臺北市政府資通安全事件通報及應變作業程序

中華民國113年9月4日府資安字第1133009892號函頒

壹、 總則

一、 臺北市政府(以下簡稱本府)為確保本府所屬公務機關、學校及受監督行政法人於發生資通安全事件時，依資通安全管理法(以下簡稱本法)、資通安全事件通報及應變辦法及各機關資通安全事件通報及應變處理作業程序等相關規定，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，特訂定本作業程序。

二、 本作業程序適用對象(以下簡稱各機關)如下:

(一) 依臺北市政府組織自治條例第六條至第八條規定設置之局、處、委員會、區公所，及該等機關所轄機關、機構。

(二) 臺北市依自治條例設置之行政法人。

三、 本作業程序之名詞定義如下:

(一) 資通安全事件:指發生於各機關之系統、服務或網路狀態，經鑑別可能有違反資通安全政策或保護措施失效之狀態，影響資通系統機能運作，構成資通安全政策威脅之事件。

(二) 資訊主管人員:指依臺北市政府各機關資訊組織及人力管理作業要點，各機關資訊業務專責一級單位主管、資訊業務專責二級單位主管、資訊推動任務編組主管或資訊業務主辦單位主管人員；與行政法人指定之主管人員。

（三）資訊業務人員：指依臺北市政府各機關資訊組織及人力管理作業要點，各機關資訊業務專責一級單位、資訊業務專責二級單位、資訊推動任務編組內，實際從事資訊業務之正式編制公務人員、約聘人員、約僱人員、約用人員及臨時人員；與行政法人實際從事資訊業務之編制人員、約聘人員、約僱人員、約用人員及臨時人員。

四、 各機關資通安全事件通報及應變程序，應包含通報資通安全事件、組成資通安全事件通報及應變小組(以下簡稱通報應變小組)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，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，資通安全事件通報及應變程序如附件一。

貳、資通安全事件通報窗口

五、 各機關應指定資通安全事件通報窗口(以下簡稱通報窗口)，納入通報應變小組成員，處理通報及聯繫相關事宜，並於機關知悉資通安全事件時，協助完成資通安全事件等級判斷，至數位發展部資通安全署(以下簡稱資安署)國家通報應變網站(以下簡稱通報應變網站)，於規定時限內完成通報。

六、 各機關依資通安全等級分級辦法應設置資通安全專責人員者，通報窗口應由該專責人員擔任；未設置資通安全專責人員或從缺者，應由機關首長或資通安全長指定適任人員擔任通報窗口，不得由委外廠商人員擔任。

七、 臺北市政府資訊局(以下簡稱資訊局)應建立通報窗口間通知及聯繫機制，各機關應確保通報窗口如實運作，維持聯絡管道全天暢通。

八、　各機關通報窗口人員名單應提交資訊局登錄，通報窗口如有異動，應於異動生效日前，以電話或公務雲(TaipeiON)通知資訊局，配合完成資料更新。

九、　各機關之通報窗口因故無法執行職務時，機關應指定熟悉相關法令、作業及系統操作程序之人員擔任代理人，並事先完成使用權限或通訊群組成員設定之申請及生效。

參、資通安全事件通報

十、　各機關知悉資通安全事件，應立即通知機關通報窗口，會同相關權責人員，完成資通安全事件等級判斷，經資通安全長或其授權人員核可，於知悉資通安全事件後一小時內至通報應變網站，由通報窗口完成通報。

十一、　各機關知悉資通安全事件，如因網路或電力中斷等事由，致無法依前點方式進行通報者，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，將該次資通安全事件應通報之內容及無法依規定方式通報之事由，告知資安署所指定或認可之人員，並於事由解除後，依原方式補行通報。

十二、　各機關知悉資通安全事件，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, 應於知悉資通安全事件後一小時內，以電話或公務雲(TaipeiON)通知該機關之通報窗口。

十三、　各機關如將部分或全部資通業務委託其他機關(構)或廠商辦理時，應與受託機關(構)或廠商約定，於知悉資通安全事件時，應即向機關權責人員，以電話或其他雙方事先約定之方式進行通報，並依機關指示提供相關之紀錄或資料。

