財團法人二二八事件紀念基金會
個人資料檔案安全維護計畫

中華民國一百一十一年三月二十五日第十三屆第二次董事暨監察人會議訂定
內政部一百一十一年四月十五日台內民字第1110114858號函備查

壹、組織規模

一、組織型態：全國性民政財團法人。

二、財產總額：新臺幣1,540,000,000元整。

三、主事務所地址：臺北市中正區南海路54號。

四、代表人(負責人)：董事長。

五、法人成員人數：約21人。

貳、個人資料檔案之安全維護管理措施

一、配置管理之人員及相當資源：

(一)管理人員：

1、配置人數：1人。

2、職責：負責規劃、訂定、修正與執行計畫及經解散後個人資料處理方法等相關事項，並每年向代表人提出報告。

(二)預算：每年約新臺幣20萬元。

二、界定蒐集、處理及利用個人資料之範圍：

(一)特定目的：人事管理、辦理各項業務或相關法律關係事務。

(二)資料類別：依個人資料保護法第2條第1款規定，指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

三、風險評估及管理機制：

(一)風險評估

1、經由本法人內部使用電腦下載或外部網路入侵而外洩。

2、經由接觸業務書件而外洩。

3、員工故意竊取、竄改、毀損或洩漏。

(二)管理機制

1、藉由使用者代碼、識別密碼設定及文件妥適保管。

2、每90天進行網路資訊安全維護及控管。

3、電磁資料視實際需要以加密方式傳輸。

4、加強對本法人成員之管制及設備之強化管理。

四、事故之預防、通報及應變機制

(一)預防：

1、本法人成員如因工作職掌而須輸出、輸入個人資料時，均須鍵入其個人之使用者代碼及識別密碼，同時在使用範圍及使用權限內為之。

2、非承辦之人員參閱相關個人資料檔案或契約書類時應得本法人執行長或經授權之管理人員之同意。

3、個人資料於本法人內部或於外部互為傳輸時，應加強管控避免外洩。

4、加強員工教育宣導，並嚴加管制。

(二)通報及應變：

1、發現個人資料遭竊取、竄改、毀損、滅失或洩漏即向本法人執行長或經授權之管理人員通報，並立即查明發生原因及責任歸屬，依實際狀況採取必要措施，控制當事人損害。

2、對於個人資料遭竊取之本法人成員或其他被蒐集個人資料者，應儘速以適當方式通知使其知悉，並告知本法人已採取之處理措施及聯絡電話窗口等資訊。

3、針對事故發生原因研議改進措施，如主管機關進行實地檢查，應視檢查結果修正相關機制。

4、如遇有1千筆以上之個人資料事故，於發現後72小時內填具個人資料事故通報及紀錄表(格式如附件)並通報主管機關。

五、 個人資料蒐集、處理及利用之內部管理程序

(一)直接向當事人蒐集個人資料時，應明確告知以下事項：

1.法人名稱。

2.蒐集之目的及法律依據。

3.個人資料之類別。

4.個人資料利用之期間、地區、對象及方式。

5.當事人得請求閱覽、製給複製本、補充或更正、停止蒐集、處理、利用或刪除其個人資料。

6.當事人得自由選擇提供個人資料，如不提供時對其權益之影響。

(二)所蒐集非由當事人提供之個人資料，應於處理或利用前向當事人告知個人資料來源及前項應告知之事項。

(三)法人成員自本法人離職時，除因執行業務所必須或經當事人書面同意者，應主動刪除或銷毀，並留存相關紀錄。

(四)利用個人資料為行銷或非原蒐集目的之使用時，當事人表示拒絕後，應立即停止利用其個人資料，並將拒絕情形通報本法人彙整後周知所屬各部門及員工。

(五)當事人表示拒絕利用其個人資料或請求閱覽、製給複製本、補充或更正、停止蒐集、處理、利用或刪除其個人資料時，聯絡窗口為：各業務承辦人；電話為：02-23326228分機207。並將聯絡窗口及電話等資料，公告於本法人主事務所適當位置，如有網站者，並揭露於網頁。如認有拒絕當事人行使上述權利之事由，應附理由通知當事人。

