票據交換所個人資料檔案安全維護計畫標準辦法草案

條文	說明
第一章　總則	第一章章名
第一條　本辦法依個人資料保護法（以下簡稱本法）第二十七條第二項及第三項規定訂定之。	本辦法之法源依據。
第二條　票據交換所應訂定個人資料檔案安全維護計畫（以下簡稱本計畫），以落實個人資料檔案之安全維護與管理，防止個人資料被竊取、竄改、毀損、滅失或洩漏。 本計畫之內容應包括第四條至第二十七條規定之相關組織及程序。	一、指定票據交換所應訂定相關安全維護計畫，以建立並執行相關管理程序或機制。 二、本辦法規定之相關組織及程序要求，票據交換所應明定於安全計畫內。
第三條　本辦法用詞定義如下： 一、個人資料管理代表：由票據交換所主任委員擔任，或由主任委員直接授權，負責督導本計畫之規劃、訂定、執行、修訂及相關決策之人員。 二、個人資料內評代表：由票據交換所主任委員授權，負責督導相關內評人員評核本計畫之執行成效之人員。 三、所屬人員：執行業務之過程必須接觸個人資料之人員，包括票據交換所之定期或不定期契約人員及派遣員工。	一、為使個人資料檔案安全維護管理組織有效運作，該組織必須有一名負責督導本計畫之規劃、訂定、執行、修訂及相關決策之個人資料管理代表。 二、票據交換所為確保本計畫之落實，應有相關內評人員負責於內部評核本計畫落實之狀況，而個人資料內評代表則負責督導統整相關評核之結果。 三、為確保個人資料檔案之安全維護，凡執行業務之過程必須接觸個人資料之人員，包括票據交換所之定期或不定期契約人員及派遣員工，均應依本計畫之相關程序，執行本計畫。
第四條　票據交換所應建立個人資料檔案安全維護管理組織，並配置相當資源，負責本計畫相關程序之規劃、訂定、執行與修訂等任務。 個人資料檔案安全維護管理組織之成員應包括個人資料管理代表與個人資料內評代表。 個人資料管理代表非由主任委員擔任時，應定期就個人資料檔案安全維護	一、為有效訂定與執行本計畫，票據交換所應建立相關管理組織並投入相當資源辦理有關事項。 二、除個人資料管理代表外，該管理組織亦應有個人資料內評代表監督或評核本計畫是否落實執行。 三、個人資料管理代表非由主任委員擔任時，為使主任委員能盡其督導及監督之責，個人資料管理代表應定期向主任委

條文	說明
管理組織執行任務情形向主任委員提出書面報告。	員以書面報告相關事項。
第二章 一般程序	第二章章名
第五條　票據交換所應依其組織與事業特性訂定個人資料保護管理政策，提報董事會通過，並公開周知，使其所屬人員均明確瞭解及遵循。 前項管理政策至少應包括下列事項之說明： 一、遵守我國個人資料保護相關法令規定。 二、以合理安全之方式，於特定目的範圍內，蒐集、處理及利用個人資料。 三、以可期待之合理安全水準技術保護其所蒐集、處理、利用之個人資料檔案。 四、設置聯絡窗口，供個人資料當事人行使其個人資料相關權利或提出相關申訴與諮詢。 五、規劃緊急應變程序，以處理個人資料被竊取、竄改、毀損、滅失或洩漏等事故。 六、如委託蒐集、處理及利用個人資料者，應妥善監督受託機關。 七、持續維運本計畫之義務，以確保個人資料檔案之安全。	一、為使票據交換所所屬人員對於個人資料之保護能有所體認，進而能落實本計畫，故票據交換所應訂定個人資料保護管理政策，將本計畫相關重點事項於政策內闡明。為達上述目的，該等政策應加以公開周知，且提報其董事會通過，以明示保護個人資料之旨。 二、政策相關重點事項包括：遵守我國個人資料保護相關法令規定、合法正當蒐集、處理及利用個人資料；應以適當之技術保護個人資料；應提供當事人行使權利之方式；規劃緊急應變程序以處理事故；監督受託機關之責任；持續維運本計畫之義務。
第六條　票據交換所應定期檢視應遵循之個人資料保護法令，並據以訂定或修訂本計畫。	一、票據交換所因其特性及其所蒐集、處理、利用之個人資料範圍之不同與變動，其所應適用之個人資料保護法令亦可能有所不同，為符合法令之規定，自應依據其自身狀況清查適用之個人資料保護相關法令。 二、個人資料保護相關法令規定，因時事變遷而有隨之變更之可能，票據交換所自應定期檢視該等法令，配合修訂其安全維護計畫。

