
# 資安及個資事件通報與應變

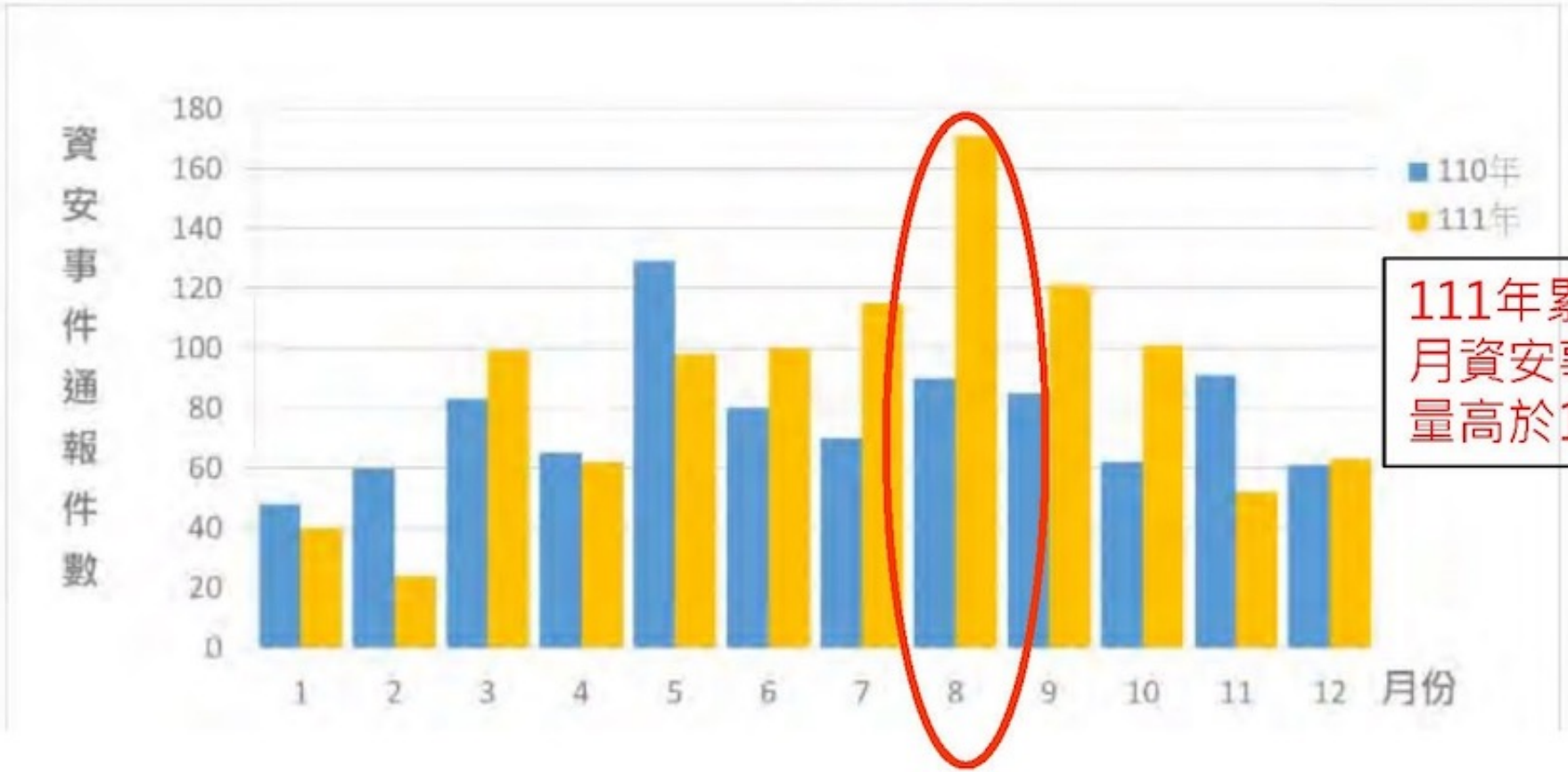
黃啓超 顧問

2023/08/11

# 大綱

- 資通安全事件判斷及通報
- 個人資料侵害事故通報及應變
- 違失案例宣導
- D051_個人電腦設定與軟體安裝查核表操作簡介

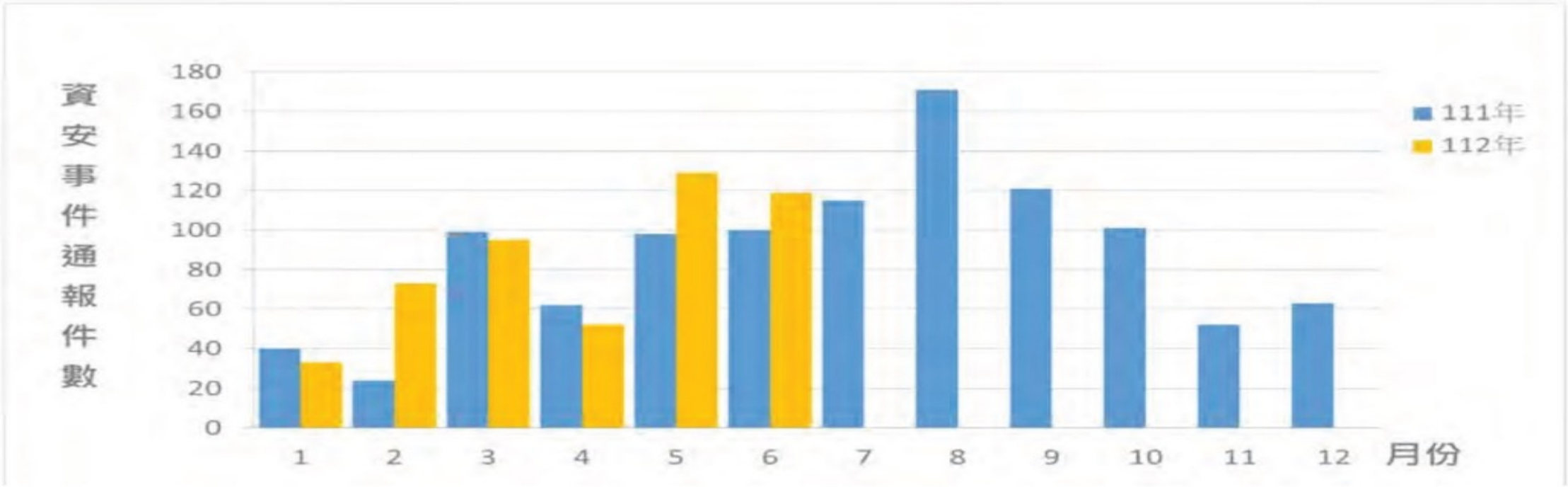
# 111年資安事件通報數量統計




資料來源：行政院國家資通安全會報-資安月報

# 112年6月資安事件通報數量統計

- 資安事件通報數量共119件，較去年同月增加19%，國家資通安全研究院偵測發現多個機關的資訊設備，嘗試下載木馬程式HiatusRAT，佔總通報數量11.77%，經機關調查後發現，受駭設備多為N牌路由器或防火牆等網通設備，後續已藉由重置與更新韌體版本進行應處，降低整體資安風險。




