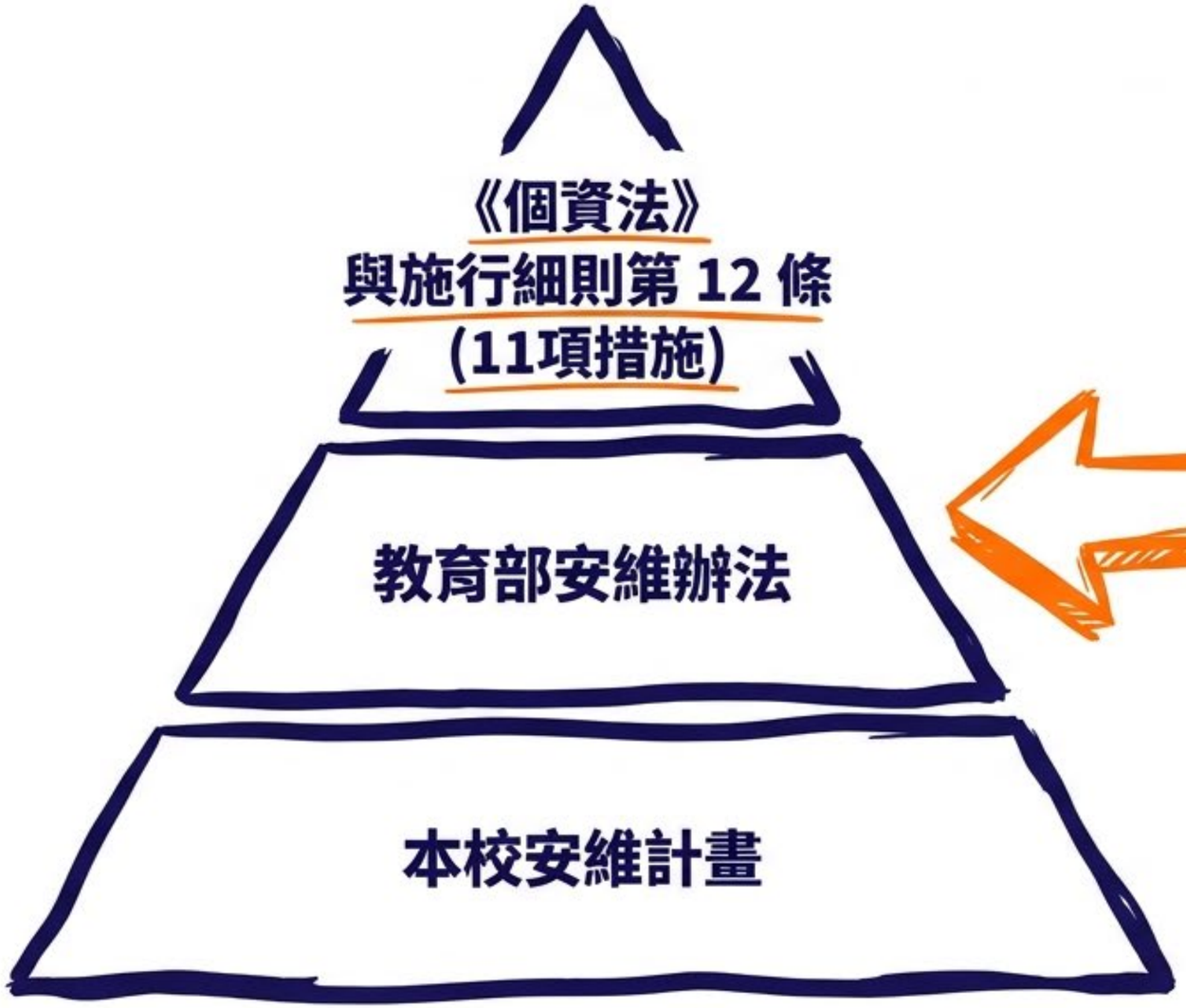
個資安全維護計畫之規劃與建立

教育機構驗證中心 俞怡中 主導稽核員
長榮大學

安全管控不是選項，而是《個資法》賦予管理者的法定避風港



個人資料檔案安全維護計畫架構

- ✓ 總則與計畫導論
- ✓ 組織治理與權責分工
- ✓ 資料盤點與風險評估
- ✓ 個人資料管理 SOP (全生命週期管理)
- ✓ 人員管理與認知宣導
- ✓ 技術控管、實體安全與軌跡留存
- ✓ 事故應變、通報與業務終止處置
- ✓ 持續改善機制

總則與計畫導論

> 計畫應首先明確其建立的目的、法律依據及適用範圍。

目的：落實技術與組織上的安全維護措施，防止個資被竊取、竄改、損毀、　滅失或洩漏。

法律依據：引用《個人資料保護法》第 27 條（或現行第 20-1 條）及其施行細則，以及教育部訂定之各事業各別實施辦法。

適用範圍：界定該計畫適用的業務範疇、地點及對象。

組織治理與權責分工

明確界定內部管理架構，確保個資保護工作「有人負責」。

指定專人或專責組織：設立個資委員會或指定專責人員負責規劃與執行。

配置資源與人力：確保有足夠的預算及設備支撐計畫落實。

管理層監督：專責人員應定期向代表人或管理人提出書面報告。

獨立稽核機制：指定查核人員定期評核計畫成效，且稽核人員與專責人員**不得為同一人**。

資料盤點與風險評估

這是落實保護措施的首要步驟，也是法定義務中的「界定範圍」。

個資盤點（界定範圍）

確認蒐集的特定目的與類別，清查所保有之個資現況並建立盤點清冊。盤點範疇應明確包含備份檔案。

風險評估與管理

分析資料流程中可能產生的風險（如外洩、不當存取），訂定適當的管控措施並呈報管理階層核定。

個人資料管理 SOP（全生命週期管理）

「將法律義務融入日常行政作業流程。」

告知義務執行：規範向當事人蒐集個資時的告知方式（書面、 網站公告等）與內容。

蒐集、處理與利用程序：確保符合「特定目的」且在「**最小必要範圍**」內利用。

特定目的外利用：明定超出原始目的利用時的適法性門檻。

正確性維護與權利行使：建立受理當事人行使查詢、更正、刪除等權利的窗口與作業程序。

委外監督管理：委託他人處理個資時，應簽署包含保護條款之契約並執行適當監督與紀錄。

人員管理與認知宣導

針對「人」的脆弱點加強防護。

保密義務：要求相關人員簽署保密切結書，且離職後仍負保密責任。

教育訓練：定期舉辦教育訓練，提升人員個資保護意識，一般人員建議每年至少接受 3 小時訓練。

技術控管、實體安全與軌跡留存

「採取實質的防護措施以保護資料安全。」

[技術控管措施]

