣證券交易所發布《建立證券商資通安全檢查機制》訂定及落實相關要點。

第三節 證券商資通安全檢查機制

一、 訂定資訊系統存取控制相關規定，並以書面、電子或其他方式告知本公司員工遵守。

二、 權限管理：

(一) 對於程式的存取使用，以此要點進行管制說明。

(二) 人員異動時及時更新其使用權限。

(三) 對於程式及檔案之存取使用，將按權限區分。

(四) 委外人員電腦通行使用權利經適當控管；委外期間結束後，立即收回該項權利，相關委外廠商權限管理權責依據《SC-01-009 系統開發及維護》辦理。

(五) 對於進駐於公司內之委外作業人員已納入公司安全管理，如欲使用內部網路資源時，有相關安全管制措施（如透過轉接方式或另建網路者，宜與內部網路作實體隔離）。

(六) 定期審查資通系統帳號及權限之適切性，並視審查結果停用資通系統閒置帳號。（客戶帳號除外）。

(七) 公司應建立資通系統帳號管理機制，包含帳號之申請、建立、修改、啟用、停用及刪除之程序。

(八) 資通系統帳號應定義人員角色及責任，授權應採最小權限原則，僅允許使用者(或代表使用者行為之程序)依公司部門權責及業務功能，完成作業所需之授權存取。

三、 密碼管理：

(一) 使用者第一次使用系統時，需更新初始密碼後方可繼續作業。

(二) 密碼使用公開安全且未遭破解之演算法(例如:雜湊演算法等不可逆運算式)產生亂碼並加密儲存。

(三) 對於使用者及客戶忘記密碼之處理，有嚴格的身分確認程序(如聯繫客服驗證基本資料、OTP、臨櫃辦理等方式)，方可再次使用系統。

(四) 建立初始密碼隨機產生之機制，並確保與使用者及客戶身分無關。

(五) 密碼輸入錯誤次數達五次者，予以中斷連線且鎖定該帳號，十五分鐘不允許該帳號繼續嘗試登入，並留存紀錄。公司於接獲客戶聯繫申請解除鎖定時，建立確實辨認身分及留存相關紀錄之機制。

(六) 除語音按鍵下單外，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，公司會進行相關處理。除客戶外，公司其他使用者之密碼至少每三個月變更一次。

(七) 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設定使用密碼，建立避免使用預設(如 administrator、root、sa)或簡易之帳號密碼及未設管理者存取權限。(路由器及交換器作業請參考「SC-01-007 通訊與作業管理」)

(八) 客戶申請採電子式交易型態者，公司得以一般或自訂電子方式交付電子密碼條，應依下列說明辦理：

1. 採一般電子方式交付電子密碼條，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，並留存相關系統紀錄。
2. 採自訂交付電子密碼條方式，訂定交付電子式交易密碼之作業程序及安全控管機制，並辨認電子式交易密碼交付對象為本人及留存相關紀錄。

四、 電腦稽核紀錄管理：

(一) 對重要系統(如主機連線系統、網路下單系統等)之稽核日誌記錄內容包括使用者識別碼、登入之日期時間、電腦的識別資料或其網址等事項。

(二) 對上開重要系統之電腦稽核紀錄，有專人定期檢視。

(三) 相關留存紀錄為確保數位證據之收集、保護與適當管理程序，至少留存三年。

(四) 核心系統電腦稽核紀錄(日誌)應建立監控機制，處理失效時，應採取適當之行動。

五、 資料輸入管理：

(一) 安全性或重要性較高之資料，經由權責主管人員核可後始得執行輸入或修改。

(二) 所輸入或修改之資料及其執行人員姓名、職稱皆留存紀錄。

(三) 對隱密性高之重要資料(例如：密碼檔)以亂碼後之資料形式存放。

(四) 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。

(五) 使用電子憑證ＩＣ卡或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：「公開資訊觀測站」、「證券商申報單一窗口」、「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，且訂定相關帳號、密碼保管及使用程序，並據以執行。