資料來源：行政院國家資通安全會報-資安月報

# 資安/個資責任誰來扛？？


資料來源：112年教育體系資安課程-校園資安與個資防護課程 鍾沛原

# 資安/個資是大家的責任！！

- 組織內每個人都要提升自己的資安及個資素養與應變能力，讓南大更好更精進。

# 資通安全事件判斷及通報

# 標準的要求（1/2）

| A.16資訊安全事故管理 | | | |
|---|---|---|---|
| 控制目標 | 資訊安全事故及改善之管理 | | |
| 控制項 | A.16.1.1 (I/P) | 責任及程序 | 應建立管理責任及程序，以確保對資訊安全事故做迅速、有效及有序之回應。 |
| | A.16.1.2 (I/P) | 通報資訊安全事件 | 應循適切之管理管道，儘速通報資訊安全事件。 |
| | A.16.1.3 (I/P) | 通報資訊安全弱點 | 應要求使用資訊系統及服務之員工及承包者，注意並通報任何系統或服務中所觀察到或可疑之資訊安全弱點。 |
| | A.16.1.4 (I/P) | 資訊安全事件評估及決策 | 應評鑑資訊安全事件，並決定是否將其歸類為資訊安全事故。 |
| | A.16.1.5 (I/P) | 對資訊安全事故之回應 | 應依文件化程序，回應資訊安全事故。 |

資料來源：教育體系資通安全暨個人資料管理規範

# 標準的要求（2/2）

| A.16資訊安全事故管理 | | | |
|---|---|---|---|
| 控制目標 | 資訊安全事故及改善之管理 | | |
| 控制項 | A.16.1.6 (I/P) | 由資訊安全事故中學習 | 應使用獲自分析及解決資訊安全事故之知識，以降低未來事故之可能性及衝擊。 |
| | A.16.1.7 (I/P) | 證據之收集 | 組織應定義及應用程序，以識別、蒐集、取得及保存可用作證據之資訊。 |

資料來源：教育體系資通安全暨個人資料管理規範

# 資通安全事件通報要求（1/3）

- 資通安全管理法-第十四條
  - 公務機關為因應資通安全事件，應訂定通報及應變機制。
  - 公務機關知悉資通安全事件時，除應通報上級或監督機關外，並應通報主管機關；無上級機關者，應通報主管機關。
  - 公務機關應向上級或監督機關提出資通安全事件調查、處理及改善報告，並送交主管機關；無上級機關者，應送交主管機關。
  - 前三項通報及應變機制之必要事項、通報內容、報告之提出及其他相關事項之辦法，由主管機關定之。

◆ 資通安全管理法-第二條：本法之主管機關為行政院。

# 資通安全事件通報要求（2/3）

- 資通安全管理法施行細則-第八條
  - 本法第十四條第三項及第十八條第三項所定資安事件調查、處理及改善報告，應包括下列事項：

    一、事件發生或知悉其發生、完成損害控制或復原作業之時間。

    二、事件影響之範圍及損害評估。

    三、損害控制及復原作業之歷程。

    四、事件調查及處理作業之歷程。

    五、事件根因分析。

    六、為防範類似事件再次發生所採取之管理、技術、人力或資源等層面之措施。

    七、前款措施之預定完成時程及成效追蹤機制。

# 資通安全事件通報要求（3/3）

- 資通安全事件通報及應變辦法
  - 使各受規範對象得妥適辦理資通安全事件之通報及應變，以降低資通安全事件之發生機率，或於事件發生時可迅速妥適因應，有效降低損害。
- 本校『資通安全事件管理程序書』（NUTN-ISMS-B011）。

# 資通安全事件回應（1/2）

- 資通安全事件通報及應變辦法
  - 資通安全事件分為四級。
  - 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。

# 資通安全事件回應（2/2）

- 資通安全事件通報及應變辦法（續）
  - 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。
  - 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。

# 資通安全事件分級（1/4）

- 第一級資通安全事件
  - 非核心業務資訊遭輕微洩漏。
  - 非核心業務資訊或非核心資通系統遭輕微竄改。
  - 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。

資料來源：資通安全事件通報及應變辦法

# 資通安全事件分級（2/4）

- 第二級資通安全事件
  - 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。
  - 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。
  - 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運作受影響或停頓，於可容忍中斷時間內回復正常運作。

資料來源：資通安全事件通報及應變辦法

# 資通安全事件分級（3/4）

- 第三級資通安全事件
  - 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。
  - 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。
  - 未涉及關鍵基礎設施維運之核心業務或核心資通系統運作受影響或停頓，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。

資料來源：資通安全事件通報及應變辦法

# 資通安全事件分級（4/4）

- 第四級資通安全事件
  - 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。
  - 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。
  - 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。

資料來源：資通安全事件通報及應變辦法

# 通報程序

- 本校『資通安全事件管理程序書』（NUTN-ISMS-B011）
  - 疑似資通安全事件發生時，發現人員應依事件所被影響的業務管理歸屬，通報該業務管理的單位（權責單位），並副知直屬主管。
  - 權責單位於收到通知後，應初步研判是異常事件或資通安全事件。
  - 若判定為資通安全事件時，則初估事件處理時間、分類、異常狀況、說明事件影響範圍及事件等級，並填寫於「資通安全事件報告單」後進行通報作業。

# 檢討與改善

- 本校『資通安全事件管理程序書』（NUTN-ISMS-B011）
  - 資通安全事件確認處理完成後，權責單位應檢討現行管理措施之完整性，並適當修訂相關作業管理規範或建置控制措施；若為重大資安事件，資通安全長應召開檢討會議。
  - 權責單位應依「矯正管理程序書」進行矯正改善作業，以避免類似安全事件重複發生。

# 個人資料侵害事故通報及應變

# 個人資料侵害之法規要求（1/3）

- 個人資料保護法-第十二條
  - 公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。
- 個人資料保護法施行細則-第二十二條
  - 本法第十二條所稱適當方式通知，指即時以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式。但需費過鉅者，得斟酌技術之可行性及當事人隱私之保護，以網際網路、新聞媒體或其他適當公開方式為之。
  - 依本法第十二條規定通知當事人，其內容應包括個人資料被侵害之事實及已採取之因應措施。

# 個人資料侵害之法規要求（2/3）

- 個人資料保護法施行細則第22條之相關解釋
  - 個資法施行細則第22條第1項「即時」之解釋與適用
    - ✓ 所稱「即時」，應指不得為不必要之拖延；又具體個案是否構成「不必要之拖延」，應依個案情節，考量公務機關或非公務機關初步查明個資侵害事故，及採取適當措施避免損害擴大所需之合理時間；通知對於當事人及時採取措施以防止立即性損害發生之必要性；以及於相關主管機關介入時，該個資侵害事故之揭露是否可能妨礙主管機關進行調查等因素為判斷。

資料來源：國家發展委員會個人資料保護專區
網址：https://pipa.ndc.gov.tw/nc_11979_32030

# 個人資料侵害之法規要求（3/3）

- 個人資料保護法施行細則第22條之相關解釋（續）
  - 個資法施行細則第22條第1項但書「需費過鉅」、「技術之可行性」、「當事人之保護」之具體判準與要件
    - ✓「需費過鉅」應以公務機關或非公務機關倘採言詞、書面、電話、簡訊、電子郵件、傳真、電子文件等「個別」通知方式，依客觀情形與社會通念，將使通知所需耗費之勞力、時間、費用與所欲防免之損害顯失衡平，造成該機關過度負擔，始足當之。
    - ✓「技術之可行性」之評估，應考量當代科技水準，擇取一項或多項與個別通知相同有效之通知方式（例如於機關網站明顯位置揭示訊息、透過新聞媒體播送訊息），確保資料當事人有最大機會知悉個資侵害事故，以及時採取措施維護其權益。
    - ✓「當事人隱私之保護」指公務機關或非公務機關應慮及通知方式是否可能另對當事人之隱私造成侵害，並應採取對當事人權益影響最小之方式為之，例如不揭示可直接或間接識別當事人之個人資料、避免透過已發生過侵害事故之溝通管道通知當事人。

