本會109年12月24日第13屆第3次理事會議討論通過
金管會110年7月19日金管銀國字第1100271542號函洽悉
本會110年8月26日第13屆第15次理監事聯席會議討論通過
本會111年11月24日第14屆第2次理監事聯席會議討論通過
金管會112年2月1日金管銀國字第1110234138號函洽悉

附件一

金融機構資通安全防護基準

第一條　中華民國銀行商業同業公會全國聯合會（以下簡稱本會）為確保金融機構資通系統具有一致性基本安全防護，特訂定本基準。

第二條　本基準用詞定義如下：

一、核心業務:由銀行依業務運作中斷對客戶影響數等風險評估結果予以決定，評估範圍如：存款業務、放款業務、匯款業務、外匯業務等。

二、核心資通系統：支持核心業務持續運作必要之系統或設備。

三、第一類電腦系統：直接提供客戶自動化服務或對營運有重大影響之系統(如電子銀行、分行櫃台、ATM 自動化服務、SWIFT 等系統)

四、第二類電腦系統：經人工介入以直接或間接提供客戶服務之系統(如作業中心、客戶服務等系統)

五、第三類電腦系統：未接觸客戶資訊或服務且對營運無影響之系統或設備(如人資、財會、總務等系統、物聯網設備)

六、連續假期：指國定假日加上週休二日，其中達三日以上者。

七、機敏資料：係指如登入帳號、固定密碼、重要參數、晶片金融卡基碼、憑證私鑰、個人資料及製卡個人化資料等。

第三條　資訊安全政策、內部組織及資產管理應符合下列要求：

一、資訊安全政策應經董事會、常務董事會決議或經其授權之經理部門核定。但外國銀行在臺分行應由其負責人簽署。

二、資訊安全相關要求應對所有員工及供應商公布或傳達。

三、應訂定資訊作業相關管理及操作規範。

四、應每年檢討資訊安全政策及前款管理及操作規範，並於發生重大變更（如新頒布法令法規）時審查，以持續確保其合宜性、適切性及有效性。

五、應依據作業流程，識別人員、表單、設備、軟體、系統等資產，建立資產清冊、網路架構圖、組織架構圖及負責人，並定期清點以維持其正確性。

六、應定義人員角色及責任並區隔相互衝突的角色。

七、應依據作業風險及專業能力選擇適當人員擔任其角色並定期提供必要教育訓練。

第四條　營運環境管理人員應符合下列要求：

一、應建立人員之註冊、異動及撤銷註冊程序，用以配置適當之存取權限；人員離調職時應儘速移除權限。

二、應列管硬體設備、應用軟體、系統軟體之最高權限帳號及具程式異動、參數變更權限之帳號。

三、應確認人員之身分及存取權限，必要時得限定其使用之機器或網路位

置（IP）。

四、人員超過十五分鐘未操作個人電腦時，應設定密碼啟動螢幕保護程式或登出系統。

五、除代登系統外於登入作業系統進行系統異動或資料庫存取時，應留存人為操作紀錄，並於使用後儘速變更密碼；但因故無法變更密碼者，應建立監控機制，避免未授權變更，並於使用後覆核其操作紀錄。

六、帳號應採一人一號管理，避免多人共用同一個帳號為原則，如有共用需求，申請及使用須有其他補強管控方式(如使用後更換密碼、代登入機制、密碼拆分保管等)，並留存操作紀錄且應能區分人員身分。

七、採用固定密碼進行身分確認者應符合下列要求：

（一） 訂定密碼檢核邏輯。

（二） 提供給人員使用之帳號於使用後三個月內應變更密碼。

（三） 提供給系統使用之帳號應採取適當之管控措施（如限制人工登入、監控告警）。

八、加解密程式或具變更權限之公用程式（如資料庫工具程式）應列管並限制使用，防止未經授權存取並保留稽核軌跡。

九、最高權限帳號使用時應先取得權責主管或授權人員同意並保留稽核軌跡。

十、具最高權限帳號、特殊功能(如程式或軟體異動、參數或組態變更權限等)權限帳號應和日常維運用帳號區隔，並定期抽查使用結果，以防範未經授權使用；如為核心資通系統，應於該等帳號被使用時，每日覆核使用結果。