包含帳號權限管理（知其必要原則）、傳輸加密、密碼政策等。

[特種個資加強防護]

針對病歷、醫療等高敏感資料，應增加隱碼機制、弱點掃描及入侵防護。

[軌跡紀錄留存]

留存使用紀錄與系統日誌，建議至至少保存五年，以符合損害賠償時效之舉證要求。

[實體環境管理]

針對存放資料的機房、檔案室採取進出管制及媒介物（如硬碟）保管措施。

事故應變、通報與業務終止處置

針對突發狀況與最後退場機制的規劃。

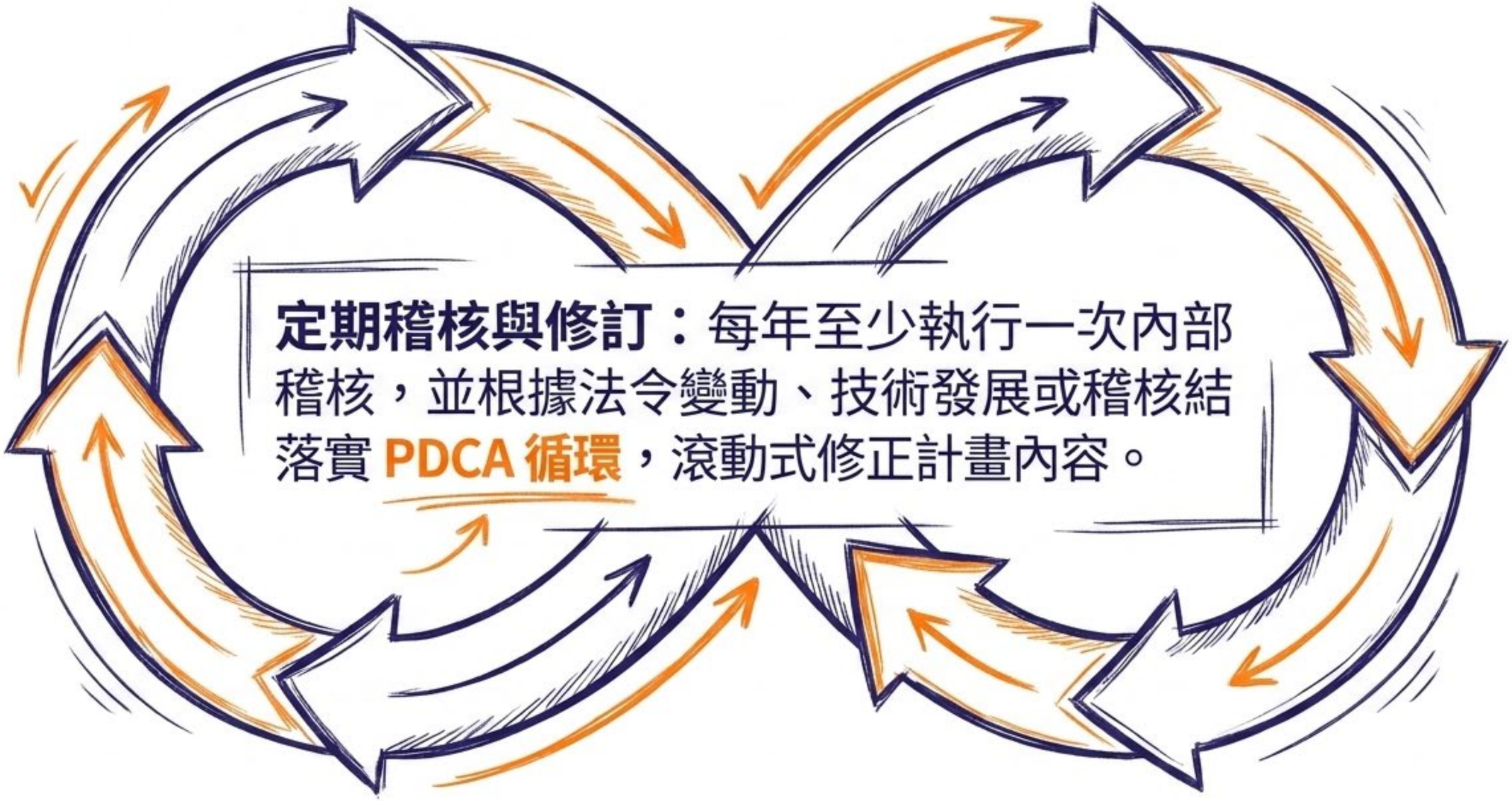
72 小時

事故應變與通報：訂定應變流程（控制損害、查明原因），並規定於知悉事故起 72 小時內通報主管機關。

五年

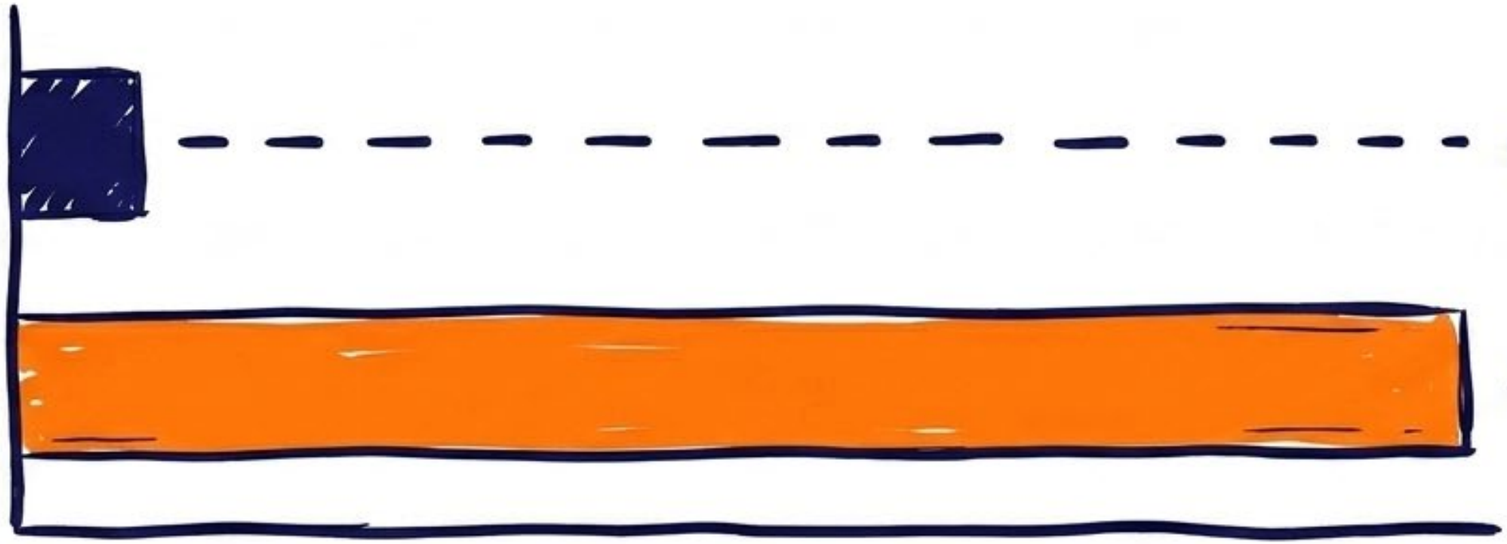
業務終止處置：明確規範單位裁撤或業務結束後，所保有之資料應如何銷毀、移轉或刪除，相關紀錄應留存五年。