資料來源：國家發展委員會個人資料保護專區
網址：https://pipa.ndc.gov.tw/nc_11979_32030

# 通報與受理程序（1/2）

- 本校『個人資料保護緊急應變處理作業說明書』（NUTN-PIMS-C002）
  - 當發生個資外洩時必須告知當事人並留下通報紀錄，若有通報而無相關通報記錄，事後將究責。
  - 接獲個資事故通報後，需依所通報之內容進行處理，並填寫本校「個人資料侵害事故通報與紀錄表」。
  - 當違反個資法規定，導致個人資料被竊取、洩漏、竄改或其他侵害者，應於查明後以適當方式通知當事人。
  - 建立聯絡機制，確保所使用的方式（例如電話、簡訊、郵寄、email等）可以通知到當事人，並留下紀錄。

# 通報與受理程序（2/2）

- 本校『個人資料保護緊急應變處理作業說明書』（NUTN-PIMS-C002）（續）
  - 各單位於發現個資遭侵害時，應通知個人資料管理窗口，由個人資料管理窗口與資通安全暨個人資料管理規範導入工作小組判斷是否為個資事故。
  - 個人資料管理窗口接獲相關個資案件通知時，應立即協同相關人員蒐集相關跡證，初步判斷是否發生個資事故及其影響程度與範圍。
  - 若經判斷為個資事故，事故處理之業管單位應立即依據「個人資料事故通報及受理流程」，啟動個資應變措施相關處理作業。
  - 若個資遭到人為竄改或失竊等涉及民、刑事案件時，應即時通報警政或檢調單位請求處理。

# 檢討與改善

- 本校『個人資料保護緊急應變處理作業說明書』（NUTN-PIMS-C002）
  - 個資事故確認處理完成後，事故發生單位應檢討現行安全控制措施之完整性，並適當修訂相關作業管理規範或建置控制措施，且於必要時召開檢討會議。
  - 事故發生單位應於事故處理完畢後，進行相關矯正預防措施，避免同類型之個資事故重複發生。
  - 各單位權責主管應監督個資事故之後續處理及安全控制的有效性。

# 違失案例宣導

相關案例資料轉載及引用來源：

1、政府資通安全防護巡迴研討會簡報（網址：https://www.nics.nat.gov.tw/Seminar.htm?lang=zh）

2、教育部112年教育體系資安推動暨稽核實務研討會-資安推動說明

# 案例1-資安事件之法遵意識

- 機關同仁進行大量圖資轉檔作業時，為求便利直接於對外伺服器端操作，遭外部有心人士讀取高階圖檔為其他利用，後經媒體揭露後始通報資安事件，致逾法遵期限。
  - 資安事件不以駭侵為限、不以重大事件為限、不以核心業務為限，只要影響機密性（C）、完整性（I）或可用性（A），不論造成原因為何，皆屬資通安全管理法規範之應通報資安事件。
  - 為利法遵時效，建議機關可先行通報，儘速完成調查後若確未造成CIA受影響，可申請撤單。

| | 事件通報 | 應變處置 | 結報<br>(提交調查、處理及改善報告) | 完成審核<br>(上級或監督機關) |
|---|---|---|---|---|
| 起算時間點 | 知悉事件 | 知悉事件 | 完成應變處置 | 接獲通報 |
| 1、2級事件 | 1小時 | 72小時 | 1個月內 | 8小時 |
| 3、4級事件 | | 36小時 | | 2小時 |

112年第一次巡迴研討會資料

# 案例2-資安事件通報逾時原因及建議

- 收到警訊亦應通報
  - 機關收到INT（入侵攻擊情資）警訊時，表示機關已有駭侵事實。
  - 須循機關內部通報程序陳報外，並應依資通安全管理法執行資安通報作業。
- 無法網站通報之處理
  - 機關若因故無法連線至通報應變網站進行通報時，可改使用下列方式進行通報：
    - ✓ 使用手機連線至網站通報。
    - ✓ 利用電話或傳真通報。
- 不熟悉通報作業
  - 無須等應處完成後才進行通報，知悉資安事件應同步通報，說明已知資訊。
  - 落實人員資安教育訓練（包括網站操作熟悉度）。

112年第一次巡迴研討會資料

# 案例3-110年稽核作業共通發現（1/2）

- 資安事件通報及應變
  - 稽核發現
    - ✓ 辦理資安事件通報及應變演練，惟未納入事件通報環節。
    - ✓ 機關自訂之通報應變程序，與通報應變辦法不符。
  - 案例
    - ✓ 演練情境以災害復原演練為主，著重於設備故障判斷與復原能力。
    - ✓ 演練範圍僅以資訊單位為主。
    - ✓ 機關自訂之通報應變程序，將中毒定義為非資安事件，不符通報應變辦法規定。
    - ✓ 機關自訂之通報應變程序，未納入事後矯正預防追蹤機制。
    - ✓ 機關收到EWA（資安預警情資）警訊，查證後確有符合資安事件定義情形。

111年第二次巡迴研討會資料

# 案例3-110年稽核作業共通發現（2/2）

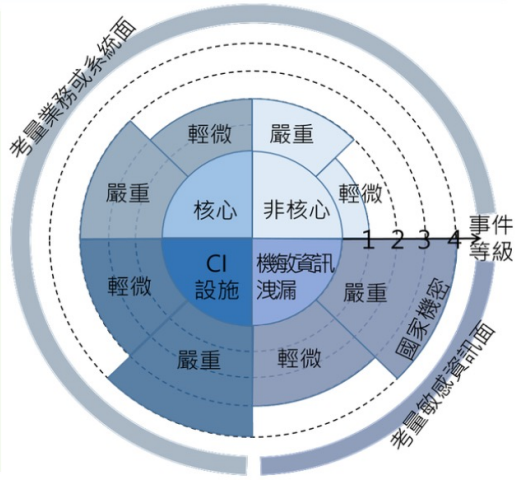
- 資安事件通報及應變（續）
  - 參考做法
    - ✓ 以業務為導向，演練情境並可參考資安威脅趨勢，納入複合式情境，如：天然災害、勒索軟體、DDoS攻擊、個資外洩處理及資安事件通報等。
    - ✓ 擴大演練範圍至相關業務單位，而非僅限資訊單位。

**規定**

**資通安全通報及應變辦法**

事件輕微或嚴重-考慮C,I,A三面向

- 機密性(C)
  - 業務資訊遭洩漏
- 完整性(I)
  - 業務資訊遭竄改
  - 資通系統遭竄改
- 可用性(A)
  - 資通系統受影響或停頓
  - 是否於可接受時間內回復




111年第二次巡迴研討會資料

# 案例4-資料外洩/人為疏失

- 機關委託廠商辦理競賽活動，並提供活動資訊，欄位包含姓名與行動電話號碼等，廠商工作人員為協助活動宣傳，將參與人員資訊上傳至個人公開網站，造成個資資料外洩。
- 防護建議
  - 建議機關選任計畫委辦廠商時，合約中應納入資通安全管理法與個資法相關要求，並監督廠商落實執行。
  - 資料放置於網站前，應審核確實公告內容含有個資之必要性，不得逾越特定目的之必要範圍。
  - 資料上傳至公開網站後，應重複確認公開之資訊內容適切性。
  - 活動結束後，應監督廠商完成資料或相關存取權限之返還、移交、刪除或銷毀，以及資料自網站下架。