十四、　以中央機關為資通安全事件通報對象之各機關，應於完成資

通安全事件通報日(含)起三天內，將通報及最新處置內容副知資訊局。

肆、資通安全事件等級審核

十五、 資訊局應於各機關完成資通安全事件通報後之下列時限內，完成資通安全事件等級審核：

（一）通報為第一級或第二級之資通安全事件者，於接獲通報後八小時內。

（二）通報為第三級或第四級之資通安全事件者，於接獲通報後二小時內。

十六、 資訊局進行審核時，得要求通報之各機關提供級別判斷所需之資料或紀錄，資訊局依規定於通報應變網站完成資通安全事件等級之審核，並提供審核依據相關資訊。

十七、 資通安全事件等級如有變更，應於通報應變網站提出等級變更申請。

伍、通報應變小組組成與事件應變會議召開

十八、 各機關知悉資通安全事件，應於下列時限內，完成通報應變小組組成：

（一）通報為第一級及第二級資通安全事件者，於知悉資通安全事件三小時內。

（二）通報為第三級及第四級資通安全事件者，於知悉資通安全事件一小時內。

十九、 通報應變小組之組成如附件二，其成員及任務如附件三。各機關得因應組織規模、人力及事件狀況予以調整。

二十、 各機關於完成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，就下列事項

進行討論，第三級或第四級資通安全事件並得視情形邀請上級機關、監督機關或資訊局出席：

（一）資通安全事件概況。

（二）評估受影響範圍。

（三）其他必要之討論事項。

陸、損害控制或復原作業

二十一、各機關知悉資通安全事件後，應於下列時間內完成損害控制或復原作業，並於通報應變網站完成通知或登錄：

（一）通報為第一級及第二級資通安全事件者，於知悉資通安全事件七十二小時內。

（二）通報為第三級及第四級資通安全事件者，於知悉資通安全事件三十六小時內。

二十二、損害控制或復原作業內容包括但不限於下列事項，應留存作業相關電子或書面紀錄：

（一）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。

（二）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，決定是否對外公告資通安全事件之相關內容。

二十三、發生第三級或第四級資通安全事件之各機關，除依前點規定辦理外，並應辦理下列事項：

（一）損害控制或復原作業完成時，向各機關之事件指揮官、通報應變小組成員及上級機關、監督機關與資訊局回報控制措施成效。

（二）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。

柒、跡證保存

二十四、各機關於日常維運資通系統時，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，並建議定期備份至與原系統不同之實體系統，上開日誌保存項目包括但不限於下列項目：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)。

二十五、各機關知悉資通安全事件，應依下列原則進行跡證保存：

（一）各機關進行跡證保存時，應優先採取隔離機制，包含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。

（二）若系統無備援機制，應備份受害系統儲存媒介（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。

（三）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。

（四）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。

二十六、各機關於簽訂資通系統或服務之委外契約時，應依前二點規定於契約中明定保存及備份規定。

捌、資通安全事件根因分析

二十七、依跡證保存之規定保存相關跡證，相關採證與可疑之惡意程

式應交付至本府指定之鑑識採證檔案交換區，另如有惡意程式應配合資安署規定上傳至 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。

二十八、除設備故障外，應依據前點保存跡證，督導委外廠商或外部專家進行根因調查，並提出紀錄分析；如有發現惡意程式，應提出惡意程式分析。

二十九、各機關應依據資通安全事件調查根因分析結果，研擬短、中、長期資安管理改善策略，其內容如下：

（一）短期：完成可立即修補項目之調整。

（二）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：盤點各機關老舊資通系統或設備，並訂定汰換期程。

（三）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：培養各機關資安人員能力或納入風險議題，進行風險管控措施。

三十、　資通安全事件調查根因及改善策略應提報各機關事件指揮官裁處，並彙整送交上級機關、監督機關及資訊局。

玖、改善追蹤

三十一、各機關進行資通安全事件改善追蹤時，應視需要召開會議，辦理下列事項：

（一）評估改善作為期程。

（二）評估執行成效，並據以調整改善策略。

（三）配合上級機關、監督機關及資訊局辦理相關改善作為。

（四）第三級或第四級，或上級機關、監督機關、資訊局指定

之資通安全事件，應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，並彙整送交上級機關、監督機關及資訊局。