條文	說明
第七條　票據交換所應依個人資料保護法令，清查所保有之個人資料，界定其納入本計畫之範圍並建立清冊，且定期確認其變動情形。	依本法施行細則第十二條第二項第二款之規定，安全維護計畫中得就界定個人資料範圍相關事項加以規定，爰明定票據交換所應清查個人資料之種類與數量並建立清冊，方能有效對其所保有之個人資料加以保護。
第八條　票據交換所應依據前條界定之個人資料範圍及其相關業務流程，分析可能產生之風險，並依據風險分析結果，訂定適當管控措施。	依本法施行細則第十二條第二項第三款之規定，安全維護計畫得就個人資料之風險評估及風險管理加以規定，爰明定票據交換所應依據其相關業務流程，判斷於蒐集、處理及利用之過程中，個人資料安全可能發生之風險，以及其風險性之高低，方能進一步以適當之方式保護個人資料並降低其風險。
第九條　票據交換所為因應其保有之個人資料被竊取、竄改、毀損、滅失或洩漏等事故，應就下列事項建立相關程序： 一、採取適當之應變措施，以降低或控制事故對當事人之損害。 二、查明事故之狀況並適時通知當事人。 三、避免類似事故再次發生。	一、發生個人資料被竊取、竄改、毀損、滅失或洩漏等事故時，常造成資料當事人財產及非財產上之損害，票據交換所應訂定相關之因應機制，以降低或控制損害。 二、事故應變之首要目標即根據事故之類型，採取應變措施以降低或控制損害。其次，應讓當事人瞭解相關狀況，使當事人亦能採取相關措施防止損害發生或擴大。最後，避免類似事故再次發生亦為應變措施之重點。
第三章 法令遵循程序	第三章章名
第十條　票據交換所為確保個人資料之蒐集符合個人資料保護相關法令要求，應就下列事項建立相關程序： 一、確認蒐集個人資料之特定目的。 二、確認具備法令所要求之特定情形或其他要件。	依本法第十九條第一項規定，蒐集個人資料應有特定目的並具備一定之法定情形，而若其他法令有特別要求，亦應遵守之，故應建立相關程序以確認之。
第十一條　票據交換所為遵守本法第八條及第九條有關蒐集個人資料之告知義務規定，應就下列事項建立相關程序： 一、確認是否得免告知。 二、除確認無須告知者外，應依據資料	依本法第八條及第九條規定，票據交換所應適時履行告知義務，故除確認有例外情況無須告知外，均應依據資料蒐集之情況，採取適當之告知方式，以有效履行告知義務。

條文	說明
蒐集之情況，採取適當之告知方式。	
第十二條　票據交換所為確保個人資料之利用符合個人資料保護相關法令要求，應就下列事項建立相關程序： 一、確保個人資料之利用符合特定目的。 二、確認是否得進行及如何進行特定目的外利用。	依本法第二十條第一項規定，個人資料應於蒐集之特定目的必要範圍內利用，但具備一定之法定情形，得為目的外之利用。因此應建立一定程序，以確保資料之利用符合特定目的。若有必要為特定目的外利用時，亦應確認其是否合法，及特定目的外利用之相關情事。
第十三條　票據交換所新增或變更特定目的時，應依下列程序為之： 一、依第十一條規定之程序為之。 二、取得當事人書面同意，但法令另有規定者，不在此限。	前條規定票據交換所於法定情形，得就其保有之個人資料為特定目的外之利用，惟該條規定乃針對個別情況下得否及如何為特定目的外之利用。若票據交換所欲繼續性地對於其所保有之個人資料進行特定目的之新增或變更時，應先依相關告知義務之程序為之。其次，除法令別有規定外，原則上應取得當事人之書面同意，方能為特定目的之新增或變更。
第十四條　票據交換所針對本法第六條之特種個人資料，應就下列事項建立相關程序： 一、確認其蒐集、處理及利用之個人資料是否包含特種個人資料。 二、確保其蒐集、處理及利用特種個人資料，符合相關法令之要求。	依本法第六條規定，非公務機關原則上不得蒐集、處理及利用醫療、基因、性生活、健康檢查及犯罪前科之個人資料。故票據交換所應先建立程序以確認是否有蒐集相關特種個人資料。如有蒐集時，並應確保蒐集、處理及利用特種個人資料，符合相關法令之要求。
第十五條　票據交換所進行個人資料國際傳輸前，應確認是否受中央銀行限制並遵循之。	依本法第二十一條規定，中央目的事業主管機關於一定之法定情形，得限制非公務機關對於個人資料進行國際傳輸，爰明定票據交換所應於傳輸前確認主管機關中央銀行是否有所限制，並加以遵守之。
第十六條　票據交換所為提供個人資料當事人行使本法第三條規定之權利，應就下列事項建立相關程序： 一、如何提供當事人行使權利。 二、確認當事人身分。 三、確認是否有本法第十條及第十一條得拒絕當事人行使權利之情況。	一、依本法第三條規定，當事人就其個人資料得行使包含查詢或請求閱覽等五項權利，且非公務機關除有本法第十條但書及第十一條第二項但書、第三項但書規定情形，應於本法第十三條規定期間內准駁當事人之請求，爰明定票據交換所應建立相關程序以供資料當事人行

