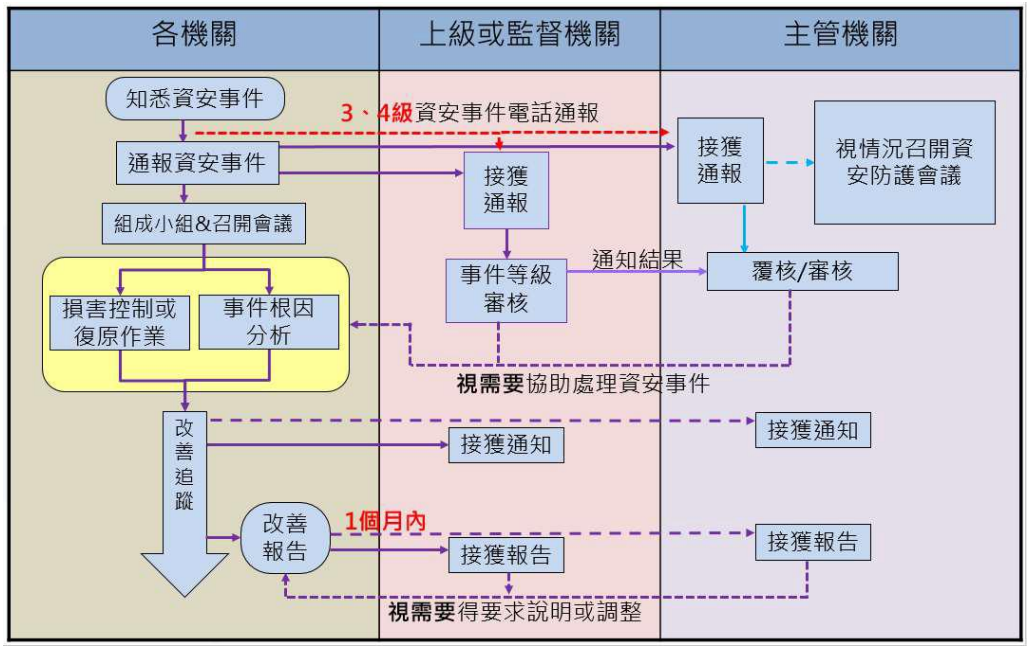
修正各機關資通安全事件通報及應變處理作業程序第三點

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；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）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。