(六) 使用代表公司憑證載具簽署之作業系統端若屬證券商應用系統者(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。

(七) 依「個人資料保護法」，妥善處理客戶及公司內部人個人資料。

(八) 公司依「個人資料保護法」妥善處理公司保有之個人資料，並定期或不定期稽核依「個人資料保護法」定義之個人資料管理情形。

(九) 前揭個人資料，其更新、更正或註銷均應報經備查，並將更新、更正、註銷內容、作業人員及時間詳實記錄。

(十) 因經營業務需要而為個人資料之蒐集、處理或國際傳輸及利用，訂定「與軟硬體廠商機密維護及損害賠償等雙方權責劃分」。

(十一) 應留存個人資料使用稽核軌跡(如登入帳號、系統功能、時間、系統名稱、查詢指令或結果）或辨識機制，以利個人資料外洩時得以追蹤個人資料使用狀況。

六、 資料輸出管理：

(一) 報表按時產生並分送各使用單位。

(二) 機密性、敏感性之報表列印或瀏覽有適當之管制程序。

(三) 投資人於公司網站查詢個人資料具有加密傳輸機制（例如： SSL）。

(四) 電子式及非電子式交易型態以電子郵件執行成交回報之傳輸，公司對姓名、帳號及信用帳號等機敏資訊，依「機敏資訊類型及隱匿之具體作法原則」辦理。

第二章 範圍

適用於本公司內所屬資訊、網路與通訊設備相關事宜，包含網路服務及提供網路服務的硬體、軟體與週邊設備如伺服器、個人電腦、網路設備、事務機器、週邊設備、機電設備、應用系統、資料庫管理系統，皆依本辦法辦理。

第三章 名詞定義

第一節 存取控制

一、 資訊設備

包含硬體與軟體，如伺服器、應用系統、資料庫、作業系統、網路設備等。

二、 正式環境系統

係指《SC-01-004_資訊資產分類與控制》所定義之正式環境群組，包含應用系統、資料庫、作業系統及網路設備軟體等。

三、 測試環境系統

係指《SC-01-004_資訊資產分類與控制》所定義之測試環境群組，包含使用於測試之應用系統、資料庫及作業系統等。

四、 所有系統

係指《SC-01-004_資訊資產分類與控制》所定義之軟體群組。

五、 稽核軌跡

稽核軌跡係用以記錄及監督系統作業之活動，追蹤及發現未經授權之存取。

六、 系統分級權限

(一) 作業系統：指隸屬最高權限群組之帳號。

(二) 資料庫：指資料庫管理員使用之帳號。

七、 實體保護

實體保護位於安全區域之定義，係指《SC-01-006 實體環境與安全》定義與劃分之規範。

八、 內部網路：

本公司內部資訊作業使用之區域。

九、 外部網路：

本公司內部以外之網路，泛指網際網路(Internet)以及外部企業與本公司介接之網路(Extranet)。

第二節　個人資料外洩防護機制

一、 使用者

本系統之使用者為本公司員工。

二、 資訊部維護營運處人員

依本程序執行各項作業程序。

三、 商品

Websense Data Security Suite

第四章 相關文件

一、 SC-01-004_資訊資產分類與控制。

二、 SC-01-006_實體環境與安全。

三、 SC-01-009_系統開發及維護。

四、 SO-06-010_個資外洩防護管理作業程序。

五、 SO-MG-006_資訊設備帳號及管理權限程序。

六、 SO-MG-001_網域密碼作業程序。

七、 SO-06-011_軌跡留存作業程序。

第五章 權責

第一節 存取控制

一、 業務擁有者 (Business Owner)

(一) 得指派權責人員進行資訊設備的維護、保管與處份，及授權資訊資產的存取。

二、 資訊資產擁有者 (Owner)

(一) 資訊資產擁有者得在業務擁有者授權的情況下，指派權責人員進行資訊設備的維護、保管與處份，及授權資訊資產的存取。

三、 資訊資產保管者 (Custodian)