持續改善機制



技術控管、實體安全與軌跡留存

第一道門栓：嚴格的密碼政策是防堵非授權存取最高效益的手段



弱密碼：瞬間遭暴力破解

複雜強密碼：需耗時數百年破解

統計顯示，絕大多數的教育機構資安事件與密碼管理不當直接相關！

1. 系統禁止弱密碼並強制定期更新。
2. 強制設定 10 分鐘內啟動螢幕保護並密碼鎖定。

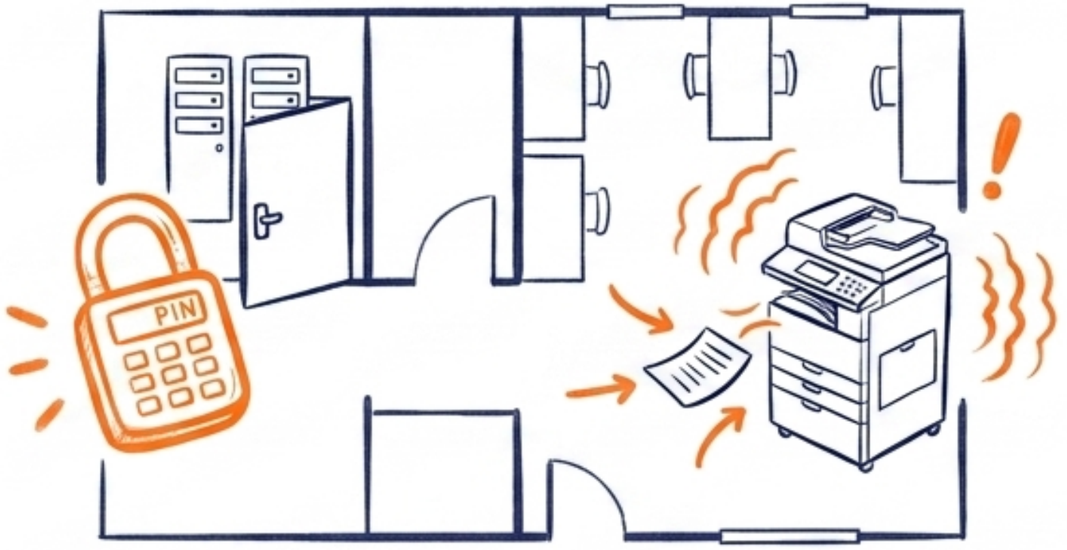
行政便利不應凌駕安全：共用帳號將摧毀身分驗證的不可否認性

便利性絕不能抵銷追責能力

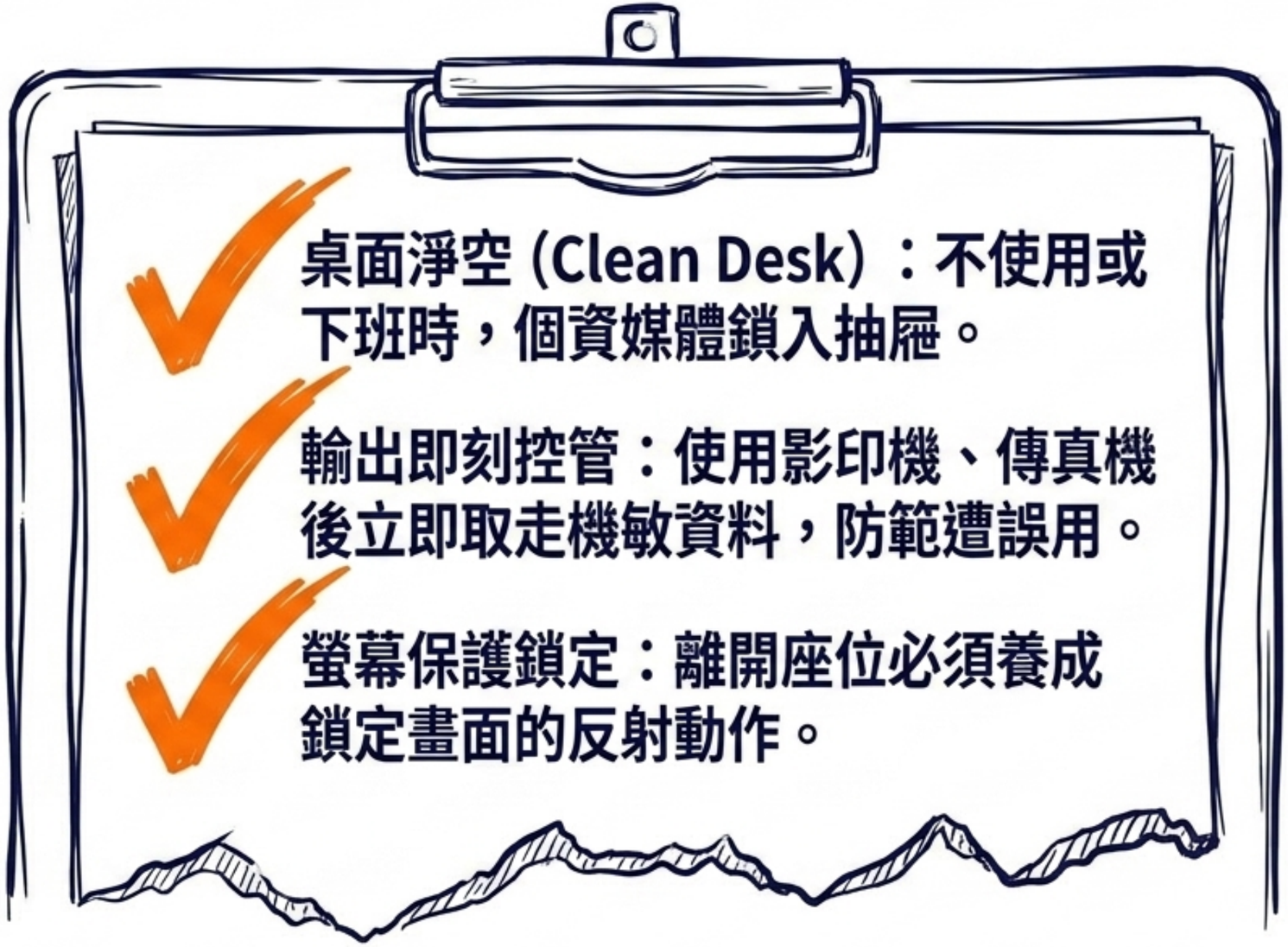
實體安全與資料媒介管理

管控環境進出，防護報廢銷毀程序

