資通安全事件通報及應變辦法

中華民國 107 年 11 月 21 日行政院院臺護字第 1070213547 號令訂定
中華民國 110 年 8 月 23 日行政院院臺護字第 1100182012 號令修正

第一章　總則

第一條　本辦法依資通安全管理法（以下簡稱本法）第十四條第四項及第十八條第四項規定訂定之。

第二條　資通安全事件分為四級。

公務機關或特定非公務機關（以下簡稱各機關）發生資通安全事件，有下列情形之一者，為第一級資通安全事件：

一、非核心業務資訊遭輕微洩漏。

二、非核心業務資訊或非核心資通系統遭輕微竄改。

三、非核心業務之運作受影響或停頓，於可容忍中斷時間內回復正常運作，造成機關日常作業影響。

各機關發生資通安全事件，有下列情形之一者，為第二級資通安全事件：

一、非核心業務資訊遭嚴重洩漏，或未涉及關鍵基礎設施維運之核心業務資訊遭輕微洩漏。

二、非核心業務資訊或非核心資通系統遭嚴重竄改，或未涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭輕微竄改。

三、非核心業務之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作，或未涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，於可容忍中斷時間

內回復正常運作。

各機關發生資通安全事件，有下列情形之一者，為第三級資通安全事件：

一、未涉及關鍵基礎設施維運之核心業務資訊遭嚴重洩漏，或一般公務機密、敏感資訊或涉及關鍵基礎設施維運之核心業務資訊遭輕微洩漏。

二、未涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭嚴重竄改，或一般公務機密、敏感資訊、涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭輕微竄改。

三、未涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作，或涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，於可容忍中斷時間內回復正常運作。

各機關發生資通安全事件，有下列情形之一者，為第四級資通安全事件：

一、一般公務機密、敏感資訊或涉及關鍵基礎設施維運之核心業務資訊遭嚴重洩漏，或國家機密遭洩漏。

二、一般公務機密、敏感資訊、涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭嚴重竄改，或國家機密遭竄改。

三、涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作。

第三條　資通安全事件之通報內容，應包括下列項目：

一、發生機關。

二、發生或知悉時間。

三、狀況之描述。

四、等級之評估。

五、因應事件所採取之措施。

六、外部支援需求評估。

七、其他相關事項。

第二章　公務機關資通安全事件之通報及應變

第四條　公務機關知悉資通安全事件後，應於一小時內依主管機關指定之方式及對象，進行資通安全事件之通報。

前項資通安全事件等級變更時，公務機關應依前項規定，續行通報。

公務機關因故無法依第一項規定方式通報者，應於同項規定之時間內依其他適當方式通報，並註記無法依規定方式通報之事由。

公務機關於無法依第一項規定方式通報之事由解除後，應依該方式補行通報。

第五條　主管機關應於其自身完成資通安全事件之通報後，依下列規定時間完成該資通安全事件等級之審核，並得依審核結果變更其等級：

一、通報為第一級或第二級資通安全事件者，於接獲後八小時內。

二、通報為第三級或第四級資通安全事件者，於接獲後二小時內。

總統府與中央一級機關之直屬機關及直轄市、縣（市）政府，應於其自身、所屬、監督之公務機關、

所轄鄉（鎮、市）、直轄市山地原住民區公所與其所屬或監督之公務機關，及前開鄉（鎮、市）、直轄市山地原住民區民代表會，完成資通安全事件之通報後，依前項規定時間完成該資通安全事件等級之審核，並得依審核結果變更其等級。

前項機關依規定完成資通安全事件等級之審核後，應於一小時內將審核結果通知主管機關，並提供審核依據之相關資訊。

總統府、國家安全會議、立法院、司法院、考試院、監察院及直轄市、縣（市）議會，應於其自身完成資通安全事件之通報後，依第一項規定時間完成該資通安全事件等級之審核，並依前項規定通知主管機關及提供相關資訊。