條文	說明
四、適時准駁當事人請求。	使權利。 二、為確保當事人行使權利，應提供一定方式，如常設之聯絡窗口，包含聯絡電話或聯絡之電子郵件信箱等，即為首要之程序。 三、為避免資料不當提供給第三人或不當刪除，票據交換所提供當事人行使權利前，應先建立程序以確認當事人身分。
第十七條　票據交換所為確認其保有個人資料之正確性，應就下列事項建立相關程序： 一、確保資料於處理過程中，正確性不受影響。 二、當確認資料有錯誤時，應適時更正。 三、定期檢查資料之正確性。 因可歸責於票據交換所之事由，未為更正或補充之個人資料，應訂定於更正或補充後，通知曾提供利用對象之程序。	一、票據交換所所保有之個人資料之正確性，攸關其是否能有效利用當事人之個人資料以提供當事人相關服務，並避免當事人發生因資料不正確所產生之損害。因此票據交換所應建立程序，確保資料於處理過程中不會發生錯誤，若資料仍有錯誤之情況，應適時更正，且應定期檢查資料之正確性。 二、若票據交換所曾提供其保有之個人資料予他人，且因可歸責於票據交換所之事由未更正或補充，致使個人資料不正確時，自應負責更正或補充個人資料後，通知曾提供利用該資料之對象，以使該不正確之資料能即時更新，避免當事人權益受損，爰參酌本法第十一條第五項，訂定第二項。
第十八條　票據交換所應定期確認其所保有個人資料之特定目的是否消失，或期限是否屆滿，若特定目的消失或期限屆滿時，應遵守本法第十一條第三項規定。	票據交換所蒐集、處理或利用個人資料均應於特定目的必要範圍內為之，若蒐集、處理、利用個人資料之特定目的已消失或期限已屆滿，則應遵守本法第十一條第三項之規定，加以刪除或停止處理利用。
第四章 安全管理措施	第四章章名
第十九條　為防止個人資料發生被竊取、竄改、毀損、滅失或洩漏等遭受侵害之情事，票據交換所應依據業務性質、個人資料存取環境、個人資料種類與數量及個人資料傳輸工具與方法等因素，採取第二十條至第二十三條之管理措施。	一、對於個人資料之保護，除於組織面給予整體規劃，及法令遵循程序之設計外，尚應考慮安全管理措施之部分，而如何規劃安全管理措施，則票據交換所應綜合考量本身之業務性質、個人資料存取環境、個人資料種類與數量及個人資料