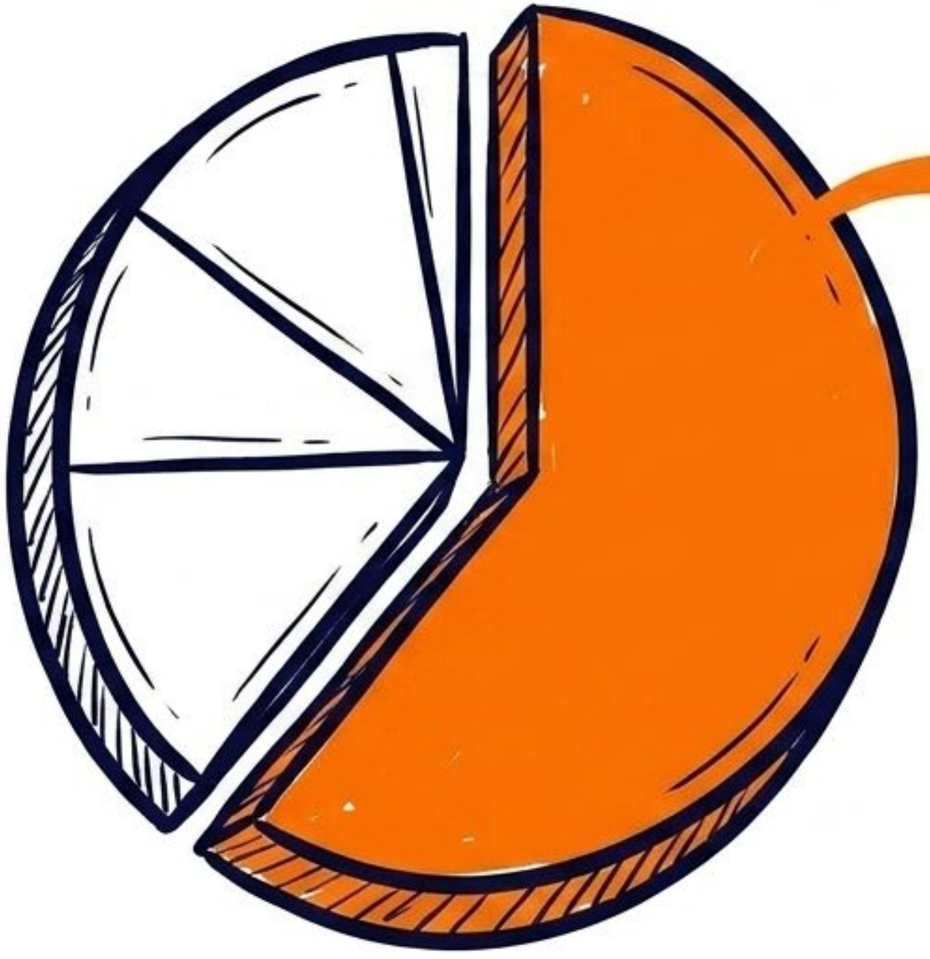
- **環境淨空**：機房建立門禁，公用影印機資料及時取回，無人時妥善上鎖。
- **媒介銷毀技術**：
  - 紙本 ➜ 實體破壞（碎紙）。
  - 硬碟 ➜ 完整資料覆寫或實體破壞。
- **校園真實情境**：老舊筆電轉作公用前，完整覆寫資料並填具紀錄表存檔備查。



人機交界的實體環境，往往是數位防禦中最容易被忽視的脆弱點



落實最小化原則：在資訊揭露與隱私權之間取得精確平衡



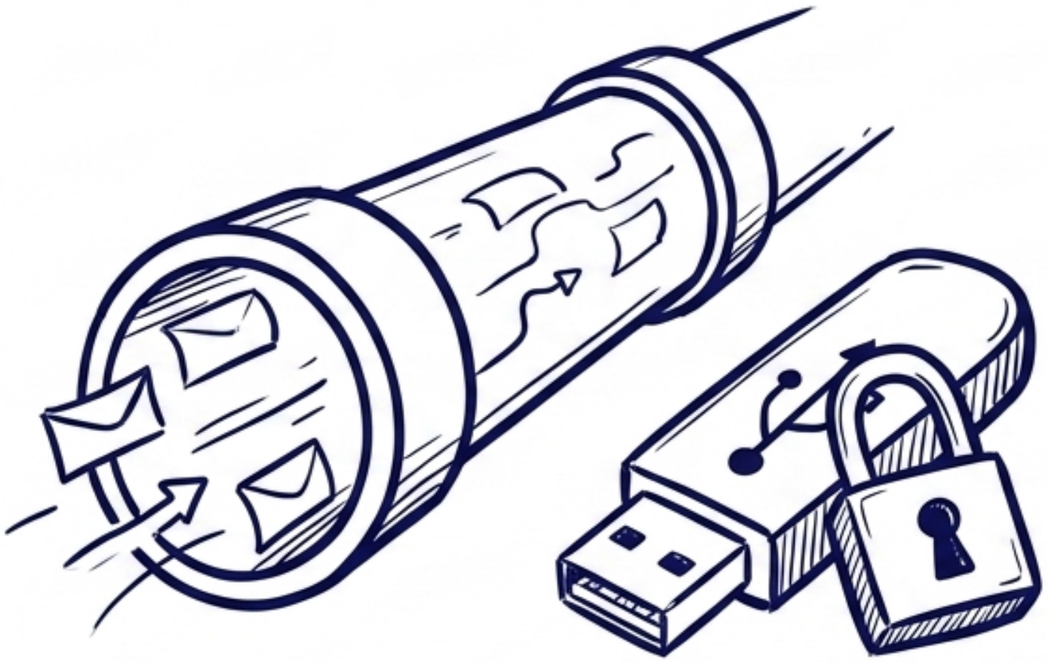
可透過隱碼機制
(Masking) 預防
的過度揭露風險

依據「教育部安維
計畫第 12-1 條」

姓名與身分證號打
上馬賽克塗鴉
(例：陳○明)