(六)負責保管及處理個人資料檔案之人員，其職務有異動時，應將所保管之儲存媒體及有關資料檔案移交。

(七)本法人成員如因其工作職掌相關而須輸出、輸入個人資料時，均須鍵入其個人之使用者代碼及識別密碼，同時在使用範圍及使用權限內為之，其中識別密碼並應保密，不得洩漏或與他人共用。

(八)由經授權之管理人員每半年清查所保有之個人資料是否符合蒐集特定目的，若有非屬特定目的必要範圍之資料或特定目的消失、期限屆滿而無保存必要者，即予刪除、銷毀或其他停止蒐集、處理或利用等適當之處置，並留存相關紀錄。

(九)所蒐集之個人資料如需作特定目的外利用，必須先行檢視是否符合個人資料保護法第20條第1項但書規定。

六、設備安全管理、資料安全管理及人員管理措施

(一)設備安全管理

1、建置個人資料之有關電腦、自動化機器相關設備、可攜式設備，資料保有單位應每2個月保養維護，於保養維護或更新設備時，並應注意資料之備份及相關安全措施。

2、建置個人資料之個人電腦，不得直接作為公眾查詢之前端工具。

3、本法人之成員或其他必要蒐集之個人資料檔案應定期每月備份。

4、重要個人資料備份應異地存放，並應置有防火設備及保險箱等防護設備，以防止資料滅失或遭竊取。

5、電腦、自動化機器或其他存放媒介物需報廢汰換或轉作其他用途時，本法人執行長或各單位主管應檢視該設備所儲存之個人資料是否確實刪除。

(二)資料安全管理

1、資通訊系統存取個人資料之管控：

（1）個人資料檔案儲存在電腦硬式磁碟機上者，應在個人電腦設置識別密碼、保護程式密碼及相關安全措施。

（2）個人資料檔案使用完畢應即退出，不得任其停留於資通訊系統螢幕上。

（3）每月進行資通訊系統防毒、掃毒之必要措施。

（4）重要個人資料應另加設管控密碼，並每90天更換密碼，非經陳報本法人執行長、各單位主管或經授權之管理人員核可，並取得密碼者，不得存取。

（5）蒐集、處理或利用個人資料達1萬筆以上時，設置使用者身分確認、個人資料顯示之隱碼、網際網路傳輸之安全加密、個人資料檔案與資料庫之存取控制及保護監控，防止外部網路入侵及非法或異常使用行為。

2、紙本資料之保管：

（1）對於各類業務書件及個人資料表應存放於公文櫃內並上鎖，本法人成員非經本法人執行長、各單位主管或經授權之管理人員同意不得任意複製或影印。

（2）對於記載個人資料之紙本丟棄時，應先以碎紙設備進行處理。

(三)人員管理措施

1、本法人依業務需求設定各級成員不同之權限，以控管其個人資料蒐集、處理與利用之情形。

2、本法人檢視各相關業務之性質，指派人員負責規範個人資料蒐集、處理及利用等流程。

3、本法人成員應妥善保管個人資料之儲存媒介物，執行業務時依個人資料保護法規定蒐集、處理及利用個人資料。

4、成員異動或離職應立即取消其使用者代碼（帳號）及識別密碼。其所持有之個人資料應辦理交接，不得在外繼續使用，並簽訂保密切結書（如在任職時之相關勞務契約已有所約定時，亦屬之)。