(一) 應善盡資訊設備保護之責。

(二) 應對資訊設備實施基本清潔及保養。

(三) 應為所保管的系地統，定期更新重大弱點之修正程式。

(四) 應評估系統安全需求與系統功能允許，據以啟動稽核軌跡，並定期檢核。

(五) 應定期對無法自動化時間同步之資訊設備執行對時。

(六) 應定期監控系統效能及容量使用狀況，如有異常，應留存處理紀錄並陳權責主管覆核。

(七) 應取得已公布之技術脆弱性之資訊或定期執行弱點掃描。

四、 使用者 (User)

(一) 應僅在所獲得之授權內，檢視、使用、存取及更新異動此項資訊設備，並妥善保護所使用的資訊設備。

五、 系統管理人員、資料庫管理人員及網路管理人員：

(一) 系統、資料庫及網路管理執行單位為維護營運處。

(二) 應明確定義作業系統之安全參數。

(三) 應於維護之系統上線前，執行適當之強化。

六、 帳號管理人員

(一) 凡適用範圍內之所有資訊設備或電腦網域中，同時具有兩位以上之使用者，且設有帳號或權限管制之系統，依據經適當授權之帳號權限申請，而設定帳號及權限之人員，即為該資訊設備之帳號管理人員。

(二) 帳號管理人員不宜為該資訊設備日常作業之使用者。

七、 帳號管理主管

(一) 審核資訊資產存取權限申請文件，並確定其與系統設定一致且適當。

八、 使用者部門

(一) 本公司所有資訊作業相關同仁。

第二節　個人資料外洩防護機制

一、 系統擁有單位（Owner）

(一) Business Owner 管理審查委員會指定代理人

(二) Ap Owner 資訊部維護營運處主管主要職責請參考資訊資產管理辦法。

二、 系統保管單位（Custodian）

(一) 維護營運處系統負責人

依照使用者提出之需求單內容，經系統 Owner 單位主管同意後，方進行規劃分析及系統開發測試作業，完成後提出資訊需求申請表，將系統安裝至正式環境供使用者使用，修改時亦同。

三、 使用單位（User）

(一) 使用者新增或修改權限，需填寫《CIS 需求申請單》提出申請。

第六章 存取控制作業內容

第一節　正式環境系統存取管理

一、 使用者帳號與權限管理

(一) 依據《SO-MG-006_資訊設備帳號及管理權限程序》進行正式的帳號申請與異動流程，以規範對所有多使用者資訊系統與服務的存取授權。

(二) 應建立各作業系統及應用系統之帳號申請及密碼重建、使用者離/調職帳號刪除書面制度與表單，並至少應有申請者部門主管、資訊資產擁有者部門主管之核准程序，且帳號異動後需經帳號管理人員主管或其代理人員覆核。

(三) 應有正式的使用者申請及註銷的程序，以作為對所有的多人使用資訊系統及服務進行存取授權之用。

(四) 第三方存取使用帳號：如委外廠商或臨時聘僱人員等，待該專案或工作結束，該專案之負責人員或部門主管應立即提出刪除或停用帳號之申請。

(五) 系統管理人員在向使用者提供初始密碼時應注意確保其安全，避免使用電話、無保護之單據或電子郵件等，且使用者應立即更改初始密碼。

(六) 使用者帳號與密碼，避免與他人共用。如因系統限制而有多人共用同一帳號之情形，應考量其他控制措施，如記錄連線來源位址、設簿登記、密碼變更等。

(七) 透過網際網路使用管理帳號登入重要系統時，應採用多因子認證機制。

(八) 應用程式或服務所使用之帳號，應考量其他控制機制，如記錄登入來源位址、限制該帳號無法供人員使用。

二、 帳號與權限審查程序

(一) 為確保對存取資料和資訊服務進行有效控制，帳號管理人員應依《SO-MG-006_資訊設備帳號及管理權限程序》進行清查作業。

(二) 應用系統之帳號與權限清查作業，應函請各業務主管單位就所轄之應用系統，督促並追蹤各營業單位(分公司)，確實辦理清查並函覆清查結果。

(三) 帳號清查應包含應用系統、作業系統、資料庫及所有軟體。

(四) 每半年至少清查一次資通系統帳號與權限，呈權責單位部門主管覆核，以確保帳號權限之適切性。(客戶使用之帳號除外)