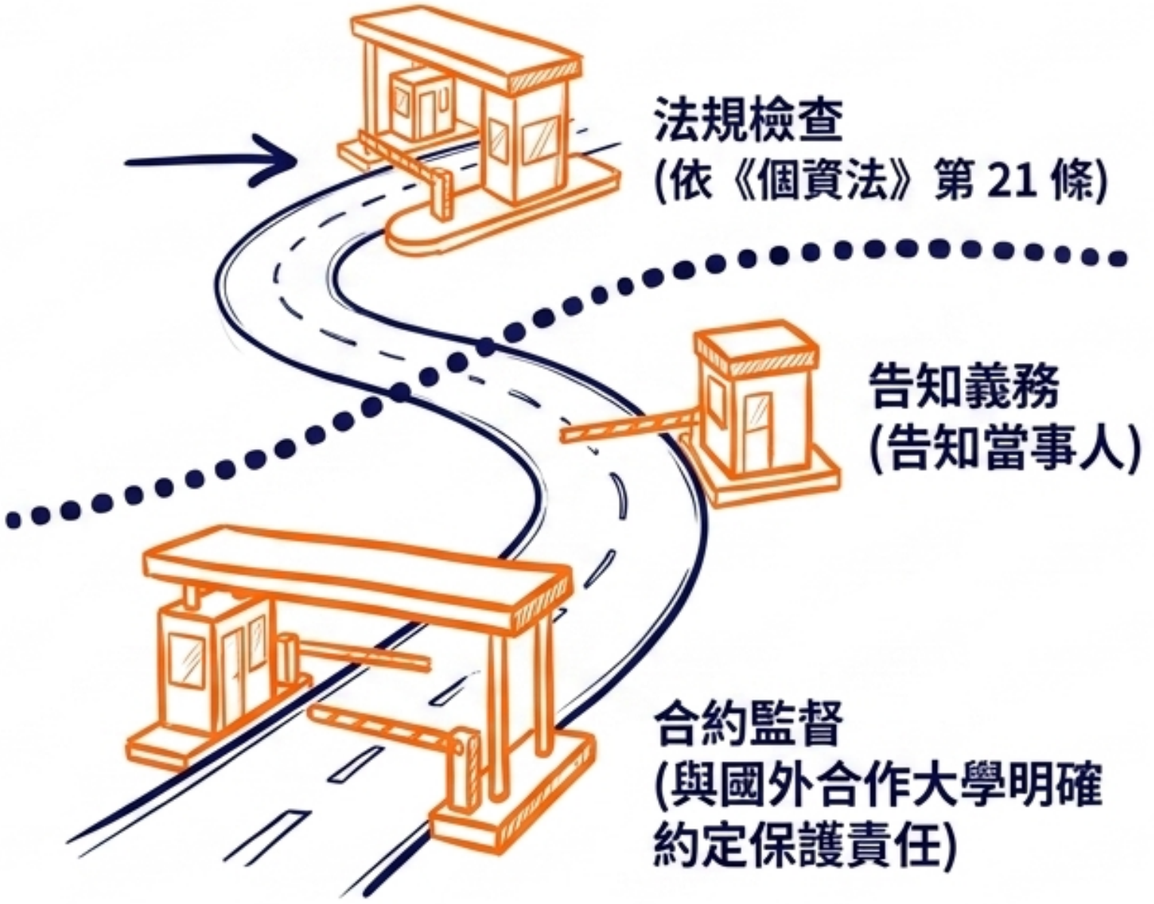
確保數據在安全管道內流動，跨越國界更須承擔保護義務

國內傳輸 - 安全管線 (SSL/TLS)



- 外部交付前必須確認合法性並加上密碼保護
- 明文傳輸是敏感研究數據遭截取的主因

國際傳輸 - 3 步檢查哨



法規檢查
(依《個資法》第 21 條)

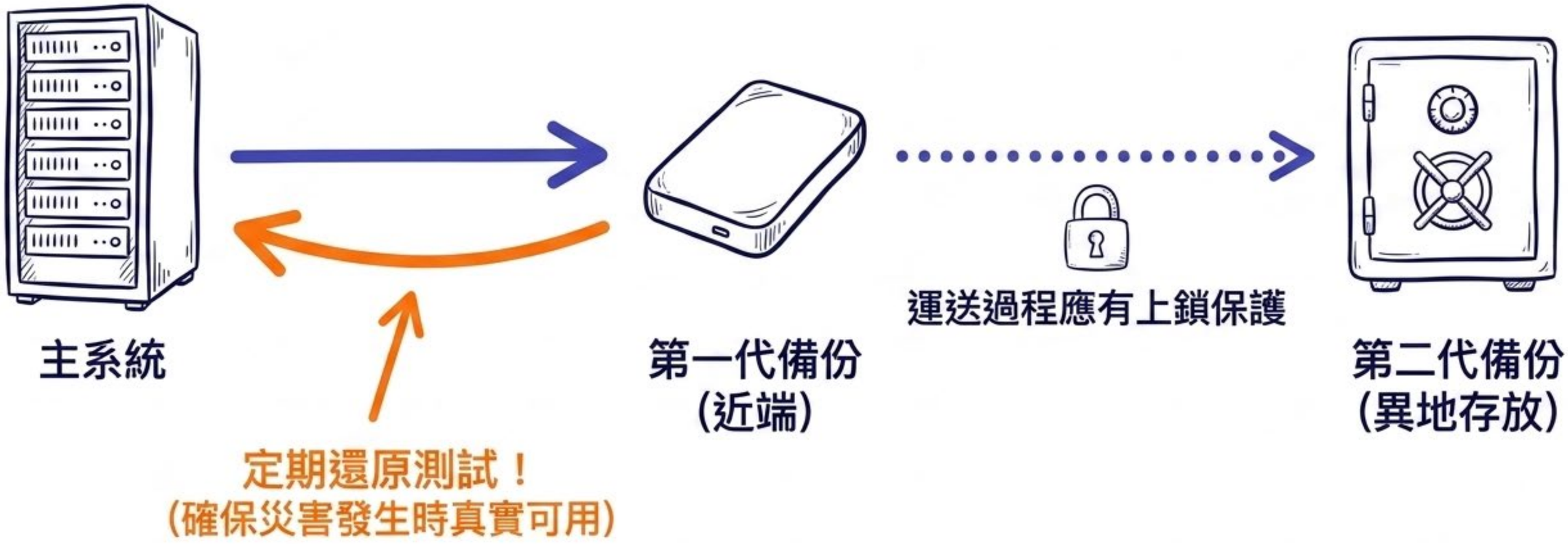
告知義務
(告知當事人)

