臺北市政府秘書處資通安全危機通報緊急應變計畫暨處置復原作業程序

中華民國91年10月22日頒訂
中華民國92年10月13日修正
中華民國96年05月31日修正

壹、 依據：

各機關處理資通安全事件危機通報緊急應變作業注意事項。

貳、 目的：

為確保本處各組室及市政大樓公共事務管理中心電腦系統作業正常運作，維護電子化作業之效率，避免因個人操作不當或蓄意破壞、病毒散佈及駭客入侵等情事，筆使電腦系統受損而影響行政效率，特訂定本危機通報緊急應變計畫暨處置復原作業程序（以下簡稱「應變計畫」）。

參、 適用時機：

本處各組室與市政大樓公共事務管理中心於發生重大資通安全事件或其他災害涉及資通安全時，應立即依本應變計畫辦理。

肆、 應變組織：

由本處資訊安全推動小組(以下簡稱資安小組）負責本處資通安全危機通報及緊急應變處理事宜。

伍、 資通安全事件等級概分為四級：

4 級：影響公共安全、社會秩序、人民生命財產。

3 級：系統停頓，業務無法運作。

2 級：業務中斷，影響系統效率。

1 級：業務短暫停頓，可立即修復。

陸、 資通安全危機事件通報作業程序：

一、 用戶端：各資訊或通信系統使用者於發生危安事故時，應立即（最遲不得超過十五分鐘）向「資安小組」反應事實或請求支援，並知會政風室後，填具「資通安全事件通報單一內部通報用」，完成內部通報程序（如附件1)。

二、 資安小組：於接獲用戶端資通安全事件通報後，經評估為「2」級以上等級者，應將事件發生之事實、可能影響之範圍、損失評估、判斷支援申請、採取之應變措施等事項，填具「資通安全事件通報單」（如附件2），透過網路、電子郵件、電話、傳真等方式，通報至「國家資通安全應變中心」及臺北市政府（資訊處）。（「國家資通安全應變中心」通報網址：www.ncert.gov.tw）

柒、 資通安全事件緊急應變作業事項：

一、 事前建置安全防護機制：

（一）各用戶端（包含個人電腦、手提式電腦、資訊服務站等資訊化設備，以下簡稱各資訊化設備）應裝置掃毒軟體，並定期更新病毒碼。

（二）各用戶端（包含各資訊化設備）應及時執行作業系統、資料庫等漏洞修補。

（三）筆記型電腦、多人共用之公用電腦、設於公共場所之資訊服務站（KIOSK）應由各單位指定專人管理。

（四）用戶端電腦應設定密碼，包含基本輸入輸出系統（BIOS ）、網域登入密碼及螢幕保護程式密碼，並隨時更改設定。

（五）密碼之設定應使用優質密碼（原則上應超過八個位元，且具有文數字及符號為宜），並應定期更新（原則上不超過三個月）。

（六）針對各種資訊化設備及資訊系統，應變更系統預設之帳號與密碼，同時避免使用簡易或規則性之帳號與密碼。

（七）網路芳鄰及資源分享以不開放為原則，如須開放有嚴謹保護措施及使用時間限制。

（八）避免使用預覽方式開啟電子郵件，不開啟來歷不明之電子郵件，對於電子郵件中帶有執行檔之附件，請勿任意開啟。

（九）各主機系統應建置並管理系統事件紀錄，包含系統、應用程式及安全日誌之啟動，並配合實際作業需求明定作業程序之控管。

（十）各主機系統及用戶端應定期備份重要資料，並區分安全等級及權限控管後，妥善異地分存。備份資料應定期回復測試，以確定其可用性。

（十一）如有委外作業，對於進駐機關內之委外作業人員應納入機關安全管理，如欲使用內部網路資源時，宜有安全管制措施。

（十二）資安小組應主動蒐集彙整資通安全事件危害通告資訊，提供用戶端最新危安事故訊息，加強用戶端之電腦知能，並視其影響之程度，教育用戶端應變方式。

二、 事中主動預警緊急應變：

（一）資安小組於發生資通安全事件或其他災害涉及資通安全事件時，應就事故之影響區分層級及緊急應變優先順序，透過電子布告欄、上網站、技術支援單位等方式，查詢解決方案，儘速依本應變計畫執行相關事項。

（二）經評估影響等級「2」級以上者，必要時本處資訊安全長應召開緊急應變會議，俾掌握處理情形。

（三）影響等級為「1」級或未召開緊急應變會議時，資安小組幹事仍應自事件通報開始至應變處置結束期間，全程主動追蹤掌握狀況與管制回報。

三、 事後復原與追蹤：

（一）受損單位執行災害復原工作，首先檢驗系統軟體、應用軟體及硬體設備是否可以正常運作，並執行系統復原及運作測試等，並俟運作正常後即進行安全備份檔案下載、資料回復及重建等相關事宜。

