資安法規重點
與
實務案例

資通安全署
113年6月

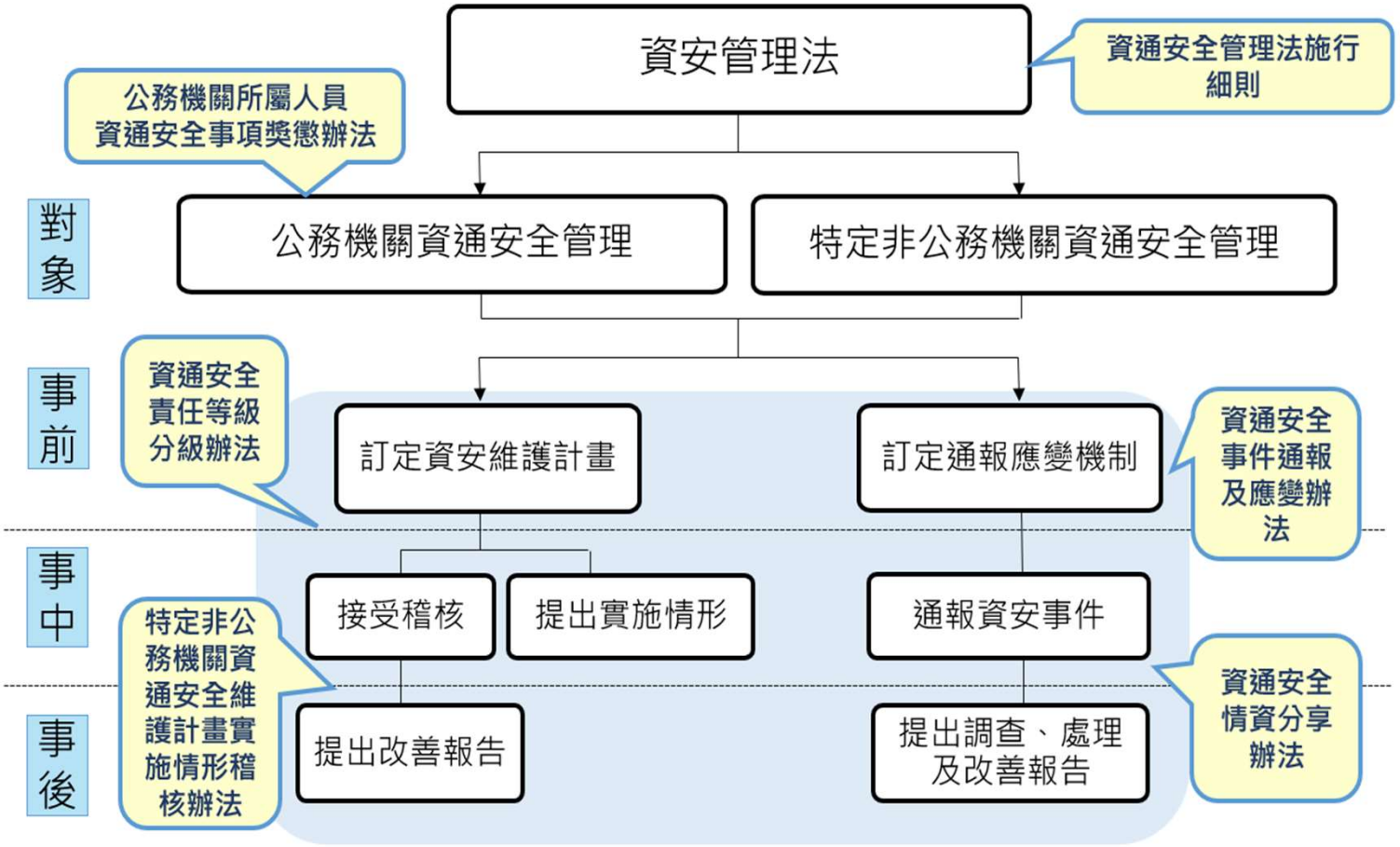
壹、

資安法現況說明

01 資安法架構

02 修正重點說明

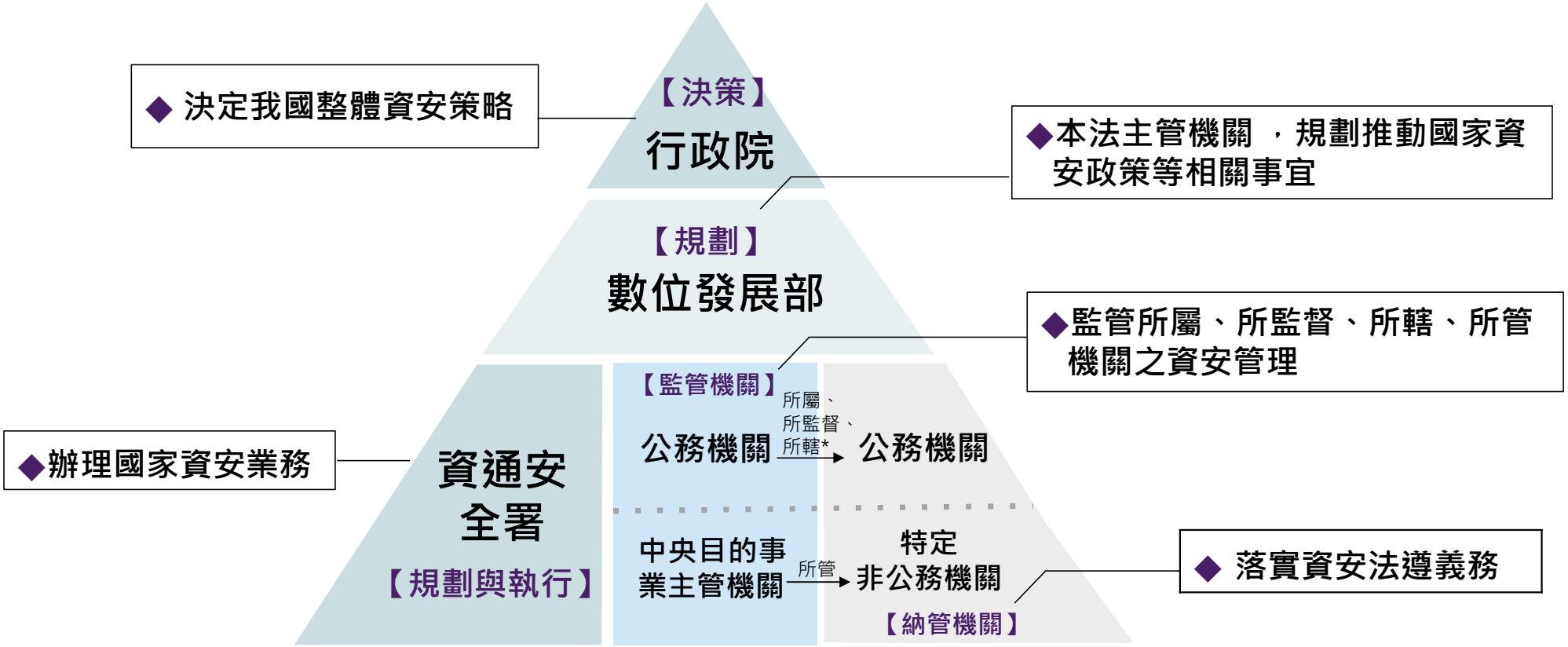
資安法架構


資安管理法
資通安全管理法施行細則
公務機關所屬人員資通安全事項獎懲辦法
對象
公務機關資通安全管理
特定非公務機關資通安全管理
事前
資通安全責任等級分級辦法
訂定資安維護計畫
訂定通報應變機制
資通安全事件通報及應變辦法
事中
接受稽核
提出實施情形
通報資安事件
特定非公務機關資通安全維護計畫實施情形稽核辦法
事後
提出改善報告
提出調查、處理及改善報告
資通安全情資分享辦法