（五）依會議決議，於知悉該事件後一個月內至通報應變網站完成結報作業。

（六）各機關完成結報作業後，相關改善事項應納入本府資安管考系統與各機關現行定期追蹤管考機制，並於府級資通安全長會議定期檢討改善。

（七）如係由資訊局支援資通安全事件之調查與鑑識者，應於事件調查完成後將報告檢送請求支援機關，內容包含事件發生時間、來源與目標 IP、駭客所在位置、攻擊方法、路徑與影響分析，以及系統復原、事件排除、修補、防禦等措施(含：系統重新安裝與設定、系統隔離修護、調整防火牆、更新系統安全或防毒軟體修正檔、弱點修補或新增防禦設備等建議)，各機關得參考本報告製作調查、處理及改善報告。

拾、紀錄留存及管理程序之調整

三十二、各機關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，相關紀錄並應經承辦之權責人員、資通安全長簽核。

三十三、各機關於完成資通安全事件之通報及應變程序後，應依據實際處理之情形，於必要時對人力配置或其他相關事項進行修正或調整。

拾壹、資通安全情資分享

三十四、各機關處理資通安全事件應依資通安全情資分享辦法，按資

安署與本府指定之情資分享方式分享資通安全情資。

前項所稱資通安全情資，指包括下列任一款內容之資訊：

（一）資通系統之惡意偵察或情蒐活動。

（二）資通系統之安全漏洞。

（三）使資通系統安全控制措施無效或利用安全漏洞之方法。

（四）與惡意程式相關之資訊。

（五）資通安全事件造成之實際損害或可能產生之負面影響。

（六）用以偵測、預防或因應前五款情形，或降低其損害之相關措施。

（七）其他與資通安全事件相關之技術性資訊。

拾貳、社交工程演練

三十五、各機關應依下列規定參與或辦理社交工程演練：

（一）使用資訊局建置之市府公務電子信箱者，每年至少兩次統一參與本府辦理之社交工程演練。

（二）未使用資訊局建置之市府公務電子信箱，自建或使用其他電子信箱系統者，得依第一款規定辦理或每年至少兩次自行或參與上級機關、監督機關辦理之社交工程演練；未參與本府社交工程演練之機關，應於完成演練後一個月內，將執行情形及成果報告送資訊局備查。

三十六、各機關之社交工程演練結果未符合資訊局所定標準者，資通安全長應召開檢討會議，並提出檢討報告送資訊局備查；機關如連續兩次以上均未符合標準時，除加強教育訓練外，並得視其情節提報府級資通安全長會議報告。

各機關之人員未符合資訊局所定標準者，應參與一小時之資通安全強化教育訓練，並以實體課程為原則，由機關聘請符

合資訊局所定資格之講師，自行辦理之。

拾參、資通安全事件通報及應變演練

三十七、資通安全事件通報及應變演練分準備、執行及檢討改善等三個階段：

（一）準備階段：調集相關人力及資源，並完成資通安全事件通報及應變演練規劃。

（二）執行階段：由演練主持人下達情境指令，依據演練流程進行推演，過程中各參與應變人員可相互討論、激盪，交流出最適當的應變行動並執行之，過程中應詳細紀錄所有情境或突發狀況下達、人員執行應變行動等時序，提供作為檢討座談會使用。

