衛生福利部北區兒童之家

資通安全事件通報及應變管理程序書

機密等級：限閱

文件編號：**IS-B-010**

版　　次：**2.0**

修訂日期：**112.01.01**

修　訂　紀　錄				
版次	**修訂日期**	**修訂頁次**	**修訂者**	**修訂內容摘要**
1.0	110.03.29		莊文欣	初版
1.1	111.02.14		黃詩華	變更文件負責人員
1.2	111.07.01		蔡慧茵	變更文件負責人員
1.3	111.09.07		蔡慧茵	新增通報作業程序第(十)、資安事件調查第(七)、紀錄流程第三第四、相關文件第四
1.4	111.12.02		蔡慧茵	修正通報作業程序第(十)
2.0	112.01.01		莊文欣	變更文件負責人員

資通安全事件通報及應變管理程序書					
文件編號	IS-B-010	機密等級	限閱	版本	2.0

目錄

資通安全事件通報及應變管理程序書					
文件編號	IS-B-010	機密等級	限閱	版本	2.0

壹、目的

為建立本家資通安全事件之通報及應變機制，迅速有效獲知並處理事件，茲遵照資通安全管理法第 14 條及本家資通安全維護計畫之規定，制定本資通安全事件通報及應變管理程序書(以下稱本管理程序)。

貳、適用範圍

發生於本家之事件，系統、服務或網路狀態經鑑別而顯示可能有違反資通安全政策或保護措施失效之狀態發生，影響資通系統機能運作，構成資通安全政策之威脅者。

參、權責

一、本家應於資通安全事件發生前，確保所屬是否落實本管理程序，並依規定指定其知悉資通安全事件之通報以及應變作業後之結案登錄方式。

二、本家應視必要性，與受託廠商約定，使其制定其本管理程序，並於知悉資通安全事件後向本家進行通報，於完成事件之通報及應變程序後，依本家指示提供相關之紀錄或資料。

三、本家應於知悉資通安全事件後，應依本管理程序之規定，儘速完成損害控制、復原與事件之調查及處理作業。完成後，應依上級或監督機關及行政院指定之方式進行結案登錄作業，並送交調查、處理及改善報告。

肆、事件通報窗口及緊急處理小組

一、本家之資通安全事件通報窗口及聯繫專線為：

序位	姓名/職稱	連絡電話
第1序位	劉竑礽/資安駐點人員	03-3525634#241
第2序位	莊文欣/行政室辦事員	03-3525634#208
第3序位	蔡慧茵/行政室室主任	03-3525634#209
第4序位	紀靜如/秘書	03-3525634#202

二、本家應以適當方式使相關人員明確知悉本家之通報窗口及聯絡方式。

三、本家所屬人員發現資通安全事件後，應立即向本家之通報窗口通報或國家資通安全通報應變網站通報登入。

四、本家應確保通報窗口之聯絡管道全天維持暢通，若因設備故障或其他情形導致窗口聯絡管道中斷，該中斷情況若持續達一小時以上者，應即將該情況告知相關人員，並即提供其他有效之臨時聯絡管道。

五、負責事件處理單位（該事件發生之單位）權責人員應與相關單位密切合作以進行事件之處理，並使用通報窗口適時掌握事件處理之進度及其他相關資訊。

六、事件經初步判斷認為可能屬重大資安事件或事態嚴重時，應即向資通安全長報告，由資通安全長成立緊急處理小組，立即協助進行處理；接獲受託廠商所通報之資通安全事件時，亦同。

七、緊急處理小組成員由資通安全長指派機關之資通安全相關技術人員擔任，或由外部專家擔任之或委託專業廠商協助，並經機關首長核可。

八、各相關權責人員應紀錄事件處理過程，並檢討事件發生原因，著手進行改善，並留存必要之證據。

伍、通報程序

一、通報作業程序

(一) 判定事件等級之流程及權責

本家之權責人員或緊急處理小組應依據以下事項，於知悉資通安全事件後，依規定完成「資通安全事件通報及應變辦法」之資通安全事件等級判斷：

1、 事件涉及核心業務或關鍵基礎設施業務之資訊與否。

2、 事件導致業務之資訊或資通系統遭竄改之影響程度，屬嚴重或輕

微。

3、 事件所涉資訊是否屬於國家機密、敏感資訊或一般公務機密。

4、 機關業務運作若遭影響或資通系統停頓，是否可容忍中斷時間內能回復正常運作。

5、 事件其他足以影響資通安全事件等級之因素。

(二) 除事件之等級外，權責人員或緊急處理小組亦應對資通安全事件之影響範圍、損害程度及本家因應之能力進行評估。

(三) 本家權責人員或緊急處理小組於完成資通安全事件等級之判斷及相關評估後，應盡速報資通安全長。

(四) 除因網路或電力中斷等事由，致無法依上級或監督機關及行政院所指定或認可之方式通報外，應於知悉資通安全事件後一小時內依所指定或認可之方式，進行事件通報。

(五) 本家因網路或電力中斷等事由，致無法依前項規定方式為通報者，應於知悉資通安全事件後一小時內以電話或其他適當方式，將該次資安事件應通報之內容及無法通報依規定方式之事由，分別告知所屬上級或監督機關及行政院，並於是由解除後，依原方式補行通報。