三、 特殊權限管理

(一) 依《SO-MG-006_資訊設備帳號及管理權限程序》進行特殊帳號申請與異動流程，以規範對特殊權限資訊系統與服務的存取授權。

(二) 特殊權限帳號，如具有資訊設備管理權限、特殊資料存取權限、其他系統資源控制權限及存取稽核軌跡之帳號，其使用應僅限於被授權核准之事項，並留存適當之稽核軌跡。

(三) 存取控制若透過 IC 卡、金鑰或鑰匙等，使用者應視同帳號，妥善保管，不可任意外借予他人使用。若有遺失時，應立即通報部門主管。

四、 密碼管理

(一) 為加強使用者之控管,除受限於系統特性外,任何使用者帳號均需輸入密碼,以進行使用者身分識別與鑑別之作業。

(二) 網域使用者帳號之密碼原則及相關作業管控詳請參照《SO-MG-001_網域密碼作業程序》。

(三) 所有帳號皆應套用密碼政策，應用程式或服務所使用之帳號可不在此限，但仍應加強管控。密碼政策如下所列：

1. 使用者於初次登錄時，應立即變更密碼。
2. 密碼長度之設定應不可少於八個字元。
3. 密碼設定應包含數字及英文，或宜包含特殊字元(例如：#$%^&*()-_=+等)、英文大小寫等。
4. 密碼至少每九十天更改一次。
5. 變更後之新密碼三次內不得連續重複。
6. 密碼禁止以明碼方式註明於說明欄位。
7. 密碼三十分鐘內累計錯誤三次即予以暫禁(Suspend)；若使用者因累計次數超過上限而被暫禁，須依《CIS 需求申請單》申請密碼重置才可再行登入。
8. 若該資訊設備或系統無法以強制方式進行上述設定之檢查或自動執行變更，帳號管理人員應告知提醒使用者自行依規定變更，否則系統設定應從嚴制訂。
9. 密碼最短使用期限不得小於 1 天(即需於隔天方可變更)。
10. 若受限於系統特性，無法以強制方式進行上述密碼政策之設定或自動執行變更，應考量補償性控制，如實體門禁、限制存取路徑或作業系統層級之密碼保護等。

11. 密碼在輸入、遞交與保存皆須採取保護機制，如加密、雜湊或使用密封之密碼函，並應避免使用無保護之單據或明文電子郵件傳送密碼。

12. 若以緊急密碼函控管最高權限帳號之密碼者，應建立緊急密碼函之管理程序。

13. 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）或簡易之帳號密碼及未設管理者存取權限。

14. 客戶申請採電子式交易型態者，公司以電子方式交付電子密碼條時，應傳送 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，此流程相關系統紀錄應留存。

五、 系統稽核

(一) 資訊資產保管者對於各項資訊設備，應評估其系統安全稽核需求，並據以啟動並記錄其稽核軌跡，並依不同功能系統或網路應有資訊資產保管者定期或配合稽核軌跡之產生時機，覆核並對於異常事件並加以追蹤調查。正式營運環境之稽核軌跡的設定可包括至少下列各項：

1. 使用者帳號與群組的新增/修改/刪除。
2. 使用者登出入日期與時間。
3. 更換身份為超級使用者 (root)。
4. 違反規定之作業，如連續錯誤簽入次數大於上限、未經授權存取機要目錄。
5. 特殊權限帳號之異動及該帳號執行之成功及失敗存取記錄。
6. 程式原始碼的存取或異動。
7. 應用系統程式變更、換版或上線。
8. 系統程式變更、換版或上線。
9. 系統故障。
10. 網路設備設定之異動。

(二) 對核心關鍵系統（如證券交易系統、網路下單系統等）之稽核日誌記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。