合約監督
(與國外合作大學明確約定保護責任)

個人行動設備 (BYOD) 模糊了安全邊界，公私資料必須嚴格隔離

離職交接鐵律：離職、調職人員應立即取消識別碼，並徹底交接/刪除私人設備內的公務資料，否則構成嚴重管理違規。

備份不只是複製，更是為校園重要資產買一份可驗證的「數位保險」



事故應變、通報與

個資侵害事故發生時，校方具備「即時應變」與「法定時限通報」的雙重法律責任。

起點

- 事故發生 → 內部發現
- 啟動雙重責任機制

法規紅線

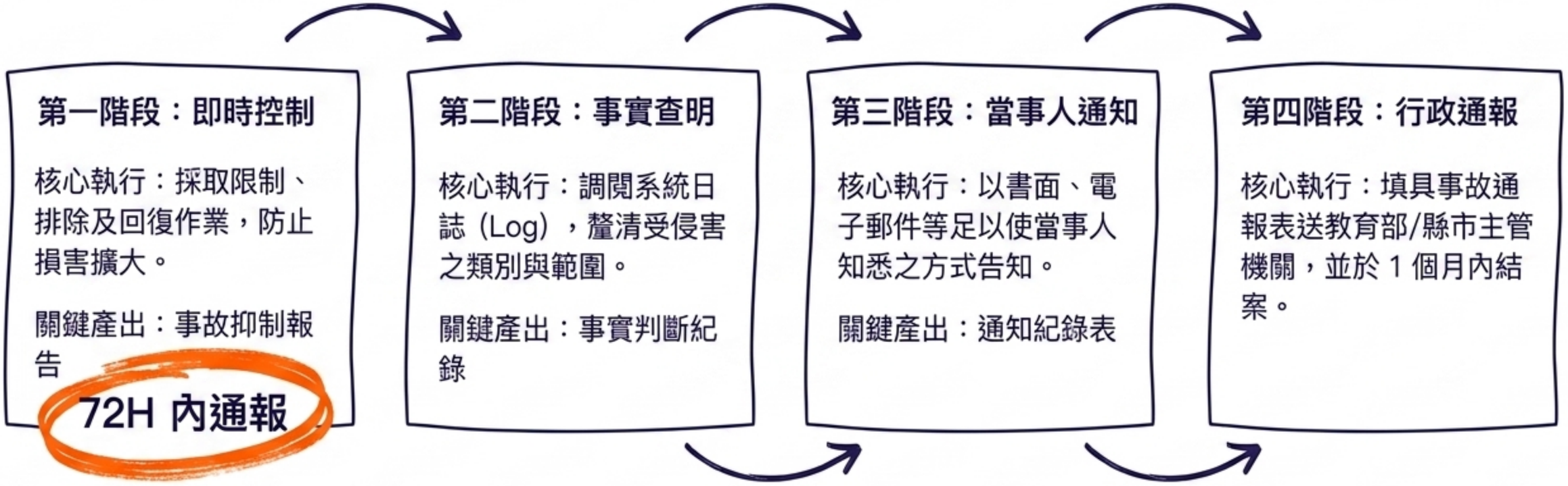
- 法律根基：《個資法》第 12 條
- 知悉個資被竊取、洩漏等侵害時，應通知當事人。