111年第二次巡迴研討會資料

# 案例5-資料外洩/設計不當（1/2）

- 事件摘要
  - 民眾收到非本人之身分證字號、姓名相關行政處分通知（電子郵件）。
  - 經機關調查，係該○○系統之帳號申請機制問題，讓使用者可直接於網頁申請帳號，未對申請者進行身分審核程序，導致民眾誤申請到業務處理帳號，收到應僅寄送給特定機構之通知（包含他人個資）。
- 應變作法
  - 應儘速下架、更正系統功能，並重新確認、測試各項功能之權限控管機制及設定是否確實符合需求。
  - 全面清查系統帳號，針對不符規則及久未使用之帳號進行處理，如停用或刪除帳號。

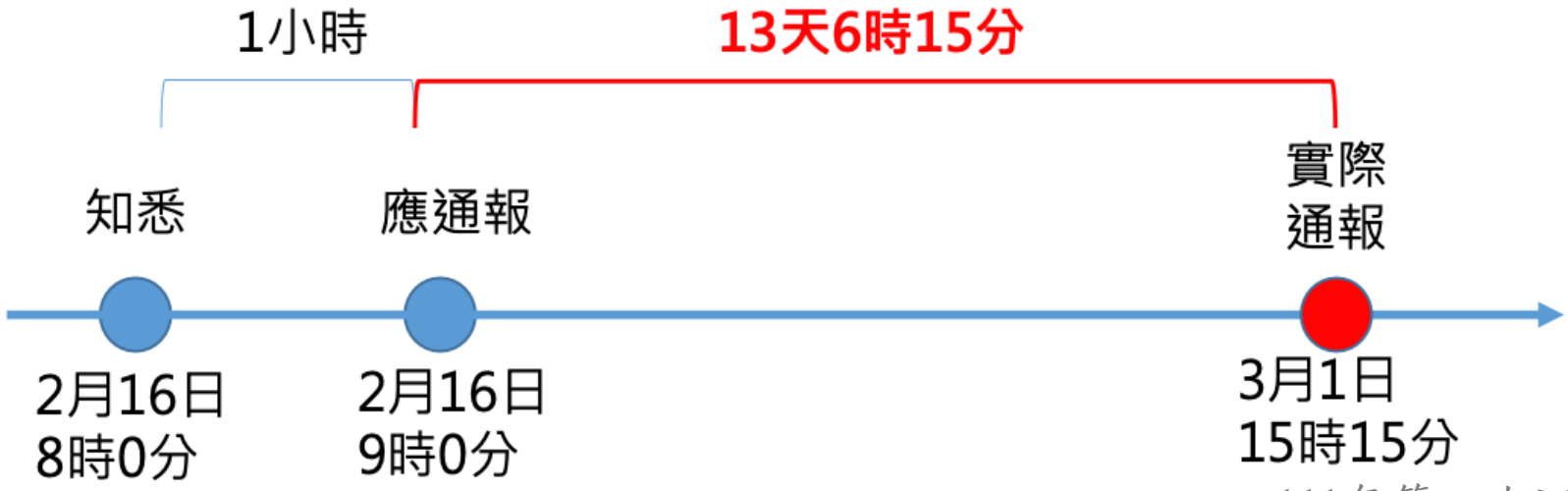
111年第一次巡迴研討會資料

# 案例5-資料外洩/設計不當（2/2）

- 改善建議
  - 落實資通系統防護基準之帳號管理相關控制措施，如建立帳號審核程序、定期審核帳號資料、定義系統使用情況及條件。

# 案例6-資安事件通報逾時

- 通報逾時案例（知悉1小時）
  - A機關111年2月16日8時通知其所屬B機關，A機關所管FB社團遭人張貼販賣老人慰問金個人資料的貼文，B機關雖有向警察機關報案，但卻遲至111年3月1日15時15分始通報3級資安事件，逾時13天6時15分。




111年第一次巡迴研討會資料

# 案例7-事件通報單問題說明（1/3）

- 事件通報須提出通報單，其中事件說明及影響範圍應就目前所知部分儘量敘明事件相關資訊，錯誤態樣如右圖。

| | |
|---|---|
| ◎ 事件分類與異常狀況 | 其他惡意程式行為之連線。 |
| ◎ 事件說明及影響範圍 | 收到技服信件。 |
| ◎ 是否影響其他政府機關(構)或重要民生設施運作? | ◆通報機關判斷：否 |
| ◎ 此事件通報來源 | 入侵事件警訊(INT) 發布編號 |

111年第一次巡迴研討會資料

# 案例7-事件通報單問題說明（2/3）

- 看不出與事件有關的說明，僅說明收到技服通知要去通報。
- 考量通報時效，雖難以完整說明真實情況，惟為了有關單位能即時掌握狀況並提供協助，仍應就所知部分詳實敘明，至少須含系統名稱、具體時間、事件確認方式、緊急應變方式等資料。


111年第一次巡迴研討會資料

# 案例7-事件通報單問題說明（3/3）

- 以下是說明較詳細的事件通報案例
  - 本機關（○○系統）於○月○日○時○分接獲系統使用者回報疑似個資可供瀏覽之情況發生，並於半小時後系統管理人員先將系統下線。與系統承辦人了解相關狀況後，調閱相關稽核LOG，含Web、Server、DB Audit、LDAP等資料，發現所有系統使用者皆取得最高權限。
- 本通報單之事件說明內容值得參考，敘明發生問題之系統名稱、知悉事件具體時間、緊急應變措施、事件確認方式及初步確認結果，有關單位可迅速掌握事件概況，即時提供相關（技術、行政及協調）方面協助。

# 案例8-資料外洩/人為疏失

- 機關辦理研討活動並請參與人員報到，表單欄位包含姓名、身分證字號及手機。
- 承辦人員未檢視上傳資料內容，將活動成果相關資訊上傳至公開網站，造成個資外洩。
- 防護建議
  - 如需蒐集個人資料，以最少必要資訊為原則。
  - 資料上傳至公開網站後，應重複確認公開資訊內容之適切性。
  - 若活動採取線上報名方式，承辦人員確認蒐集資料內容，測試資料蒐集與相關作業流程。
  - 持續加強機關人員個人資料保護意識。

111年第一次巡迴研討會資料

# 案例9-資料外洩/社交工程

- 某機關透過臉書（Facebook）粉絲專頁宣導活動資訊，並利用Message接收報名資訊
- 粉絲專頁管理員疑似遭社交工程攻擊成功，導致帳號密碼外洩，進而造成民眾個資存在外洩疑慮。
- 防護建議
  - 經營公務用途之社群應妥善管理帳號，相關人員亦應提高資安意識。
  - 避免利用網路公開平台蒐集敏感資料，若因活動需求，則應重複確認資料存取設定與保存之妥適性。
  - 持續加強機關人員資安防護與個資保護意識。

111年第一次巡迴研討會資料

# 案例10-資料外洩/設定錯誤

- 某機關接獲民眾檢舉，於社交平台發現有人兜售該機關保管之個人資料。
- 經調查發現為離職員工濫用系統存取權限，擅自下載機關所持有的民眾個資並進行兜售。
- 防護建議
  - 定期清查系統帳號使用情況。
  - 應將審查系統帳號刪除（停用）作業納入離職流程。
  - 落實個資「認知宣導及教育訓練」。
  - 將資通系統調整零信任架構（長期目標）。