（三）檢討改善階段：演練結束後，由主持人召集所有參與人員舉行檢討座談會，針對流程一一檢視是否應變得宜，及如何再精進，人員並藉由檢討座談會，從中學習及調整。

三十八、資通安全事件通報及應變演練方式，得視對於作業影響程度及實際作業需要，採實際作業演練或兵棋推演。

前項所稱兵棋推演，指利用桌上及紙上作業模擬資通安全事件發生情境，藉此訓練應變人員面對各種情境之判斷能力及應變效率。

三十九、府級資通安全事件通報及應變演練規定如下：

（一）本府每年至少辦理一次府級資通安全事件通報及應變演練。

（二）府級資通安全事件通報及應變演練辦理時，各機關應按資通安全事件等級，依規定完成資通安全事件通報

及審核、通報應變小組組成、事件應變會議召開及其他應變措施。

（三）各機關如未符合資訊局所定之標準者，本府得於三個月內對該機關重新進行演練，至符合標準為止。

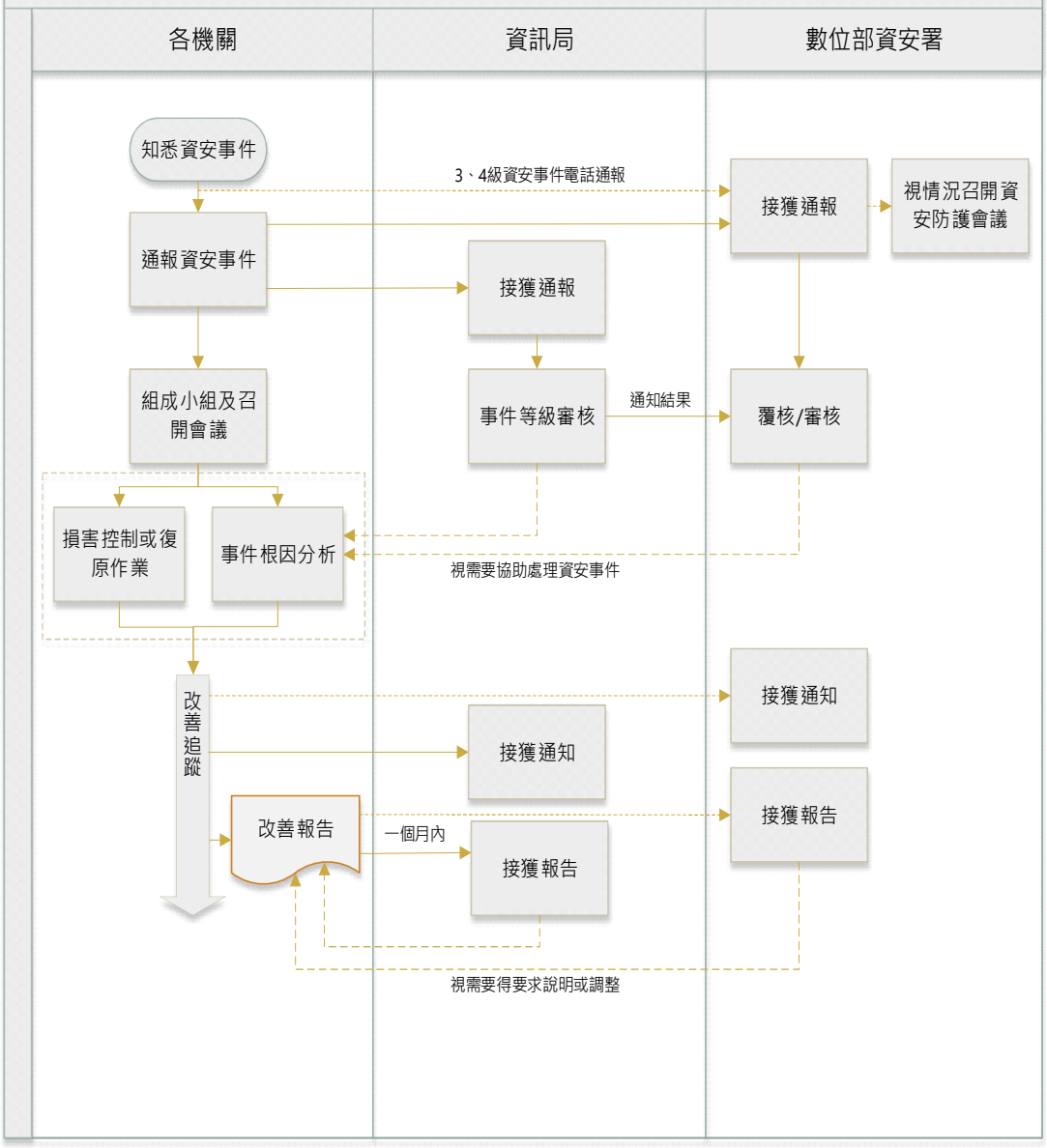
四十、　各機關得視需要自行辦理資通安全事件通報及應變演練。

拾肆、其他

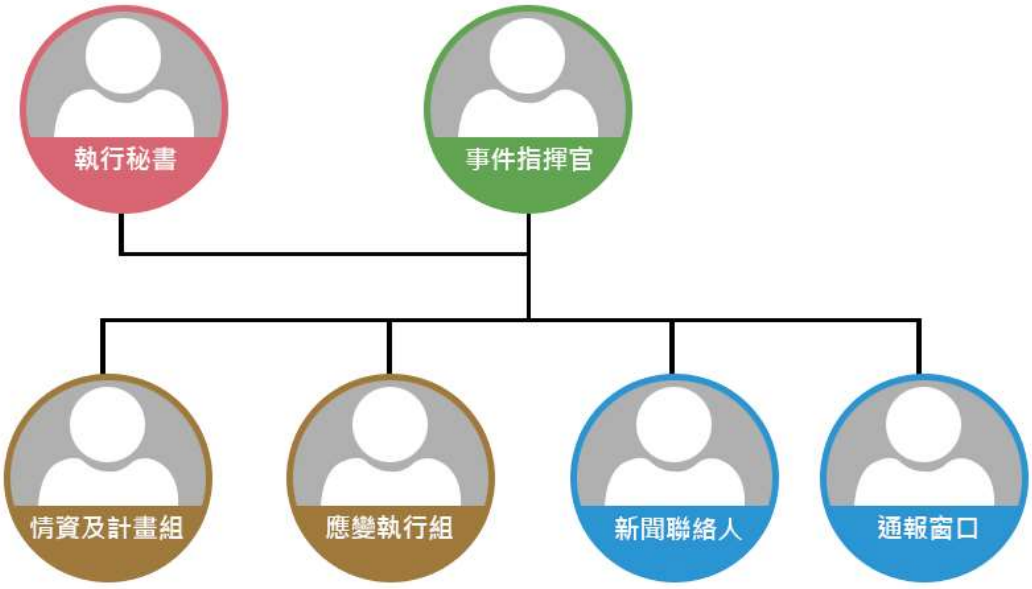
四十一、學校資通安全事件通報及應變程序應依「臺灣學術網路各級學校資通安全通報應變作業程序」辦理，並準用本作業程序第六點至第九點、第十二點至第十四點、第二十三點第二款及第二十四點至第二十六點規定。