終點目標

- 免責條件：《個資法》第 50 條
- 唯有證明已盡防止義務者（建立應變機制），代表人才可免於同額罰鍰處分。

黃金期限：72 小時內通報

將法律義務落地為可操作的「應變四部曲」，確保校園在危機中不亂章法。



明確的「應變工作小組」分工，是確保行政通報不逾時的制度保障。

通知當事人的重點在於「誠實告知」與「有效保護」，而非隱瞞事實。

個資被侵害之事實

校方已採行之應變措施

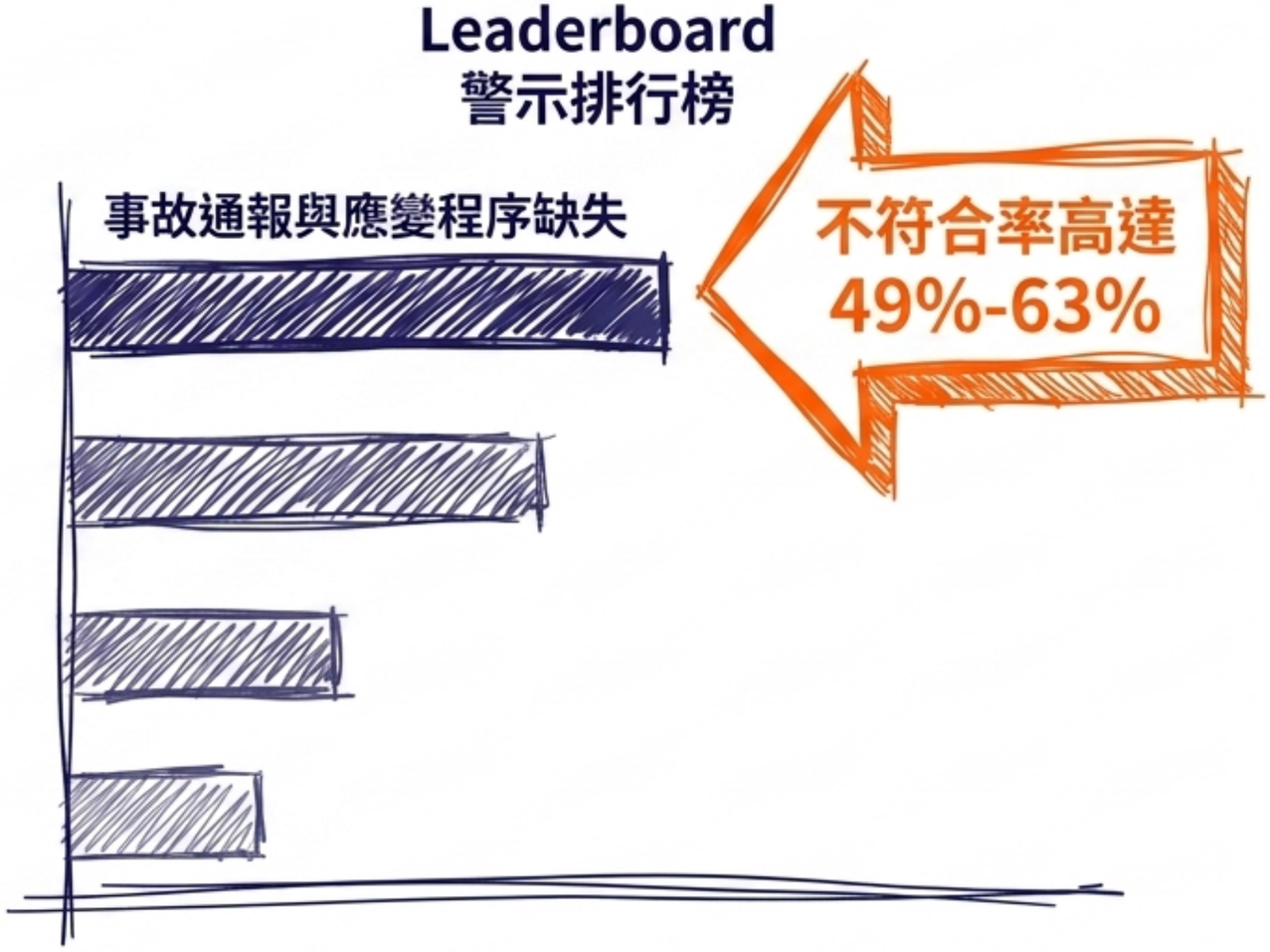
提供諮詢之聯絡窗口與方式

具體作法：通知應採言詞、書面、電話、簡訊、Email 等足以使當事事人知悉之方式。（註：需費過鉅時得採網際網路或公告方式為之）

通報主管機關是行政監督的強制項，逾期通報需附理由說明且將列入重點稽核。

法定要求：知悉起 72 小時內通報，處理結束 1 個月內呈報備查。

高危險情境：
學校在週五下午發現個資外洩，若未能在週一下午前完成通報，主管機關得依《個資法》第 22 至 25 條條發動實地檢查，並加強監督管理。



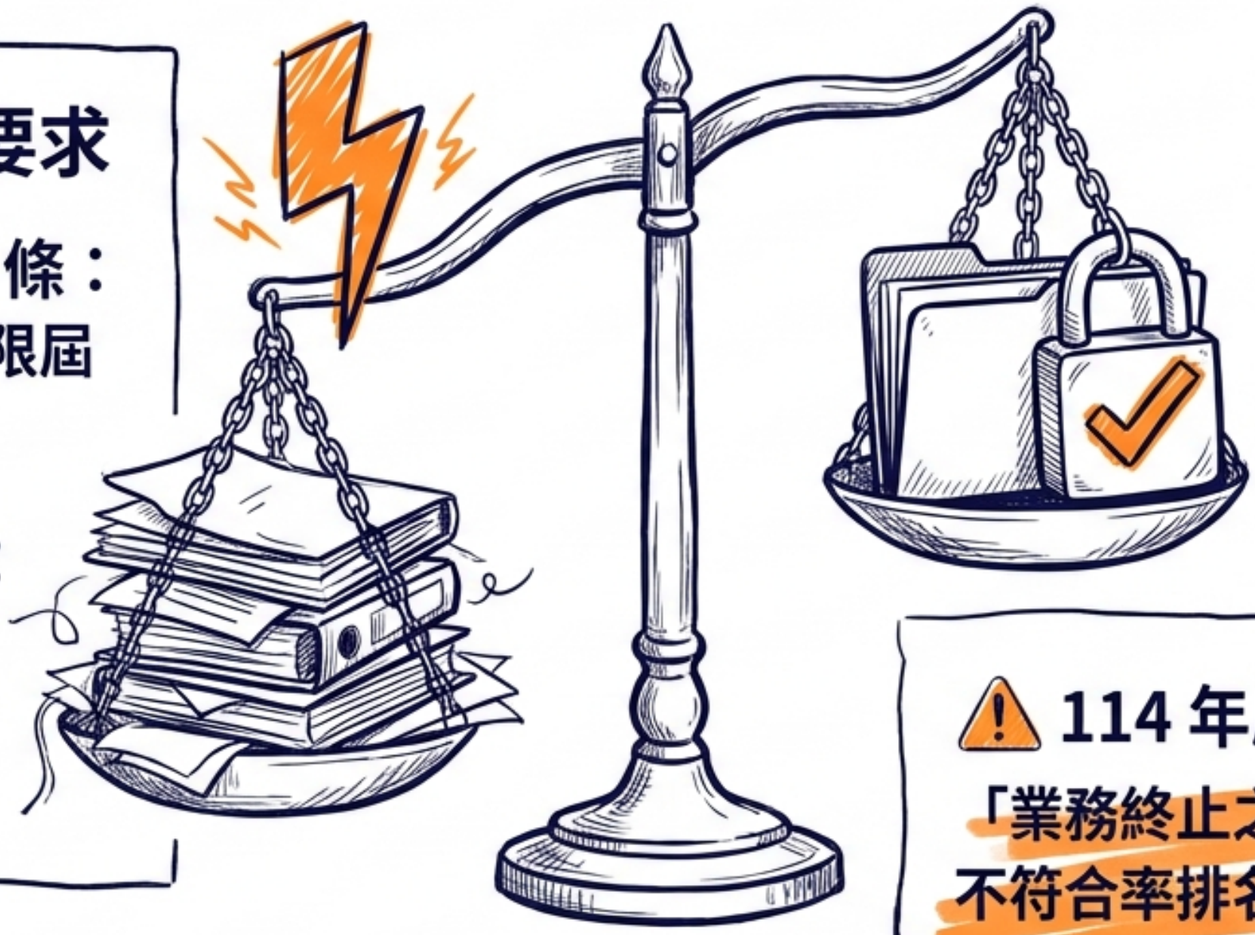