5、本法人與他人所簽訂之相關勞務契約或承攬契約均列入保密條款及相關之違約罰則，以確保其遵守對於個人資料內容之保密義務（含契約終止後)。

6、本法人涉及相關業務之成員每90天應變更識別密碼1次，並於變更識別密碼後始可繼續使用電腦。

七、認知宣導及教育訓練

(一)本法人每年進行個人資料保護法基礎認知宣導及教育訓練至少1次，使員工知悉應遵守之規定，前述教育宣導及訓練應留存紀錄。

(二)對於新進人員應特別給予指導，務使其明瞭個人資料保護相關法令規定、責任範圍及應遵守之相關管理措施。

八、資料安全稽核機制

(一)本法人每6個月辦理個人資料檔案安全維護稽核，查核確認所保有之個人資料現況，並查察本法人是否落實本計畫規範事項，針對查察結果不符合事項及潛在不符合之風險，應規劃改善與預防措施，並確保相關措施之執行。執行改善與預防措施時，應依下項事項辦理：

1、確認不符合事項之內容及發生原因。

2、提出改善及預防措施方案。

3、紀錄查察情形及結果。

(二)前項查察情形及結果應作成稽核報告，由本法人執行長或經授權之

管理人員簽名確認，稽核報告至少保存5年。

九、使用紀錄、軌跡資料及證據保存

(一)本法人建置個人資料之電腦，其個人資料使用查詢紀錄檔，每月定期備份加密，並將該紀錄檔之儲存媒介物保存於適當處所以供檢查。

(二)個人資料使用紀錄以紙本登記，應存放於公文櫃內並上鎖，非經本法人執行長、各單位主管或經指定之管理人員同意，不得任意取出。

(三)使用紀錄、軌跡資料及相關證據至少留存5年。

十、個人資料安全維護之整體持續改善

(一)本法人將隨時依據計畫執行狀況，技術發展及相關法令修正等事項，檢討本計畫是否合宜，並予必要之修正，於修正後15日內報主管機關備查。

(二)針對個資安全稽核結果有不符合法令之虞者，規劃改善與預防措施。

十一、解散或被廢止備案後之個人資料處理方法

本法人解散或被廢止備案後，所保有之個人資料不得繼續使用，並依實際情形採下列方式處理，並將相關紀錄報送主管機關保存至少5年：

(一)銷毀：銷毀之方法、時間、地點及證明銷毀之方式。

(二)移轉：移轉之原因、對象、方法、時間、地點及受移轉對象得保有該項個人資料之合法依據。

(三)其他刪除、停止處理或利用個人資料：刪除、停止處理或利用之方法、時間或地點。

附件

<table>
<tr><td colspan="3">個人資料事故通報及紀錄表</td></tr>
<tr><td>財團法人名稱：
財團法人二二八事件紀念金會

通報機關：內政部</td><td colspan="2">通報時間：　　年　　月　　日　　時　　分
通報人：　　簽名(蓋章)
職稱：
電話：
Email：
地址：</td></tr>
<tr><td>發生時間</td><td colspan="2">年　　月　　日　　時　　分</td></tr>
<tr><td rowspan="2">發生種類</td><td rowspan="2">□竊取
□竄改
□毀損
□滅失
□洩漏
□其他侵害情形</td><td>個人資料侵害之總筆數(大約)
＿＿＿＿＿筆</td></tr>
<tr><td>□一般個人資料＿＿筆
□特種個人資料＿＿筆</td></tr>
<tr><td>發生原因及摘要</td><td colspan="2"></td></tr>
<tr><td>損害狀況</td><td colspan="2"></td></tr>
<tr><td>個人資料侵害可能結果</td><td colspan="2"></td></tr>
<tr><td>擬採取之因應措施</td><td colspan="2"></td></tr>
<tr><td>擬通知當事人之時間及方式</td><td colspan="2"></td></tr>
<tr><td>是否於發現個人資料外洩後72小時內通報</td><td colspan="2">□是
□否，理由：</td></tr>
</table>

備註：

1.特種個人資料，指有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料。

2.一般個人資料，指特種個人資料以外之個人資料。