



德欣寰宇科技
安全、穩定、效率

國立臺南藝術大學

資通安全暨個人資料 保護教育訓練

一般使用者及主管 | 通識教育訓練 (3 小時)

德欣寰宇科技 專案支援部資安顧問

中華民國 115 年10月22日 09:00~12:00



簡報大綱

一

資通安全與個資保護新知宣導

資安法、個資法最新修法 | 危害國家產品禁用 | 為什麼年年要盤點 | 通報規範 | 辦公室資安/個資注意事項

二

C 級機關應辦事項及委外廠商作業規範

資安法與全部子法一次看懂 | 附表五 C 級應辦事項 | 資訊業務委外與採購實務

三

電子社交工程與潛在資安風險

攻擊的是「人」 | 開信、開附件、點連結的風險 | 停、看、查三步驟自保

四

新興議題時事與生成式 AI 使用規範

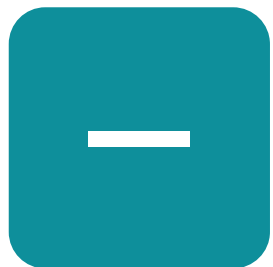
近一年最有感的資安大事 | 威脅手法怎麼演變 | 行政院生成式 AI 參考指引

上課前，先講結論

資安不是資訊處的事，是每一位教職員工的事

只要您把這三件事帶回辦公室， 這 3 小時就值得了。

- ① 慢一秒 只要有訊息要你「點連結、填帳號密碼、傳送檔案、匯款付費」，先停一秒，用別的管道確認。
- ② 看得到 每年盤點不是作業，是讓學校知道「我們有什麼、誰在管、放在哪」。
- ③ 講出來 出事不要自己處理、不要自己刪。1 小時內通報，才是正確動作。



資通安全與個資保護新知宣導

Cyber Security & Personal Data Protection Updates

- 1 最新資安法、個資法修法簡介以及與學校的關聯
- 2 危害國家產品禁用規範
- 3 為什麼每年都要做資訊資產 / 個資盤點
- 4 資安通報及未來個資事件通報規範
- 5 辦公室資安與個資相關注意事項

1-1 為什麼「學校」會被資安法管？

不是「要不要做資安」，而是「法律規定一定要做，而且每年被打分數」。

法 我們是「公務機關」

- 《資通安全管理法》第 3 條：依法行使公權力之中央、地方機關（構）
- 國立大學為教育部所屬公立學校，屬公務機關
- → 法規不是「參考」，是「應辦」

級 我們被核定為 C 級

- 依《資通安全責任等級分級辦法》
- 機關維運自行或委外設置、開發之資通系統者 = C 級
- 校務系統、選課、報名、網站都算

查 每年要被檢核

- 教育部高教深耕計畫「資安專章」績效評核
- 114 年版共 13 大指標、含教育訓練成效評估
- 內部稽核、外部稽核、實地稽核都會抽問同仁

責 做不到有罰則

- 資安法修法後，未通報罰鍰上限提高至 1,000 萬元
- 個資外洩另有個資法的損害賠償與行政罰
- 公務員另有行政責任

資料來源：資通安全管理法（全國法規資料庫）；資通安全責任等級分級辦法（115.01.07 修正）；教育部 114 年度大專校院資安專章績效項目評核表。本校責任等級以學校核定公文為準。

1-1 資安法到底管哪些人？（第 3 條用詞定義）

資安法不是「全國都管」，而是精準畫了兩個圈：公務機關、特定非公務機關。

身分別	定義（摘要）	包含誰
公務機關	依法行使公權力之中央、地方機關（構）或公法人； 不包括軍事機關及情報機關	各部會、地方政府、 國立大學 / 公立學校
特定非公務機關	以下三類： ① 關鍵基礎設施提供者 ② 公營事業 ③ 政府捐助之財團法人	台電、中華電信、各大醫院、 金融機構、法人研究機構
關鍵基礎設施提供者	維運或提供關鍵基礎設施之全部或一部， 經中央目的事業主管機關指定並報行政院核定者	CI 九大領域中被指定者
不適用	軍事機關、情報機關（另依其專法辦理）	國防部所屬軍事機關等

本校落在第一個圈→公務機關，而且是「全部適用」，不是「參考辦理」。

資料來源：資通安全管理法第 3 條（用詞定義）。114.09.24 修正公布後主管機關由行政院改為數位發展部。

1-1 南藝大在這張法規地圖上的座標

同一所學校，在不同法規裡有不同身分。

面向	南藝大的定位	代表什麼
資通安全管理法	公務機關（教育部所屬國立大學）	全部適用，不是參考辦理
責任等級	C 級（維運自行或委外設置、開發之資通系統）	適用附表五應辦事項
上級 / 監督機關	教育部	通報、稽核、評核都經教育部
通報管道	教育機構資安通報平台 https://info.cert.tanet.edu.tw	1 小時內完成通報
個資法身分	公務機關（公立學校）	未來受個人資料保護委員會監督
額外考評	教育部高等教育深耕計畫「資安專章」績效評核	每年打分數、排名
適用規範	教育體系資通安全暨個人資料管理規範（適用類型二）	各大學建議導入之控制項

提醒：責任等級每三年提交或核定一次，組織或業務調整時須變更；實際等級以學校核定公文為準。

1-1 資安法體系：母法 + 8 部子法，一次看懂

資安法不是一部法，是一整套。8 部子法中，有 4 部跟您的日常工作直接有關。

#	法規名稱	這部在管什麼	與一般同仁的關係
1	資通安全管理法	母法：誰要管、要做什麼、罰則	★★★
2	資通安全管理法施行細則	維護計畫內容、 委外應注意事項 (\$4)	★★
3	資通安全責任等級分級辦法	A ~ E 分級、各級應辦事項 (附表一 ~ 十)	★★★
4	資通安全事件通報應變及演練辦法	事件分級、1 小時通報、演練	★★★
5	資通安全維護計畫實施情形稽核辦法	誰來稽核、怎麼稽核	★
6	資通安全情資分享辦法	資安情資怎麼蒐集與分享	★
7	公務機關所屬人員辦理資通安全事項作業辦法	人員的責任與獎懲	★★
8	危害國家資通安全產品審查辦法	哪些產品不能買、不能用	★★★
9	國家資通安全會報設置辦法	國家層級的組織運作	-

早年常聽到的「資安法六子法」是舊稱；現行數位發展部公告的體系為母法 + 8 部子法。

資料來源：數位發展部「資通安全管理法及子法」法規專區 <https://moda.gov.tw/ACS/laws/regulations/624>

1-1 資安法 114/9/24 首次大修：五大重點

《資通安全管理法》108/1/1 施行，114/9/24 總統公布首次大幅修正。

1 主管機關改為數位發展部

- 由行政院改為數位發展部 (moda)
- 資安署負責實際執行與督導

2 禁用危害國安產品入法

- 原本是行政院的「限制使用原則」
- 修法後明定於母法，位階提高
- 另訂《危害國家資通安全產品審查辦法》

3 委外必須簽書面契約

- 權利義務、違約責任都要寫清楚
- 機關也必須參加主管機關規劃的演練

4 專責人員要做適任性查核

- 拒絕查核或未通過者
- 不得辦理涉及國家機密、軍事或國防秘密事項

5 罰則大幅提高 + 新增調查權

- 未通報事件：罰鍰上限提高至 1,000 萬元
- 屆期未改善：上限 500 萬元
- 拒絕、規避重大事件調查：10 萬 ~ 100 萬元

什麼時候上路？

- 114/8/29 立法院三讀、114/9/24 總統公布
- 施行日期由行政院另定
- → 子法已先行在 115 年 1 月密集修正

資料來源：總統府網站-公報查詢：<https://www.president.gov.tw/Page/294/50002>；行政院新聞稿；全國法規資料庫。施行日期以行政院公告為準。

1-1 115 年 1 月：兩部子法同週修正，馬上生效

法規不是三年才動一次。光是 115 年 1 月的兩天內，就有兩部子法改版並立即施行。

115/1/5

資通安全事件通報應變及演練辦法
修正發布並自同日施行

115/1/7

資通安全責任等級分級辦法
修正發布並自同日施行

4級

資安事件影響等級
(刪除「敏感資訊」判定要件)

1小時

公務機關知悉事件後
通報時限明定於條文

中央法規 > 法規名稱

序號 法規名稱

法規名稱少→多

變更排序

1. 資通安全事件通報應變及演練辦法 (民國 115 年 01 月 05 日) EN

中央法規 > 法規名稱

序號 法規名稱

法規名稱少→多

變更排序

1. 資通安全責任等級分級辦法 (民國 115 年 01 月 07 日) EN

名稱改了 「資通安全事件通報及應變辦法」→「資通安全事件通報應變及**演練**辦法」，把「演練」納入名稱。

附表全改 責任等級分級辦法修正第 1、3、10、11 條與附表一～七、附表十，C 級應辦事項內容同步調整。

對我們的意義 學校的四階文件（程序書、辦法、表單）必須跟著改版，教育訓練教材也要同步更新。

資料來源：數位發展部 115.01.05 修正「資通安全事件通報應變及演練辦法」、115.01.07 數授資法字第1145000416號令修正「資通安全責任等級分級辦法」；行政院公報 <https://gazette.nat.gov.tw>

1-1 個資法 114/11/11 修正公布：四大重點

個資法 114/11/11 總統修正公布，施行日期由行政院另定→但「準備期」就是現在。

法規名稱：個人資料保護法 **EN**

修正日期：民國 114 年 11 月 11 日

生效狀態：※本法規部分或全部條文尚未生效，最後生效日期：未定 [連結舊法規內容](#)

1. 一百一十二年五月三十一日增訂之第 1-1 條條文，施行日期，由行政院定之。
2. 一百一十四年十一月十一日修正第 1-1、12、18、21、22~26、41、47~49、52、53、55 條條文；增訂第 1-2、20-1、21-1~21-5、51-1、53-1 條條文及第三章之一章名、第一節節名、第二節節名；刪除第 27 條條文，施行日期，由行政院定之。

1 成立「個人資料保護委員會」

- 我國將有獨立、統一的個資主管機關 (PDPC)
- 過去各目的事業主管機關各管一塊的時代結束
- 部分行業由原主管機關續管 6 年

2 個資事故「必須通報」入法

- 達一定條件者，應向個資會通報
- 通報內容、方式、期限由子法訂定
- 未通報有罰則

3 通知當事人不得再拖

- 不能再以「還在調查」或「我沒違法」為由延後通知
- 必須採取適當的因應措施並留存紀錄

4 安全維護措施違失可「逕予裁罰」

- 未訂定或未落實安全維護計畫，可不經限期改正直接開罰
- 不服處分直接進入行政訴訟

1-1 個資事故：現在 vs. 修法後

學校內部流程不用大改，但「對外通報」這一段會從「視情況」變成「法定義務」。

現在的做法（校內 PIMS 流程）

- 發現者 → 通知單位個資保護專責人員
- 行政小組了解事故 → 通知權責單位執行小組
- 清查外洩範圍、影響與應變措施
- 判斷是否違反個資法 → 必要時召開委員會
- 登錄「PIMS-D-025 個人資料侵害事故通報與紀錄表」
- 同步判定是否為資安事件，必要時走資安外部通報

修法後會多出來的義務

- 對外通報** 達門檻者須向個資會通報（草案：72 小時內）
- 通知當事人** 草案：知悉起 72 小時內個別通知
- 無法個別通知** 草案：得以網路、新聞媒體等方式連續公開至少 30 日
- 留存紀錄** 因應措施、通知內容都要留下可稽核的紀錄
- 罰則** 未通報、未落實安維計畫均有罰則

校內流程依據：PIMS-D-024 個資事故通報及受理流程；PIMS-C-002 個人資料保護緊急應變處理作業說明書。修法後義務依個資會籌備處 115.01.22 預告之子法草案，最終以發布條文為準。

1-1 個資會 115/1/22 預告：三項子法草案重點

三項子法草案於 115/1/22 預告，預告期 60 日。「每年清查個資」正式寫進法規。

子法草案	適用對象	重點內容
個人資料保護長及相關人員 職掌職能條件及訓練辦法	公務機關	明定個資保護長（DPO）的資格、職掌與訓練要求
個人資料檔案 安全維護管理辦法	公務機關 及非公務機關	共通措施：定期清查個資並界定範圍、通報與應變機制、人員安全管理、 教育訓練、設備與資通系統安全、業務終止後刪除銷毀
個人資料事故 通知通報及應變辦法	公務機關 及非公務機關	通知當事人：知悉起 72 小時內個別通知 通報主管機關：涉特種個資、系統保有個資達 1 萬筆以上，或影響個資達 100 筆以上者 ， 72 小時內通報

注意：以上為草案內容，正式條文以個資會發布版本為準；本校宜先依草案方向預作準備。

資料來源：個人資料保護委員會籌備處 115.01.22 預告；理律法律事務所〈個資會籌備處預告個資法施行細則修正案及三項子法草案〉<https://www.leeandli.com/TW/NewslettersDetail/7584.htm>

1-1 所以，法規改了對「我」有什麼影響？

法規是寫給機關看的，但真正做事的是每一位同仁。

情境	以前	以後（修法上路後）
我不小心把含學生名冊的檔案寄錯人	通知單位個資窗口，內部處理	同樣要通報，而且學校有72小時的法定時鐘在跑
我買了一台便宜的網路攝影機裝在工作室	可能沒人注意	禁用規範已提升至法律位階，須列冊、不得介接公務環境
我覺得盤點表每年都一樣，直接沿用去年的	行政作業	「定期清查個資」將是法定安全維護措施之一
系統廠商說「我用我自己的帳號比較快」	便宜行事	委外須書面契約、帳號管控，稽核會查
收到可疑郵件又開啟，想說刪掉應該沒事	個人判斷	社交工程開啟率是學校被評分的指標，也可能是入侵起點
我每年的 3 小時資安訓練沒上完	提醒補課	C 級應辦事項明定「每人每年 3 小時」，列入專章評核

1-2 危害國家資通安全產品禁用規範

法源：資通安全管理法；各機關對危害國家資通安全產品限制使用原則

重點不是「哪裡製造」，
而是「誰家的牌子」。

從嚴認定 不論原產地是我國、大陸地區或第三地區，只要屬於「大陸廠牌」，一律列入限制範圍。

範圍很廣 資通訊產品包含軟體、硬體與服務→APP、作業系統、個人電腦、伺服器、手機、網通設備、無人機、印表機、物聯網設備，以及客服與軟硬體維護服務。

法律升級 資安法修正後提升至法律位階，並訂有《危害國家資通安全產品審查辦法》。

資料來源：行政院國家資通安全會報「各機關對危害國家資通安全產品限制使用原則」；數位發展部「危害國家資通安全產品審查辦法」。

mod^o 數位發展部 主管法規查詢系統
Ministry of Digital Affairs Laws and Regulations Retrieving System