(六) 資通安全事件等級如有變更，權責人員或緊急應變小組應告知通報窗口，使其續行通報作業。

(七) 本家於委外辦理資通系統建置、維運或提供資通服務之情形時，應於合約中訂定委外廠商於知悉資通安全事件時，應即向本家之權責人員或窗口，以指定之方式進行通報。

(八) 本家於悉知資通安全事件後，如認該事件之影響涉及其他機關或應由其他機關依其法定職權處理時，權責人員或緊急應變小組應於知悉資通安全事件後一小時內，將該事件依上級機關或行政院所指定或認可之方式，通知該機關。

(九) 本家執行通報應變作業時，得視情形向直屬上級機關提出技術支援或其他協助之需求。

(十) 第三級或第四級資通安全事件，應另以電話或其他適當方式通知上級機關；數位發展部資通安全署就第三級或第四級資通安全事件，依國土安全緊急通報作業規定轉報行政院國土安全辦公室。

二、接獲自身通報之評估作業程序

(一) 本家之權責人員或緊急應變小組進行本條第一項之審核過程中，得請求通報之公務機關提供級別判斷所需之資料或紀錄。

陸、應變程序

一、事件發生前之防護措施規劃

本家應於平時妥善實施資通安全維護計畫，並以組織營運目標與策略為基準，透過「業務流程衝擊分析表」，規劃業務持續運作計畫並實施演練，以預防資安事件之發生。

二、損害控制機制

(一) 負責應變之權責人員或緊急應變小組，應完成以下應變事務之辦理，並留存應變之紀錄

1、 資安事件之衝擊及損害控制作業。

2、 資安事件所造成損害之復原作業。

3、 資安事件相關鑑識及其他調查作業。

4、 資安事件之調查與處理及改善報告之方式。

5、 資安事件後續發展與其他事件關聯性之監控。

6、 資訊系統、網路、機房等安全區域發生重大事故或災難，致使業務中斷時，應依據本家事前擬定之緊急計畫，進行應變措施已恢復業務持續運作之狀態。

7、 其他資通安全事件應變之相關事項。

(二) 對於第一級、第二級資通安全事件，本家應於悉知事件後 72 小時內完成前項事務之辦理，並應留存紀錄；第三級、第四級資通安全事件，本家應於悉知事件後 36 小時內完成損害控制或復原作業，並執行上述事項，及留存相關紀錄。

(三) 本家完成通報及應變程序之辦理後，應依所隸屬之上級機關或行政院所指定或認可方式進行結案登錄。

(四) 本家於悉知受託廠商發生與受託業務相關之資通安全事件時，應於悉知委外廠商發生第一、二級資通安全事件後 72 小時內，確認委外廠商已完成損害控制或復原事項之辦理；於悉知委外廠商發生第三、四級資通安全事件後 36 小時內，確認委外廠商完成損害控制或復原事項之辦理。

柒、資安事件後之復原、鑑識、調查及改善機制

一、本家完成本管理程序後，應針對事件所造成之衝擊、損害及影響進行調整改善，並應於事件發生後一個月內完成資通安全事件調查、處理及改善報告。

二、資通安全事件調查、處理及改善報告應包括以下項目：

(一) 事件發生、完成損害控制或復原作業之時間。

(二) 事件影響之範圍及損害評估。

(三) 損害控制及復原作業之歷程。

(四) 事件調查及處理作業之歷程。

(五) 為防範類似事件再次發生所採取之管理、技術、人力或資源等層面之措施。

(六) 前款措施之預定完成時程及成效追蹤機制

(七) 惡意程式建議得請防毒軟體或資安服務公司檢測，並上傳至 Virus Check 網站(https://viruscheck.tw/)分析，以更新或強化相關偵測及聯

防機制，不宜上傳至其他平臺。

捌、紀錄留存及管理程序

一、本家應將資通安全事件之通報與應變作業之執行、事件影響範圍與損害程度以及其他通報應變之執行情形留存完整之紀錄，該文件並應簽核。

二、本家於完成本管理程序後，應依據資安事件通報紀錄之內容及實際處理情形，於必要時對本管理程序、人力配置或其他相關事項進行修正或調整。

三、日常維運資通系統時，作業系統日誌(OS event log)、網站日誌(web log)、應用程式日誌(AP log)、登入日誌(logon log)建議定期備份至與原稽核系統不同之實體系統，其保存時間最少六個月之日誌紀錄。

四、於「資訊機房工作日誌」確認系統日誌備份正常與否。

玖、演練作業

一、本家應配合衛生福利部資通安全事件通報應變辦法規定辦理之社交工程演練、資通安全事件通報及應變進行演練。

壹拾、 相關文件

一、業務流程衝擊分析表

二、資訊機房工作日誌