國立傳統藝術中心

資訊安全政策

一、目的

國立傳統藝術中心為強化資訊安全管理，建立安全及可信賴之電子化作業環境，以確保資料、系統、設備及網路安全，有效運用本中心各項資訊設備，以保障民眾權益。特訂定本政策俾便中心推行資訊安全管理時有所遵循。

二、依據

(一)行政院及所屬各機關資訊安全管理規範及要點。

(二)電腦處理個人資料保護法。

(三)CNS17799 資訊安全管理之作業要點。

三、資訊安全定義

所謂資訊安全係將管理程序及安全防護技術應用於各項資訊作業，包含作業執行時所使用之各項資訊系統軟、硬體設備、存放各種資訊及資料之檔案媒體及經由列表機所列印之各式報表，以確保資訊蒐集、處理、傳送、儲存及流通之安全。

四、資訊安全目標

(一)、確保資料之機密性及防止非法使用、資訊系統及設備之完整性、可用性及安全性。

(二)、確保員工對資訊安全有一定認知，確保資訊業務運作之有效性及持續性。

(三)、舉辦資訊安全教育訓練，確保員工對資訊安全有一定認知。

(四)　、確保資安措施符合政策及法令要求，每年至少內部稽核 1 次。

五、資訊安全範圍

資訊安全的範圍包括 (1)管理制度、(2)作業流程、(3)人員、(4)軟體、(5)應用系統、(6)電腦作業系統、(7)硬體、(8)通訊設備、(9)資料、文件、媒體的儲存及(10)實體設施等。

以避免如因人為疏失、蓄意或天然災害等因素，遭致不當使用、洩漏、竄改、破壞等情事，而對本中心可能帶來之風險及危害程度。

本中心資訊安全管理事項如下：

(一)資訊安全權責分工。

(二)資訊安全教育訓練。

(三)網路安全管理。

(四)系統存取管制

(五)系統發展及維護安全管理。

(六)資訊資產安全管理。

(七)資訊安全內部稽核。

(八)資訊安全事件通報管理。

資訊安全分工原則

(一)資訊安全政策規範之研議及安全技術之研究、建置、評估相關事項由秘書室負責辦理。

(二)資料及資訊系統之安全需求等風險評估、資訊資產安全管理及保護等事項，由各組室業務單位負責辦理。

(三)資訊機密維護及內部稽核管理事項，由秘書室會同相關單位負責辦理。

(四)人員進用由人事室負責辦理。

(五)資訊設備相關機電消防配套措施及管理事項，由秘書室負責辦理。

(六)本中心資訊及網路系統因遭受破壞、不當使用所造成危安或重大災害事件，應在最短期間，將處理情形記錄填具「資通安全事件通報單」檢送秘書室備查，並提報資訊安全事件通報管理單位。

(七)教育訓練由人事室會同相關單位（秘書室）負責辦理。

資訊安全教育訓練

定期實施資訊安全教育訓練，宣導資訊安全政策及相關實施規定。

依其職能為基礎，針對管理、業務及資訊等不同工作類別之需求人員，視實際需要辦理資訊安全教育訓練及宣導，促使瞭解資訊安全的重要性，各種可能的安全風險，以提高同仁對資訊安全意識，促其遵守資訊安全規定。