請輸入關鍵字 整合查詢

最新訊息 法規體系 法規檢索 草案預告 相關網站

現在位置：法規內容

📍 法規內容

法規名稱：	危害國家資通安全產品審查辦法
公發布日：	民國 114 年 12 月 19 日
發文字號：	數位資法字第1145000392號 令
法規體系：	資通安全目
立法理由：	中華民國114年12月19日訂定總說明及逐條說明.pdf

1-2 三大禁用原則：背起來只要三句話

這三句話就是稽核委員最常問的三個問題。

① 公務用的，不能是大陸廠牌

- 公務用資通訊產品不得使用大陸廠牌，也不得在公務設備上安裝非公務用軟體
- 公務電腦不要裝來路不明的小工具、瀏覽器外掛

② 私人設備，不能碰公務

- 個人資通訊設備不得處理公務事務，也不得與公務環境介接
- 不要用私人手機熱點接校內公務網段、私人電腦禁止連結校務系統後台

③ 已經有的，要列冊、要隔離

- 既有已使用或已採購的大陸廠牌產品應列冊管理且不得與公務環境介接
- 逐年汰除，數量要能呈現下降趨勢

資料來源：各機關對危害國家資通安全產品限制使用原則；教育部 114 年度大專校院資安專章指標 12.1「禁止採購大陸廠牌資通產品作法及教育訓練宣導」。

1-2 校園裡哪些東西算「資通訊產品」？

我買的只是一台攝影機，又不是電腦 → 只要會連網、會處理資料、會被控制，就是資通訊產品。

類別	常見品項	本校特別容易忽略的
軟體	應用軟體、作業系統、APP、瀏覽器外掛	影音剪輯 / 修圖 / 轉檔的免費工具、字幕軟體、線上轉檔網站
硬體	個人電腦、伺服器、手機、網通設備、印表機、物聯網設備	展場 IP 攝影機、無線投影器、直播編碼器、空拍機（無人機）、智慧電視 / 電子看板、場館門禁與環控設備
服務	客服服務、軟硬體維護服務、雲端服務	展演串流平台、線上售票 / 報名系統、雲端相簿、廠商遠端維護連線、資料代管

採購前先問三句：這是什麼廠牌？有沒有連網？會不會接到校內網路？

1-2 真實案例：安控大廠「貼牌 MIT」事件

案例 | 2025 年 3 月 檢調偵辦 公視新聞網 PNN

昇銳電子涉進口中國製監視器，改貼「台灣製造」標籤，流入政府機關與企業

事件經過與規模

- 檢調認定自 2009 年起進口中國監視主機零組件，在台組裝後貼標 MIT 出售
- 114/3/19 檢調搜索，董事長以 100 萬元交保、副董 30 萬元交保
- 涉案金額：進口監視主機逾 1 億美元，總額約新台幣 33 億元
- 部分主機被發現會連回中國雲端伺服器
- 行政院清查各部會使用昇銳產品約 3,400 項；國防部確認 954 部主機
- 經濟部及所屬 49 部、園區合計 275 項，估計汰換經費約 4,000 萬元
- 審計部於 114 年度中央政府總決算審核報告示警：僅管制「最終品牌」不足，
- 應擴及關鍵零組件來源、產品資安驗證與採購規格

對學校的啟示

- ▶ 不是只看發票上的「台灣製造」就安全→規格書要寫清楚關鍵零組件來源
- ▶ 監視器、門禁、環控這類「不像電腦的電腦」，正是最容易被忽略的破口
- ▶ 場館、展場、宿舍的監控設備，採購與驗收都要留下查驗紀錄
- ▶ 契約要納入禁用條款與不實標示的違約責任，並要求廠商切結
- ▶ 既有設備要列冊，逐年編列汰換預算

公視新聞網報導 <https://news.pts.org.tw/article/743238>

新聞影音 (YouTube) <https://www.youtube.com/watch?v=ks7PF2Y-gPo>

中央社：董事長 100 萬交保 <https://www.cna.com.tw/news/asoc/202503200345.aspx>

聯合報：審計部示警公務機關採購釀資安漏洞 <https://udn.com/news/story/6656/9665695>

1-2 真實案例：安控大廠「貼牌 MIT」事件(新聞報導)



參考公視新聞網：

2025/03/21

昇銳電子涉進口中國監視器
貼標MIT流入企業及政府

<https://www.youtube.com/watch?v=ks7PF2Y-gPo>

時間：02:04

1-2 學校採購情境：這樣可以嗎？

教育部 114 年資安專章有兩項指標直接在看這件事： 12.1 採購限制與宣導、12.2 出租場域禁用規定。

✓ 可以這樣做

- ，排定汰換年度招標文件載明「不得為大陸廠牌資通訊產品」，並要求廠商簽署切結書
- 要求投標廠商提供產品原廠證明、關鍵零組件來源說明
- 勞務採購要求投標 / 得標廠商不得為大陸地區廠商
- 驗收時實際查驗機身標示、韌體來源與連外行為
- 場地出租契約納入禁用規定，廠商自備設備不得接校內公務網路
- 既有疑慮設備列冊、隔離於獨立網段

落實管理危害國家資通安全產品		
12.1禁止採購大陸廠牌資通產品作法及教育訓練宣導	A.訂定落實採購限制與宣導措施。	1.採購程序管控紀錄、具體實例 2.宣導佐證(公告函文、會議紀錄、訓練教材簡報)
	B.全校範圍既有列冊管理及管控措施、汰除。	列冊管理紀錄、汰除紀錄、數量統計(應呈現逐年下降之比例)
	C.將禁用規範納入相關招標文件及契約。	納入禁用條款佐證
12.2出租場域禁用規定及教育訓練宣導	A.修訂場地委外契約或禁用規定。	規範文件或契約修訂紀錄
	B.將禁用規範納入相關合約條款(不溯及既往)。	契約納入禁用條款佐證
	C.落實宣導措施。	宣導佐證 (公告函文、會議紀錄、訓練教材簡報)
	D.定期檢視及調整規範與宣導內容。	檢視或調整紀錄

X 常見的 NG 做法

- 「反正很便宜、規格又符合」就直接下單
- 只看外箱寫 MIT，不查廠牌與原廠
- 把禁用條款寫在簽呈裡，卻沒寫進招標文件與契約
- 展演活動廠商自己帶攝影機、路由器，直接插校內網路孔
- 老舊設備「還能用就繼續用」，沒有列冊也沒有汰換計畫
- 維護廠商用自己的雲端平台代管錄影檔，沒人問資料存在哪裡

資料來源：教育部 114 年度大專校院資安專章績效項目評核表指標 12.1、12.2；各機關對危害國家資通安全產品限制使用原則。

<https://sites.google.com/ntub.edu.tw/infosecurity/%E4%B8%8B%E8%BC%89%E5%B0%88%E5%8D%80>

1-3 為什麼每年都要做資訊資產 / 個資盤點?

依據: IS-B-003 資訊資產管理程序書、PIMS-B-003 個人資料檔案風險評鑑與管理程序書

你保護不了 你不知道存在的東西。

盤點 = 畫地圖
盤點 = 定價值

不知道學校有哪些資訊系統、哪些文件或資料、放在誰的電腦裡，就不可能保護它，出事也查不出影響範圍。
資產總價值 = 機密性 + 完整性 + 可用性，分 1~5 級；個資檔案另依「個資範圍」分 1~4 級。

盤點 = 算風險
盤點 = 被評分

有了價值才知道錢要花在哪。

盤點結果是風險評鑑的輸入；沒有資產清冊/個資清冊，風險評鑑就是憑感覺。
教育部資安專章 3.1 / 3.2 / 3.3 / 4.1 四項指標，都要求「全校範圍」且要有統計完成比率。

3.1 資訊資產清冊持續推動全校盤點、更新	A1. 資訊資產盤點 - 合規週期。	以部分盤點清冊佐證(權位充分、汰除更新)、全校統計比率文件(完整114年成果、115年已完成及預計完成)
	A2. 資訊資產盤點 - 落實範圍為全校。	全校統計比率文件應包含: 盤點日期、預期完成日期、全校單位數量、完成單位數量及預計完成單位數量
	B. 辦理全校(資訊資產盤點)教育訓練及成效評估。 C. 定期檢視清冊內容正確性及評估資產價值。	1. 教育訓練紀錄 2. 成效評估文件(如: 內稽抽問、抽樣測驗) 檢視紀錄 說明: 透過內部稽核或其他有效檢視方式。 完整盤點清冊(權位充分、汰除更新)、全校統計比率文件(115年已完成)
3.2 全校範圍系統持續完整盤點	A1. 定期(IP網段或網域名稱)資產系統盤點 - 合規週期。 A2. 定期(IP網段或網域名稱)資產系統盤點 - 落實範圍為全校。	全校統計比率文件應包含: 盤點日期、預期完成日期、全校單位數量、完成單位數量及預計完成單位數量
	B. 盤點清冊包含系統RTO/RPO、防護標準落實情況。 C. 辦理全校(資產系統盤點)教育訓練及成效評估。	盤點清冊 1. 教育訓練紀錄 2. 成效評估文件(如: 內稽抽問、抽樣測驗)
	D. 定期評估系統的防護需求等級並更新清冊。	評估與更新紀錄(透過內部稽核、管審會或其他有效檢視方式)。
3.3 全校範圍IoT持續完整盤點及安全管控	A1. 定期盤點學校公務用IoT設備 - 合規週期。 A2. 定期盤點學校公務用IoT設備 - 落實範圍為全校。	以部分盤點清冊佐證(權位充分、汰除更新)、全校統計比率文件(完整114年成果、115年已完成及預計完成)
	B. 辦理全校IoT安全使用宣導與成效評估。 C. IoT安全管控(密碼複雜度/網路存取限制/漏洞修補等)。	全校統計比率文件應包含: 盤點日期、預期完成日期、全校單位數量、完成單位數量及預計完成單位數量 宣導佐證(公告函文、會議紀錄、訓練教材簡報)、成效評估文件(如: 內稽抽問、抽樣測驗)
	A. 訂定風險準則、評估規劃與訓練。 B1. 執行風險評鑑 - 週期(應與各類盤點一致)。 B2. 執行風險評鑑 - 落實範圍為全校。 C. 風險處理計畫(風險改善追蹤)。 D. 風險處理結果。	安控措施紀錄或稽核報告 程序書或相關規範文件 風險評鑑結果、全校統計比率文件 風險評鑑結果、全校統計比率文件 風險處理計畫 風險處理報告
4.1 全校執行風險評估		

1-3 校內怎麼規定？（本校四階文件）

不是今天上課的講師要你做，是學校自己的程序書寫明「每年至少 1 次」。

規定	內容	文件依據
資訊資產多久盤一次	全校各單位每年至少進行 1 次資產盤點與清冊覆核	IS-B-003 §6.4
什麼時候要「加盤」	① 有新增、變更或移除資訊資產 ② 系統有重大異動 ③ 作業環境改變 ④ 組織有重大變革	IS-B-003 §6.5
誰要做	各資訊資產權責單位鑑別並建立清冊，本校承辦單位彙整統一控管	IS-B-003 §6.2
表單是哪一張	IS-D-012 資訊資產清冊；異動填 IS-D-028 資訊資產異動安全評估表	IS-B-003 柒 / IS-B-006
個資多久盤一次	每年執行 1 次個資清冊；另於「營運組織變更」「作業流程改變」時加做	PIMS-B-003 §6.3
個資表單	PIMS-D-007 個人資料檔案清冊 → PIMS-D-009 風險評鑑彙整表	PIMS-B-003 柒

提醒：四階文件已因應 ISO/IEC 27001:2022 改版修正，請以本校「資訊處」<https://ic.tnnua.edu.tw/> 網站最新資料為準。

1-3 資訊資產六大類：清單上不要只寫電腦

很多單位只盤「看得到的硬體」，結果最重要的名冊、合約、委外人員都漏了。

I 資訊資產

- 業務資訊、組織紀錄、使用者資訊
- 資料庫、備份資料、合約、系統文件
- 操作手冊、教育訓練教材、計畫與程序書

V 服務資產

- 資訊服務、通訊服務
- 作業環境設施服務(含委外提供的服務)

S 軟體與應用程式

- 作業系統、標準與特殊應用程式
- 程式開發工具、測試程式、通訊軟體

H 硬體資產

- 主機、伺服器、個人電腦、筆電、印表機
- 影印事務機、網路設備、儲存設備
- USB 隨身碟、NAS、監視器、IoT 設備

M 人員

- 管理者、系統 / 網路管理員、資料管理員
- 機房管理員、程式開發人員
- 行政人員、清潔人員、臨時人員、外包駐點人員

G 組織與聲譽

- 對本校的信心指數
- 對本校所提供服務的信心指數
- 本校的聲譽與形象

資料來源：本校 IS-B-003 資訊資產管理程序書 §6.6 資訊資產分類。

1-3 資訊資產六大類：清單上不要只寫電腦

I 資訊資產

資料庫、文件、合約、備份、
操作手冊、教材、計畫與程序書



V 服務資產

資訊系統維護、設備維護、通訊、
環境設施(UPS、空調)廠商



S 軟體作業與應用程式

作業系統、校務系統、套裝軟體、
開發工具、通訊軟體



H 硬體資產

主機、個人電腦、筆電、手機、
印表機、網路與儲存設備、
監視錄影設備



M 人員

管理者、系統管理員、行政人員、
工讀生、外包駐點人員



G 組織與聲譽

內外部關注方對本校的資安期望，
影響營運或聲譽者



資訊資產

守護學校的
重要資產

1-3 每年盤點怎麼做？四個動作

盤點不是填表比賽。四個動作做完，單位才真的「知道自己有什麼」。

STEP 1 看流程

- 先想清楚：我這個單位有哪些業務流程？
- 從流程找資產，不要從櫃子找資產
- 例：招生報名 → 線上報名系統 + 報名表 + 繳費名冊

STEP 2 列清冊

- 資訊資產填 IS-D-012 清冊
- 個資填 PIMS-D-007 個人資料檔案清冊
- 欄位要寫到：名稱、保管人、存放位置、數量

STEP 3 評價值

- 機密性 + 完整性 + 可用性 = 資產總價值 (1 ~ 5 級)
- 個資依「含不含姓名 / 身分證號 / 特種個資」評 1 ~ 4 級
- 價值越高，保護措施越嚴