111年第一次巡迴研討會資料

# 案例11-弱密碼及身分驗證缺失（1/3）

- 事件說明
  - ○○署委託A大學建置維運學生業務相關網站，A大學網站維運團隊於查看網站日誌紀錄（log）時，發現AP管理者帳號有來自陌生國外IP成功登入的紀錄，且疑似上百筆個資遭到非授權的存取。
- 發生原因
  - AP管理者帳號存在弱密碼問題，且管理後臺並未限制存取來源。
  - 什麼樣的弱密碼？
    - ✓ 管理者帳號：[學校縮寫]+流水號，密碼：123456789。
  - 帳密設定功能頁面，遺漏將管理者納入密碼複雜度限制要求範圍。

# 案例11-弱密碼及身分驗證缺失（2/3）

- 建議改善事項
  - 落實資通系統及其帳號權限（應涵括作業系統、應用系統、資料庫等各類帳號）的盤點清查，並加強特權帳號之管理。
  - 資通系統應依其防護需求等級，落實防護基準之身分驗證管理控制措施相關要求。
  - 加強帳戶防護機制。
    - ✓ 資通系統使用密碼進行驗證時，應強制最低密碼複雜度。
    - ✓ 密碼複雜度規範對象，應包含所有具管理權限之帳號。
    - ✓ 密碼複雜度檢查程序，應被納入所有密碼變更功能。
    - ✓ 建議啟用多因子認證，並減少管理者帳號數量。

# 案例11-弱密碼及身分驗證缺失（3/3）

- 建議改善事項（續）
  - 機關宜訂定密碼複雜度共通規範，如禁止使用與帳號名稱相同、身分證字號、學校/機關代碼、易猜測之弱密碼、廠商預設密碼或其他公開資訊等。
  - 網站管理後臺及機關內部使用之物聯網（IoT）設備，存取控制應以限制IP來源範圍為原則。
  - 身分驗證功能應使用伺服器後端程式驗證，切勿依賴前端驗證。加強帳戶防護機制。
  - 所有前端向後端API請求功能，須加入身分驗證機制，並依人員身分或業務需求授予最小權限，以防止未授權存取敏感功能。
  - 弱密碼及身分驗證缺失問題，建議納入機關安全性檢測項目。

# 案例12-個資檔案未受適當保護（1/3）

- 事件說明
  - 調查局通知某2所公立高中將保有學生個人資料的檔案直接公開於學校官網，且未進行加密或遮蔽，並可透過Google搜尋引擎發現，可能洩漏上百筆個人資訊。
- 發生原因
  - 學校承辦人缺乏個資保護意識，針對敏感資訊安全處理亦未具相關知能。

# 案例12-個資檔案未受適當保護（2/3）

- 建議改善事項
  - 敏感性或機密資料應以加密方式進行儲存及傳輸。
  - 全面清查網站包含個資檔案，確認有無保留之必要，並針對需保留部分，確認已實施存取控制或進行適當遮罩處理。
  - 網站更新或上傳檔案時應具備覆核機制，以確認內容不包含敏感資訊（如個人資料、網站帳密等）。
  - 強化個資檔案生命週期安全管理，落實重要個資檔案使用前之申請審核，及保存期限或業務終止後之確認刪除等管理措施。
  - 使用者寄送郵件時，應謹慎檢查收文者正確性。

# 案例12-個資檔案未受適當保護（3/3）

- 建議改善事項（續）
  - 依資通安全責任等級分級辦法第11條規定，機關人員應依所屬類型（一般使用者及主管、資通安全專職人員、資通安全專職人員以外之資訊人員）完成對應之資安教育訓練法定時數要求。
  - 落實全體人員（包含工讀生）個資保護教育訓練，且應要求新進人員盡速完成，以提升人員個資保護意識及知能，避免因不熟悉相關規範或個資安全處理方式造成資安事件。
  - 機關、學校各單位主管應積極督促所轄人員完成上述教育訓練，建議由專責單位（如人事單位）定期追蹤管考以確保成效。

# 案例13-雲端服務使用不當（1/2）

- 事件說明
  - 某公立高級中學○○室以Google表單蒐集學生資料，因表單設定失當，致使填報人可查看其他已填人員之填寫資訊（包含個人資料），可能造成個資外洩。
- 發生原因
  - 承辦人於設計Google表單時，因對於其管理設定功能不熟悉，錯誤勾選允許檢視其他回應選項。

# 案例13-雲端服務使用不當（2/2）

- 建議改善事項
  - 依各級學校使用資通系統或服務蒐集及使用個人資料注意事項
    - ✓ 應加強並留意表單設計所開啟的功能，是否會造成機敏資料或個人資料外洩情事。
    - ✓ 以Google表單為例，於製作完成發送前，應確實做好相關設定，並實際操作檢驗，確認無風險疑慮再行送出。
  - 針對雲端服務之使用，加強人員教育訓練與安全宣導。

# 案例14-未落實SSDLC要求（1/3）

- 事件說明
  - ○○大學活動報名相關系統，因系統老舊遭駭客利用元件漏洞上傳程式，取得系統執行權限後植入惡意程式，並連結學校Portal進而竊取教職員工之個資。
- 發生原因
  - 系統版本老舊，且未修補第三方元件安全漏洞。
  - 重要資料庫未最小授權，系統具備完整讀取校務資料庫之介接權限。
  - 系統處理敏感資訊，惟未被納入學校資安規範適用範圍。

# 案例14-未落實SSDLC要求（2/3）

- 建議改善事項
  - 資通系統應依其防護需求等級，落實防護基準對於系統發展生命週期的需求、設計、開發、測試、部署與維運、委外等各階段之控制措施。
    - ✓ 需求或設計階段，應建立安全需求檢核項目。如身分驗證機制，除考量使用者之便利性，亦應注意被濫用之安全風險。
    - ✓ 測試階段應進行弱點掃描安全檢測，並進行中、高風險弱點修補。針對系統重要功能（如忘記密碼功能）建立安全檢核機制，以避免安全邏輯造成資安問題。亦建議納入盲測或惡意行為測試。
  - 如因應業務需求緊急上線，仍應保留安全性檢測及弱點修補所需時間，避免因重大安全漏洞被利用，導致機關嚴重損失。

# 案例14-未落實SSDLC要求（3/3）

- 建議改善事項（續）
  - 盤點系統第三方元件使用情形，注意相關弱點情資通報（如行政院技服中心、TACERT之ANA【資安訊息情資】），並落實弱點修補或實施風險管理措施。
  - 爭取相關預算經費，加速更新與升級老舊系統。
  - 系統開發維運團隊人員應參與SSDLC相關專業訓練課程。
  - 機關應建立系統介接作業之權限審核機制。
  - 重要資料庫應以最小權限原則進行存取授權，依介接系統之業務功能，提供所需資料表及資料欄位。
  - 落實資通安全維護計畫，全面盤點資通系統及評估核心/重要業務，將涉及敏感資訊者納入重點實施範圍，並執行相對應之防護基準。

# 補充-資安警訊是否需要通報（1/2）

- 資安預警警訊（NICS-EWA-20XX-XXXXXXX）
  - 若機關收到國家資通安全研究院寄發資安預警警訊，表示機關疑似發生資安事故，建議機關針對警訊內容進行檢視，若發現有入侵事實，則須依循資通安全管理法，執行資安通報作業。
- 入侵事件警訊（NICS-INT-20XX-XXXXXXX）、網頁攻擊警訊（NICS-DEF-20XX-XXXXXXX）
  - 若收到國家資通安全研究院寄發入侵事件警訊、網頁攻擊警訊，表示已發現機關遭受資安事件影響，機關應於收到警訊通告後，循機關內部程序上報外，並須依循資通安全管理法，執行資安通報作業。