網路安全管理

與外界網路連接之網點，設立防火牆控管外界與內部網路之資料傳輸及資源存取。機密性及敏感性的資料或文件，不存放在對外開放的資訊系統中，機密性文件不以電子郵件傳送。

定期對內部網路資訊安全設施與防毒進行查核，並更新防毒系統之病毒碼，及各項安全措施。

系統存取管制

作業系統及安全管理需求訂定通行密碼核發及變更程序並作成記錄。

登入各作業系統時，依各級人員執行任務所必要之系統存取權限，由系統管理人員設定賦予權限之帳號與密碼，並定期更新。

離（休）職人員，應立即取消各項資訊資源之所有權限，並列入離（休）職之必要手續。人員職務調整及調動，應依系統存取授權規定，限期調整其權限。

系統開發及維護安全管理

各業務單位對系統開發與資料庫系統管理維護，其功能、性能、與週期等要求，要明確規定系統的安全要求。

建立系統備援設施，定期執行必要的資料、軟體備份及備援作業，以便發生災害或儲存媒體失效時，可迅速回復正常作業。

資訊資產安全管理

資訊資產依分類、等級及風險評鑑原則

(一)分類

依據各項作業內容特性，將資產分為電子化資訊資產、實體資產、軟體資產、服務、書面文件及人員等分類。

(二)等級

依照各類資產所具有之機密性、完整性及可用性評估該資產反應出之價值，由各組業務實務性質分類。

(三)風險評鑑

根據資產本身之脆弱性、威脅及衝擊，評鑑其風險等級。經分級與評鑑後，依其所具備之價值，各組室施以適當程度之安全控管。

(四)不可接受風險等級

執行風險評鑑後，將資產區分為不同風險等級，其中屬於「不可接受風險」之資產，應訂定風險控制計畫據以監督控管，並落實執行追蹤控制。

資訊安全內部稽核

依據資安檢核表評估單位整體資安風險、提出改善建議事項。

確保資安措施符合政策及法令要求，每年至少內部稽核 1 次。

資訊安全事件通報管理

資通安全事件通報程序如下（附件一）：

一、 資通安全事件等級概分為四級：

『A』級：影響公共安全、社會秩序、人民生命財產。

『B』級：系統停頓，業務無法運作。

『C』級：業務中斷，影響系統效率。

『D』級：業務短暫停頓，可立即修復。

二、資通安全事件危機通報作業注意事項：

（一） 如發生資通安全事件應具體反應事實或請求支援，並通報至單位

「通報連絡人」。該連絡人則依據事實狀況、評估相關可能因素，儘速協助使用者進行緊急應變處置，以降低資安事件之危害，並配合填具「資通安全事件通報單」(附件二)，完成內部通報流程。

（二） 資通安全事件影響層面如遇重大災害，且影響層面深廣、受損程度嚴重時(如外力入侵、資通訊網路系統骨幹中斷重大突發事件等，或水、火災、地震、天然災害等涉及資通安全事件者)，屬應儘速向行政院研究發展考核委員會通報；惟如屬一般性【D級（含）以下】，僅涉及單位內、受損程度輕微時（如內部危安、電腦病毒感染)，則由資訊人員先行處置。