STEP 4 做處理

- 價值與風險高的，排入改善計畫
- 確認不再需要的資料，依規定刪除、銷毀並留紀錄
- 異動要填 IS-D-028 資訊資產異動安全評估表

小技巧：先盤「如果外洩或不見，我會被長官問到的東西」，通常就是最高價值的那幾項。

1-3 最常漏掉的資產 vs. 最常漏掉的個資

例如：展演、典藏、校友與捐款等活動，個資散落的點可能較多。

最常漏掉的「資產」

- 放在個人電腦桌面的工作檔與共用資料夾
- 單位自己架的小網站、報名表單、Google 表單
- 展場 / 教室的 IP 攝影機、無線投影器、電子看板
- 老舊但仍上線的系統（沒人敢關，也沒人在管）
- 外接硬碟、隨身碟、光碟、母帶與數位典藏媒體
- 委外廠商的駐點人員與其使用的帳號

最常漏掉的「個資檔案」

- 招生、甄試、術科考試的報名與評分資料
- 學生作品授權同意書、肖像權同意書、展演參與名單
- 校友會名冊、捐款芳名錄與捐款人聯絡資料
- 工讀生、臨時人員、評審委員、講座講者的身分與匯款資料
- LINE 群組與 Email 群發名單（含家長聯絡方式）
- 紙本簽到表、借用單、問卷與訪談逐字稿

個資定義參考：本校 PIMS-B-003 §5；個資法第 2 條、第 6 條（特種個資）。

1-3 盤點做得好不好，教育部怎麼打分數？

評分看的是「全校比率」→ 只要有單位沒交，全校分數就掉。【高等教育深耕計畫資安專章】

指標	辦理事項（摘要）	一般同仁要配合的事
3.1 資訊資產清冊全校盤點、更新	A1 合規週期、A2 範圍落實全校、B 辦理教育訓練及成效評估、C 定期檢視正確性	按時交回單位清冊、參加訓練並通過測驗
3.2 資通系統完整盤點	A1/A2 定期盤點、B 清冊含 RTO/RPO 與防護基準、C 教育訓練、D 定期評估等級	單位自建系統、網站一定要申報，不要「私設」
3.3 IoT設備盤點與管控	A1/A2 盤點公務用 IoT、B 安全使用宣導、C 密碼複雜度 / 網路存取限制 / 漏洞修補	新購攝影機、感測器要報資訊處；務必修改預設帳號密碼
4.1 全校執行風險評估	A 訂定風險準則、B1/B2 執行風險評鑑（週期應與各類盤點一致）、C 風險處理計畫、D 處理結果	依清冊誠實評估，不要為了好看而低估

資料來源：高等教育深耕計畫第二期專章(資安強化) -115年度執行成果評量表（指標 3.1、3.2、3.3、4.1）。

1-3 盤資訊資產-IoT設備盤點與管控



連網事務機、印表機



網路攝影機(監控系統)



NAS 網路儲存設備



無線基地台、分享器



數位電子看板、智慧電視



能源管理、門禁、空調控制



1-3 本校 113年 盤點實況

以下統計由顧問實際彙整本校 113 年各單位繳交之清冊計算，同一單位取最新版本。

43份

資訊資產清冊
(單位繳交)

2,018筆

資訊資產
總盤點筆數

2,466筆

風險評鑑
評估項目

745筆

個人資料檔案
(61 份清冊)

看得到全貌 全校 43 個填報單位、2,018 筆資產、2,466 筆風險、745 筆個資檔案→這就是「我們有什麼」。

也看得到落差 其中 2 個單位的資產清冊筆數為 個位數，等於這個單位在或許沒有落實全盤。

接下來三頁 我們看資產價值怎麼分布、風險集中在哪裡，以及填表時最常出錯的地方。

統計基礎：本校 ISMS_PIMS 資產盤點及風險評鑑 114 年度資料（資產清冊 43 份、風險評鑑 43 份、個資盤點 61 份），由顧問程式彙整。

1-3 統計一：資產六大類的真實分布

前面講過「清單上不要只寫電腦」。現在看實際數字 → 硬體佔了 76.5%。

主類別	筆數	占比	這代表什麼
H 硬體資產	1,544	76.5%	電腦、筆電、印表機、攝影機——看得到、摸得到的都盤了
M 人員	229	11.3%	多為「本單位人員」一筆帶過
S 軟體與應用程式	202	10.0%	多為作業系統與 Office，自建小系統常被漏掉
I 資訊資產	37	1.8%	名冊、合約、資料庫、備份→最該保護的，卻只有 37 筆
V 服務資產	5	0.2%	委外服務、雲端服務幾乎沒人盤
G 組織與聲譽	1	0.05%	全校只有 1 筆

結論：本校盤點目前仍以財產清冊思維為主。未來請各單位優先補上「資訊資產 (I)」與「服務資產 (V)」。

統計基礎：本校 114 年資訊資產清冊 43 份、2,018 筆（顧問彙整）。

1-3 統計二：資產價值與風險值分布

風險值 = 資產價值等級 × 衝擊程度等級 × 可能性等級。看看我們實際填出來長什麼樣。

分布	內容	觀察
資產價值等級 (1~5 級)	1 級 678 筆 (33.6%) 2 級 1,178 筆 (58.4%) 3 級 142 筆 (7.0%) 4 級 19 筆 (0.9%) 5 級 0 筆	92% 集中在 1~2 級， 高價值資產可能被低估
風險值分布 (R = 價值×衝擊×可能性)	1~3: 1,122 筆(45.5%) 4~9: 1,134 筆 (46.0%) 2~18: 192 筆 (7.8%) 24 以上: 17 筆 (0.7%)	風險值 ≥24 共 17 筆 (0.7%) 這些或許就是要列入風險計畫的
可能性等級	1 級 2,024 筆 (82.1%) 2 級 389 筆 (15.8%) 3 級以上 53 筆 (2.1%)	逾八成填「1」， 等於認為「幾乎不會發生」
衝擊程度等級	1 級 1,024 筆 2 級 1,180 筆 3 級 114 筆 4 級 148 筆	衝擊評估相對合理

可接受風險值由管理審查會議核定；風險值偏低多半不是真的安全，而是「可能性」被一律填成 1。

統計基礎：本校 114 年風險評鑑彙整表 43 份、2,466 筆（顧問彙整）。

1-3 統計三：威脅與脆弱點，我們只想到硬體

風險三分之二是「機器壞掉」→ 但真正比較容易有事的是社交工程信件或委外廠商與個資外洩。

威脅 Top 5 (共 2,466 筆)

設備故障 892 筆 (36.2%)

硬體故障 733 筆 (29.7%)

人力短缺 128 筆 (5.2%)

機密 / 敏感資訊竊取或破壞 124 筆 (5.0%)

非法人士攻擊入侵或當作攻擊跳板 114 筆 (4.6%)

「設備故障」 + 「硬體故障」合計 1,625 筆，占 65.9%

脆弱點 Top 5

未進行定期性的維護及效能檢查 805 筆

設備零組件品質不佳 635 筆

前兩項合計 1,440 筆，占 58.4%

資訊安全意識及訓練不足 133 筆

未定期修補系統軟體的漏洞 108 筆

設備老舊 / 未進行定期性維護 86 筆

統計基礎：本校 114 年風險評鑑彙整表 2,466 筆（顧問彙整）。威脅與脆弱點用語依 IS-D-013 威脅及弱點評估表。

1-3 統計四：個資盤點的真實樣貌 (745 筆)

個資不是只在校務系統裡 → 七成在紙本，而且一半以上屬於高價值。

面向	統計結果	解讀
資料形式	紙本 525 筆 (70.5%) 電子 217 筆 (29.1%)	個資主要存在紙本，不在系統裡
資產價值	極高(4) 48 筆 高(3) 328 筆 中(2) 338 筆 一般(1) 28 筆	高與極高合計 376 筆，占 50.6%
特種個資	有 61 筆 (8.2%) 【請務必妥善保管】	健康檢查、輔導、病歷等，保護標準最高
保管數量	500 筆以內 568 筆 (76.2%) 500 ~ 5,000 筆 109 筆 5,000 ~ 50,000 筆 46 筆 逾 50,000 筆 7 筆	7 筆屬「逾 5 萬筆或不知數量」，應優先列管
是否委外	是 13 筆 (1.7%)	偏低，委外處理個資可能被低估
風險值	≥12 共 91 筆 (11.8%) 可能性填「1」者 707 筆 (92.1%)	可能性幾乎都填最低，與 ISMS 同一問題
個資類別 Top	C001 辨識個人者 702 C051 學校紀錄 332 C003 政府資料中之辨識 272 C011 個人描述 203 C111 健康紀錄 35	C003 多為身分證號，是外洩損害最大的欄位

統計基礎：本校 114 年個資盤點及風險評鑑 61 份、745 筆個資檔案、768 筆風險評鑑（顧問彙整）。

1-3 填寫注意事項（一）：資訊資產清冊

以下「常見問題」全部來自 113 年實際繳回的 43 份清冊，不是假設。

✓ 這樣填才對

- 編碼格式「主類別 - 次類別 - 流水號」，例：H-PC-001
- 保管人、使用人、放置地點三欄都要填，不能留空
- 物聯網設備（攝影機、事務機、感測器）務必勾選「是否為物聯網設備」
- 先從業務流程找資產，再補硬體；至少要有名冊、合約、資料庫、備份
- 委外提供的服務要列為「服務資產」

X 113 年實際發生的填寫問題

- 主類別寫法不一致** 代號 25 筆、中文全名 1,980 筆、誤填次類別 3 筆、異名 10 筆
- 資訊資產嚴重偏少** 全校只有 37 筆 (1.8%)
- 服務資產幾乎空白** 全校只有 5 筆
- 欄位留空** 保管人空白 6 筆、放置地點空白 22 筆、價值等級空白 1 筆
- 價值一律填低** 3 級以上僅 161 筆 (8.0%)

統計基礎：本校 114 年資訊資產清冊（顧問彙整）。填寫規則依 IS-B-003 §6.6、§6.7 及清冊內「資訊資產編碼原則」工作表。

1-3 填寫注意事項（二）：風險評鑑與個資清冊

填表不是為了交差，是為讓學校在出事時能回答「影響多少人、哪些資料」。

風險評鑑：三個最常被退件的地方

可能性不要一律填 1 82% 填 1；請依「年度發生頻率」誠實評估（3 次以下 = 2 級）

威脅不要只寫硬體故障 至少要有有人為疏失、釣魚郵件、委外廠商、個資外洩等情境

風險擁有者不可空白 114 年有 43 筆空白；應為權責單位主管

- 資產清冊與風險評鑑的筆數、編碼要對得起來
- 風險值 ≥ 12 者要有對應的風險處理計畫

個資清冊：四個最常見錯誤

欄位錯位 「資料形式」誤填「否」3 筆、「是否委外」誤填法規名稱 3 筆、「特種資料」誤填筆數或特定目的 8 筆

筆數寫法不統一 應使用下拉選項，勿自行輸入「0 筆」「501 筆」「5000 筆(含)以內」

委外欄低報 只要有廠商碰得到這份資料就是「是」

控制措施寫太籠統 「上鎖的櫃子」要寫清楚放哪裡、誰有鑰匙

統計基礎：本校 114 年風險評鑑彙整表（2,466 筆）與個資盤點及風險評鑑（745 筆）之欄位值統計。

1-4 資安通報及未來個資事件通報規範

依據：資通安全事件通報應變及演練辦法（115.01.05 修正）；本校 IS-B-012 安全事件管理程序書

**通報不是認錯，是止血。
晚一小時，損害可能差十倍。**

- 法定義務** 《資通安全事件通報應變及演練辦法》（115/1/5 修正施行）：公務機關知悉資通安全事件後，應於 1 小時內至指定平臺通報。
- 不是你判斷** 事件等級由受理機關審核認定，不是由發現的人決定。您的工作是「盡快講」。
- 兩條線都要走** 若同時涉及個人資料，資安通報與個資事故處理要同步啟動（校內 PIMS-D-024 已明定「同步判定是否為資安事件」）。

1-4 資安事件分四級：越嚴重，時間壓得越緊

115/1/5 修正後為一至四級（四級最嚴重），並刪除三、四級中「敏感資訊」的判定要件。

等級	大致情形	通報	損害控制 / 復原	調查改善報告
第一級	非核心業務資訊或系統遭輕微洩漏、竄改， 或中斷可於可容忍中斷時間內回復	1 小時內	72 小時內	完成後 1 個月內
第二級	非核心業務資訊或系統遭嚴重洩漏、竄改； 或核心業務（非關鍵基礎設施）輕微受影響	1 小時內	72 小時內	完成後 1 個月內
第三級	核心業務（非關鍵基礎設施）嚴重受影響； 或一般公務機密、關鍵基礎設施核心業務輕微受影響	1 小時內	36 小時內	完成後 1 個月內
第四級	一般公務機密或關鍵基礎設施核心業務嚴重受影響； 國家機密遭洩漏竄改；核心系統無法於可容忍時間內回復	1 小時內	36 小時內	完成後 1 個月內

第三、四級屬「重大資通安全事件」。受理機關審核時限：一、二級 8 小時內，重大事件 2 小時內。

資料來源：資通安全事件通報應變及演練辦法第 2、6、7、8 條（115.01.05 修正發布施行）。

1-4 校內通報流程：您只要做第 1 步

校內流程有四步，但對一般同仁而言，**重要的只有第一步：講出來，而且要快。**

STEP 1 發現

- 看到異常就通報，不要自己判斷嚴不嚴重
- 通報方式：電話、Email、書面
- 同時副知直屬主管

STEP 2 研判

- 權責單位研判是否為資訊安全事件
- 一般故障 → 走報修程序
- 構成資安事件 → 填 IS-D-055 異常事件紀錄表

STEP 3 陳報

- 處理單位初估處理時間與事件等級
- 評估是否須通報教育部
- 陳報執行秘書裁示

STEP 4 外通報

- 資安處理組登入教育機構資安通報平台
- <https://info.cert.tanet.edu.tw>
- 1 小時內完成通報

校內窗口：資訊處 (06) 693-0100 分機 1703、1709

校園行政系統 <http://203.71.53.11/FIX/>

所有人員(含：本校人員、約聘僱人員與委外駐點人員)，發現疑似資訊安全事件時，皆負有即時通報之責任。

1-4 發現事故的當下，該做與不該做

資安事件處理的第一準則：先止血、保全跡證，再查原因。

✓ 該做

- 保持現況：中毒電腦「拔網路線」，但不要關機
- 立刻用電話通知資訊處與直屬主管（不要只傳 Email）
- 記下時間、看到的畫面、做過的動作（可拍照）
- 若是個資外洩，同步通知單位個資保護專責人員
- 配合清查影響範圍：哪些資料、幾筆、哪些當事人
- 後續依指示填寫紀錄表，留下完整軌跡

