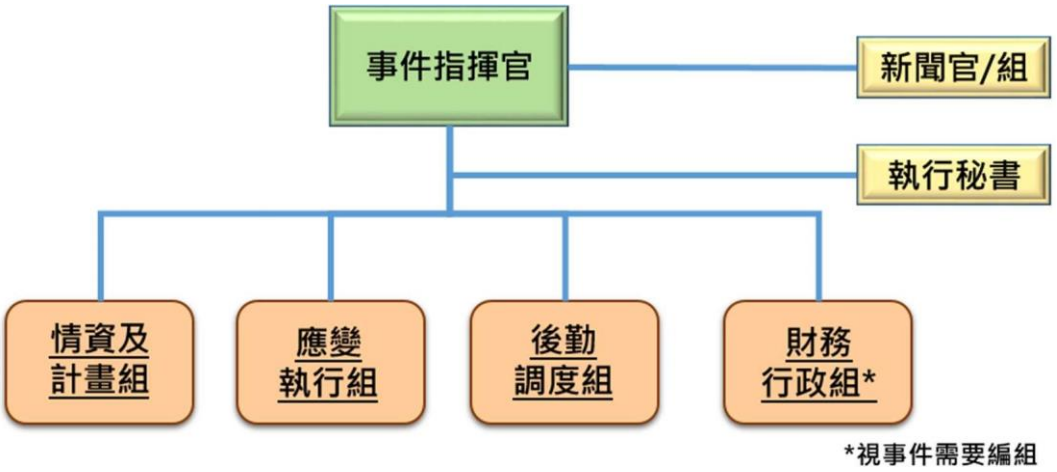
修正各機關資通安全事件通報及應變處理作業程序

一、為確保資通安全管理法(以下簡稱本法)納管之公務機關及特定非公務機關(以下簡稱各機關)於發生資通安全事件時，依本法及資通安全事件通報及應變辦法相關規定即時通報及應變，迅速完成損害控制或復原作業，降低資通安全事件對各機關業務之衝擊影響，並確保資通安全事件發生時之跡證保存，特訂定本程序。

二、各機關應成立資通安全事件通報及應變小組(以下簡稱通報應變小組)，於平時進行演練，並於發生資通安全事件時，依事件等級進行通報及應變作業。

通報應變小組組成建議如圖一，各分組代表如表一，其任務如下：



圖一、資通安全事件通報及應變小組組成

表一、資通安全事件通報及應變小組各分組代表

	第一級、第二級 資通安全事件	第三級、第四級 資通安全事件
事件指揮官	機關資訊(安)單位主管	機關資通安全長
新聞官/組	事件指揮官或其授權人員	
執行秘書	機關資通安全專責人員 或資訊人員	機關資訊(安)單位主管
情資及計畫組 組長	機關資通安全專責人員 或資訊人員	機關資訊(安)單位主管 或資通安全專責人員
應變執行組組長	機關資通安全專責人員 或資訊人員	機關資訊(安)單位主管 或資通安全專責人員
後勤調度組組長	機關資通安全專責人員 或資訊人員	機關資訊(安)單位主管 或資通安全專責人員
財務行政組組長	機關財務或秘書單位主管	

（一）事件指揮官

為通報應變小組總召集人，綜理全般業務，直接督導各單位聯絡人員及機關新聞官/組。

（二）新聞官/組

視事件需要由事件指揮官或其授權人員擔任新聞官或分組代表，資通安全事件對外發布新聞或說明之單一窗口，綜整與定期更新訊息及擬定溝通計畫。

（三）執行秘書

為事件指揮官幕僚，負責督辦通報應變小組各項業務。

（四）情資及計畫組

1. 本分組負責辦理下列事宜：

(1) 資通安全事件通報及情資分享：透過資通安全監控中心(SOC)、防毒軟體及系統釐清事件影響，並清查各單位受影響情形，據以完成資通安全事件各階段通報，分享惡意程式 IoC 等。

(2) 應變策略及計畫研擬：於發生重大資通安全事件時，依據事件情況研擬損害控制、復原作業及跡證保存計畫。

2. 本分組由機關資通安全專責人員、資訊人員及委外廠商或外部專家組成，上級機關、中央目的事業主管機關或相關機關，亦應視情況或納入政風單位派員參與，以提供必要之支援協助。