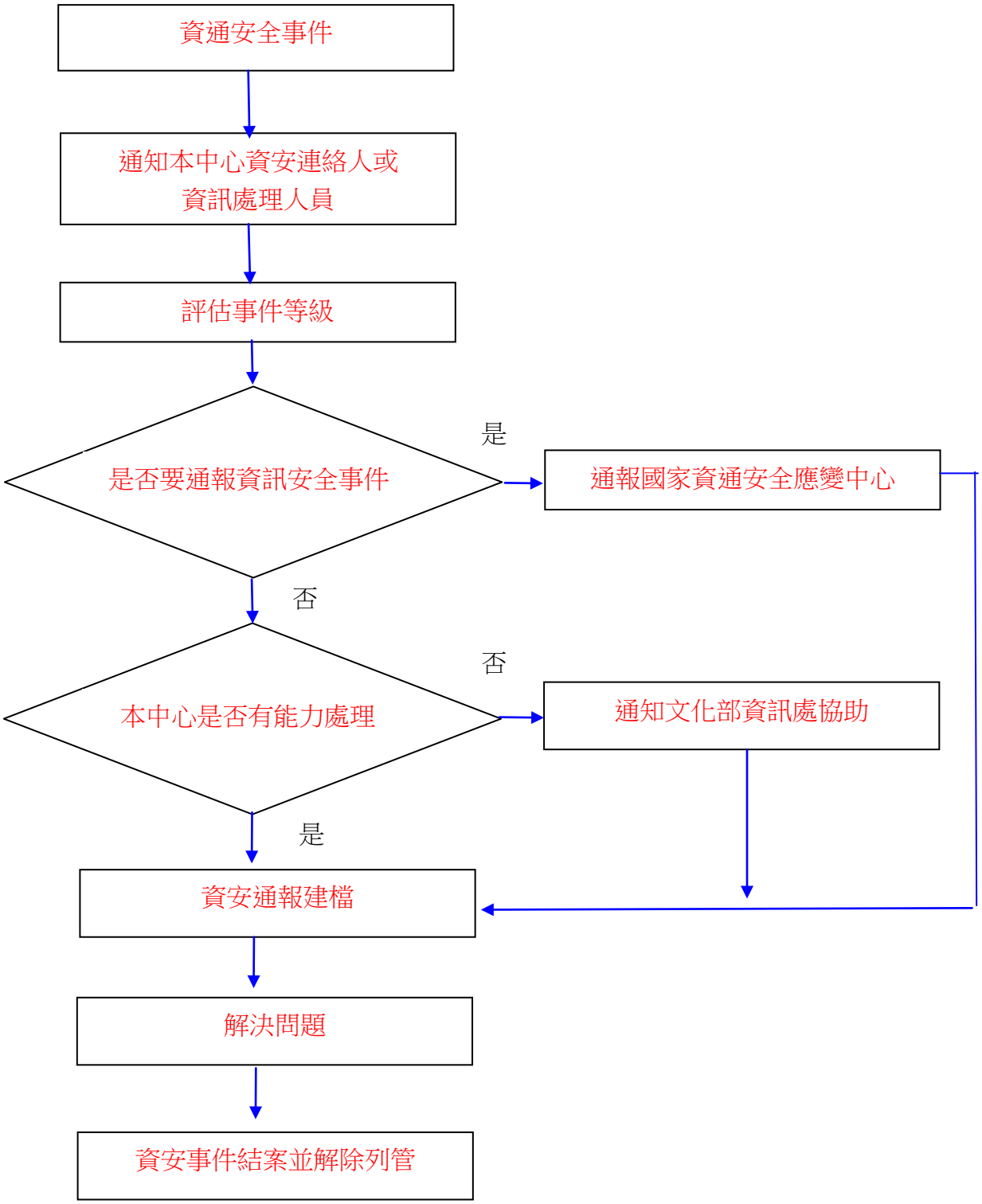
（三） 各單位如遇資通安全事件，危及人員生命或設備遭到破壞等涉及民、刑事案件時，應即時通報檢調單位請求處理。

（四） 如發生災損，有關通報單之災害損失評估內容包括如下：作業影響情況、設備或系統損害情況、作業延誤情況、資料受損項目、估算資通訊系統作業及資料回復所需時間、備援中心設備及人員支援狀況等。

六、附則

本「資訊安全政策」經本中心審核後實施，修正時亦同。

國立傳統藝術中心資安事件通報程序（附件一）



國立傳統藝術中心資通安全事件通報單（附件二）

填報時間：____年____月____日____時____分　　編號：

一、發生資通安全之機關（機構）聯絡資料： 機關名稱：_____ E-MAIL：_____ 聯絡人：_____ 電話：_____ 傳真：_____			
二、資通安全事件通報事項： １、事件發生時間：____年____月____日____時____分 ２、主機（伺服器）資料： ◎ IP 位址（IP Address）: ◎ 網域名稱（Domain name）: ◎ 主機（伺服器）廠牌、機型： ◎ 作業系統名稱、版本、序號： ◎ 網際網路資訊位址（Web URL）: ◎ 已裝置之安全機制： ３、資通安全事件資料： 影響等級：□「A」級：影響公共安全、社會秩序、人民生命財產。 □「B」級：系統停頓，業務無法運作。 □「C」級：業務中斷，影響系統效率。 □「D」級：業務短暫停頓，可立即修復。 ◎ 事件說明： ◎ 可能影響範圍及損失評估： ◎ 應變措施：			
三、期望支援項目：			
四、解決辦法：			
五、已解決時間：____年____月____日____時____分			
機關首長或 授權人簽章		承辦人簽章	