政策目標1：明確機關權責，強化合作協力

法規現況

- 強化合作協力：為建構我國資通安全整體環境，明定各機關權責事項，並強化國家資通安全會報功能，政府部門應配合執行。



【註】所轄公務機關：在直轄市政府係指直轄市山地原住民區公所及直轄市山地原住民區民代表會；在縣政府係指鄉（鎮、市）公所、鄉（鎮、市）民代表會

政策目標2：提升特定非公務機關資安人力

法規現況

應設置專職人員及資安長

✓ 強化特定非公務機關資通安全能量，比照公務機關應設置資安長及資安專職人員。

增訂對所屬人員之獎懲規定

✓ 特定非公務機關對於所屬人員辦理資通安全業務績效優良者，應予獎勵。

✓ 特定非公務機關所屬人員未依本法規定辦理，情節重大者，由特定非公務機關依規定予以懲處。

政策目標3：強化納管機關資安管理

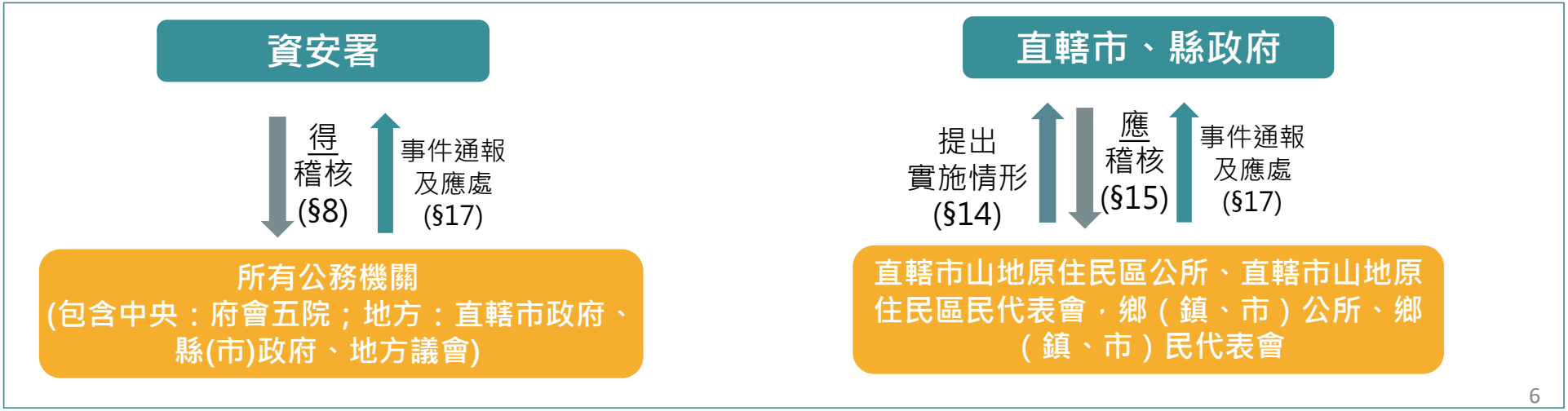
法規現況

● 強化聯防體系：協助無上級機關發現潛在風險

現況問題

- 無上級機關之公務機關，依現行法無外部稽核機制*審計部109年總決算審核報告指出
  - ✓ 中央：府會五院
  - ✓ 地方：直轄市政府、縣(市)政府、地方議會、直轄市山地原住民區公所、直轄市山地原住民區民代表會，鄉（鎮、市）公所、鄉（鎮、市）民代表會。

修正重點



政策目標4：明確法源

- **特定財團法人定義**

法規現況

政策重點

- 為避免各界混淆資安法以及財團法人法所規範之財團法人，政策目標如下：

全國性
- **財團法人法定義之政府捐助財團法人：捐助比例50%以上**
- **民間捐助財團法人+ (財團法人法)主管機關指定**

差異分析

- 資安法納管對象應以**對人民生活、經濟活動及公眾或國家安全有重大影響者**為政策目標
- **現行對象**：納管156個財團法人
- **目標對象**：納管136個財團法人