條文	說明
	傳輸工具與方法等因素。 二、安全管理措施可分為人員管理、作業管理、物理環境管理、技術管理之不同要求，第二十條至第二十三條將分別針對上述要求加以規定。
第二十條　票據交換所應採取下列人員管理措施： 一、指定蒐集、處理及利用個人資料個別作業（以下簡稱「作業」）流程之負責人員。 二、就個別作業設定所屬人員不同之權限並控管之，以一定認證機制管理其權限，且定期確認權限內容設定之適當與必要性。 三、要求所屬人員負擔相關之保密義務。	一、針對人員管理之部分，首先應先確認實際進行個人資料之蒐集、處理及利用之負責人員為何，方可確認相關管理程序之權責歸屬。 二、票據交換所所屬人員與個人資料相關之各項作業，若有設定權限控管之必要，則應以一定認證機制管理之，並確認其權限設定是否適當或必要。避免人員取得不適當之權限，得以接觸非於作業必要範圍內之個人資料。 三、票據交換所應要求其所屬人員負擔相關之保密義務，使所屬人員能明瞭其責任，必要時亦可以訂定契約條款之方式為之，以作為相關權責之紀錄。
第二十一條　票據交換所應採取下列作業管理措施： 一、訂定蒐集、處理及利用之作業注意事項。 二、運用電腦及相關設備處理個人資料時，應訂定使用可攜式儲存媒體之規範。 三、儲存個人資料時，確認是否有加密之必要，如有必要，應採取適當之加密機制。 四、傳輸個人資料時，因應不同之傳輸方式，確認是否有加密之必要，如有必要，應採取適當之加密機制，並確認資料收受者之正確性。 五、應依據其保有資料之重要性，評估個人資料是否有備份必要，如有必要，應予備份。對於備份資料應確	一、針對個人資料蒐集、處理及利用的個別相關作業，票據交換所應基於本計畫之原則規定，訂定具體之作業注意事項，使所屬人員有所依循。 二、使用可攜式儲存媒體，可能提高處理個人資料之電腦及相關設備遭受惡意程式攻擊及個人資料外洩之風險，因此若有使用可攜式儲存媒體之情況，應訂定相關使用規範。 三、針對個人資料處理之不同態樣，包括儲存、傳輸及備份之狀況，如資料有加密之必要，即應採取適當之加密機制。 四、於傳輸個人資料之情況，除有必要時採取加密機制，並應確認資料收受者之正確性，以避免資料不當外洩。 五、針對有備份必要之個人資料，除有必要時採取加密機制，儲存備份資料之媒體

條文	說明
認是否有加密之必要，如有必要，應採取適當之加密機制，儲存備份資料之媒體，亦應以適當方式保管，且定期進行備份資料之還原測試，以確保備份之有效性。 六、儲存個人資料之媒體於廢棄或移轉與他人前，應確實刪除媒體中所儲存之資料，或以物理方式破壞之。 七、妥善保存認證機制及加密機制中所運用之密碼，如有交付他人之必要，亦應妥善為之。	亦應以適當方式保管，且定期進行備份資料之還原測試，以確保備份之有效性。 六、儲存個人資料之媒體於廢棄或移轉與他人前，應確實刪除媒體中所儲存之資料，或以物理方式破壞之，以避免資料不當外洩。 七、如作業程序中相關認證機制與加密機制有運用密碼之必要時，該密碼亦應妥善加以保存。
第二十二條　票據交換所應採取下列物理環境管理措施： 一、依作業內容之不同，實施必要之門禁管理。 二、妥善保管個人資料之儲存媒體。 三、針對不同作業環境，建置必要之防災設備。	在實體之物理環境管理方面，票據交換所亦應針對不同之作業內容、作業環境及個人資料之種類與數量，實施必要之門禁管理，以適當方式或場所保管個人資料之儲存媒體，並建置必要之防災設備。
第二十三條　票據交換所利用電腦或相關設備蒐集、處理或利用個人資料時，應採取下列技術管理措施： 一、於電腦、相關設備或系統上設定認證機制，對有存取個人資料權限之人員進行識別與控管。 二、認證機制使用帳號及密碼之方式時，使其具備一定安全之複雜度並定期更換密碼。 三、於電腦、相關設備或系統上設定警示與相關反應機制，以對不正常之存取為適當之反應與處理。 四、對於存取個人資料之終端機進行身分認證，以識別並控管之。 五、個人資料存取權限之數量及範圍，於作業必要之限度內設定之，且原則上不得共用存取權限。 六、採用防火牆或路由器等設定，避免	一、票據交換所若利用電腦或相關設備蒐集、處理或利用個人資料時，針對相關電腦系統技術，亦應有相應之管理措施，本條即臚列相關技術管理措施，供票據交換所視其實際作業之必要予以實施。 二、本條所臚列之技術管理措施約可分為： （一）系統存取權限之設定及實施：以認證機制，對有存取個人資料權限之人員進行識別與控管，若認證機制使用密碼之方式時，並應有適當之管理方式，並定期測試權限機制之有效性（第一款至第四款、第八款）。 （二）系統存取權限之控管：系統存取權限之設定應於必要範圍內為之，避免非作業必要之人員得存取相關資料，增加個人資料不當外洩之風