業務終止処置

為什麼「刪除與銷毀」是法定義務？

法律不允許永久保存個資；主動銷毀是管理者的法定責任。

法規與安維要求

- 《個資法》第 11 條：特定目的消失或期限屆滿，應主動刪除。
- 教育部安維計畫：必須包含「業務終止後個人資料處理方法」。

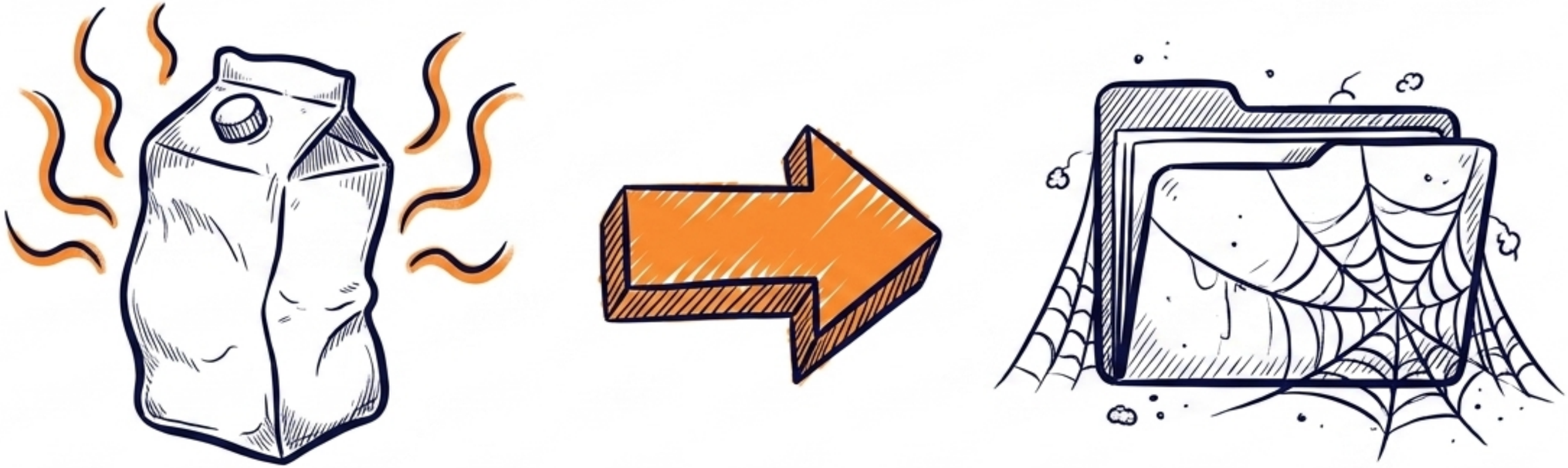


114 年度行政檢查警訊

「業務終止之紀錄留存不足」為不符合率排名前列的缺失項目！

個資檔案就像「冰箱裡的過期鮮奶」

留存越久，不僅無益，更會對組織產生「毒性」風險。



採購鮮奶 vs. 蒐集個資

- 為了飲用（特定目的）：不再需要時，若不清理，會產生異味並讓誤食者生病（外洩風險與賠償）。
- 佔據空間（行政負擔）：無效資料徒增管理成本。

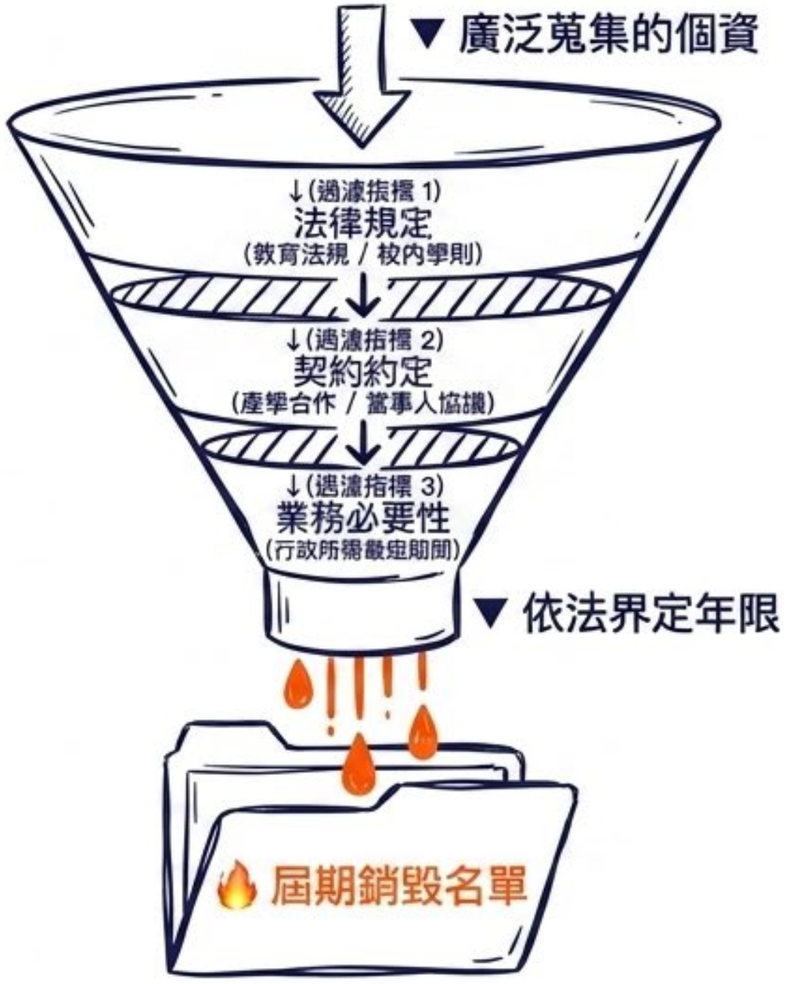
專業大掃除

銷毀作業就是校園數位環境的定期清理，確保只留下「新鮮且必要」的資訊。

年限界定的黃金準則

嚴禁預設無限期保存

保存年限必須對應法律或契約，嚴禁「預設無限期保存」。



銷毀程序 SOP 四部曲

將抽象法律義務轉化為可執行的標準作業程序。