▲減少納管26個-政府捐助比例未達50%且未經指定者

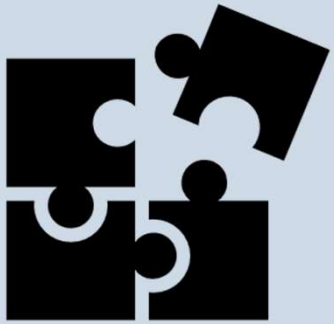
▲增加納管 6 個-中央目的事業機關所指定民間捐助之全國性財團法人

滾動調整資安法制，落實智慧國家願景

法規現況

1

明確機關權責
強化合作協力



2

精進資安
人力策略

3

強化納管機關
資安管理

資通安全管理法修法專區　https://moda.gov.tw/ACS/laws/draft-notice/1395

貳、

資安事件通報

01 公務機關資安事件通報統計

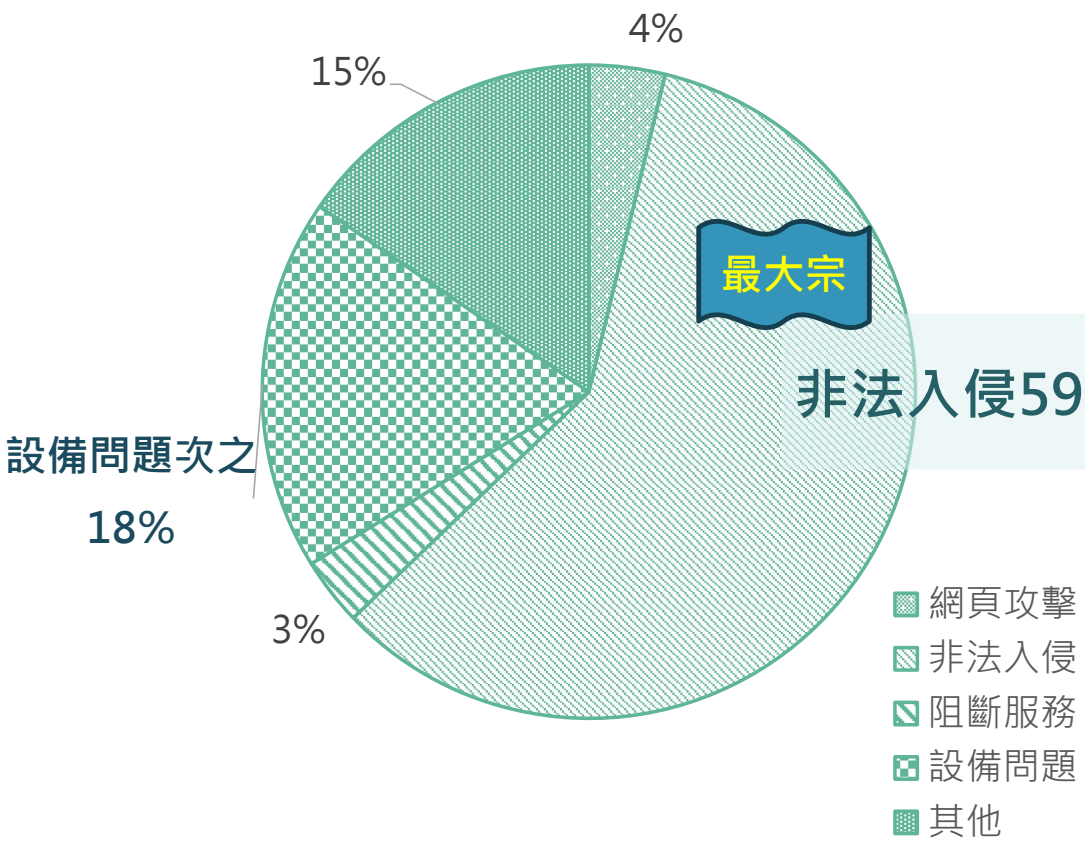
02 備妥無法於通報網通報之作法

03 事件通報常見問題與建議

資安事件通報統計

近1年資安事件分類占比

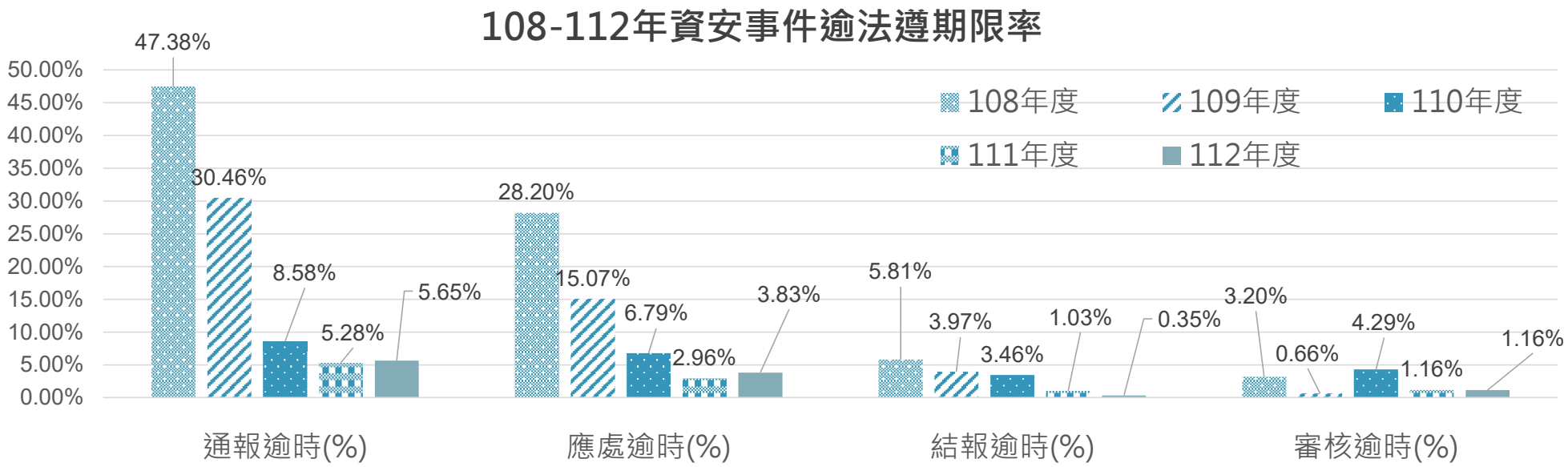
(統計範圍及對象：資安法納管對象不含實兵)



非法入侵為大宗主因：多為**弱密碼/密碼遭暴力破解、應用程式漏洞、網站設計不當**

設備問題以**醫療體系**為大宗，**財政體系次之，教育體系增多(機房失火影響向上集中機關)**

資安事件逾法遵期限建議措施



逾時原因

1. **未有法遵意識**如應處完成後才進行通報
2. **業務人員異動，未落實業務交接**
3. **資安專責人員不足**
4. **不熟悉通報應變網站操作**
5. **未落實代理人制度**

建議措施

1. 可參考網站操作手冊**及落實教育訓練**
2. **落實職務異動交接**
3. **落實代理人制度**
4. **加強法遵意識。**

備妥無法於通報網通報之作法

法規現況

事件通報

通報網帳號未完成異動程序時

或

例行性維護或系統異常時