十一、 提供網際網路服務之伺服器及 AD(網域服務)主機，對於最高權限帳號及特殊功能權限帳號，應採雙因子認證。

十二、 應針對核心資通系統、第一類及第二類電腦系統依最小權限(least privilege)及僅知原則(need-to-know)配發權限予人員使用並定期審查帳號、權限之合理性及異常存取紀錄，以符合職務分工及牽制原則。

第五條　個人資料保護應符合下列要求：

一、為維護所保有個人資料之安全，應採取下列資料安全管理措施：

（一） 訂定各類設備或儲存媒體之使用規範，及報廢或轉作他用時，應採取防範資料洩漏之適當措施。

（二） 針對所保有之個人資料內容，有加密之需要者，於蒐集、處理或利用時，採取適當之加密措施。

（三） 作業過程有備份個人資料之需要時，對備份資料予以適當保護。

二、保有個人資料存在於紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片、電腦、自動化機器設備或其他媒介物者，應採取下列設備安全管理措施：

（一） 實施適宜之存取管制。

（二） 訂定妥善保管媒介物之方式。

（三） 依媒介物之特性及其環境，建置適當之保護設備或技術。

三、為維護所保有個人資料之安全，應依執行業務之必要，設定相關人員接觸個人資料之權限及控管其接觸情形，並與所屬人員約定保密義務。

四、應針對核心資通系統及各類電腦系統確認所保有之個人資料進行風險評估及控管。

五、應針對核心資通系統及各類電腦系統建置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、應建立資料外洩防護機制，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網路檔案等方式傳輸，並應留存相關紀錄、軌跡及證據。

七、如刪除、停止處理或利用所保有之個人資料後，應留存下列紀錄：

（一）刪除、停止處理或利用之方法、時間。

（二）將刪除、停止處理或利用之個人資料移轉其他對象者，其移轉之原因、對象、方法、時間，及該對象蒐集、處理或利用之合法依據。

第六條　機敏資料隱密及金鑰管理，應符合下列要求：

一、如有下列情形者，應建立訊息隱密性機制：

（一）機敏資料儲存於使用者端操作環境。

（二）機敏資料於網際網路上傳輸。

（三）使用者身分確認資料（如固定密碼、設備資訊、生物特徵）儲存於系統內。

二、透過網際網路傳輸途徑辦理電子銀行之業務，其客戶身分確認資料如為固定密碼者，其固定密碼於儲存時應先進行不可逆運算（如雜湊演算法），另為防止透過預先產製雜湊值推測密碼，應進行加密保護或加入不可得知之資料運算；採用加密演算法者，其金鑰應儲存於經第三方認證並符合 NIST FIPS 140-2 L3 之硬體安全模組內並限制明文匯出功能。

三、於營運環境採用硬體安全模組保護金鑰者，該金鑰應由非系統開發及維護單位之二個單位以上產製並分持管理其產製之基碼單，另金鑰得以加密方式匯出至安全載具（如晶片卡）或備份至具存取權限控管之位置，供維護單位緊急使用。

四、應減少金鑰儲存之地點，並僅允許必要之管理人員存取金鑰，以利管理並降低金鑰外洩之可能性。

五、當金鑰使用期限將屆或有洩漏疑慮時，應進行金鑰替換。

六、機敏資料儲存於雲端服務業者，應遵循銀行公會所訂定之雲端服務相關自律規範辦理。

第七條　營運環境之實體安全應符合下列要求：

一、應避免主機房及異地機房同時在地震斷層帶、海岸線、山坡地、海平面下、機場飛航下、土石流好發區域、百年洪水氾濫區域、核災警戒範圍區域、工安高風險區域其中之一，並應有相關防護措施，以避免受到地震、海嘯、洪水、火災或其他天然或人為災難之損害。

