

115學年度新進人員資安宣導 - 資安政策與認知教育訓練

大綱

- 1 本校資訊安全政策
- 2 資訊安全管理制度
- 3 校園資安認知宣導
- 4 高教深根計劃資安專章
- 5 惡意電子郵件社交工程認知與防範

資訊安全政策

為了促使本校資安管理制度(ISMS)能貫徹執行、有效運作、監督管理、持續進行，維護本校重要資訊系統的機密、完整性與可用性，特製訂本校「資訊安全管理政策」。

https://ltuincvideo.ltu.edu.tw/#112_12

資訊服務持續營運目標



落實資訊安全，強化服務品質



加強資安訓練，確保持續營運



做好緊急應變，迅速災害復原

97年開始導入ISO 27001資安標準並通過驗證取得資安證書。本校所有核心資通系統已納入資訊安全管理系統(ISMS)適用範圍並完成ISMS導入，並將分三階段依序導入資訊安全管理系統(ISMS)至全校。

年度	導入單位	數量
112年	112年度ISMS及PIMS已導入單位：「教務處、學務處、人事室」三個一級單位(共15個二級單位)。	15
113年	113年度ISMS及PIMS已導入單位(共36個單位)：「董事會、校長室、總務處(總務長室、營繕組、事務組、保管組、文書組、出納組、環安組、節能中心)、綜合規劃處(處長室、校務發展中心、品質管理暨評鑑中心、媒體設計中心、公關事務暨新聞中心、專案計畫管制中心)、產學合作處(處長室、職能暨就業輔導中心、實習暨證照培訓中心、產學合作發展中心、創新育成暨專利技轉中心、文化創意產業研發中心)、學生發展處(處長室、原住民族學生資源中心)、國際事務處(處長室、境外生服務中心、東協與南亞國家研究中心)、進修部(主任室、教務組、學生事務組、總務組)、圖書館、推廣教育部、南湖社區大學、秘書室、會計室」。	36
114年	114年度 ISMS 及 PIMS 擴大導入單位(共41個單位)：校務稽核室、淨零永續產學研中心、大學儲備軍官訓練團專案辦公室、國際與兩岸交流組、國際專修部、林副校長室、王副校長室、楊副校長室、智慧科技學院院長室、資訊管理系、資訊科技系、智慧製造科技系、資訊專業實習暨證照培訓中心、設計學院院長室、視覺傳達設計系、數位媒體設計系、創意產品設計系、設計專業實習暨證照培訓中心、藝術中心、時尚學院院長室、流行設計系、服飾設計系、時尚經營系、時尚專業實習暨證照培訓中心、商管學院院長室、企業管理系、行銷與流通管理系、國際企業系、財務金融系、會計資訊系、錢幣博物館、商管專業實習暨培訓中心、民生學院院長室、觀光與休閒管理系、應用外語系、幼兒保育系、民生專業實習暨證照培訓中心、通識教育中心、語言中心、動漫遊戲美術應用學士學位學程籌備處、企業管理系高階經營管理碩士在職專班(EMBA)」。	41