- ✓ 以**紙本通報單(通報網首頁文件下載區)**進行通報，並以通報機關與審核機關約定方式傳送(電子郵件加密、傳真、電話等)，**留下完整時間註記(含通報及審核)**，以利後續確認法遵時間。(Tel: 02-27339922、Fax：02-27331655、E-Mail：service@nics.nat.gov.tw)
- ✓ 請備妥無法於系統通報之作法，並請機關納入**演練**，以強化整體處理作業。

https://www.ncert.nat.gov.tw/

2024/01/03	說明文件	CI紙本通報單_11301.rar MD5：53acd655572717fbdf000d91a042d4cc 關鍵基礎設施資通安全事件通報單
2024/01/03	說明文件	紙本通報單11212.rar MD5：735833c7084777e46ed9fc03add0ad09 紙本通報單

國家資通安全通報應變網站帳號盤點

- 依資通安全責任等級分級辦法附表十，機關應**定期審查**資通系統帳號之申請、建立、修改、啟用、停用及刪除，並定期審核。
- 為確保資安人員名單正確性，以利資安事件發生時可及時聯絡，請機關**落實盤點「國家資通安全通報應變網站」帳號**，及**更新機關資安長資訊**，並請依機關帳號權限管理相關規定，定期檢視更新。

參、

近期政府機關資安事件案例

01 近期資安事件案例

02 政府機關社群平臺使用注意事項

03 資安警訊通報查處

政府機關社群平臺使用注意事項

- 機關FB粉絲專頁遭駭客上傳不當影片，調查發現該專頁管理者為離職員工申請之**私人帳號**，未妥善管理帳號遭盜用。
- 機關FB粉絲專業管理人員因**誤點社交工程郵件**，導致管理者帳號密碼被盜取，因粉專私訊對話內留有民眾報名個資，故有個資外洩疑慮。