二、應建立機房門禁管制，並將營運設備集中於機房內，以確保僅允許經授權人員進出；非授權人員進出應填寫進出登記，並由內部人員陪同及監督；進出登記紀錄應定期審查，如有異常應適當處置。

三、應於主機房及異地機房內建立全天候監視設備並確保監視人員操作範圍無死角。

四、應有足夠營運使用之電力、供水、用油等供應措施，當發生供應措施

中斷時，應至少維持七十二小時運作時間，並應介接二家以上網際網路電信營運商，或本地與異地二線以上互為備援。

五、油槽儲存及消防安全應符合相關法規規定。

六、應設置環境監控機制，以管理電信、空調、電力、消防、門禁、監視及機房溫濕度等，並自動告警及通知。

七、應具備與機房相當之操作環境，或獨立可管制人員操作系統及設備之監控室，該監控室應符合下列要求：

(一) 應具門禁及監視設備，且必須留存連線及使用軌跡，並定期稽核管理。

(二) 系統維運人員應經授權進入監控室使用監控室內專屬電腦設備；或應使用指定設備由內部網路以一次性密碼登入並經服務管控設備（如防火牆）使用監控室內專屬電腦設備。

(三) 連線過程須以內部網路、專線或虛擬私有網路進行。

(四) 監控室之網路設備及電腦設備應符合本基準相關規定。

第八條　營運管理應符合下列要求：

一、應評估避免於營運環境安裝程式原始碼，惟系統需具備程式原始碼，如：Python、SQL command 等方能運行之營運環境不在此限。

二、應建立定期備份機制及備份清冊，備份媒體或檔案應妥善防護，確保資訊之可用性及防止未授權存取。

三、應驗證備份資料之完整性、可用性及儲存環境的適當性。

四、應留存相關紀錄並建立適當保護機制及管理程序，相關紀錄至少留存一年。

五、應訂定系統安全強化標準，建立並落實系統安全設定。

六、應納管最高權限帳號，避免系統維護人員未經申請持用最高權限帳號辦理日常維護作業。

七、應加強連續假期之資安防護並符合下列要求：

(一) 應評估系統及電腦於連續假期開機必要性，如無必要則須關閉連線服務或電源。

(二) 應評估於連續假期結束後第一個營業日是否提前到班，以確保核心資通系統及第一類電腦系統正常運作。

第九條　核心資通系統、第一類電腦系統之營運環境容量管理應符合下列要求：

一、應依據資源使用狀況及容量需求，亦須考量軟體更新、生命週期、軟硬體運作相容性等因素，評估採用多重備援或冗餘配置(Redundancies)等方式，適時進行資源調整及擴充。

二、應定期評估核心資通系統是否有單點故障風險(Single Point of Failure)，並導入高可用性或高可靠度的措施（如 Active Active、Active Standby 或 Disaster Recovery），避免因單點故障造成整體異常之情形。

三、應依業務性質及設備功能等對核心資通系統訂定相關負載量要求，以強化系統穩定性，確保業務持續運作不中斷。

四、應針對核心資通系統特性、風險因素及所需效能，設定監控項目(如效能，容量空間，負載量、頻寬等)、規則(如警示種類)、程序或規範。

五、應定期將監控結果適時通知相關權責單位，於完成相關處理及應變

後，留存紀錄由權責單位核示。

第十條　脆弱性管理應符合下列要求：

一、應建立上網管制措施，限制連結非業務相關網站，以避免下載惡意程式。

二、應建立病毒偵測機制並定期更新病毒碼或建立白名單管控機制，以避免安裝未授權程式。

三、應隨時掌握資安事件，針對高風險或重要項目立即進行清查及應變。

四、應定期進行弱點掃描，並針對其掃描或測試結果進行風險評估，針對不同風險訂定適當措施及完成時間，填寫評估結果及處理情形，採取適當措施並確保作業系統及軟體安裝經測試且無弱點顧慮之安全修補程式。