X 不該做

- 自己重灌、自己掃毒、自己刪檔（證據就沒了）
- 覺得「應該沒事」先觀察一天再說
- 怕被責備而不通報——未通報的風險遠大於出錯
- 在 LINE 群組公開討論事故細節
- 擅自對外回覆媒體、家長或當事人
- 付贖金或私下與駭客接觸

參考：本校 IS-B-012 安全事件管理程序書；PIMS-C-002 個人資料保護緊急應變處理作業說明書（對外發言由個資事故對外發言人統一處理）。

1-5 辦公室資安與個資相關注意事項

依據：IS-B-006 實體安全管理程序書、IS-C-001 人員資訊安全守則

**駭客攻擊需要技術；
但撿走你桌上的名冊，不需要。**

實體安全是第一道防線 本校把工作區域分為「一般辦公區域」與「安全管制區域」（如資訊處電腦機房），兩者規定不同。

最常被稽核抓到的 桌面沒淨空、螢幕沒鎖定、文件沒上鎖、訪客沒登記。

這些都寫在校內文件裡 IS-B-006 實體安全管理程序書、IS-C-001 人員資訊安全守則→不是建議，是規定。

1-5 一般辦公室區域：校內明文規定的六件事

以下六條，逐字出自本校 IS-B-006 §6.3 「一般辦公室區域控制措施」與 IS-C-001。

① 最後一個走的人要鎖門

- 無人時或下班最後一人離開時，須將辦公室關門上鎖
- 非上班時間出入須使用門禁卡、鑰匙或類似方式

② 桌面淨空

- 離開座位時遵守桌面淨空政策
- 敏感等級以上文件與可攜式設備存放於儲櫃並上鎖

③ 看到陌生人要問

- 隨時注意身分不明或可疑的人員
- 發現時主動詢問並儘速通知相關單位

④ 清理資源回收筒

- 定期清理個人電腦的資源回收筒
- 避免「已刪除」的重要資料其實還在

⑤ 東西不能隨便帶走

- 未經授權不得將設備、軟體、儲存媒體或文件攜出本校
- 有需要須經權責主管核准

⑥ 螢幕要自動上鎖

- 個人電腦、終端機：設定螢幕保護程式（15分鐘以內）並設定密碼保護
- 伺服器：5分鐘以內

資料來源：本校 IS-B-006 實體安全管理程序書 §6.3、§6.6；IS-C-001 人員資訊安全守則 §6。

1-5 個人電腦與帳號：校內守則速查 (IS-C-001)

這一頁可以印出來貼在辦公室 → 它就是稽核時最常被抽問的清單。

項目	規定	白話說明
螢幕保護	設定螢幕保護程式 (15 分鐘以內) 並設定密碼保護	離座就按 Win + L, 不要等 15 分鐘
系統更新	作業系統漏洞應即時更新修補	不要一直按「稍後提醒我」
防毒	應安裝防毒軟體並即時更新病毒碼	不要為了裝軟體而關掉防毒
備份	應定期將重要資料備份存放	重要檔案至少兩份、不同地方
密碼	妥慎保存, 不得書面記錄或張貼於電腦、螢幕, 並定期更換	便利貼貼在螢幕上是稽核必抓
郵件	開啟來路不明之電子郵件及其附件時應謹慎小心	第三堂課會細講
銷毀	敏感等級以上紙本不再使用時, 應以碎紙機銷毀並刪除電子檔	不要整疊丟進回收箱
媒體丟棄	丟棄曾儲存本校資訊的電子媒介前, 須刪除並徹底消磁或銷毀至無法解讀	舊隨身碟不要直接送人
軟體版權	不得私自安裝非法電腦軟體; 禁止下載不明來源軟體	破解版 = 惡意程式最愛的載體
保密	應填具 IS-D-020 保密切結書, 職務上所獲悉資訊非經授權不得外洩	含學生、校友、捐款人資料

資料來源：本校 IS-C-001 人員資訊安全守則 v3.1 §6; IS-B-006 §6.6。

1-5 紙本與輸出：最容易外洩的，往往不是電腦

教育體系規範 A.11.2.9「桌面淨空及螢幕淨空政策」講的就是這四件事。

印 印表機 / 影印事務機

- 列印敏感或機密資訊後，應立即從印表機取走
- 共用事務機請用「安全列印 / 刷卡取件」
- 事務機也是 IoT 設備，務必修改預設帳號密碼

碎 碎紙機

- 敏感等級（含）以上紙本不再使用時，應以碎紙機銷毀
- 同時刪除電子檔
- 銷毀要留紀錄（IS-D-066 文件銷毀申請單）

櫃 上鎖的櫃子

- 文件及儲存媒體不使用或下班時應存放在櫃子內
- 機密性、敏感性資訊應上鎖，最好放防火櫃
- 含紙本簽到表、借用單、評分表

郵 收發與傳真

- 保護一般郵件進出的地點
- 注意無人看管的傳真機
- 寄送紙本名冊請用彌封並確認收件人

資料來源：教育體系資通安全暨個人資料管理規範 A.11.2.9；本校 IS-C-001、IS-B-003。

1-5 可攜式設備、攜出與報廢

「設備離開你的視線」就是風險的開始 → 攜出、借用、送修、報廢，四個時點最常出事。

U 隨身碟與外接硬碟

- 未經主管許可，嚴禁將機密資訊存入可攜式儲存媒體
- 必要時須加密，不得以明文直接儲存
- 用畢後立即清空；重要媒體應上鎖或專人管理

N 筆電與行動裝置攜出

- 需以密碼保護，防止偷取、遺失或未授權使用
- 攜出須經保管單位主管同意並填表；
- 歸還時刪除作業資料並掃毒
- 不得任意安裝或下載軟體

O 無人看管的設備

- 應做好防竊措施（固定、上鎖、監視錄影）
- 開放性系統不得存有敏感等級以上資料
- 展場、琴房、工作室的電腦尤其要注意

X 報廢與再利用

- 報廢或移轉前應確實清除限閱等級以上資訊
- 含儲存媒體者須格式化、刪除或實體銷毀後方可移交
- 含個資者宜以物理摧毀或授權技術毀壞

資料來源：本校 IS-B-003 §6.8、IS-B-006 §6.6；教育體系資通安全暨個人資料管理規範 A.11.2.5～A.11.2.8。



離開辦公室前的60秒自我檢查

養成好習慣，保護機關與個人資訊安全！



出門前
花60秒
多一分安心！

1 電腦已鎖定或登出
(Win + L)



2 桌面沒有留下
含姓名、身分證號、聯絡
方式的紙本



3 抽屜 / 櫃子已上鎖，
鑰匙不在桌上



4 印表機、影印機上沒有
未取走的文件



5 隨身碟、外接硬碟已收妥，
不在桌面上



6 白板上沒有留下密碼、
帳號或敏感資訊



7 待銷毀的紙本已投入
碎紙機 (不是回收箱)



8 視訊會議、投影畫面
已關閉



9 窗戶、門已關閉上鎖
(若為最後離開者)



10 有訪客或廠商今天來過？
進出紀錄是否已登記



 小小的檢查，避免大大的風險！ 保護資料，從你我做起，讓資安成為日常習慣

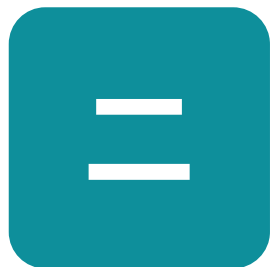


這些都是您上完課要知道的

1. 離開座位要把電腦設定螢幕保護程式(15 分鐘以內)並設定密碼保護。
2. 資訊資產若沒有盤點，會無法識別到可能面臨的風險情境，導致無法有效進行風險評鑑作業。
3. 文件及儲存媒體不使用或下班時應存放在櫃子內。
4. 依據《資通安全事件通報應變及演練辦法》的規定，應於知悉後**1小時**內進行外部通報
5. 最小權限原則是指**依職務需求給予必要權限**
6. 發生資通安全事件或個人資料外洩的事件時，**應該要立刻進行通報**。
7. 業務如需蒐集、處理或利用個人資料，**「不可」**蒐集越多個人資料。
8. 依據個資法當事人權益，當事人**「有權」**要求刪除其個人資料。
9. 蒐集個資時，應告知蒐集目的、蒐集哪些個人資料與利用的方式等資訊。
- 10. 健康檢查資料**屬於《個人資料保護法》第6條規範的特種個資。
11. 若個人資料的特定目的消失了，依規定應該要**刪除或銷毀**
12. 資通安全與個人資料保護是**資訊、業務單位及教職員所有人**的責任







C 級機關應辦事項及 委外廠商作業規範

Mandatory Items for Level-C Agencies & IT Outsourcing

- 1 資通安全管理法與全部子法體系整理
- 2 責任等級 A ~ E 怎麼分？南藝大為什麼是 C 級
- 3 附表五：C 級公務機關應辦事項逐項拆解
- 4 資訊業務委外：採購前、契約中、履約中、驗收後

2-1 責任等級 A ~ E：誰是哪一級？

只要學校有「會登入、有權限區分」的系統，就落入 C 級 → 校務系統、選課、報名、差勤都算。

等級	認定情形 (摘要)	典型機關
A 級	涉及國家機密、外交國防、全國性民眾服務； 或屬全國性關鍵基礎設施提供者	中央部會、全國性 CI
B 級	涉及區域性民眾服務、區域性個資檔案； 或屬區域性關鍵基礎設施提供者	直轄市政府、區域型機構
C 級	維運自行或委外設置、開發之資通系統者 (指具有權限區分及管理功能者)	多數國立大學 / 校院
D 級	自行辦理資通業務，但未維運自行或委外設置、開發之資通系統	小型機關
E 級	無資通系統且未提供資通服務； 或全部資通業務由上級或指定機關兼辦、代管	代管型單位

同時符合多個等級者，以最高等級為準（第 9 條）；每三年提交或核定一次，組織或業務調整時須變更（第 3 條）。

資料來源：資通安全責任等級分級辦法第 2 ~ 10 條（115.01.07 修正）。本校等級以學校核定公文為準。

2-1 附表五：C 級公務機關應辦事項（管理面）

「應辦事項」＝法律規定一定要做的最低標準，做不到就是不符合。

辦理項目	辦理內容	誰負責
資通系統分級及防護基準	依附表九完成資通系統分級，並完成附表十控制措施；之後每年至少檢視一次分級與防護基準是否妥適	資訊處＋系統權責單位
資訊安全管理系統之導入	全部核心資通系統導入 CNS 27001 / ISO 27001 或同等以上標準，並持續維持	全校 (ISMS)
資通安全專職人員	配置至少 1 人	學校
內部資通安全稽核	每 2 年辦理 1 次	稽核小組
營運持續計畫演練	全部核心資通系統每 2 年辦理 1 次	系統權責單位

資料來源：資通安全責任等級分級辦法附表五（115.01.07 修正）
<https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=A0030304>

2-1 附表五：C 級公務機關應辦事項（技術面）

紅字是 115/1/7 修正後 C 級新增的重點：弱點管理（VANS）正式成為 C 級應辦事項。

辦理項目	細項	頻率 / 內容
安全性檢測	弱點掃描	全部核心資通系統每 2 年辦理 1 次
安全性檢測	滲透測試	全部核心資通系統每 2 年辦理 1 次
資通安全健診	網路架構檢視	每 2 年辦理 1 次
資通安全健診	網路惡意活動檢視	每 2 年辦理 1 次
資通安全健診	使用者端電腦惡意活動檢視	每 2 年辦理 1 次
資通安全健診	伺服器主機惡意活動檢視	每 2 年辦理 1 次
資通安全健診	目錄服務系統設定及防火牆連線設定檢視	每 2 年辦理 1 次
資通安全弱點管理	-	知悉弱點時適時修補或緩解；依主管機關指定方式導入並持續維運
資通安全防護	防毒軟體 / 網路防火牆	完成啟用、持續使用並適時更新或升級
資通安全防護	具有郵件伺服器者	應備有電子郵件過濾機制

資料來源：資通安全責任等級分級辦法附表五（115.01.07 修正）。

2-1 附表五：認知與訓練面——這一頁和「您」直接有關

今天這 3 小時，就是法規要求「一般使用者及主管每人每年 3 小時通識教育訓練」。

對象	訓練要求	今天這堂課算嗎
資通安全專職人員	每人每年接受 12 小時以上資通安全專業課程訓練或職能訓練	不算（需專業課程）
專職人員以外之 資訊人員	每人每 2 年接受 3 小時以上專業課程或職能訓練， 且每人每年接受 3 小時以上通識教育訓練	通識部分算
一般使用者及主管	每人每年接受 3 小時以上通識教育訓練	算，而且這 3 小時剛好
資通安全專業證照 及職能訓練證書	資通安全專職人員各持有證照及證書至少 1 張，並持續維持有效性	-

請務必完成簽到（IS-D-023 教育訓練簽到表）與課後成效評估→教育部資安專章指標 9.1 會查「成效評估」與「未完成者的後續追蹤」。

資料來源：資通安全責任等級分級辦法附表五（115.01.07 修正）；教育部 114 年資安專章指標 9.1。

2-1 115/1/7 修法，C 級要注意的四個變化

法規剛改完，今年的自評與專章填報都要用新版。

1 弱點管理正式入列

- 技術面新增「資通安全弱點管理」
- 知悉弱點要適時修補或緩解
- 並依主管機關指定方式導入（即 VANS）並持續維運

2 辦理期限重新起算

- 第 11 條明定：辦理期限自修正施行之日起算
<https://law.moj.gov.tw/LawClass/LawSingle.aspx?pcode=A0030304&flno=11>
- → 115/1/7 是新的起跑點

3 免辦有正式程序

- 因技術或資通系統設計因素確有困難者
- 得經同意並報主管機關備查後免辦
- 不是「做不到就算了」，是要走程序留紀錄
<https://law.moj.gov.tw/LawClass/LawSingle.aspx?pcode=A0030304&flno=11>

4 等級三年一審

- 每三年提交或核定責任等級一次
- 組織或業務調整時須依程序變更等級
- 學校新增重要系統時要重新檢視
<https://law.moj.gov.tw/LawClass/LawSingle.aspx?pcode=A0030304&flno=3>