建議防範措施

- 建立社群平臺帳號管理機制並定期審核，**不限於機關自建系統**，應包含社群平台(FB、IG、Youtube等)、網站平台(協作平台、blog等) 。
- 帳號驗證啟用**雙重驗證機制**。
- 人員異動(離職)**應停用或刪除帳號**。
- **加強內部同仁資安觀念**，留意社交郵件，勿瀏覽不明網頁或點擊惡意連結。

資安警訊通報查處1/3

落實通報、鑑識釐清、精進強化

INT 警訊

1. **確認機關發生資安事件，才會發送INT警訊：**
   已偵測出機關有異常連線行為，而連線目的地與資安院中繼站清單相符，才會發出INT 警訊通知機關。
2. **收到INT警訊，請通報資安事件：**機關收到此類警訊時，應依資通安全管理法執行資安通報作業
3. **警訊內容若涉多個機關所管IP，由對應IP之機關分別通報：**
   考量通報時效，未及釐清時，可先由單一機關做整體通報，後續再由對應機關個別通報。
4. **未鑑識出結果，並非代表無受駭：**相關軌跡可能因被駭客清除、未妥善保留相關事證、跡證遭破壞、鑑識能量不足等而無法查證。

資安警訊通報查處2/3

資安鑑識注意事項

INT
警訊

1. **不侷限於異常連線追查：**中繼站可能會停用或移轉，鑑識範圍應應增加廣度，建議一併檢視案關周邊系統之安全性。例：**建議可由入侵所經過軌跡至受駭系統(如外部防火牆至資料庫系統)併同進行檢視**，若機關鑑識量能有限，可依自身情形評估適時向上級或主管機關提出支援。
2. **完整檢測**：除主機映像檔外，建議納入防火牆紀錄、主機及資料庫日誌等，查明相關異常活動及惡意程式，釐清駭入根因，以及早做出相對應之策略。
3. 委託鑑識廠商履約範圍及有效性，加強資安事件問題查找能力

資安警訊通報查處3/3

接獲情資續處

EWA 警訊

1. **EWA警訊發送時機：**機關系統或設備疑似存在弱點或可疑程式、疑似發起對外攻擊或發送惡意郵件，但尚未確認是否受駭。
2. **檢視確認，如被駭侵，請通報資安事件：**請機關依警訊內容，先進行檢視，若發現入侵事實(機密性、完整性或可用性受影響)，應依資通安全管理法執行資安事件通報作業。
3. **如有一步情資確認受駭，應於知悉時通報資安事件：**機關接獲EWA警訊，表示機關有被駭風險，實務上可能因機關釐清量能或跡證不足，第一時間未能發現受駭情形；**若機關後續發現或接獲本署以其他方式(如email)提供駭侵事證**，須依資安法執行資安通報作業。

肆、

資安事件跡證保存

跡證保存錯誤態樣

錯誤類型	實際情境	建議處理
判斷失誤	● 未能找出所有受駭之設備，使部份設備仍被駭客控制	● 擴大清查所有與受駭設備連線之主機
人為不當操作	● 持續操作已被駭侵的設備，徒增過多操作軌跡(如將異常程式壓縮存放於原設備)	● 停止操作受駭設備，進行硬碟或映像檔備份後，以備份檔進行鑑識分析
跡證保存不足	● 僅備份防火牆日誌，沒有備份其他相關網通設備或相關設備日誌	● 備份各項資通系統與資通及防護設備日誌
	● 日誌未依規定保存足夠天數	● 日誌應依規定保存至少6個月以上

資安事件跡證保存

- 資安事件發生時為保有跡證進行事件根因分析，**日誌紀錄**建議**定期備份**至與原日誌系統**不同實體**

附表十 資通系統防護基準 控制措施	保存範圍	保存項目
保留日誌至少 6 個月 (普級以上適用)	**各項資通系統**與**資通及防護設備**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)

參照「各機關資通安全事件通報及應變處理作業程序」、「政府機關（構）資安事件數位證據保全標準作業程序」

優先採取隔離機制

- ✓ **斷網**以避免攻擊擴散，由**資安人員**保全數位跡證。
- ✓ 備份受駭系統 (採映像檔備份或硬碟**備份**)，以供事件根因分析，並以乾淨儲存媒介**重建**。