五、應避免採用已停止弱點修補或更新之系統軟體及應用軟體，如有必要應採用必要防護措施。

六、應偵測惡意網站連結並定期更新惡意網站清單。

七、應建立入侵偵測或入侵防禦機制並定期更新惡意程式行為特徵。

八、應定期執行電子郵件社交工程演練及教育訓練。

九、應偵測釣魚網站，如有發現應採取必要措施。

十、應建立 DDoS 攻擊監控及事故應變機制，並每年進行程序演練或實際演練。

十一、應評估建置網頁應用程式防火牆(Web Application Firewall)。

十二、應偵測提供網際網路服務之系統其網頁與程式異動，記錄並通知相關人員處理。

十三、第一類電腦系統上線前及針對異動程式至少每半年進行程式碼掃描或黑箱測試，如無法進行前述掃描或測試者，應以人工執行程式碼檢核，並針對其掃描或測試結果進行風險評估，依據不同風險訂定適當措施及完成時間，執行矯正、記錄處理情形並追蹤改善。

第十一條　測試環境管理應符合下列要求：

一、應評估並辦理第十條第二款至第五款。

二、應避免同時共用不同環境(如營運環境、測試環境、辦公環境)之設備、憑證金鑰、資源存取帳密及使用者配置檔(User Profiles)。

三、應限制連接網際網路，如有需要應遵循銀行公會所訂定之相關電子銀行相關自律規範辦理。

第十二條　辦公環境管理應符合下列要求：

一、提供客戶使用之公用電腦管理

（一）應至少辦理第十條第一款及第二款。

（二）應限制可攜式儲存裝置介面存取(如 USB 埠)。

（三）應提醒避免瀏覽器留存客戶輸入資訊，並定期清理客戶留存資料(如帳號、cookie)。

（四）如有設定重新安裝或系統還原時，應先安裝安全修補程式，並更新病毒碼或建立白名單管控機制後，再開放使用。

二、開放網際網路連線使用之視訊會議使用管理

（一）應適時更換視訊會議代碼或密碼，避免重複使用。

（二）機敏性會議應採用高強度密碼或多因子進行身分驗證。

（三）應確認與會者身分後再進行會議，以確保會議內容不外流。

（四）應評估使用線上紀錄功能，避免會議內容外洩風險。

（五） 參加會議時應關閉非必要功能，注意發送及分享資訊，避免機敏資料外洩

三、 異地辦公之 VPN 使用管理

（一） 應將 VPN、網路基礎架構設備之主機更新至最適版本，並使用安全設定。

（二） 應提醒用於連入遠端作業環境之主機，應先安裝安全修補程式、更新病毒碼後再進行連線。

（三） 應確認 IT 及資安人員已完成準備，包含日誌檢視、攻擊偵測、事件應變及事件復原機制。

（四） 應採用高強度密碼或多因子進行身分驗證。

（五） 應確認 VPN 資源足以應付大量使用，若情況允許，可以透過設定流量管制，以讓有高流量需求的員工有充足的資源能夠使用。

四、 異地辦公之虛擬桌面(VDI)使用管理

（一）應針對伺服器及虛擬桌面軟體進行妥善設定，避免員工可以將虛擬桌面連接到本機印表機印出檔案內容，透過虛擬桌面存取本機主機檔案，連接可卸除裝置或透過剪貼簿於兩端剪貼資料。

（二）應適時進行軟體更新以修補最適漏洞，並向員工宣導不應安裝可疑程式避免中毒。

（三）應設定虛擬桌面在一段閒置時間後將螢幕鎖定或中斷連線，以免遭到被入侵之本機主機操控。

（四）應禁止員工使用自動抓取關鍵字之鍵盤軟體，以免機敏資訊外洩。

（五）應採用高強度密碼或多因子進行身分驗證。

（六）建議使用全硬碟加密機制或限制下載，以防止虛擬桌面之檔案遭誤存於本機裝置中。

第十三條　網路管理應符合下列要求：

一、 網路應區分網際網路、非武裝區（Demilitarized Zone；以下簡稱 DMZ）、營運環境及其他（如內部辦公區）等區域，並使用防火牆進行彼此間之存取控管。機敏資料僅能存放於安全的網路區域，不得存放於網際網路及 DMZ 等區域。對外網際網路服務僅能透過 DMZ 進行，再由 DMZ 連線至其他網路區域。