（五）應變執行組

1. 本分組負責辦理下列事宜：

(1) 執行損害控制：依據情資及計畫組研擬之應變策略及計畫，調度資訊及資通安全人員執行災害搶救及損害管制，防止次波攻擊及損害擴散。

(2) 復原作業：依據情資及計畫組研擬之復原作業，完成系統重建、弱點掃描或漏洞修補等事宜。

(3) 跡證保全及留存：確保受害系統與相關系統及網路設備事件日誌之保存及管理。

2. 本分組由機關資通安全專責人員、資訊人員、業務單位及委外廠商組成，上級機關、中央目的事業主管機關或相關機關得於機關申請支援時派員參與。

（六）後勤調度組

1. 本分組負責辦理下列事宜：

(1) 事件根因查找：依據系統保存跡證，完成鑑識分析，並追查防堵惡意中繼站。

(2) 提出改善建議：依據事件調查根因，提出短、中、長期改善建議。

(3) 彙整改善報告。

(4) 撰寫調查、處理及改善報告。

(5) 追蹤管考：針對機關單位已結案或未結案事項，如有未盡改善事宜，將另案追蹤管考。

2. 本分組由機關資通安全專責人員、資訊人員及委外廠商或外部專家組成，上級機關、中央目的事業主管機關或相關機關得於機關申請支援時派員參與。

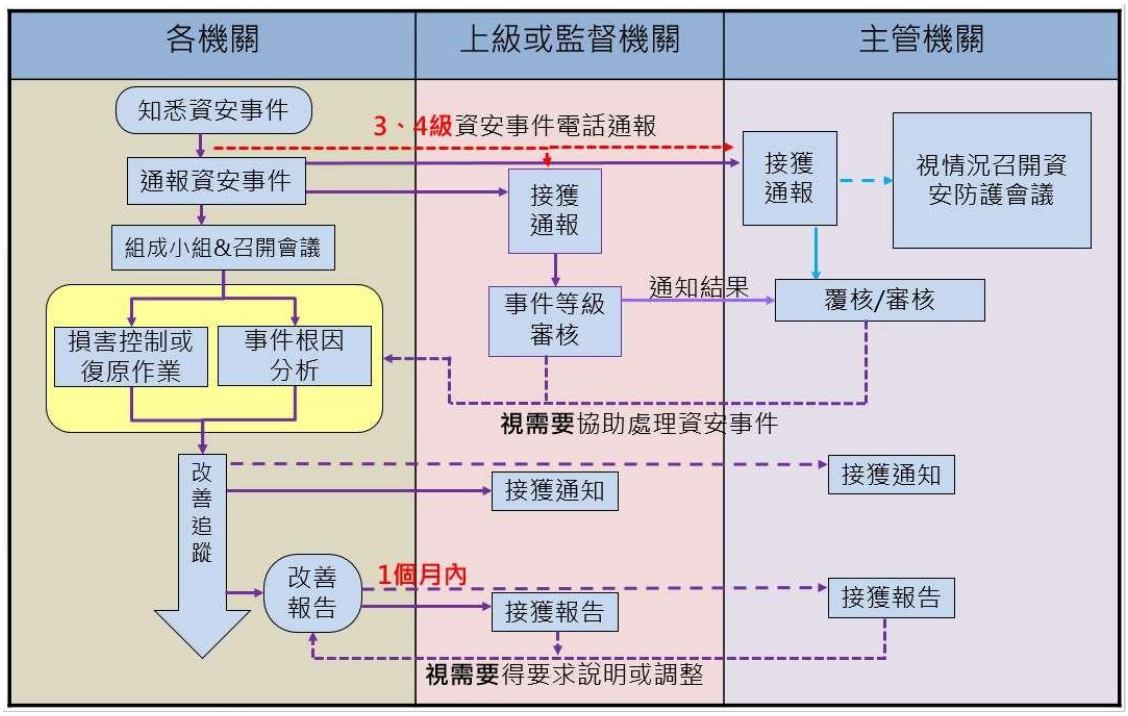
（七）財務行政組

本分組視事件需要由機關財務或秘書單位組成，負責辦理預算調撥及提供行政支援事宜。

各機關得以現有分組為基礎，依各機關編制及業務分工，經機關資通安全長同意後調整通報應變小組組成及各分組代表，另得視資通安全事件或機關資通環境需要調整各分組任務。

三、各機關之資通安全事件通報及應變程序，應包含通報資通安全事件、組成通報應變小組與召開事件應變會議、損害控制或復原作

業、事件根因分析及改善追蹤等項目(如圖二)，並依本法施行細則第六條第一項第九款規定納入資通安全維護計畫中，各項程序如下：



圖二、資通安全事件通報及應變程序

（一）通報資通安全事件

1. 各機關應依本法及資通安全事件通報及應變辦法規定，由情資及計畫組依主管機關或中央目的事業主管機關指定方式完成事件通報。

2. 第三級或第四級資通安全事件，各機關除依前目規定通報外，應另以電話或其他適當方式通知上級機關或中央目的事業主管機關，無上級機關者，應通知主管機關；行政院資通安全處(數位發展部資通安全署成立後為該署)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） 組成通報應變小組與召開事件應變會議