資料來源：國家資通安全通報應變網站常見問題集

# 補充-資安警訊是否需要通報（2/2）

- 漏洞/資安訊息警訊（NICS-ANA-20XX-XXXXXXX）
  - 國家資通安全研究院寄發資安訊息警通知機關重大漏洞/資安訊息。若經相關檢測後，發現遭入侵情事，仍需至通報應變網站進行通報登錄。
- 緊急應處警訊（NICS-ALT-20XX-XXXXXXX）
  - 為掌握相關軟/硬體使用或漏洞修補等情形，會視情形寄發至特定機關，若收到國家資通安全研究院寄發緊急應處警訊，請依照警訊內容至通報應變網站填寫調查回覆，若逾時未完成，將每日寄發通知信提醒收件機關尚未完成調查回覆，並副知審核機關。若經相關檢測後，發現遭入侵情事，仍需至通報應變網站進行通報登錄。

資料來源：國家資通安全通報應變網站常見問題集

# D051_個人電腦設定與軟體安裝查核表操作簡介

# D051_個人電腦設定與軟體安裝查核表

| 個人電腦設定與軟體安裝查核表 | | |
|---|---|---|
| 文件編號：NUTN-ISMS-D051 | 版次：1.4 | 機密等級：限閱 |
| 紀錄編號： | 填表日期：　　年　　月　　日 | |

| | |
|---|---|
| 管理人員 | |
| 設備資料 | 1. 資訊資產名稱：＿＿＿＿＿＿＿＿＿＿財產序號：□□□□□□<br>2. 作業系統：□Windows＿＿＿＿(請填寫版本) □其他＿＿＿＿＿＿ |

| | 查　核　項　目 | 結果 | 檢查說明 |
|---|---|---|---|
| 1 | 電腦系統帳號密碼設定 | □是□否 | 系統重新開機查看是否需要登入帳號 |
| 2 | 完成稽核原則設定 | □是□否 | 執行 CMD：gpedit.msc<br>電腦設定→Windows 設定→安全性設定→本機原則→稽核原則→每個項目的「成功/失敗」全部開啟 |
| 3 | 完成密碼原則設定 | □是□否 | 執行 CMD：gpedit.msc<br>✓ 電腦設定→Windows 設定→安全性設定→帳戶原則→密碼原則→密碼最長有效期=180天、密碼最小長度=8<br>✓ 電腦設定→Windows 設定→安全性設定→帳戶原則→帳戶鎖定原則→帳戶設定閥值=3、帳戶鎖定/重設時間=10 分鐘 |
| 4 | 刪除/關閉不必要帳號。 | □是□否 | 如關閉 Guests |
| 5 | 完成鐘訊校時設定 | □是□否 | 鐘訊同步主機 140.133.2.81 或 time.windows.com |
| 6 | 關閉自動播放(CD-ROM、USB) | □是□否 | ✓ 方法一：執行 CMD：gpedit.msc→電腦設定→系統管理範本→Windows 元件→自動播放原則<br>✓ 方法二：左下角 Windows 設定→裝置→自動播放→為所有媒體與裝置使用自動播放功能→關閉 |
| 7 | 帳號密碼無置於顯而易見之處 | □是□否 | 桌面上無任何可見易得的帳號密碼資訊 |
| 8 | 完成螢幕保護程式設定 | □是□否 | 10 分鐘以內啟動，並點選「密碼保護」 |
| 9 | 安裝防毒軟體，防毒軟體病毒碼已更新至最新版。 | □是□否 | □Kaspersky　□Windows Defender<br>□其他＿＿＿＿＿＿ |
| 10 | 防毒軟體設定定期掃描 | □是□否 | 完整掃描及弱點掃描，並修復掃描到的問題。 |
| 11 | 開啟 WINDOWS 系統自動更新程式 | □是□否 | 確實進行軟體更新，修補漏洞，保持更新至最新狀態。 |
| 12 | 無非法及未經授權軟體。 | □是□否 | ✓ 查看控制台→新增/移除程式、查看程式集。<br>✓ 如有發現來路不明或未授權檔案，請立即移除。例如 winrar、teamviewer、AnyDesk<br>✓ 如有 P2P 分享軟體，請立即移除。 |
| 13 | 其他軟體之更新 | □是□否 | Office 應用程式、Adobe Acobat Reader、Java 更新、其他合法軟體的更新狀況 |
| 14 | 電腦檔案及 Mail2000 郵件之刪除 | □是□否 | 電腦檔案及 Mail2000 郵件刪除後，務必立即清理資源回收桶(垃圾桶)。 |

| 管理人 | 檢核人 | 單位主管 | 資通安全官 |
|---|---|---|---|
| | | | |

# 1.電腦系統帳號密碼設定

- 檢查說明：
  - 系統重新開機查看是否需要登入帳號。

# 2.完成稽核原則設定

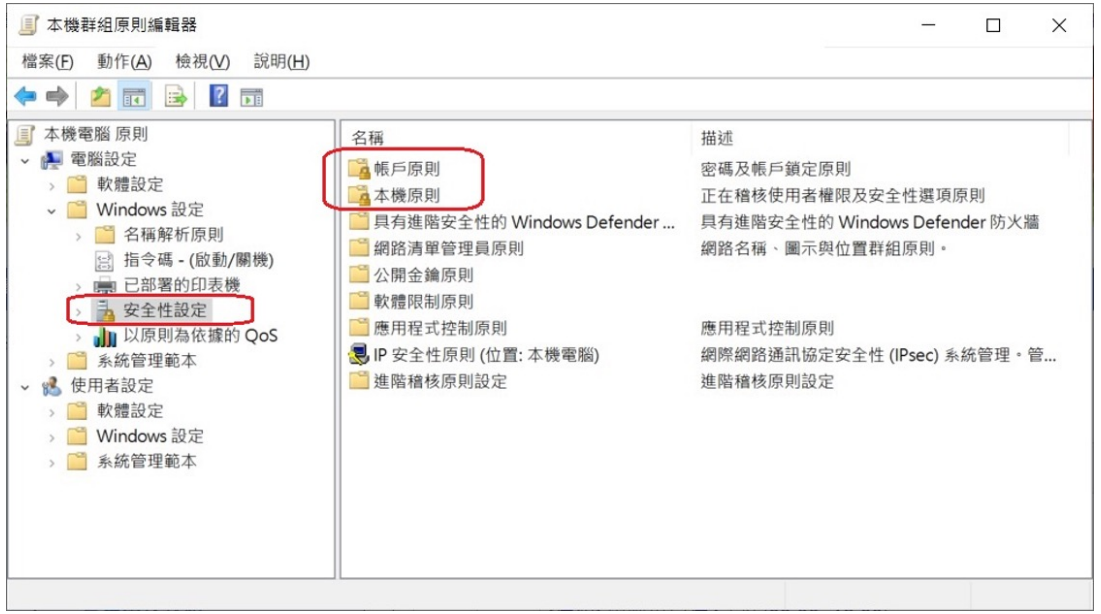
- 檢查說明：
  - 執行CMD：gpedit.msc
  - 電腦設定→Windows設定→安全性設定→本機原則→稽核原則→每個項目的「成功/失敗」全部開啟。

# 3.完成密碼原則設定

- 檢查說明：
  - 執行CMD：gpedit.msc
  - 電腦設定→Windows設定→安全性設定→帳戶原則→密碼原則→密碼最長有效期=180天、密碼最小長度=8。
  - 電腦設定→Windows設定→安全性設定→帳戶原則→帳戶鎖定原則→帳戶設定閥值=3、帳戶鎖定/重設時間=10分鐘。