「臺灣學術網路各級學校資通安全通報應變作業程序」如與資安署法令不一致者，應依資安署法令規定辦理。

附件一：各機關資通安全事件通報及應變程序



附件二：各機關資通安全事件通報及應變小組組成



附件三：各機關資通安全事件通報及應變小組成員及任務

分組/職務	成員	任務
事件指揮官	1. 各機關(行政法人、資訊局除外)發生第一級及第二級資通安全事件時，事件指揮官為資訊單位主管或資通安全長，未設置資訊單位者，事件指揮官為資通安全長；各機關發生第三級及第四級資通安全事件時，事件指揮官為資通安全長或機關首長。 2. 行政法人發生第一級及第二級資通安全事件時，事件指揮官為資訊(安)業務權責單位主管或資通安全長；各機關發生第三級及第四級資通安全事件時，事件指揮官為資通安全長或機關首長。 3. 資訊局發生第一級及第二級資通安全事件時，事件指揮官為資通安全中心主任或資通安全長；資訊局發生第三級及第四級資通安全事件時，事件指揮官為資通安全長或機關首長。	為通報應變小組總召集人，綜理全般業務，直接督導各分組及成員。
執行秘書	1. 事件指揮官為機關首長時，執行秘書為資通安全長。	協助事件指揮官，督辦通報應變小組各項業務。