應變3步驟

1. 拔線
2. 找人
3. 系統重建

建立鑑識映像檔注意事項

- 使用新的裝置來製作鑑識映像檔
- 映像檔須妥善保存，避免遭竊或遺失
- 映像檔製作完成後，應驗證hash值

- **如果可能的話，採Bit-by-Bit方式製作映像檔，以取得全部完整硬碟資料**
- **製作映像檔工具以下包含但不限於**
  - Windows與Unix/Linux的dd工具
  - 商用數位鑑識軟體及磁碟複製設備

數位證據保全標準作業程序

政府機關（構）資安事件數位證據保全標準作業程序

一、訂定目的

為使各級政府機關（構）於執行資安事件調查時能有效保全及運用數位證據，及執行人員於執行數位證據識別、蒐集、擷取、封緘及運送作業時有所依循，爰參考相關數位鑑識國際標準(ISO/IEC 27037 Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence，數位證據識別、蒐集、擷取及保存指引)，特訂定本作業程序。

二、適用機關

各級政府機關（構）(以下簡稱各機關)。

三、適用時機

各機關基於資安事件之調查，需進行電腦系統之數位證據識別、蒐集、擷取、封緘及運送作業時，適用本作業程序。

四、人員職掌

（一）數位證據保全人員

執行數位證據識別、蒐集、擷取、封緘及運送作業。

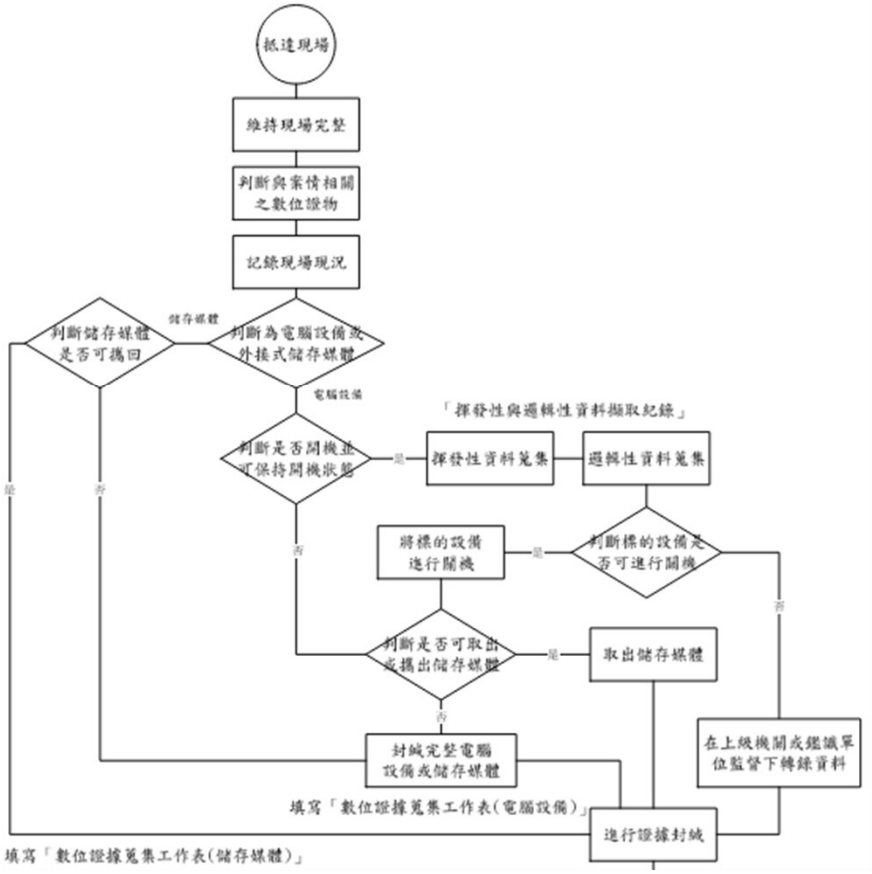
（二）記錄人員

1、視現場狀況，於數位證據保全人員執行數位證據識別、蒐集、擷取及封緘作業過程中，以錄影、拍照及其他方式記錄資安事件現場。

2、協助資安事件調查現場之秩序維持。

五、名詞定義

數位證據保全標準作業流程圖



數位發展部資通安全署

Administration for Cyber Security, moda

資安是持續精進的風險管理

參考資訊-資通安全署

- https://www.acs.gov.tw/

參考資訊-國家資通安全研究院

- https://www.nics.nat.gov.tw/