資料來源：資通安全責任等級分級辦法第 3、10、11 條及附表（115.01.07 修正發布施行）。

2-1 應辦事項 ↔ 教育部 114 資安專章：同一件事，兩份考卷

應辦事項是「及格線」，資安專章是「排名賽」。專章拿分的關鍵字永遠是：全校、比率、成效評估。

主題	資安法應辦事項（法定最低標準）	資安專章評核（教育部加碼看什麼）
資產 / 系統盤點	依附表九完成系統分級並每年檢視	3.1 / 3.2 / 3.3：要「全校範圍」、要統計完成比率、要辦教育訓練並做成效評估
風險評鑑	透過資訊安全管理系統(ISMS)導入要求	4.1：訂定風險準則→執行評鑑→風險處理計畫→處理結果，逐層加分
安全檢測	弱點掃描、滲透測試每 2 年 1 次	4.2 / 4.3：做得比法規「更多、更頻繁」加分；高風險弱點修補率要拿得出數字
委外管理	委外應簽書面契約（修法後入法）	6.1：程序書納入法遵、建立契約範本、落實查核追蹤、廠商人員完成資安訓練
教育訓練	一般使用者及主管每人每年 3 小時	9.1：要有成效評估、未達標要有強化措施、要提報管理審查會議
社交工程	（由主管機關規劃演練）	10.2：惡意郵件開啟率 < 10%、惡意連結點擊率 < 6%；受誘騙者要有後續加強措施
禁用產品	危害國安產品限制使用（修法後法律位階）	12.1 / 12.2：採購限制與宣導、既有列冊與汰除、出租場域禁用規定

資料來源：資通安全責任等級分級辦法附表五；教育部 114 年度大專校院資安專章績效項目評核表。

2-2 資訊業務委外注意事項

依據：資通安全管理法施行細則 §4；本校 IS-B-011 資訊作業委外安全管理程序書

學校資安做得再好，
只要有一家廠商沒跟上，整條線就斷了。

■ **委外不等於卸責** 資通安全管理法施行細則第 4 條明定機關委外時應考量與監督的事項；資安法修正後更要求「應簽訂書面契約」。

■ **廠商出事 = 學校出事** 委外廠商知悉資安事件，依本校契約規範須於 1 小時內通報學校；學校仍須對外負責。

■ **採購單位是第一道關卡** 規格書與契約沒寫，後面想補就來不及了→這是整個委外管理成敗的關鍵。

2-2 委外的四大風險：不是廠商壞，是流程有洞

過去三年的大型資安事件，有相當比例的起點不在機關自己，而在供應鏈。

帳 帳號與權限

- 廠商用「最高權限帳號」直接進資料庫
- 專案結束帳號沒關、離職人員帳號還活著
- 共用帳號導致出事查不出是誰做的

資 資料攜出

- 為了「回去測試比較方便」把真實名冊拷貝帶走
- 測試環境用正式個資，且沒有加密
- 上線後測試帳號、測試資料沒清除

碼 程式與供應鏈

- 交付的程式內藏後門、隱密通道或惡意程式
- 使用未授權的第三方元件、開源套件未更新
- 廠商自己被駭，成為攻擊學校的跳板

約 契約與驗收

- 招標文件沒寫資安要求，驗收時無從要求
- 沒有稽核權，想查也查不了
- 合約終止時資料沒返還、沒刪除、沒確認

參考：本校 IS-B-011 §6；ASRC 2026 社交工程趨勢預測（供應鏈與廠商郵件遭入侵）。

2-2 真實案例：委外廠商遭入侵



摩斯漢堡公告

親愛的顧客您好：

提醒您，近日詐騙猖獗，接到可疑電話或E-mail信件
不透露任何個人資訊、**不進行**任何ATM操作、**不提供**個人銀行帳戶、
請您立即掛斷電話或刪除信件，保持警覺切勿上當！

警政署防詐騙專線：165

摩斯漢堡敬上

參考東森新聞：

2026/10/02

摩斯漢堡驚傳個資外洩！疑
委外廠商平台遭駭

https://www.youtube.com/watch?v=GmqozW_KjDE

時間：00:53

2-2 委外法源一次看：採購前請先把這幾份叫出來

這十份就是委外案的「法遵清單」。採購單位只要漏掉其中一份，稽核就會留下缺失。

類別	文件名稱	最該看的地方
法律	資通安全管理法	委外應簽訂書面契約；危害國安產品限制
命令	資通安全管理法施行細則 §4	委外應考量與監督的事項（法遵最低要求）
命令	資通安全責任等級分級辦法 附表九 / 附表十	附表九：防護需求分級原則；附表十：防護基準
指引	資通系統籌獲各階段資安強化措施	需求、設計、開發、測試、維運各階段的資安要求
指引	政府資訊作業委外安全參考指引	委外安全條款的撰寫參考
範本	公共工程委員會 資訊服務採購契約範本	直接可套用的契約條款
規範	政府網站服務管理規範	委外做網站時必須遵循
校內	IS-B-011 資訊作業委外安全管理程序書	本校自己的規定，稽核直接比對這一本
校內	PIMS-B-010 個人資料業務委外處理程序書	委外涉及個資時的監督義務
校內	IS-D-054 合約商保密切結書 / PIMS-D-023 委外廠商保密切結書	廠商人員必簽

資料來源：本校 IS-B-011 資訊作業委外安全管理程序書 §2 參考依據、§6 作業說明。

2-2 委外生命週期：五個階段，五個把關點

委外管理不是「簽完約就交給廠商」，而是從需求評估一路管到契約終止。

STEP 1 需求

- 評估委外必要性（技術 / 人力 / 時效 / 成本）
- 依附表九評估資通系統防護需求等級，並「標示給廠商知悉」
- 以資訊經費 5% 估算資安經費

STEP 2 招標

- 載明禁用大陸廠牌條款與切結書
- 要求廠商配置資安專業人員及能力
- 要求提供人員學經歷與在職證明

STEP 3 簽約

- 納入保密、稽核權、事件通報（1 小時）
- 智財權、違約責任、技術移轉
- 廠商人員簽 IS-D-054 / PIMS-D-023 保密切結書

STEP 4 履約

- 帳號獨立、有效期限、不得給最高權限
- 駐點、進出機房、資料攜出都要申請
- 定期開會、審查稽核紀錄與服務水準

STEP 5 驗收/終止

- 上線前清除測試資料與測試帳號
- 檢查有無後門、惡意程式，取得安全性檢測證明
- 合約終止時確認返還、移交、刪除或銷毀資料

依據：本校 IS-B-011 §6.1 ~ §6.11；資通系統籌獲各階段資安強化措施。

2-2 採購前必做三件事（採購單位請特別注意）

這三件事如果採購前沒做，之後補不回來，而且是稽核與專章評核必查項目。

必做事項	怎麼做	依據
① 標示防護需求等級	若涉資通系統籌獲，於徵求時依「資通安全責任等級分級辦法附表九」評估等級，並於招標文件標示系統防護需求等級供委外廠商知悉	IS-B-011 §6.3 附表九
② 編列資安經費	至少以資通系統籌獲案「資訊經費的 5%」估算資安經費；無法達成者應敘明原因與擬採行之資安作為，報資安長或機關核准	IS-B-011 §6.3
③ 納入禁用條款	招標文件與契約載明不得為大陸廠牌資通訊產品，並請廠商簽署「使用資通訊產品禁制事項切結書」	限制使用原則 專章 12.1 C 項

提醒：資通系統防護需求等級為「高級」者，主辦單位應定期或不定期對委外廠商辦理資安稽核；「中級」者得視需求辦理。

2-2 契約必載的資安條款：對照校內 IS-B-011 檢查

這 12 條逐條出自本校 IS-B-011。把它當成契約審查的 Checklist 使用。

條款	內容重點
人員資格	廠商應提供參與人員之學歷、工作資格、在職證明；重要成員非經同意不得更換
管理能力	辦理受託業務之程序及環境，應具備完善之資通安全管理措施或通過第三方驗證
法令遵循	人員、分包商、供應鏈均須遵守資安與個資相關法令，並簽訂保密同意書
合法軟體	履約所使用之軟體均須為合法軟體，違反者由廠商承擔法律責任
事件通報	違反資安法令或知悉資安事件時，須於 1 小時內通報學校，並提出緊急應變處置
稽核權	學校有權稽核廠商使用之工具軟體及作業執行紀錄，廠商不得異議
專業人力	應配置經適當訓練、擁有資安專業證照或類似經驗之資通安全專業人員
惡意程式	交付之系統、軟硬體與文件須先檢查有無惡意程式及隱密通道，並提出安全性檢測證明
測試清理	上線前應清除正式環境之測試資料與帳號、管理資料與帳號
離職管理	開發或負責人員離職時應繳回設備、軟體及作業權限，並主動通知學校移除帳號
保密存續	保密責任不因合約終止而失效，至學校解除機密為止
契約終止	應確認廠商返還、移交、刪除或銷毀因履約而持有之資料

資料來源：本校 IS-B-011 資訊作業委外安全管理程序書 §6.3 合約資訊安全需求、§6.4 資通安全責任、§6.8 系統開發及維護。

2-2 委外的兩道最低防線

依據：資通安全管理法；本校 IS-B-011 §6.3、§6.9；教育部資安專章指標 61

**契約沒有資安條款，等於沒有要求；
人員沒簽保密切結書，等於沒有拘束。**

- ① **契約資安條款** 資安法修正後明定「委外應簽訂書面契約」，權利義務與違約責任都要寫清楚。沒寫進招標文件與契約，驗收時提不出要求，稽核時也拿不出佐證。
- ② **人員保密切結書** 廠商派誰來做，誰就要簽。保密責任不因合約終止而失效，至本校解除該資訊之機密等級為止。
- 兩者缺一不可** 條款拘束「公司」，切結書拘束「到場作業的人」。只做一半，責任就會斷在中間。

資料來源：本校 IS-B-011 資訊作業委外安全管理程序書 §6.3 合約資訊安全需求、§6.9 委外作業人員安全管理（保密協議）。

2-2 誰要簽什麼？四張切結書一次講清楚

這四張表都在校內資安專區可以下載，是稽核與專章評核必查的佐證。

表單編號 / 名稱	誰要簽	什麼時候簽	重點
IS-D-020 保密切結書	本校教職員工	到職時 / 承辦敏感業務前	承諾職務上獲悉之資訊、資料、檔案、技術、財務或業務機密，非經主管授權不得對外透露或濫用
IS-D-054 合約商保密切結書	委外廠商 參與作業人員	簽約後、進場作業前	每一位到場或可存取本校資料的廠商人員都要簽，不是公司簽一張就好
PIMS-D-023 委外廠商保密切結書	涉及個資之 委外廠商	簽約時	委外處理個資時適用，搭配 PIMS-B-010 個人資料業務委外處理程序書
PIMS-D-022 員工個人資料保密同意書	本校人員	承辦個資業務時	個資保密的個別承諾

保密期間：保密責任不因合約終止而失其效力，至本校對該等保密資訊解除機密為止（IS-B-011 §6.3）。

資料來源：本校 IS-B-011 柒、輸出表單 / 紀錄；IS-C-001 §6.17；PIMS-B-010；校內資安專區 <http://its.tnnua.edu.tw>

2-2 資安條款參考採購契約範本

招標相關文件及表格

招標相關文件及表格 (最新版日期)

1. 投標須知範本
2. 參考最有利標精神投標須知範本
3. 公開取得電子報價單投標須知範本 (工程、財物採購)
4. 媒體服務採購投標須知範本
5. 工程採購契約範本
6. 統包工程採購契約範本
7. 節能績效保證專案統包工程採購契約範本
8. 財物採購契約範本
9. 勞務採購契約範本
10. 公共工程技術服務契約範本
11. 公共工程專案管理契約範本
12. 資訊服務採購契約範本
13. 災害搶險搶修開口契約範本
14. 災後復建工程設計、監造技術服務開口契約範本
15. 資訊雲端服務採購契約範本

12. 資訊服務採購契約範本

請使用最新版

相關檔案

資訊服務採購契約範本(1131226)  (357.38KB)  (89.36KB)  (690.75KB)

修正明細對照(1131226)  (50.69KB)  (23.34KB)  (106.17KB)

資訊服務採購契約範本(1121123)  (343.55KB)  (86.75KB)  (588.71KB)

修正明細對照(1121123)  (78.34KB)  (25.26KB)  (98.86KB)

資訊服務採購契約範本(1120711)  (339.97KB)  (85.99KB)  (586.34KB)

修正明細對照(1120711)  (35.93KB)  (22.08KB)  (60.48KB)

資訊服務採購契約範本(1110429)  (793.14KB)

修正明細對照(1110429)  (188.03KB)

資訊服務採購契約範本(1110407)  (861.58KB)

修正明細對照(1110407)  (118.59KB)

資訊服務採購契約範本

(113.12.26修正)

招標機關(以下簡稱機關)及得標廠商(以下簡稱廠商)雙方同意依政府採購法(以下簡稱採購法)及其主管機關訂定之規定訂定本契約,共同遵守,其條款如下:

第一條 契約文件及效力

(一)契約包括下列文件:

1. 招標文件及其變更或補充。
2. 投標文件及其變更或補充。
3. 決標文件及其變更或補充。
4. 契約本文、附件及其變更或補充。
5. 依契約所提出之履約文件或資料。

(二)契約文件,包括以書面、錄音、錄影、照相、微縮、電子數位資料或樣品等方式呈現之原件或複製品。

(三)契約所含各種文件之內容如有不一致之處,除另有規定或係明顯打字或書寫錯誤之情形外,依下列原則處理:

1. 招標文件內之投標須知及契約條款優於招標文件內之其他文件所附記之條款。但附記之條款有特別聲明者,不在此限。
2. 招標文件之內容優於投標文件之內容。但投標文件之內容經機關審定優於招標文件之內容者,不在此限。招標文件如允許廠商於投標文件內特別聲明,並經機關於審標時接受者,以投標文件之內容為準。
3. 文件經機關審定之日期較新者優於審定日期較舊者。
4. 大比例尺圖者優於小比例尺圖者。
5. 決標紀錄之內容優於開標或議價紀錄之內容。
6. 招標文件內之標價清單,其品項名稱、規格、數量,優於招標文件內其他文件之內容。
7. 同一優先順位之文件,其內容有不一致之處,屬機關文件者,以對廠商有利者為準;屬廠商文件者,以對機關有利者為準。

(四)契約文件之一切約定得互為補充,如仍有不明確之處,應依公平合理原則解釋之。如有爭議,依採購法之規定處理。

<https://www.pcc.gov.tw/content/index?eid=9819&type=C&lang=1>

2-2 資安條款參考採購契約範本 (續)