主管機關接獲前二項之通知後，應依相關資訊，就資通安全事件之等級進行覆核，並得依覆核結果變更其等級。但主管機關認有必要，或第二項及前項之機關未依規定通知審核結果時，得就該資通安全事件逕為審核，並得為等級之變更。

第六條　公務機關知悉資通安全事件後，應依下列規定時間完成損害控制或復原作業，並依主管機關指定之方式及對象辦理通知事宜：

一、第一級或第二級資通安全事件，於知悉該事件後七十二小時內。

二、第三級或第四級資通安全事件，於知悉該事件後三十六小時內。

公務機關依前項規定完成損害控制或復原作業後，應持續進行資通安全事件之調查及處理，並於一個月內依主管機關指定之方式，送交調查、處理及改

善報告。

前項調查、處理及改善報告送交之時限，得經上級或監督機關及主管機關同意後延長之。

上級、監督機關或主管機關就第一項之損害控制或復原作業及第二項送交之報告，認有必要，或認有違反法令、不適當或其他須改善之情事者，得要求公務機關提出說明及調整。

第七條　總統府與中央一級機關之直屬機關及直轄市、縣（市）政府，就所屬、監督、所轄或業務相關之公務機關執行資通安全事件之通報及應變作業，應視情形提供必要支援或協助。

主管機關就公務機關執行資通安全事件之應變作業，得視情形提供必要支援或協助。

公務機關知悉第三級或第四級資通安全事件後，其資通安全長應召開會議研商相關事宜，並得請相關機關提供協助。

第八條　總統府與中央一級機關之直屬機關及直轄市、縣（市）政府，對於其自身、所屬或監督之公務機關、所轄鄉（鎮、市）、直轄市山地原住民區公所與其所屬或監督之公務機關及前開鄉（鎮、市）、直轄市山地原住民區民代表會，應規劃及辦理資通安全演練作業，並於完成後一個月內，將執行情形及成果報告送交主管機關。