(三) 上述核心關鍵系統(應用系統、作業系統、資料庫、網路設備等)之電腦稽核紀錄，應定期接受專責人員檢視。

(四) 應保護系統稽核軌跡，以免受到未經授權的修改，應考慮以下措施：

1. 限制僅有相關工作上或業務上之需求者，始能經過適當的授權程序，查閱稽核軌跡。
2. 應即時將稽核追蹤資料檔案備份到難以更改之中央伺服器或媒體。

3. 稽核軌跡之查閱應只限於資料的唯讀存取，如果不能以唯讀方式進行稽核軌跡存取時，應複製另外一份系統檔案供使用，且使用結束時，應予以其清除。

(五) 系統稽核軌跡應至少保留三年，並應保護以免受到非法更改和刪除。

(六) 有涉及蒐集、處理、利用個人資料之資訊系統，其系統稽核軌跡應至少保留五年。

(七) 對國內外交易之所有必要紀錄，應至少保留五年。但法律另有較長保存期間規定者，從其規定。

(八) 稽核軌跡(Log)處理過程、處理權責、規範異常通報流程與應變處理方針等，詳細作業辦法請參照《SO-06-011_軌跡留存作業程序》。

六、 鐘訊同步

(一) 為確保稽核日誌的準確性，應使用自動化時間同步工具對時，無法自動化時間同步之資訊設備(如錄影設備或未連線之伺服器)，如在台灣地區依照中原標準時間由資訊資產保管者至少每半年進行人工對時乙次。

七、 技術脆弱性管理

資訊設備保管者應適時取得使用中資訊系統已公布之技術脆弱性之資訊，或每半年至少執行一次弱點掃描，評估是否應採取適當的措施，以處理所面臨之風險。必要時可聘請外部專家或顧問，協助進行資訊系統之安全及弱點評估。

第二節　測試環境系統存取管理(有個資風險的系統)

一、 使用者帳號及權限管理

(一) 使用者帳號與密碼，避免與他人共用。如因系統限制而有多人共用同一帳號之情形，應考量其他控制措施，如記錄連線來源位址、設簿登記、密碼變更等。

(二) 使用者與第三方所保管之帳號及權限應於人員離(調)職或合約終止時予以調整、停用或刪除。

(三) 測試環境系統之帳號及特殊權限審查機制：

每半年由資訊設備保管者檢查測試環境中委外廠商人員是否持有最高權限之帳號，以預防委外廠商人員於測試環境中擁有最高權限進行系統資源之存取。

二、 密碼管理

(一) 為加強使用者之控管，除受限於系統特性外，任何使用者帳號均需輸入密碼，以進行使用者身分識別與鑑別之作業。

(二) 所有帳號其密碼長度不可少於 6 個字元，應用程式或服務所使用之帳號不在此限，但仍應加強管控。

(三) 密碼禁止以明碼方式註明於說明欄位。

(四) 若受限於系統特性，無法以強制方式進行上述密碼政策之設定，應考量補償性控制，如實體門禁、限制存取路徑或作業系統層級之密碼保護等。

三、 鐘訊同步

(一) 應使用自動化時間同步工具對時，無法自動化時間同步之資訊設備，應由資訊資產保管者至少每半年對時一次，並留存相關紀錄。

第七章 個人資料外洩防護機制作業內容

一、 依「個人資料保護法」針對保有個人資料之資通系統建立個人資料外洩防護機制，管制個人資料檔案透過輸出入裝置、通訊軟體、系統操作複製至網頁或檔案等方式傳輸，並應留存相關紀錄、軌跡及證據，妥善處理客戶及公司內部人個人資料。

二、 公司每年定期依「個人資料保護法」定義之個人資料管理情形執行稽核。

三、 本公司個人資料更新、更正或註銷均應報經備查，並將更新、更正、註銷內容、作業人員及時間詳實記錄。

四、 詳細個人資料外洩防護機制規範，請參照《SO-06-010_個資外洩防護管理作業程序》。

第八章 輸出文件記錄

無。