資安指標	對於所維護之系統，未於規定期限取得認證日數	每次認證超過期限	每逾○○日計○點
	知悉發生資安事件之通報、損害控制或復原作業時效	應於1小時內通知機關（或接獲機關通知1小時內），並採取適當之應變措施	每逾○○小時計○點
	完成損害控制或復原作業之時效	應於知悉資通安全事件後72小時（重大資安事件為36小時）內完成損害控制或復原作業	每逾○○小時計○點
	調查及處理資安事件之時效	完成損害控制或復原作業後，應於1個月內送交調查、處理及改善報告（或協助機關調查處理）	每逾○○日計○點

[illegible]

保密同意書

茲緣於簽署人 (簽署人姓名, 以下稱簽署人) 參與 (廠商名稱, 以下稱廠商) 得標 (機關名稱) (以下稱機關) 資訊業務委外案 (案名) (以下稱「本案」), 於本案執行期間有知悉或可得知悉或持有政府公務秘密及業務秘密, 為保持其秘密性, 簽署人同意恪守本同意書下列各項規定:

- 第1條 簽署人承諾於本契約有效期間內及契約期滿或終止後, 對於所得知或持有的一切機關未標示得對外公開之公務秘密, 以及機關依契約或法令對第三人負有保密義務之業務秘密, 均應以善良管理人之意妥為保管及確保其秘密性, 並限於本契約目的範圍內, 於機關指定之處所內使用之。非經機關事前書面同意, 不得為本人或任何第三人之需要而複製、保有、利用該等秘密或將之洩漏、告知、交付第三人或以其他方式使第三人知悉或利用該等秘密, 或對外發表或出版, 亦不得攤至機關或機關指定處所以外之處所。
- 第2條 簽署人知悉或取得機關公務秘密與業務秘密應限於其執行本契約所必需且僅限於本契約有效期間內。簽署人同意公務秘密與業務秘密, 應僅提供、告知有需要知悉該秘密之廠商或團隊成員人員。
- 第3條 簽署人在下述情況下解除其所應負之保密義務:
原負保密義務之資訊, 由機關提供以前, 已合法持有或已知且無保密必要者。
原負保密義務之資訊, 依法令已解密、依契約機關業已不負保密責任、或已為公眾所知之資訊。
原負保密義務之資訊, 係自第三人處得知或取得, 該第三人就該等資訊並無保密義務。
- 第4條 簽署人若違反本同意書之規定, 機關得請求簽署人及其任職之廠商賠償機關因此所受之損害及追究簽署人洩密之刑責, 如因而致第三人受有損害者, 簽署人及其任職之廠商亦應負賠償責任。
- 第5條 簽署人因本同意書所負之保密義務, 不因離職或其他原因不參與與本案而失其效力。
- 第6條 本同意書一式叁份, 機關、簽署人及 (廠商) 各執一份。

簽署人姓名及簽章:
身分證字號:
聯絡電話:
戶籍地址:
所屬廠商名稱及蓋章:

2-2 實例：學校要開發一套「線上報名系統」

把法規變成一個採購案的動作清單 → 這就是「委外作業規範」真正的樣子。

前 採購前（需求單位 + 採購單位）

- 這套系統會收姓名、身分證號、電話、繳費帳號 → 個資價值等級「高」
- 依附表九評估防護需求等級，並在招標文件標示
- 資訊經費 100 萬 → 資安經費至少抓 5 萬
- 規格書寫入：禁用大陸廠牌、SSDLC、交付前安全性檢測證明
- 會辦資訊處與個資窗口

中 履約中（需求單位監督）

- 廠商帳號由學校建立，載明需求、權限與有效期限
- 不給資料庫最高權限；駐點作業在指定地點
- 測試一律用假資料，不得攜出真實報名資料
- 遠端維護採「原則禁止、例外允許」，事前申請、事後關閉
- 定期開會並留會議紀錄

後 上線與結案

- 上線前：清除測試帳號與測試資料、確認無後門
- 由學校人員測試驗收後才可上線
- 納入 IS-D-012 資訊資產清冊與 PIMS-D-007 個資檔案清冊
- 結案：廠商歸還資料並刪除留存檔案，簽署確認
- 帳號全數停用，防火牆規則移除

依據：本校 IS-B-011 §6.3、§6.8、§6.9；IS-B-009 存取控制管理程序書；IS-B-010 系統獲取開發與維護程序書。

2-2 另一個藝大特別要注意的：場地出租與展演委外

教育部 114 年資安專章指標 12.2 就是專門在看「出租場域禁用規定及教育訓練宣導」。

✓ 該做

- 場地委外契約 / 出租規定納入禁用大陸廠牌資通訊產品條款
- 廠商自備之攝影、直播、網路設備不得介接校內公務網路
- 提供獨立的訪客網段（與公務網段隔離）
- 活動期間拍攝、錄影涉及個資，先取得肖像與個資同意
- 活動結束確認影像、報名名單的保存期限與刪除方式
- 定期檢視及調整規範與宣導內容，並留下宣導紀錄

X 常見疏漏

- 「只是借場地，不用管資安」
- 廠商直接把設備插在教室 / 展場的網路孔上
- 活動報名表單用廠商的系統收，名單留在廠商手上
- 直播設備是不明廠牌的網路攝影機
- 契約是舊版，從來沒加過資安條款
- 沒有任何宣導紀錄，評核時拿不出佐證

資料來源：教育部 114 年度大專校院資安專章績效項目評核表指標 12.2（A 修訂場地委外契約或禁用規定、B 納入合約條款、C 落實宣導、D 定期檢視調整）。





電子社交工程與 潛在資安風險

Social Engineering & Phishing Awareness

- 1 社交工程攻擊的是「人」，不是電腦
- 2 開信、開附件、點連結，風險各自在哪
- 3 三步驟自保原則：停、看、查

3-1 社交工程攻擊的是「人」，不是電腦

教育部每年都會對各校實施社交工程演練，結果列入資安專章評分

再貴的防火牆，
也擋不住一個願意按下「啟用內容」的使用者。

■ **定義** 社交工程 (Social Engineering) 是利用人的信任、好奇、恐懼與急迫感，誘使你主動交出帳密、開啟檔案或進行匯款。

■ **為什麼有效** 它不需要突破任何技術防線→因為「你」就是那道被授權的門。

■ **學校為什麼是目標** 人多、流動率高、信箱公開、系統多、預算採購頻繁，而且大家習慣彼此信任。

3-1 常見的社交工程的6個類型

釣魚郵件 Phishing

大量發送的假冒郵件，誘騙點擊連結或提供資料

魚叉式釣魚 Spear Phishing

鎖定特定對象，量身打造、更難辨識的精準攻擊

假冒身份 Pretexting

假冒 IT 人員、主管或廠商，編造情境騙取信任

誘餌 Baiting

以免費贈品、熱門檔案為餌，誘使下載惡意程式

電話詐騙 Vishing

透過電話冒充公務機關、銀行人員誘騙操作或匯款

簡訊詐騙 Smishing

假冒物流、繳費通知簡訊，誘導點擊惡意連結

3-1 駭客利用的四個人性弱點

這四個字只要記住，九成的釣魚信都會露出馬腳。

權 權威

- 校長室交辦、主計室急件、資訊處系統通知
- 冒用長官或單位名義，讓你不敢多問

急 急迫

- 24 小時內未處理將停用帳號
- 今天下班前要完成核銷
- 製造時間壓力，讓你來不及思考

奇 好奇

- 您的照片被張貼在...
- 薪資調整名冊
- 這學期考績排名
- 標題正好搔到你想看的那一點

熟 熟悉

- 冒用同事、校友、廠商、學生的名字與口吻
- 甚至直接接在你和廠商的真實信件往來後面回覆

參考：ASRC 2026 年社交工程技術趨勢預測；內政部警政署保安警察第一總隊資安訊息
<https://www.1spc.npa.gov.tw>

3-1 學校最常見的六種釣魚劇本

共通點：都要你「點一下、登入一下、填一下」。

劇本	信件長什麼樣	破綻在哪
信箱容量 / 密碼到期	「您的信箱已滿，請立即登入擴充」附一個登入頁連結	學校不會用外部網域要你輸入校內帳密
公文 / 會議通知	「附件為本週行政會議紀錄，請查收」附 .docm 或 .zip	公文通常走公文系統，不會用個人信箱夾帶巨集檔
薪資 / 考績 / 人事	「114 年度考績名冊」「年終獎金發放明細」	人事資料不會用群發郵件夾帶試算表寄給你
廠商報價 / 請款	接在真實往來信件後回覆，並「更新匯款帳號」	任何帳號變更一律電話回撥原通訊錄號碼確認
雲端檔案分享	「○○○與您共用了一份文件」按鈕導向假登入頁	滑鼠停留看真實網址；用自己的書籤進雲端
QR Code 通知	PDF 或海報內嵌 QR Code，要你用手機掃描登入	手機看不到完整網址，正是攻擊者要的效果

參考：ASRC 2026 社交工程趨勢預測 (Quishing、Reply-chain Attack)；微軟 2026 年第一季資安報告。

3-2 開信、開附件、點連結：風險不一樣

同樣一封信，三個動作的風險差距很大。知道差在哪，才知道該停在哪一步。

STEP 1 開信

- 單純「讀取」純文字信件，風險相對最低
- 但預覽圖片會讓對方知道你的信箱是「活的」
- → 建議關閉自動下載圖片
- → 可疑信件不要回覆、不要按「取消訂閱」

STEP 2 開附件

- 風險中高：附件可直接在你的電腦上執行程式
- 最危險：巨集 (.docm/.xlsm) 、壓縮檔內的 .exe/.scr/.lnk
- 也要小心加密壓縮檔（密碼寫在信裡 = 為了躲過掃毒）
- → 不確定就不要開，先打電話問寄件人

STEP 3 點連結

- 風險最高：假登入頁一秒就拿走你的帳密
- 連結文字和真實網址可以完全不一樣
- 短網址、QR Code 會把真實網址藏起來
- → 永遠用自己的書籤或自行輸入官方網址登入

一句話版本：信可以看，附件要問，連結不要點。

3-2 附件的四種危險型態

請先在檔案總管開啟「顯示副檔名」→ 這是最便宜也最有效的一個設定。

1 啟用巨集的 Office 檔

- .docm、.xlsm、.pptm
- 開啟後出現黃色列「啟用內容」→ 千萬不要按

2 壓縮檔包執行檔

- .zip / .rar 內藏 .exe、.scr、.js、.lnk、.bat
- 檔名常偽裝成「報價單.pdf.exe」

3 加密壓縮檔

- 密碼直接寫在信件內文
- 目的就是讓郵件過濾機制掃不到內容

4 偽裝的捷徑與圖示

- .lnk 捷徑檔、改成 Word/PDF 圖示的執行檔
- 一鍵就下載並執行惡意程式

3-2 連結的四種偽裝

攻擊者的目標只有一個：讓你看不到真正要去哪裡。

偽 相似網域

- tnnua.edu.tw → tnnua-edu.com、
tnnua.edu.tw.xx.cn
- 多一個字、少一個字、換個尾碼

隱 顯示文字 ≠ 真實網址

- 畫面寫「校務系統」，實際連到別處
- → 滑鼠停在連結上，看左下角的真實網址

短 短網址

- bit.ly、reurl.cc 之類會把目的地藏起來
- 公務信件用短網址本身就很可疑

掃 QR Code(Quishing)

- 把惡意連結藏在 PDF、海報、Email 的 QR Code 裡
- 手機掃描通常看不到完整網址
- 2026 年成長最快的釣魚手法之一

參考：ASRC 2026 年社交工程技術趨勢預測；資安署關於 QR Code 詐騙之宣導。

3-3 三步驟自保原則：停、看、查

三個字，三秒鐘，可以擋掉絕大多數的社交工程攻擊。

STEP 1 停

- 要你點連結、填帳號密碼、傳檔案、匯款的訊息，先停三秒
- 越急的信越要慢
- 問自己：我有在等這封信嗎？

STEP 2 看

- 看寄件者「真實位址」，不是看顯示名稱
- 看網址：是不是官方網域？有沒有多字少字？
- 看口氣與錯字：排版怪、稱謂空白、簡體字
- 看附件副檔名與是否要你啟用巨集

STEP 3 查

- 用「另一個管道」確認：打電話、當面問
- 不要回覆原信、不要撥信中的電話
- 帳號密碼一律自己開書籤登入官網
- 還是不確定 → 轉寄給資訊處，不要自己試

校內協助窗口：資訊處 (06) 693-0100 分機 1703、1709 | 寧可多問一句，不要多點一下。

3-3 正確做法 vs. 常見錯誤

演練成績不是重點，重點是：中招的當下，你會不會講出來。

✓ 正確做法

- 滑鼠停在連結上先看真實網址
- 需要登入時，一律自己輸入網址或用書籤
- 任何「變更匯款帳號」一律電話回撥原號碼確認
- 不確定的附件，先打電話問寄件人
- 誤點後立刻斷網、改密碼、通報資訊處
- 把可疑信件「轉寄」給資訊處協助判讀

X 常見錯誤

- 按「取消訂閱」想擺脫垃圾信（等於確認信箱有效）
- 直接回信問「請問你是誰」（等於確認你會回信）
- 用信件裡提供的電話或 LINE 去確認
- 覺得「我只是開了附件，沒輸入密碼，應該沒事」
- 誤點後默默刪信，不敢講
- 把可疑信件用「截圖」貼到 LINE 群組公審