各機關於完成第三級或第四級資通安全事件之初步損害控制

後應召開事件應變會議，會議形式不拘，由事件指揮官主持討論下列事項，並得視情況邀請上級機關、中央目的事業主管機關或主管機關出席：

1. 資通安全事件概況。

2. 評估受影響範圍。

3. 其他必要之討論事項。

（三） 損害控制或復原作業

1. 由應變執行組執行損害控制或復原作業，並辦理下列事項：

(1) 確認具體受害範圍，並優先恢復對外服務及核心資通系統運作，防止次波攻擊及擴散情形。

(2) 評估各系統是否於可容忍中斷時間內恢復服務及對利害關係人之影響，決定是否對外公告事件之相關內容。

(3) 於完成損害控制或復原作業後，依主管機關或中央目的事業主管機關指定之方式完成通知作業。

2. 第三級或第四級資通安全事件，除依前目規定辦理外，並應辦理下列事項：

(1) 定時向事件指揮官、通報應變小組成員、上級機關或中央目的事業主管機關回報控制措施成效；無上級機關者，應回報主管機關。

(2) 倘涉及個人資料外洩，應評估通知當事人之適當方式，依個人資料保護法第十二條規定辦理。

（四） 事件根因分析

由後勤調度組執行，依資通安全事件等級，建議辦理事項如下：

1. 依第四點跡證保存之規定保存相關跡證，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。

2. 除設備故障外，後勤調度組應依據前目保存跡證，由組長督導委外廠商或外部專家進行根因調查，並提出紀錄分析；如發現惡意程式，應提出惡意程式分析。

3. 依據事件調查根因分析結果，機關應評估短、中、長期資安管理改善策略，其內容如下：

   (1) 短期：完成可立即性修補項目之調整，例如更換密碼或修補程式弱點等。

   (2) 中期：依據事件根因提出三至六個月內完成之強化作為，例如盤點機關老舊設備，並訂定汰換期程。

   (3) 長期：依據事件受害情形，視需要提出二年內完成之管理改善建議，例如培養機關資安人員能力。

4. 由執行秘書將事件調查根因及改善策略提報事件指揮官裁處，並由機關資通安全專責人員彙整送交上級機關或中央目的事業主管機關；無上級機關者，應送交主管機關。

（五） 改善追蹤

各機關進行事件改善追蹤時，應視需要召開會議，並據以辦理下列事項：

1. 評估改善作為期程。

2. 評估執行成效，並據以調整改善策略。

3. 配合上級機關、中央目的事業主管機關或主管機關辦理相關改善作為。

4. 第三級或第四級資通安全事件，應由執行秘書將各階段改善措施執行成效定期回報事件指揮官至完成各項改善措施為止，並由機關資通安全專責人員彙整送交上級機關或中央目的事業主管機關；無上級機關者，應送交主管機關。

5. 依主管機關或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；第三級或第四級資通安全事件，應另以密件公文將該報告送交主管機關及上級或監督機關。

6. 機關送交調查、處理及改善報告後，相關改善事項應納入機關現行定期追蹤管考機制。

四、跡證保存

為確保資通安全事件發生時，各機關所保有跡證足以進行事件根因分析，各機關依資通安全事件等級，建議辦理下列事項，並應視事件情形辦理其他必要之跡證保存事項：

（一） 各機關於日常維運資通系統時，應依自身資通安全責任等級保存日誌(log)，並建議定期備份至與原稽核系統不同之實體系統，其保存範圍及項目如表二。

表二、保存範圍及項目

資通安全責任等級	保存範圍	保存項目
A	機關應保存全部資通系統與各項資通及防護設備最近六個月之日誌紀錄。	1. 作業系統日誌(OS event log) 2. 網站日誌(web log) 3. 應用程式日誌(AP log) 4. 登入日誌(logon log)
B	機關應保存全部核心資通系統與相連之資通及防護設備最近六個月之日誌紀錄。	
C	機關應保存全部核心資通系統最近六個月之日誌紀錄。	

註：若資訊系統已向上集中者，則可由上級機關保存。

（二）發生資通安全事件時，機關應依下列原則進行跡證保存：

1. 機關進行跡證保存時，應優先採取隔離機制，包含設備關機、網路連線中斷或隔離、關閉服務、限制連線、限制權限、有限度修補漏洞等方式，以降低攻擊擴散。
2. 若系統無備援機制，應備份受害系統儲存媒介(例如硬碟、虛擬機映像檔)後，以乾淨儲存媒介重建系統，於完成系統測試後提供服務。
3. 若系統有備援機制，應將服務切換至備援系統提供服務，並保留受害系統及設備，於完成事件根因分析或完整備份後重建系統，經系統測試後切換至原系統提供服務。
4. 若備援設備亦為受害範圍，於重建受害系統時應以維持最低限度對外運作為原則，保存受害跡證。

（三） 各機關於簽訂資通系統或服務之委外契約時，應依前二款規定於契約中明定紀錄保存及備份規定。