四階文件網路位址

因應「教育體系資通安全管理規範」，
制訂本校資訊安全管理制度
(ISO 27001：2022)。



IMS(7)：資安暨個資保護管理程序書



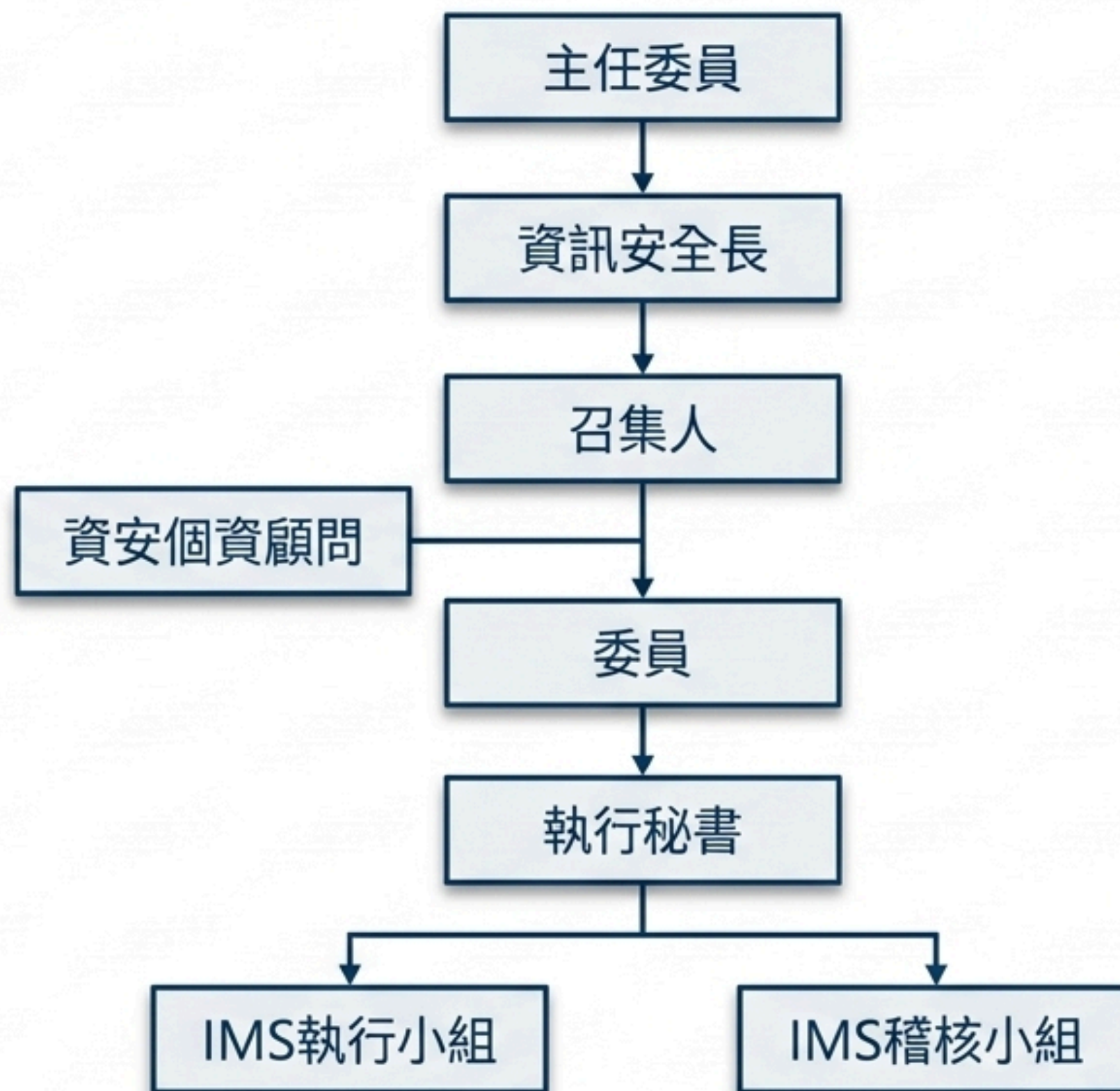
ISMS(20)：資安管理程序書



PIMS(3)：個資保護管理程序書

<https://portal.ltu.edu.tw>

資安暨個資保護委員會組織架構



內部稽核