分組/職務	成員	任務
	2. 各機關(行政法人、資訊局除外)之事件指揮官為資通安全長時，執行秘書為資訊單位主管或從略，未設置資訊單位者，由事件指揮官指派適任人員或從略；事件指揮官為資訊單位主管時，執行秘書由事件指揮官指派適任人員或從略。 3. 行政法人之事件指揮官為資通安全長時，執行秘書為資訊(安)業務權責單位主管或從略；事件指揮官為資訊(安)業務權責單位主管時，執行秘書由事件指揮官指派適任人員或從略。 4. 資訊局之事件指揮官為資通安全長時，執行秘書為專門委員或簡任高級分析師或從略；事件指揮官為資通安全中心主任時，執行秘書為高級分析師、資安股股長或從略。	
新聞聯絡人	由各機關新聞聯絡人或發言人兼任，或由事件指揮官因應個別事件需要指派適任人員。	資通安全事件對外發布新聞或說明之單一窗口，負責綜整與定期更新訊息及擬定溝通計畫或策略。
通報窗口	各機關如依資通安全等級分級辦法設置有資通安全專責人員，通報窗口應由資通安全專責人員擔任，未設	1. 協助完成資通安全事件等級判斷及核准。

分組/職務	成員	任務
	置資通安全專責人員或從缺時,由各機關首長或資通安全長指派適任人員，	2. 於知悉資通安全事件後一小時內至通報應變網站，完成通報。 3. 事件如涉及其他機關或應由其他機關依其法定職權處理時，依本作業程序或資訊局指定或認可之方式、時限及對象完成相關機關通報。
情資及計畫組	1. 各機關(行政法人、資訊局除外)事件指揮官為機關首長或資通安全長時,情資及計畫組長為資訊單位主管，未設置資訊單位者，由事件指揮官指派適任人員；事件指揮官為資訊單位主管時，情資及計畫組長由事件指揮官指派資訊單位內適任人員。 2. 行政法人事件指揮官為機關首長或資通安全長時,情資及計畫組長為資訊(安)業務權責單位主管；事件指揮官為資訊(安)業務權責單位主管時,情資及計畫組長由事件指揮官指派資訊(安)業務權責單位內適任人員。 3. 資訊局事件指揮官為機關首長或資通安全長時,情資及計畫組長為資通安全中心主任；事件指揮官為資通安	1. 資通安全事件通報及情資分享：透過本府或機關資通安全監控中心(SOC)、內外部情資、資安或網路設備釐清事件影響，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，分享惡意程式或中繼站等。 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。 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。 4. 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。 5. 追蹤管考:針對各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。

分組/職務	成員	任務
	全中心主任時，情資及計畫組長為高級分析師或資安股股長。 4. 情資及計畫組成員包括資通安全專責人員、資訊人員、委外廠商或外部專家組成，機關政風單位、上級機關及相關機關亦得視情況參與，提供必要之支援協助。	6. 提出改善建議：依據事件調查根因，提出短、中、長期改善建議。
應變執行組	1. 各機關(行政法人、資訊局除外)事件指揮官為機關首長或資通安全長時，應變執行組長為資通安全事件發生單位主管；事件指揮官為資訊單位主管時，應變執行組長由資通安全事件發生單位主管指派該單位內二級單位主管或職等或職務最高編制內人員擔任。 2. 行政法人事件指揮官為機關首長或資通安全長時，應變執行組長為資通安全事件發生單位主管；事件指揮官為資訊(安)業務權責單位主管時，應變執行組長由資通安全事件發生單位主管指派該單位內二級單位主管或職等或職務最高編制內人員擔任。	1. 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. 調查、處理及改善報告：彙整、撰寫提報調查、處理及改善報告。

分組/職務	成員	任務
	3. 資訊局事件指揮官為機關首長或資通安全長時，應變執行組長為資通安全事件發生單位主管；事件指揮官為資通安全中心主任時，應變執行組長由資通安全事件發生單位股長或高級分析師。 4. 應變執行組成員包括資通安全專責人員、資訊人員、委外廠商或外部專家，各機關財務單位、秘書單位亦得視情況參與，提供必要之支援協助。	