條文	說明
儲存個人資料之系統遭受無權限之存取。 七、使用可存取個人資料之應用程式時，確認使用者具備使用權限。 八、定期測試權限認證機制之有效性。 九、定期檢視個人資料之存取權限設定正當與否。 十、於處理個人資料之電腦系統中安裝防毒軟體，並定期更新病毒碼。 十一、對於電腦作業系統及相關應用程式之漏洞，定期安裝修補之程式。 十二、定期瞭解惡意程式之威脅，並確認安裝防毒軟體及修補程式後之電腦系統之穩定性。 十三、具備存取權限之終端機不得安裝檔案分享軟體。 十四、測試處理個人資料之資訊系統時，不使用真實之個人資料，如使用真實之個人資料時，應明確規定其使用之程序。 十五、處理個人資料之資訊系統有變更時，應確認其安全性並未降低。 十六、定期檢查處理個人資料之資訊系統之使用狀況及個人資料存取之情形。	險。且應定期檢視存取權限之必要性及是否需要調整（第五款、第九款）。 （三）採用防火牆或路由器等設定，避免儲存個人資料之系統遭受無權限之存取（第六款）。 （四）存取個人資料之應用程式之控管（第七款）。 （五）避免惡意程式與系統漏洞對作業系統之威脅（第十款至第十二款）。 （六）檔案分享軟體之控制（第十三款）。 （七）系統測試時，使用個人資料之程序（第十四款）。 （八）資訊系統變更時，其安全性之確認（第十五款）。 （九）檢查系統之使用狀況與個人資料存取之情形（第十六款）。
第五章 認知宣導及教育訓練	第五章章名
第二十四條　票據交換所應對所屬人員施以認知宣導及教育訓練，使其明瞭個人資料保護相關法令之要求、所屬人員之責任範圍及各種作業程序。	為落實執行本計畫相關管理程序，票據交換所應透過認知宣導及教育訓練使所屬人員均能明瞭個人資料保護相關法令之要求、所屬人員之責任範圍及各種作業程序。
第六章 計畫稽核及改善程序	第六章章名
第二十五條　票據交換所為確保本計畫之有效性，應定期檢查本計畫是否落實執行。	本計畫及依據本計畫所訂定之相關程序，票據交換所所屬人員是否皆已落實執行，必須通過一定之檢查機制方能確定。

條文	說明
第二十六條　為持續改善本計畫，票據交換所應建立下列程序： 一、本計畫發生未落實執行時之改善程序。 二、本計畫有變更時之變更程序。	一、於前條檢查過程中，若發現有未落實執行之情況，票據交換所應建立程序，協助相關所屬人員加以改善。 二、若本計畫有窒礙難行或因應法令之增修，而有變更之需要時，亦應有變更之相關程序。
第七章 紀錄機制	第七章章名
第二十七條　本計畫各項程序執行時，票據交換所至少應保存下列紀錄： 一、個人資料交付、傳輸之紀錄。 二、確認個人資料正確性及更正之紀錄。 三、提供當事人行使權利之紀錄。 四、個人資料刪除、廢棄之紀錄。 五、存取個人資料系統之紀錄。 六、備份及還原測試之紀錄。 七、所屬人員權限新增、變動及刪除之紀錄。 八、所屬人員違反權限行為之紀錄。 九、因應事故發生所採取行為之紀錄。 十、定期檢查處理個人資料之資訊系統之紀錄。 十一、教育訓練之紀錄。 十二、本計畫稽核及改善程序執行之紀錄。	為確認本計畫及依據本計畫所訂定之相關程序是否落實執行，以及釐清個人資料於蒐集、處理及利用過程之相關權責，票據交換所應保存相關紀錄以供查驗。
第八章 施行日期	第八章章名
第二十八條　本辦法自發布日施行。	本辦法施行日期。