參考：本校 IS-C-001 §6.11「開啟來路不明之電子郵件及其附件時應謹慎小心」、§6.12「當有跡象顯示系統可能中毒時，應儘速通知相關人員」。

3-3 教育部社交工程演練：學校要達到的標準

這不是「參考值」，是教育部資安專章指標 10.2 的加分門檻。

< 10%

惡意郵件開啟率

< 6%

惡意連結（或檔案）點擊率

100%

受誘騙者須有後續加強措施

1 次/年

資安事件通報程序
宣導及應變演練

演練會做什麼 學校會收到模擬的釣魚信，統計各單位開啟率與點擊率，並提報會議。

中了怎麼辦 不會懲處，但會列入受誘騙者名單，須接受後續加強措施（教材、宣導、再測）。

真正的風險 演練信中了只是扣分；真信中了，就是全校個資與系統的實際損失。

資料來源：教育部 114 年度大專校院資安專章績效項目評核表指標 10.2、10.3。

3-3 萬一中招了：四個動作，越快越好

誤點不可恥，不講才危險。資安事件處理最怕的就是「時間差」。

STEP 1 斷

- 立刻拔掉網路線或關閉 Wi-Fi
- 不要關機（關機會破壞跡證）
- 不要自行重灌或掃毒

STEP 2 報

- 電話通知資訊處與直屬主管
- 說明時間、看到的畫面、做過的動作
- 涉及個資同時通知單位個資專責人員

STEP 3 改

- 用「另一台乾淨的電腦」更改密碼
- 校務系統、郵件、雲端全部改
- 有開啟雙因素驗證的一併檢查

STEP 4 追

- 配合清查影響範圍與受影響資料
- 依指示填寫異常事件紀錄表
- 檢視近期寄出的信件是否被冒用

記住：1 小時內通報是法定義務，而這個時鐘從「學校知悉」開始跑。

3-4 近期實例【釣魚郵件 Phishing】

1.先檢查來信網址

看到信
千萬不要直接點
選超連結

日來源: MOMO會員權益 <alert@alerm.zhn-pc-leyu.com> 收信:
標題: momo購物網-雲端發票中獎通知
日期: Wed, 16 Sep 2026 11:47:02

momo
線上購物

發票中獎通知

親愛的會員，您好：

恭喜您！您在 momo購物網消費的電子發票已中獎。

重要提醒
請務必完成「發票歸戶」才能領取獎金。
根據財政部規定，電子發票需完成歸戶手續。
獎金將透過會員帳號所綁定之信用卡進行處理，並依平台相關規範辦理。

發票資訊

發票號碼	PC-66998687
發票類型	雲端電子發票
獎別	五獎 新臺幣 1,000 元

如需查詢相關紀錄：
請透過 [雲端發票官方平台會員中心](#) 登入後查詢。
建議檢視會員基本資料與帳戶設定是否維持最新狀態。
相關資料將依既定程序辦理。

[前往雲端發票平台會員中心](#)

※ 本通知信由系統自動發送，請勿直接回覆。
※ 如有任何疑問，請洽 momo 客服專線：0800-521-988。
※ 領獎相關規定依財政部統一發票給獎辦法辦理。

⚠ 防詐騙提醒：momo 購物網不會以電話或簡訊要求您提供信用卡號、提款卡號或網銀密碼。如收到可疑郵件，請勿點擊連結，請直接至官方網站查詢。如有疑慮，請撥打 165 反詐騙專線確認。

momo
momo購物網 | 會員中心 | 客服中心
富邦媒體科技股份有限公司 Fubon Media Technology Co., Ltd.
Copyright © 2025 momo購物網 All Rights Reserved.

3-4 近期實例【釣魚郵件 Phishing】



財政部
電子發票整合服務平台
E-Invoice Platform



首頁

消息

最新消息

常用功能 +

快速上手 +

影音專區



小心發票中獎詐騙信件

陌生連結勿點擊，個資勿隨便輸入
如有接獲，請立即撥打**165防詐騙專線**



正確

平台電子信箱 einvoice@einvoice.nat.gov.tw

平台官網網址 <https://www.einvoice.nat.gov.tw>

認明政府機關專用網址結尾

2.上網找真實的網址

3-4 近期實例【釣魚郵件 Phishing】

詐騙的網址

https://einvoice-nat.u3i8o.icu/s/653dd63d

財政部
電子發票整合服務平台
E-Invoice Platform

中 EN

手機條碼 自然人憑證 行動自然人憑證

手機號碼

驗證碼(密碼)

圖形驗證碼 5 7 3 7 2

登入

申請手機條碼 >

忘記驗證碼(密碼) >



正確

平台電子信箱 einvoice@einvoice.nat.gov.tw

平台官網網址 <https://www.einvoice.nat.gov.tw>

認明政府機關專用網址結尾

正確的網址

財政部
電子發票整合服務平台
E-Invoice Platform

中 EN

手機條碼 自然人憑證 行動自然人憑證

手機號碼

驗證碼(密碼)

圖形驗證碼 9 0 4 2 2

登入

申請手機條碼 >

忘記驗證碼(密碼) >

3-4 近期實例【釣魚郵件 Phishing】

詐騙信件

親愛的 Momo 會員，您好：

本通知由 Momo 購物網會員服務系統發送，內容為您 114 年 9-12 月期雲端發票對獎結果，請您查收。

中獎發票資訊如下：

- 發票號碼：PC-68569782
- 發票類型：雲端發票
- 獎別：五獎
- 回饋金額：新臺幣 1,000 元

後續處理步驟：

登入發票整合服務平台

輸入信用卡

點確認

遭盜刷 1 萬 6657 元

114 年 1 月~至今

175 人遭詐



參考TVBS新聞：

2026/1/27

雲端發票中獎通知信 竟是假
網站 女慘噴1.6萬

https://www.youtube.com/watch?v=9eBi_dNUzQ8

時間：01:00

恭喜您中獎了！小心！雲端發票假官網詐財





四

新興議題時事與 生成式 AI 使用規範

Emerging Threats & Generative AI Guidelines

- 1 近一年跟我們最切身相關的資安大事
- 2 威脅手法怎麼演變
- 3 生成式 AI 使用規範 (行政院使用生成式 AI 參考指引)

4-1 114 年大事年表（上半年）

114 年對教育體系而言不是「別人的事」→ 醫院、大學、政府採購全部中招。

時間	事件	出處
114/01	海纜事故頻傳：中華電信海纜 1/3 遭貨輪破壞、臺馬二號 1/22 中斷；單月 4 次，超過 113 年全年 3 次	iThome 資安月報 2025 年 1 月
114/01	親俄駭客 NoName057 對台發動第三波 DDoS；台塑、大眾電腦等受攻擊，駭客宣稱目標含主計總處、櫃買中心及 20 多個交通與地方政府網站	iThome 資安月報 2025 年 1 月
114/02	CrazyHunter 勒索軟體攻擊馬偕醫院，逾 600 台電腦感染、急診逾 500 台當機	報導者 / 公視新聞網
114/02 ~ 03	彰化基督教醫院、亞洲大學附屬醫院接連遭駭；馬偕約 1,660 萬筆、彰基約 428 萬筆病患資料遭外洩販售	報導者
114/03	CrazyHunter 攻擊目標從醫院擴大至上市櫃公司	iThome 資安月報 2025 年 3 月
114/03	昇銳電子涉進口中國製監視器貼標 MIT，流入政府機關與企業；董事長 100 萬元交保	公視新聞網 PNN (含新聞影音)
114/04	警方鎖定 CrazyHunter 主嫌為中國浙江 20 歲男子，發布通緝	公視新聞網 PNN (含新聞影音)
114/06	中部某私立大學遭 Nova 勒索軟體攻擊，駭客聲稱取得 10 GB 資料	華碩雲端 2025 資安事件回顧

出處：iThome 資安月報 2025/1 <https://www.ithome.com.tw/news/167154>、2025/3 <https://www.ithome.com.tw/news/168181>；報導者 <https://www.twreporter.org/a/hospitals-sensitive-data-breach>；公視 <https://news.pts.org.tw/article/743238>、/745172

4-1 114 年大事年表（下半年）

下半年兩部母法接連修正，同時企業端資安重訊明顯增加。

時間	事件	出處
114/07	國家資通安全研究院發行「資安週報」試刊號（114/7/7 起每週發布）	國家資通安全研究院
114/08	檢警查出台嫌勾結中國人士，將醫院外洩個資轉賣詐騙集團，2 人移送法辦	公視新聞網 PNN （含新聞影音）
114/08	報導指出駭客攻擊上市櫃公司案件呈倍數成長，台灣資安威脅大增	工商時報 2025/08/18
114/09/24	《資通安全管理法》總統修正公布（108/1/1 施行以來首次大修）	全國法規資料庫
114/11/11	《個人資料保護法》總統修正公布，將設個人資料保護委員會	全國法規資料庫
114/12	單月 8 家上市櫃公司發布資安重大訊息（大樹醫藥、久裕興業科技、台郡、炎洲及炎洲流通、三陽 / 南陽實業、信邦電子、至上電子）	iThome 資安月報 2025 年 12 月
114/12	鴻騰精密遭 INC Ransom 入侵；華碩手機相機部分原始碼因供應商遭駭外流	iThome 資安月報 2025 年 12 月
114 全年	全球登記在案的 CVE 漏洞達 48,448 個（113 年為 40,303 個），平均每天約 132 個漏洞被揭露	iThome / CVEdetails

出處：iThome 資安月報 2025/12 <https://www.ithome.com.tw/news/173137>；工商時報 <https://www.ctee.com.tw/news/20250818700678-430502>；公視 <https://news.pts.org.tw/article/767787>；全國法規資料庫 law.moj.gov.tw

4-1 115 年到目前為止 (1~10 月)

115 年開年就是法規連續修正，加上一件和「帳號權限」直接有關的大型個資裁罰案。

時間	事件	與學校的關聯
115/01/05	「資通安全事件通報應變及演練辦法」修正發布施行（名稱新增「演練」、改為一至四級）	校內 IS-B-012 須配合改版
115/01/07	「資通安全責任等級分級辦法」修正發布施行，附表五新增「資通安全弱點管理」	C 級應辦事項內容變更
115/01/22	個資會籌備處預告個資法施行細則修正草案及三項子法草案（72 小時通報）	個資事故處理將有法定時限
115/02~09	酷澎（Coupang）約 20 萬名台灣用戶個資遭非法讀取；數發部行政檢查查出離職人員權限未刪除、台韓共用備份金鑰、金鑰未定期更換，9/21 裁處公司及代表人各 75 萬元	權限管理與委外控管的教科書級案例
115/08	審計部示警：公務機關採購資通訊產品僅管制最終品牌，未及於關鍵零組件來源與資安驗證	採購規格與驗收要再加嚴
115/10	104人力銀行遭駭！「12萬筆」個資恐外洩	網站非法入侵

出處：數位發展部數位產業署 <https://moda.gov.tw/ADI/news/latest-news/19026>；聯合報 <https://udn.com/news/story/7241/9773666>；聯合報 <https://udn.com/news/story/6656/9665695>；全國法規資料庫。

4-1 近期實例 酷澎個資外洩



參考公視新聞網：

2026/09/09

酷澎個資外洩影響20萬台灣
用戶 消基會籲盡速成立專責
機構

<https://www.youtube.com/watch?v=ZaDDXi8hXCM>

時間：02:02

主管機關行政處分結果出爐。
數發部數位產業署官網資料顯示

(<https://moda.gov.tw/ADI/news/personal-data-and-other-sanctions/e-commerce-industry/1825#qaH20102>)，酷澎台灣因違反《個人資料保護法》第27條第1項規定，依同法第48條第2項及第50條規定，對公司及代表人各裁處新台幣75萬元罰鍰，合計150萬元，並命限期改正。

<https://ec.ltn.com.tw/article/breakingnews/5583334>

4-1 近期實例 104人力銀行遭駭



參考公視新聞網：

2026/10/06

104人力銀行遭駭!「12萬筆」個資恐外洩

<https://www.youtube.com/watch?v=pMZjNkpj1Fg>

時間：01:01



TVBS
NEWS

104人力銀行遭駭!12萬求職者"個資恐外洩

掌握新聞脈動 ▶ 訂閱TVBS NEWS頻道

4-1 官方數據：115 年 1 ~ 9 月公務機關資安事件通報

資料來源為國家資通安全研究院「資安週報」

每期公布之「本週總計接獲○件公務機關與特定非公務機關事件通報」。

660件

第 27 ~ 64 期合計
(115/1/9 ~ 115/9/27)

17.8件/週

週平均通報件數

39件

單週最高
(第 44 期 115/5/4 ~ 5/10)

25.2件/週

對照：114 年 7 ~ 12 月
26 期合計 656 件

每週都在發生 38 期中有 37 期揭露件數，沒有一週是零。資安事件不是偶發，是常態。

件數下降不代表變安全 115 年前三季週均 17.8 件，低於 114 年下半年的 25.2 件，但攻擊手法同步升級。

這還只是「有通報的」 統計只涵蓋公務機關與特定非公務機關的法定通報，未含未通報與民間案件。

統計基礎：國家資通安全研究院「資安週報」第 27 ~ 64 期 (115/1/9 - 115/9/27) 各期「事件通報」段落；另第 1 ~ 26 期 (114/7/7 - 115/1/4) 合計 656 件。網址
https://www.nics.nat.gov.tw/core_business/information_security_information_sharing/cybersecuritynews/

4-1 官方數據：通報類型與外部曝險排名

「異常連線」長期居冠 → 代表大多數事件的起點，是有人用不該有的方式連進來。

非法入侵事件最大宗類型（按週次統計）

異常連線 28 週 (80.0%)

系統遭入侵 3 週

未經授權存取 2 週

植入惡意程式 1 週

資料外洩 1 週

- 說明：115/1~9 共 38 期，其中 35 期有明確敘明「公務機關非法入侵事件中以 ○○ 占多數」，上表為該敘述之週次統計。

A、B 級關鍵基礎設施外部曝險前 5 大風險

元件高風險漏洞 884 項

過時或弱加密協定 732 項

TLS 憑證不受信任 694 項

CSP 設定不當 240 項

未部署 WAF 107 項

- 說明：第 64 期對 93 個 A、B 級 CI 進行 EASM 檢測，前 10 大風險合計 2,795 項，前三項即占 82.6%。

統計基礎：國家資通安全研究院「資安週報」第 27~64 期（左）、第 64 期（115/09/21 - 115/09/27）EASM 檢測結果（右）。原始週報以圖表呈現各類型細部件數，本表為依各期文字敘述所作之週次統計。

4-1 案例一：醫院勒索事件→大學也在名單上

案例 | 2025 年 2~8 月 CrazyHunter 公視新聞網 PNN / 報導者

國內某醫院(3間)遭勒索，病患個資在暗網販售，外洩資料含特種個資

事件經過與規模

- 攻擊者先探測網路、取得網域控制站 (AD) 權限，再把惡意程式偽裝成印表機驅動程式躲過防毒
- 單一院區逾 600 台電腦遭感染；急診室逾 500 台電腦當機，一度無法存取病歷
- OO醫院：約 32.5 GB、1,660 萬筆病患資料被開價 10 萬美元出售
- OO醫院：約 10 GB、428 萬筆資料被公開，含看診、健保申報、人事與手術紀錄
- 病歷、基因、健康檢查屬《個資法》第 6 條「特種個人資料」，保護標準最高
- 114/4 警方鎖定中國浙江 20 歲男子並通緝；114/8 再查出台嫌將外洩個資轉賣詐騙集團