# ◆項次2、3執行步驟說明

- 於Windows視窗「搜尋列」輸入gpedit.msc後按enter鍵。
- 出現「本機群組原則編輯器」畫面，點選『電腦設定→Windows設定→安全性設定』進行變更設定。

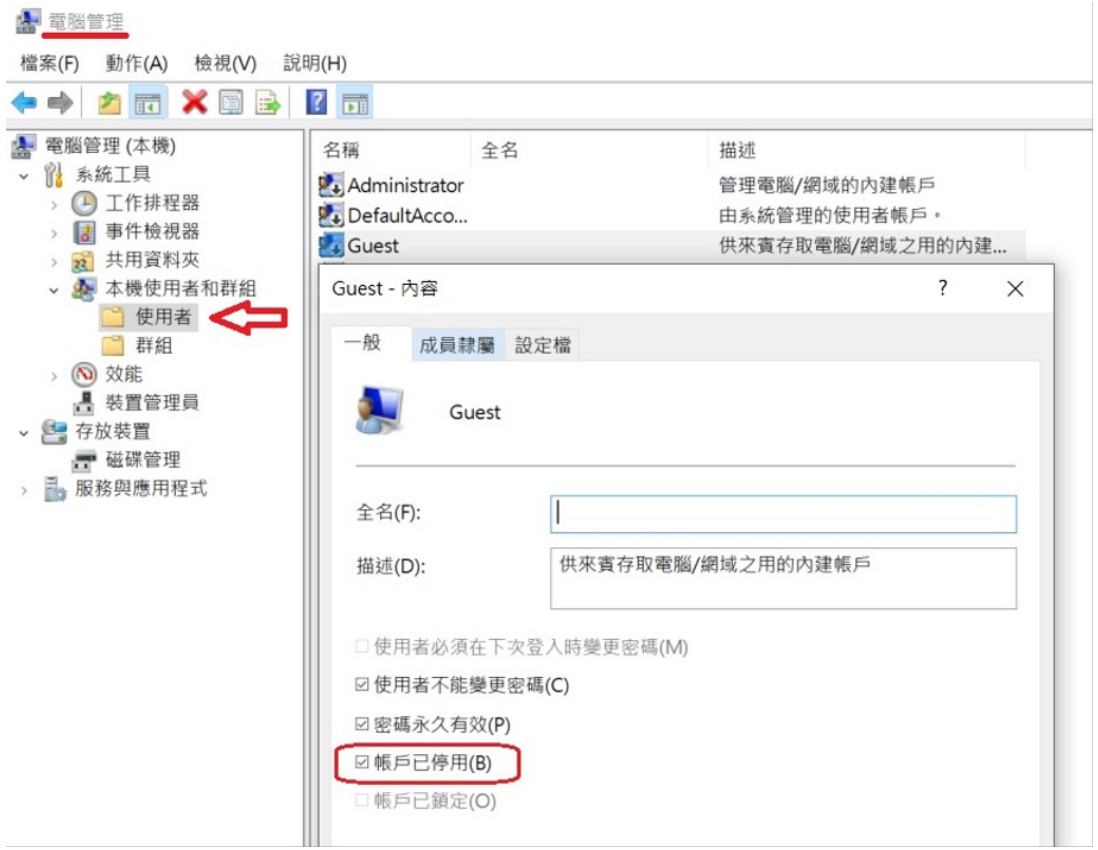


# 4.刪除/關閉不必要帳號

- 檢查說明：
  - 如關閉Guests。

# ◆項次4執行步驟說明

- 點選執行「開始／Windows系統管理工具／電腦管理」。
- 出現右方畫面，點選本機使用者和群組之使用者，點選Guest帳號，確認Guest帳號已停用。



# 5.完成鐘訊校時設定

- 檢查說明：
  - 鐘訊同步主機140.133.2.81或time.windows.com。

# ◆項次5執行步驟說明

- 開啟控制台，點選在「日期和時間」，切換至「網際網路時間」。
- 點選「變更設定」，設定網際網路時間時間伺服器。（140.133.2.81或time.windows.com）。

# 6.關閉自動播放（CD-ROM、USB）

- 檢查說明：
  - 方法一：執行CMD：gpedit.msc→電腦設定→系統管理範本→Windows元件→自動播放原則（參考項次2、3之步驟）。
  - 方法二：左下角Windows設定  →裝置→自動播放→為所有媒體與裝置使用自動播放功能→關閉。