前項演練作業之內容，應至少包括下列項目：

一、每半年辦理一次社交工程演練。

二、每年辦理一次資通安全事件通報及應變演練。

總統府與中央一級機關及直轄市、縣（市）議會，應依前項規定規劃及辦理資通安全演練作業。

第九條　公務機關應就資通安全事件之通報訂定作業規範，其內容應包括下列事項：

一、判定事件等級之流程及權責。

二、事件之影響範圍、損害程度及機關因應能力之評估。

三、資通安全事件之內部通報流程。

四、通知受資通安全事件影響之其他機關之方式。

五、前四款事項之演練。

六、資通安全事件通報窗口及聯繫方式。

七、其他資通安全事件通報相關事項。

第十條　公務機關應就資通安全事件之應變訂定作業規範，其內容應包括下列事項：

一、應變小組之組織。

二、事件發生前之演練作業。

三、事件發生時之損害控制機制。

四、事件發生後之復原、鑑識、調查及改善機制。

五、事件相關紀錄之保全。

六、其他資通安全事件應變相關事項。

第三章　特定非公務機關資通安全事件之通報及應變

第十一條　特定非公務機關知悉資通安全事件後，應於一小時內依中央目的事業主管機關指定之方式，進行資通安全事件之通報。

前項資通安全事件等級變更時，特定非公務機關應依前項規定，續行通報。

特定非公務機關因故無法依第一項規定方式通報者，應於同項規定之時間內依其他適當方式通報，並註記無法依規定方式通報之事由。

特定非公務機關於無法依第一項規定方式通報

之事由解除後，應依該方式補行通報。

第十二條　中央目的事業主管機關應於特定非公務機關完成資通安全事件之通報後，依下列規定時間完成該資通安全事件等級之審核，並得依審核結果變更其等級：

一、通報為第一級或第二級資通安全事件者，於接獲後八小時內。

二、通報為第三級或第四級資通安全事件者，於接獲後二小時內。

中央目的事業主管機關依前項規定完成資通安全事件之審核後，應依下列規定辦理：

一、審核結果為第一級或第二級資通安全事件者，應定期彙整審核結果、依據及其他必要資訊，依主管機關指定之方式送交主管機關。

二、審核結果為第三級或第四級資通安全事件者，應於審核完成後一小時內，將審核結果、依據及其他必要資訊，依主管機關指定之方式送交主管機關。

主管機關接獲前項資料後，得就資通安全事件之等級進行覆核，並得為等級之變更。

第十三條　特定非公務機關知悉資通安全事件後，應依下列規定時間完成損害控制或復原作業，並依中央目的事業主管機關指定之方式辦理通知事宜：

一、第一級或第二級資通安全事件，於知悉該事件後七十二小時內。

二、第三級或第四級資通安全事件，於知悉該事件後三十六小時內。

特定非公務機關依前項規定完成損害控制或復原作業後，應持續進行事件之調查及處理，並於一個月內依中央目的事業主管機關指定之方式，送交調查、處理及改善報告。

前項調查、處理及改善報告送交之時限，得經中央目的事業主管機關同意後延長之。

中央目的事業主管機關就第一項之損害控制或復原作業及第二項送交之報告，認有必要，或認有違反法令、不適當或其他須改善之情事者，得要求特定非公務機關提出說明及調整。

特定非公務機關就第三級或第四級資通安全事件送交之調查、處理及改善報告，中央目的事業主管機關應於審查後送交主管機關；主管機關就該報告認有必要，或認有違反法令、不適當或其他須改善之情事者，得要求特定非公務機關提出說明及調整。

第十四條　中央目的事業主管機關就所管特定非公務機關執行資通安全事件之通報及應變作業，應視情形提供必要支援或協助。

主管機關就特定非公務機關執行資通安全事件應變作業，得視情形提供必要支援或協助。

特定非公務機關知悉第三級或第四級資通安全事件後，應召開會議研商相關事宜。

第十五條　特定非公務機關應就資通安全事件之通報訂定作業規範，其內容應包括下列事項：

一、判定事件等級之流程及權責。

二、事件之影響範圍、損害程度及機關因應能力之評估。

三、資通安全事件之內部通報流程。

四、通知受資通安全事件影響之其他機關之時機及方式。

五、前四款事項之演練。

六、資通安全事件通報窗口及聯繫方式。

七、其他資通安全事件通報相關事項。

第十六條　特定非公務機關應就資通安全事件之應變訂定作業規範，其內容應包括下列事項：

一、應變小組之組織。

二、事件發生前之演練作業。

三、事件發生時之損害控制，及向中央目的事業主管機關請求技術支援或其他必要協助之機制。

四、事件發生後之復原、鑑識、調查及改善機制。

五、事件相關紀錄之保全。

六、其他資通安全事件應變相關事項。

第四章　附則

第十七條　主管機關就各機關之第三級或第四級資通安全事件，得召開會議，邀請相關機關研商該事件之損害控制、復原及其他相關事宜。

第十八條　公務機關應配合主管機關規劃、辦理之資通安全演練作業，其內容得包括下列項目：

一、社交工程演練。

二、資通安全事件通報及應變演練。

三、網路攻防演練。

四、情境演練。

五、其他必要之演練。

第十九條　特定非公務機關應配合主管機關規劃、辦理之資通安全演練作業，其內容得包括下列項目：

一、網路攻防演練。

二、情境演練。

三、其他必要之演練。

主管機關規劃、辦理之資通安全演練作業，有侵害特定非公務機關之權利或正當利益之虞者，應先經其書面同意，始得為之。

前項書面同意之方式，依電子簽章法之規定，得以電子文件為之。

第二十條　公務機關於本辦法施行前，已針對其自身、所屬或監督之公務機關或所管之特定非公務機關，自行或與其他機關共同訂定資通安全事件通報及應變機制，並實施一年以上者，得經主管機關核定後，與其所屬或監督之公務機關或所管之特定非公務機關繼續依該機制辦理資通安全事件之通報及應變。

前項通報及應變機制如有變更，應送主管機關重為核定。

第二十一條　本辦法之施行日期，由主管機關定之。

本辦法修正條文自發布日施行。