對學校的啟示

- ▶ AD (網域) 一旦失守，全校電腦等一起淪陷→這是最該優先保護的系統
- ▶ 惡意程式會偽裝成驅動程式、系統檔；只靠防毒軟體不夠，需要端點偵測與備份
- ▶ 學校也有「特種個資」：學生輔導紀錄、健康檢查、身心障礙與病假證明
- ▶ 備份要異地、要定期還原測試，否則被加密時一樣救不回來
- ▶ 外洩的資料最終會流入詐騙集團，傷害的是學生、家長與校友

公視新聞網：警方通緝中國籍主嫌 <https://news.pts.org.tw/article/745172>

新聞影音 (YouTube) <https://www.youtube.com/watch?v=J6iw8YrqUgo>

公視新聞網：外洩個資遭轉賣詐騙集團 <https://news.pts.org.tw/article/767787>

新聞影音 (YouTube) <https://www.youtube.com/watch?v=hjZOIJ2X9A0>

報導者：首宗特種資料外洩風暴 <https://www.twreporter.org/a/hospitals-sensitive-data-breach>

4-1 案例一：醫院勒索事件(續)



參考公視新聞網：

2025/04/02

馬偕醫院病患個資遭駭 警方
通緝20歲中國男子

<https://www.youtube.com/watch?v=J6iw8YrqUgo>

時間：02:12



晚間新聞
PTS EVENING NEWS

駭客入侵醫院系統竊個資 不只馬偕受害

4-1 從近一年事件學到的四件事

四件事，剛好對應我們前面講的：教育訓練、權限管理、個資盤點、營運持續演練。

1 入口往往很平凡

- 一封釣魚信、一組弱密碼、一台沒更新的設備
- 不是什麼高深的零時差漏洞

2 橫向移動很快

- 一台中招 → 取得網域權限 → 全院 / 全校
- 權限區隔與最小權限原則是關鍵

3 資料會被二次利用

- 勒索不成就賣資料，買家是詐騙集團
- 外洩的傷害會持續好幾年

4 復原能力決定損失

- 有沒有異地備份、有沒有做過還原測試
- 決定你是停機一天還是停機一個月

4-2 威脅手法怎麼演變？

資料來源：ASRC 2026 年社交工程技術趨勢預測

從「亂槍打鳥」 變成「量身訂做」。

■ **以前** 滿是錯字的簡體字垃圾信、一看就假的中獎通知、同一封信發給十萬人。

■ **現在** AI 生成的通順中文、用你熟悉的在地用語、針對你的職務量身撰寫，還附上像真的公文格式。

■ **更麻煩的是** 攻擊已經多模態化 → 深偽語音、假視訊、偽造的業務文件一起上。

4-2 同樣一招，十年前 vs. 現在

結論：「用肉眼看有沒有錯字」已經不再是有效的判斷方法。

手法	以前	現在
釣魚信	錯字連篇、簡體字、翻譯腔	AI 生成，用詞在地、語氣自然，幾乎看不出破綻
冒充長官	只有文字訊息	深偽（Deepfake）語音留言、甚至視訊會議中的假人臉
夾帶惡意連結	直接貼網址	藏進 QR Code（Quishing）、PDF、雲端分享頁
冒用廠商	另開一封新信	入侵廠商信箱，接在真實信件串後回覆（Reply-chain Attack）
誘導安裝	叫你下載 .exe	偽裝成合法 App 的 PWA、惡意瀏覽器擴充功能
目標	廣撒亂槍打鳥	鎖定特定單位、特定承辦人（魚叉式攻擊）

資料來源：ASRC 對於 2026 年社交工程技術趨勢預測（內政部警政署保安警察第一總隊轉知）
<https://www.1spc.npa.gov.tw>

4-2 ASRC 預測 2026 四大趨勢

對照一下：這四項裡有三項，都是「人」被騙，不是機器被攻破。

1 AI 驅動的社交工程

- 生成式 AI 撰寫自然、在地化的釣魚信
- 多模態：深偽語音、影片、擬真的業務文件

2 QR Code 釣魚 (Quishing)

- 惡意連結藏在 QR Code，常嵌在 PDF 或文件中
- 誘導改用手機掃描——手機不顯示完整網址

3 供應鏈與廠商信箱入侵

- 長期監看往來信件，在請款期間插入假帳號
- Reply-chain Attack：接在真實信件串後回覆

4 瀏覽器層面的威脅

- 惡意瀏覽器擴充功能
- 以技術偽裝成合法應用程式，繞過作業系統防護

資料來源：ASRC 對於 2026 年社交工程技術趨勢預測。

4-3 生成式 AI 使用規範

資料來源：行政院及所屬機關（構）使用生成式 AI 參考指引（112.10.03）

AI 可以用，但公務使用有規矩 而且這份規矩學校「要遵守」。

法源 《行政院及所屬機關（構）使用生成式 AI 參考指引》，112/10/3 訂定，共 10 點。

適用我們嗎 第九點明定：公營事業機構、公立學校、行政法人及政府捐助之財團法人「得準用」本參考指引。

核心精神 AI 是輔助工具，不是決策者；而且「公務資訊不能隨便餵給它」。

4-3 行政院生成式 AI 參考指引：十點重點（1~5）

指引要點	條文重點	白話說明
第一點	為提升行政效率，並避免國家安全、資訊安全、人權、隱私、倫理及法律等風險，訂定本指引	不是禁止用 AI，是要你用得安全
第二點	AI 產出之資訊，須由業務承辦人就其風險進行客觀且專業之最終判斷；不得取代承辦人之自主思維、創造力及人際互動	AI 寫的東西，責任還是你的
第三點	製作機密文書應由業務承辦人親自撰寫，禁止使用生成式 AI (機密文書指國家機密文書及一般公務機密文書)	機密公文一律手寫，沒有例外
第四點	不得向生成式 AI 提供涉及公務應保密、個人及未經機關同意公開之資訊，亦不得詢問可能涉及機密業務或個人資料之問題 (封閉式地端部署經確認安全性後，得依機密等級分級使用)	不要把學生名冊、身分證號、未公開的簽呈貼進 AI
第五點	不可完全信任 AI 產出之資訊，亦不得以未經確認之產出內容直接作成行政行為或作為公務決策之唯一依據	AI 會一本正經地胡說八道

資料來源：行政院及所屬機關（構）使用生成式 AI 參考指引第一點至第五點（112.10.03 訂定）。

4-3 行政院生成式 AI 參考指引：十點重點（6～10）

指引要點	條文重點	白話說明
第六點	使用生成式 AI 作為執行業務或提供服務之輔助工具時，應適當揭露	對外的成果要說明有用 AI 協助
第七點	應遵守資通安全、個人資料保護、著作權及相關資訊使用規定，並注意侵害智慧財產權與人格權之可能性；各機關得訂定使用規範或內控管理措施	藝術大學特別注意： AI 生成的圖像、音樂、影片可能涉及著作權與肖像權
第八點	各機關應就所辦採購事項，要求得標之法人、團體或個人注意本參考指引，並遵守機關所訂定之規範或內控管理措施	委外廠商也要一起遵守，要寫進採購文件
第九點	公營事業機構、公立學校、行政法人及政府捐助之財團法人，得準用本參考指引	包含本校
第十點	行政院及所屬機關（構）以外之機關得參照本參考指引，訂定使用生成式 AI 之規範	其他機關可自訂規範

資料來源：行政院及所屬機關（構）使用生成式 AI 參考指引第六點至第十點（112.10.03 訂定）。

4-3 校務情境：可以丟給 AI 的 vs. 絕對不行的

判斷方法很簡單：如果這段內容你不敢貼在學校公布欄上，就不要貼進 AI。

✓ 可以（去識別化後）

- 潤飾一段已公開的活動宣傳文案
- 把公開的會議逐字稿整理成重點摘要（先移除人名）
- 請 AI 解釋一個法規名詞、提供簡報架構建議
- 翻譯公開的招生簡章、展覽介紹
- 產生練習題、課程大綱草稿
- 寫程式片段（不含真實連線字串與帳密）

X 絕對不行

- 貼上學生名冊、身分證號、成績、輔導紀錄
- 貼上尚未公開的簽呈、評審名單、招標文件
- 請 AI 撰寫機密文書或一般公務機密文書
- 貼上系統原始碼中的帳號密碼、API 金鑰、資料庫連線字串
- 貼上校友、捐款人、評審委員的聯絡資料
- 把 AI 產出的內容未經查證就發文、公告或回覆民眾

依據：行政院及所屬機關（構）使用生成式 AI 參考指引第三點、第四點、第五點。

4-3 四個常被問到的問題

這四題是教育訓練時同仁最常舉手問的。答案全部都在指引十點裡面。

Q1 我用的是公司付費版，資料不會外洩吧？

- 指引第四點不分免費或付費，一律不得提供應保密、個人及未公開之公務資訊
- 例外只有「封閉式地端部署」且經確認系統環境安全性後，依機密等級分級使用

Q2 AI 幫我畫的展覽海報可以直接用嗎？

- 指引第七點：應注意侵害智慧財產權與人格權之可能性
- 生成素材的授權範圍、是否近似既有作品，使用前要確認
- 對外發布時依第六點適當揭露

Q3 我請廠商用 AI 幫學校做系統，可以嗎？

- 指引第八點：機關應就所辦採購事項，要求得標廠商注意本指引
- → 請把「AI 使用規範」寫進招標文件與契約

Q4 AI 寫的公文如果出錯，誰負責？

- 指引第二點：須由業務承辦人就風險進行客觀且專業之最終判斷
- 第五點：不得以未經確認之產出內容直接作成行政行為
- → 責任在承辦人，不在 AI

結語：今天請帶回去的三件事

國立臺南藝術大學 資通安全暨個人資料保護教育訓練

資安不是把事情做到完美， 是把風險控制在可以承受的範圍。

- ① **慢一秒** 要你點連結、填帳號密碼、傳檔案、匯款的訊息，一律先停、再看、最後查。寧可多問一句，不要多點一下。
- ② **看得到** 每年確實完成資訊資產與個資盤點。你盤得出來的，才守得住；盤不出來的，出事也查不到。
- ③ **講出來** 出事第一時間通報，不要自己處理、不要自己刪。1 小時的法定時鐘，從「學校知悉」那一刻開始跑。
→做不到 100 分沒關係，但不要成為那個破口。

校內窗口與平台速查

把這一頁拍下來，比記住任何一條法條都有用。

需要做什麼	去哪裡	備註
查資安 / 個資四階文件	本校資通安全暨個資保護專區 https://its.tnnua.edu.tw/	ISMS/PIMS 四階文件、文件修訂公告
通報資安事件	電話通知資訊處：(06) 693-0100 分機 1703、1709	先打電話，不要只傳 Email
設備故障報修	校園行政系統 - 電腦報修 http://203.71.53.11/FIX/	一般故障走報修，不走資安通報
個資事故	通知單位個人資料保護專責人員（聯絡窗口）	填 PIMS-D-025 個人資料侵害事故通報與紀錄表
查學校隱私權政策	https://www.tnnua.edu.tw/p/412-1000-1767.php	含個資保護聯絡窗口
教育機構資安通報	https://info.cert.tanet.edu.tw	由資安處理組執行，1 小時內完成

參考資料與出處 (1 / 2) 法規

所有數據與條文均標註出處；法規具時效性，實務運用時請再查證官方最新版本。

資通安全 (全國法規資料庫 law.moj.gov.tw / 數位發展部 moda.gov.tw)

- 資通安全管理法 (114.09.24 總統修正公布，施行日期由行政院定之)
- 資通安全責任等級分級辦法 (115.01.07 修正發布施行) 及附表一～附表十
- 資通安全事件通報應變及演練辦法 (115.01.05 修正發布施行)
- 資通安全管理法施行細則、資通安全維護計畫實施情形稽核辦法、資通安全情資分享辦法
- 公務機關所屬人員辦理資通安全事項作業辦法、危害國家資通安全產品審查辦法、國家資通安全會報設置辦法
- 各機關對危害國家資通安全產品限制使用原則 (行政院國家資通安全會報)
- 資通系統籌獲各階段資安強化措施、政府資訊作業委外安全參考指引、政府網站服務管理規範

個人資料保護

- 個人資料保護法 (114.11.11 總統修正公布，施行日期由行政院定之)
- 個人資料保護委員會籌備處 115.01.22 預告施行細則修正草案及三項子法草案 (預告期 60 日)

生成式 AI

- 行政院及所屬機關 (構) 使用生成式 AI 參考指引 (112.10.03 訂定，共 10 點)

參考資料與出處 (2 / 2) 機關文件、新聞與研究

機關文件與規範

- 教育部 114 年度大專校院資安專章績效項目評核表 (v2.6)
- 教育體系資通安全暨個人資料管理規範 (109 年 8 月修正)
- 本校四階文件：IS-A-002、IS-B-003、IS-B-006、IS-B-009、IS-B-010、IS-B-011、IS-B-012、IS-C-001；PIMS-B-003、PIMS-B-010、PIMS-C-002、PIMS-D-024

新聞與研究報告 (含影音)

- 公視新聞網 PNN：昇銳電子涉進口中國監視器貼標 MIT news.pts.org.tw/article/743238
 - 影音：<https://www.youtube.com/watch?v=ks7PF2Y-gPo>
- 公視新聞網 PNN：馬偕醫院病患個資遭駭、警方通緝中國籍主嫌 news.pts.org.tw/article/745172
 - 影音：<https://www.youtube.com/watch?v=J6iw8YrqUgo>
- 公視新聞網 PNN：馬偕、彰基遭駭，外洩個資遭轉賣 news.pts.org.tw/article/767787
 - 影音：<https://www.youtube.com/watch?v=hjZOIJ2X9A0>
- 報導者：首宗特種資料外洩風暴 twreporter.org/a/hospitals-sensitive-data-breach
- 聯合報：審計部示警公務機關採購釀資安漏洞 udn.com/news/story/6656/9665695
- ASRC 對於 2026 年社交工程技術趨勢預測 (內政部警政署保安警察第一總隊轉知)
- 華碩雲端：2025 台灣資安重大事件回顧

Q & A

國立臺南藝術大學 資通安全暨個人資料保護教育訓練

謝謝各位的聆聽。 接下來是提問時間。

別忘了簽到 請完成 IS-D-023 教育訓練簽到表，並配合課後成效評估（這是專章評核的佐證）。

有疑問隨時問 資訊處 (06) 693-0100 分機 1703、1709 | 校內資安專區 <http://its.tnnua.edu.tw>

最後一句 資安做得好，沒有人會注意到；資安出了事，所有人都會記得。謝謝大家。



TSC – FB Site



TSC – Blog Site