（二）危機處理時，應保留事件發生之線索，以釐清事件發生之原因與責任歸屬，並找出防護系統之漏洞，尋求補強保護方法，避免事件再次發生。

（三）若有需要，應向本府資訊局檢調單位申請追蹤鑑識、偵查支援。

捌、 資通安全事件分類：

（一）內部危安事件：發現遭人為惡意破壞情事時，應迅速通報「資安小組」並保留事件發生之線索，以利爾後調查分析。

（二）外力入侵事件：發現病毒感染或非法入侵時，應停止資通作業並移除網路連線，採實體隔離方式避免災情擴散，同時通報「資安小組」處理。

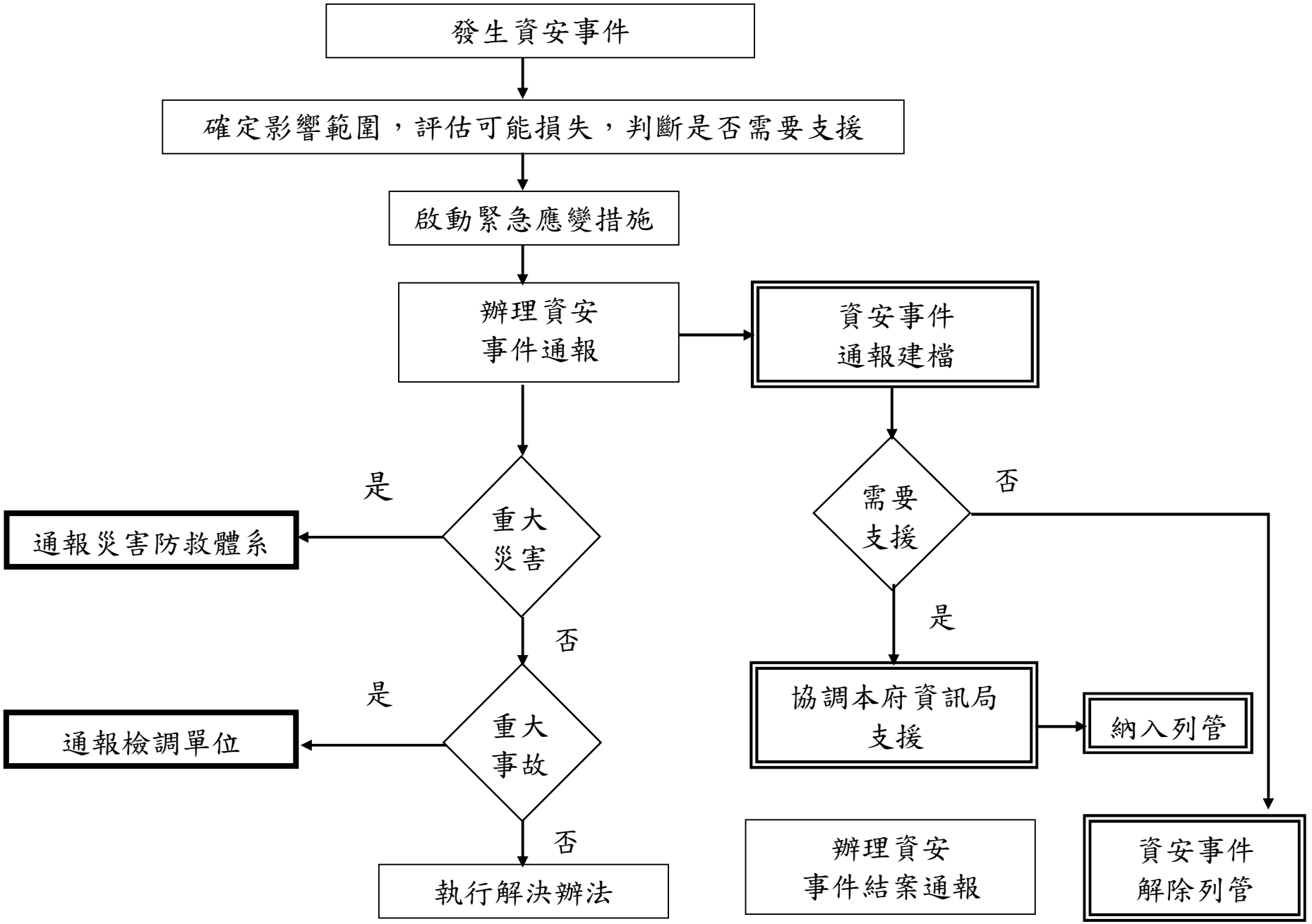
（三）天然災害或重大突發事件：如遇颱風、水災、地震等天然災害或火災、爆炸等重大突發事件時，各用戶端應迅速攜帶重要資料及程式等離開現場，並儲存於安全處所，待危安事件結束後，即進行系統重建復原工作。

（四）通報與應變作業流程詳附圖1。

玖、本應變計畫得依實際運作情形，隨時修訂之。

附圖 1

資安事件通報及應變作業流程



附件1

臺北市政府秘書處資通安全事件通報單-內部通報用

組別:	用戶端姓名:	聯絡電話:
資通安全發生時間:		
資通安全通報時間:		
資通安全事件簡述:		

中　華　民　國　　年　　月　　日

附件2

臺北市政府秘書處資通安全事件通報單

承辦人員姓名：　　聯絡電話：
接獲資通安全事件通報時間：
處理資通安全事件時間：
等級： □4 級：影響公共安全、社會秩序、人民生命財產。 □3 級：系統停頓，業務無法運作。 □2 級：業務中斷，影響系統效率。 □1 級：業務短暫停頓，可立即修復。
作業影響情況: 設備及系統受損情況： 請求支援項目

中　華　民　國　　年　　月　　日