二、 系統僅得開啟必要之服務及程式，使用者僅能存取已被授權使用之網路及網路服務。內部網址及網路架構等資訊，未經授權不得對外揭露。

三、 防火牆及具存取控制（Access control list，ACL）網路設備，應遵循下列措施：

（一） 應定期檢視參數設定。

（二） 應檢視所開啟的通訊埠與業務需求相符。

（三） 應每半年檢視 DMZ 之防火牆規則。

（四） 應定期檢視高風險設定及六個月內無流量之防火牆規則評估其必要性及風險。

（五） 應針對已下線系統於半年內調整或停用防火牆規則。

四、 使用遠端連線進行系統管理作業時，應使用加密通訊協定，並不得

將密碼紀錄於工具軟體內。

五、經由網際網路連接至內部網路進行遠距之系統維護管理工作，應遵循下列措施：

（一）應建立授權機制，依據其申請項目提供必要授權。

（二）應定義允許可連結之遠端設備，並確保已安裝必要資訊安全防護。

（三）應加強變更作業之身分認證，於每次登入時得採用照會或二項以上安全設計並取得主管授權，惟緊急故障排除仍須於事後向主管核備。

（四）應建立監控機制，留存操作紀錄，並由主管或獨立單位定期覆核

六、提供員工經由外部網際網路連線使用之應用系統，應遵循下列措施：

（一） 應定期執行弱點掃描、滲透測試及程式原始碼掃描並盡速完成弱點修補。

（二） 建立網頁防竄改機制並將該等系統納入監控範圍。

（三） 確保委外廠商交付之系統或程式無惡意程式及後門程式。

第十四條　系統生命週期管理應符合下列要求：

一、應訂定資訊系統開發設計規範並落實執行。

二、應監督委外開發之應用軟體，並確保其有效遵循本基準規定。

三、應確保系統軟體和應用軟體安裝最適安全修補程式。

四、應針對系統架構重大變更或異動時，訂定復原程序，並於上線前進行程序演練或實際演練。

五、應分別從技術、功能、情境等建立測試案例並進行端點對端點測試。

六、對於測試用之機敏資料，應先進行資料遮蔽處理或管制保護。

七、於開發階段起至營運階段，應遵循變更控制程序處理並留存相關紀錄；營運環境變更（如執行、覆核）應由二人以上進行，以相互牽制。

八、系統軟硬體變更應先進行技術審查並測試；套裝軟體不應自行異動，並應先進行風險評估。程式不應由開發人員自行換版或產製比對報表，應建立程式原始碼管理機制，以符合職務分工及牽制原則。

第十五條　核心資通系統與第一類電腦系統中個人網路銀行、企業網路銀行、行動銀行、ATM 自動化服務、分行櫃台及 SWIFT 之系統轉換、架構重大調整或跨版本升級前，應符合下列要求：

一、系統轉換前之準備工作：

轉換前關鍵準備工作，如：架構審查、上線變更審查及風險評估、上線協調會議等具資安控制性之事項，應請資安專責單位參與，並由資安長發揮統籌資安政策推動與資源調度之工作。

（一） 應建立架構審查機制，從 AP、DB、資安、網路、平台、營運等面向進行評估，並評估一次過版或平行運轉可行性。

（二） 應檢視相關設備容量，評估營運及業務需求所需備載容量（如跨行交易平台、企業應用系統整合 EAI、企業服務匯流排 ESB 等）。應建置擬真測試環境，測試新系統或功能相容於既