# 7.帳號密碼無置於顯而易見之處

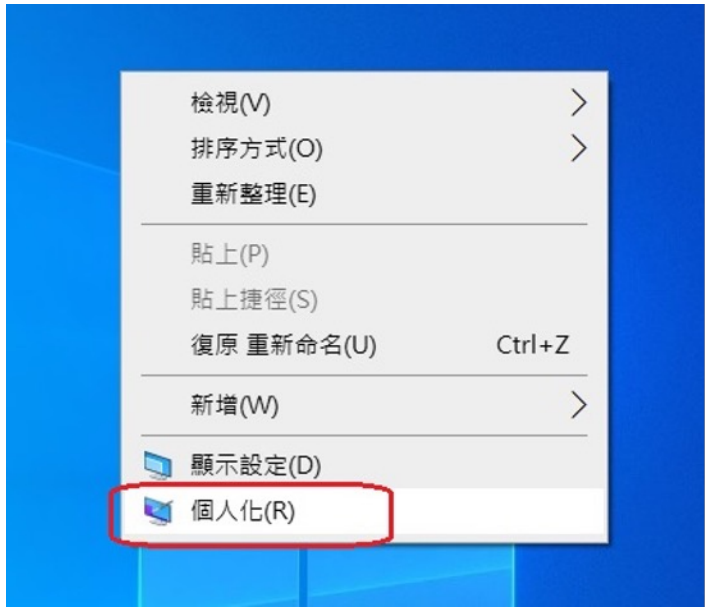
- 檢查說明：
  - 桌面上無任何可見易得的帳號密碼資訊。

# 8.完成螢幕保護程式設定

- 檢查說明：
  - 10分鐘以內啟動，並點選「密碼保護」。

# ◆項次8執行步驟說明（1/2）

- 於電腦桌面點按滑鼠右鍵，出現選單點選「個人化」。
- 點選「鎖定畫面」，再點選「螢幕保護設定」。設定等候時間為10分鐘，並勾選「繼續執行後，顯示登入畫面」。



# ◆項次8執行步驟說明（2/2）


# 9.安裝防毒軟體，防毒軟體病毒碼已更新至最新版

- 檢查說明：
  - 啟動Windows Defender。

# ◆項次9執行步驟說明

- 點選執行「設定／更新與安全性／Windows安全性／防火牆與網路保護」。
- 確認防火牆已開啟。

# 10.防毒軟體設定定期掃描

- 檢查說明：
  - 完整掃描及弱點掃描，並修復掃描到的問題。

# ◆項次10執行步驟說明

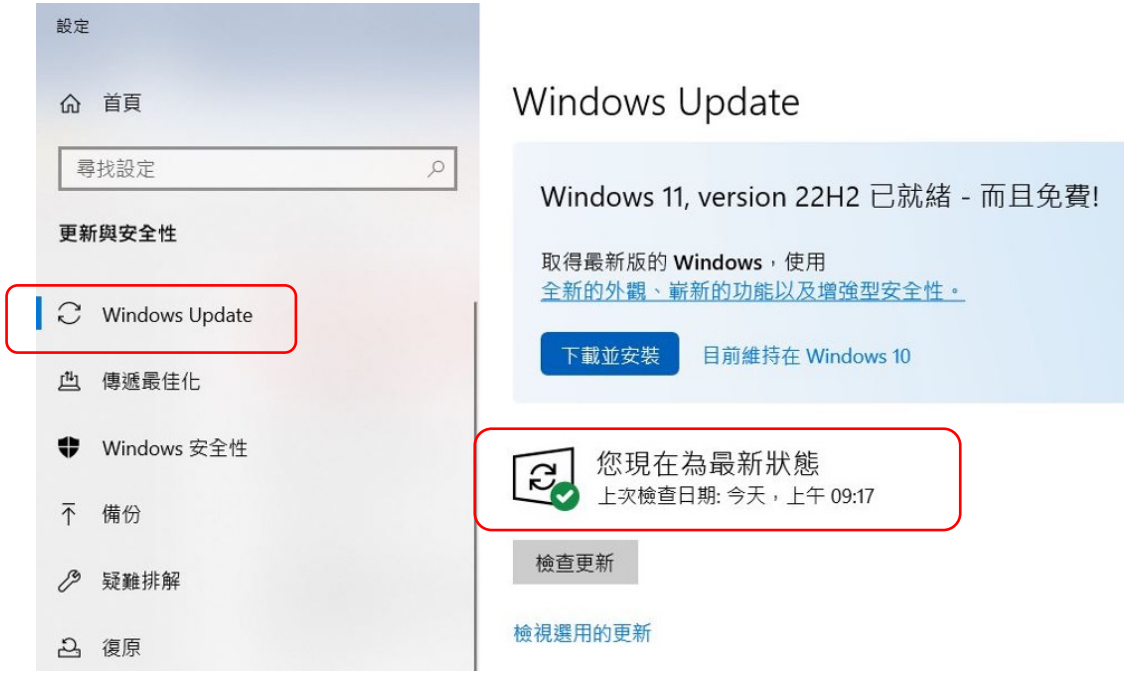
- 點選執行「設定／更新與安全性／Windows安全性／病毒與威脅防護」。
- 確認「沒有目前的威脅」。

# 11.開啟WINDOWS系統自動更新程式

- 檢查說明：
  - 確實進行軟體更新，修補漏洞，保持更新至最新狀態。

# ◆項次11執行步驟說明

- 點選執行「設定／更新與安全性／WindowsUpdate。
- 點選「檢查更新」，確認「現在為最新狀態」。



# 12.無非法及未經授權軟體

- 檢查說明：
  - ➢ 查看控制台→新增/移除程式、查看程式集。
  - ➢ 如有發現來路不明或未授權檔案，請立即移除。例如winrar、teamviewer、AnyDesk
  - ➢ 如有P2P分享軟體，請立即移除。

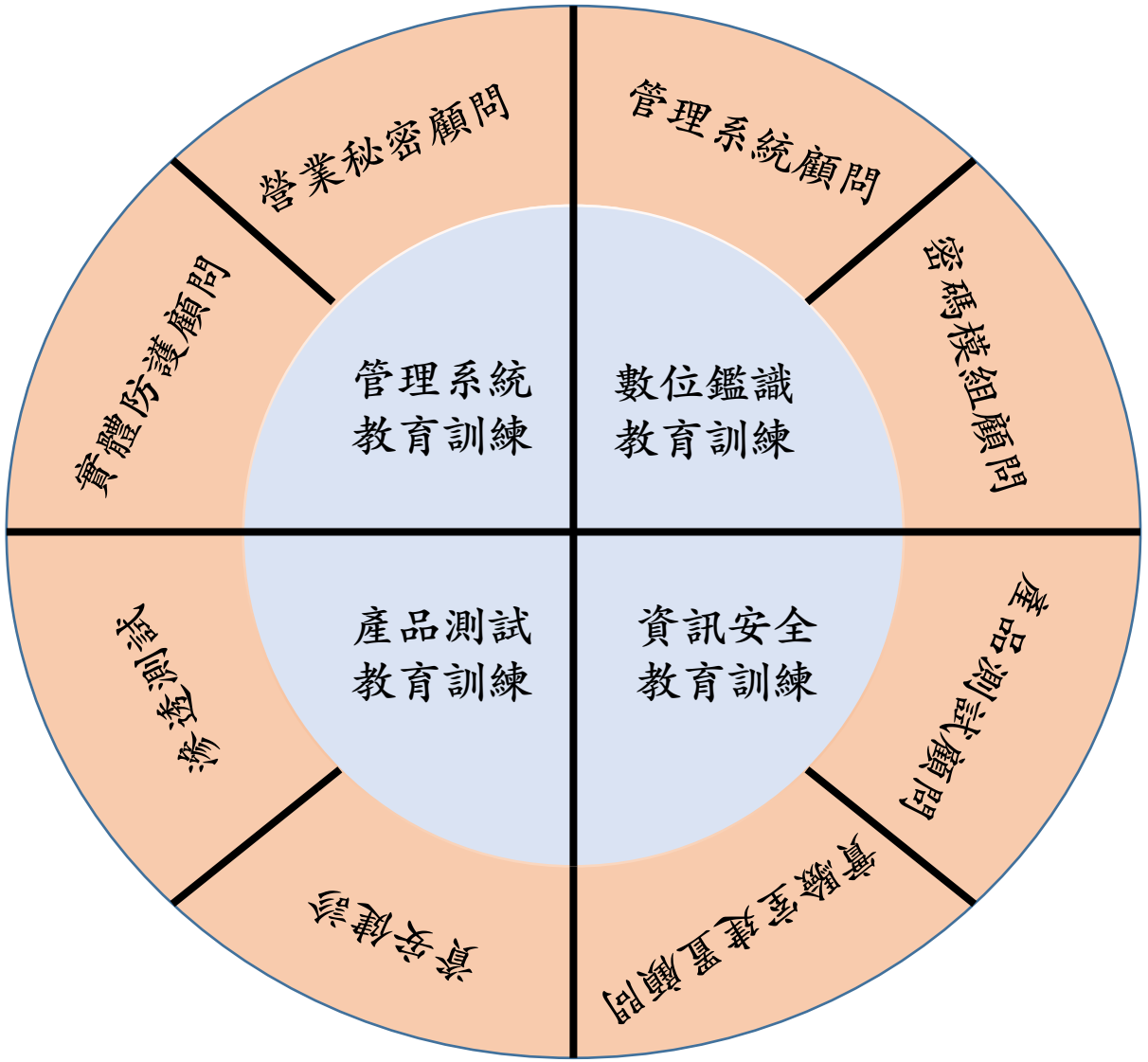
✓ 著作權法第91-1條...侵害他人之著作財產權者，處三年以下有期徒刑、拘役，或科或併科新臺幣五十萬元以下罰金。

# 13.其他軟體之更新

- 檢查說明：
  - Office應用程式、Adobe Acobat Reader、Java更新、其他合法軟體的更新狀況。

# 14.電腦檔案及Mail2000郵件之刪除

- 檢查說明：
  - 電腦檔案及Mail2000郵件刪除後，務必立即清理資源回收桶（垃圾桶）。


營業秘密顧問
管理系統顧問
實體防護顧問
密碼模組顧問
管理系統
教育訓練
數位鑑識
教育訓練
產品測試
教育訓練
資訊安全
教育訓練
滲透測試
資安健診
實驗室建置顧問
產品測試顧問

# 優士創造您的資安優勢