有營運環境之架構、設備及參數。

（三） 應檢視各項測試個案，依據影響範圍進行功能測試(如單元、整合、迴歸等）及非功能測試(如壓力、相容等)，並進行整體性演練。

（四） 應建立上線及復原計畫，並建立多個檢核點及啟動復原之決策條件。

（五） 應進行上線變更審查及風險評估，辨識複雜度及影響範圍，檢視測試個案及上線復原計畫之完整性。

（六） 應要求廠商上線支援，並能緊急提供備品、更高容量設備、問題查找及修改人力。

（七） 應預留復原作業及上線驗證時間。

（八） 應召開上線協調會議，安排工作項目並確保各項準備到位。

（九） 應提前公告，佈署足夠客服資源並進行教育訓練(含異常話術)。

二、 系統轉換作業：

（一） 成立指揮中心，逐步執行上線計畫，檢視每一個檢核點，必要時召開復原決策會議。

（二） 執行系統及資料備份，以因應復原時所需。

（三） 驗證各項變更作業，確保如預期結果。

（四） 驗證各項資料內容，確保資料完整性。

（五） 逐步啟動各項作業並監控網路及系統，確保提供足夠資源。

三、 系統轉換後之事件管理：

（一） 持續系統監控，確保資料正確、功能正常、系統穩定。

（二） 落實事故應變，以消費者權益及持續營運優先處理。

（三） 成立應變小組，集中管理問題並適時調配各單位資源。

（四） 追蹤問題根因，提出短中長期改善方案並持續追蹤。

第十六條　資訊安全事故管理應符合下列要求：

一、應將各作業系統、網路設備、資安設備之日誌，及稽核軌跡集中管理，進行異常紀錄分析，設定合適告警指標並定期檢討修訂。

二、應建立資訊安全事故通報、處理、應變及事後追蹤改善作業機制，並應留存相關作業紀錄；另應定期辦理演練，以確保資安事故發生時相關通報、處理及應變作業之有效性。

三、如有資訊安全事故發生時，其系統交易紀錄、系統日誌、安全事件日誌應妥善保管，並應注意處理過程中軌跡紀錄及證據留存之有效性。

第十七條　營運持續管理應符合下列要求：

一、應進行營運衝擊分析，定義最大可接受系統中斷時間，設定系統復原時間及資料復原時點，並考量下列因素，採取必要備援機制：

（一） 應考量如有系統復原時間限制狀況下，必要時建立同地或異地備援機制(Disaster Recovery；DR)。

（二） 應評估單點故障(Single Point of Failure)風險，必要時導入高可用性或高可靠度的措施（如 Active Active、Active Standby），避免造成整體服務中斷之情形。

（三） 應依業務性質及設備功能等對系統訂定相關負載量要求並進行妥適監控，以強化系統穩定性，確保業務持續運作不中

斷。

（四） 應監控批次作業(如監控資源使用情況並應注意是否已執行完成所有作業程序，以避免影響正常交易)。

二、應建立對於重大資訊系統事件或天然災害之應變程序，並確認相對應之資源，以確保重大災害對於重要營運業務之影響在其合理範圍內。

三、應每年驗證及演練其營運持續性控制措施，以確保其有效性，並應保留相關演練紀錄及召開檢討會議。

四、如遇尖峰作業、大量活動(如支付)或例行業務處理量較大(如撥薪)等時段，應特別注意各類異常情形之監控並加強檢核系統資源，俾事先提出因應措施。

第十八條　法令遵循管理應符合下列要求：

一、應盤點與資訊安全相關法規規定，並將相關資訊安全要求與內部控制制度結合，定期進行法令遵循自評，以確保資訊安全之法令遵循性。

二、應透過內部控制制度進行定期檢核，並應於每年依據銀行公會所訂定之資訊安全評估相關自律規範，提出電腦系統資訊安全評估報告。

第十九條　本基準經本會理事會通過並函報金融監督管理委員會核備後實施，修正時亦同。