每學期定期執行內部稽核，確保資訊安全管理制度的各項管制目標、控制措施、運作過程以及各項程序是否皆符合。

成立資安文件管理、資安風險管理、資安稽核、資安事件管理小組及資安窗口，並由本校資訊網路中心負責統籌與推動。

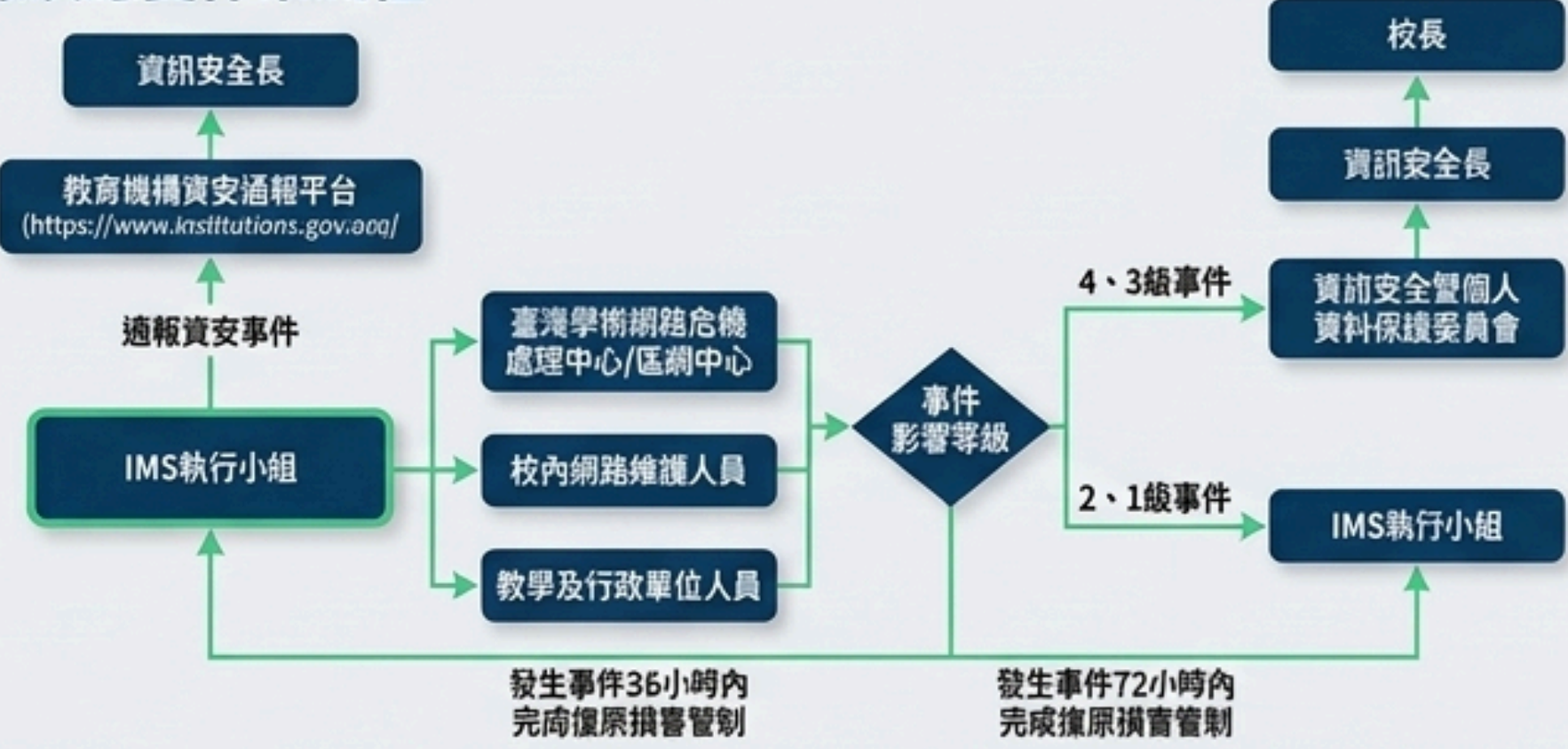
矯正與預防處理流程



資安事件通報程序

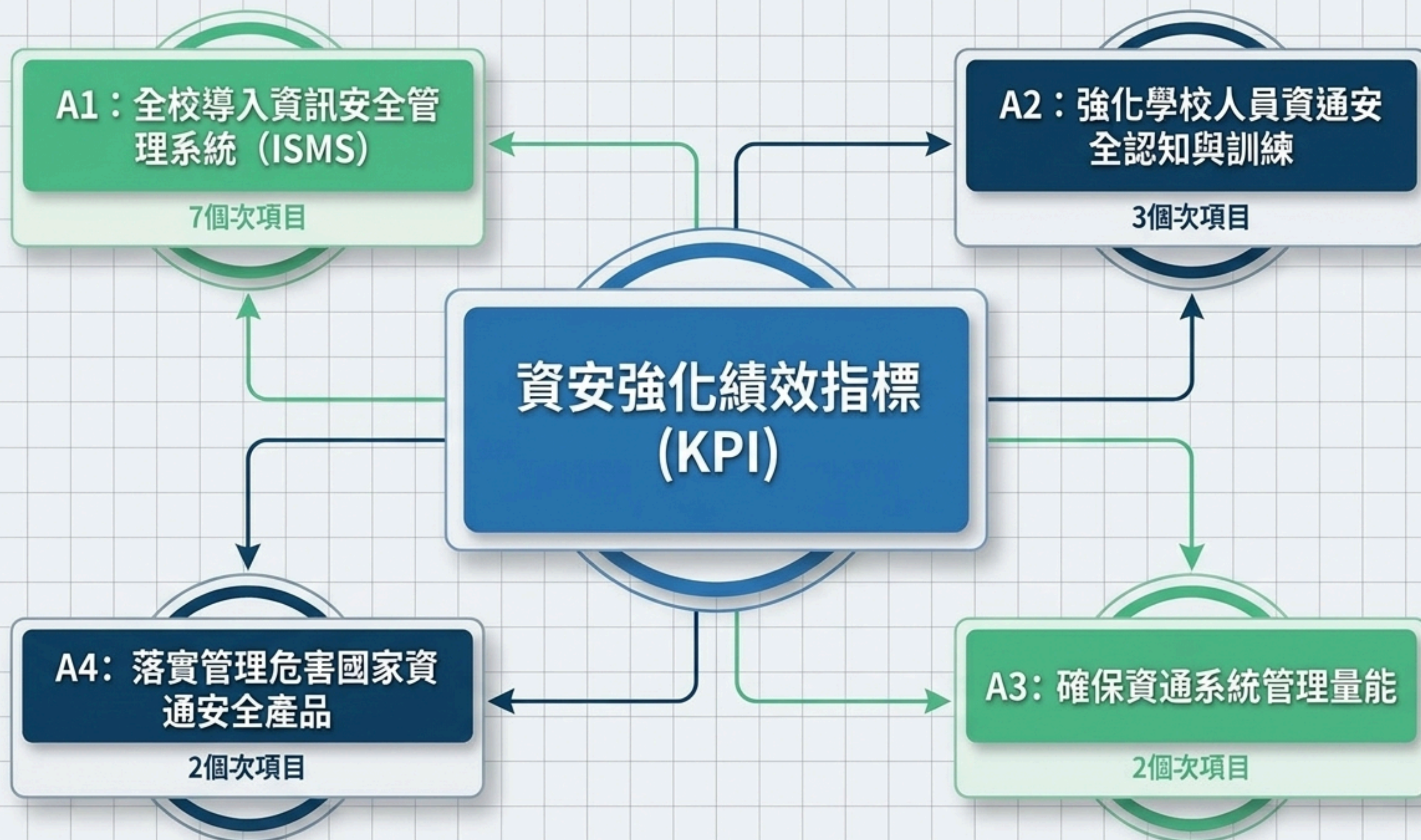


資安事件通報及應變作業流程



資安事件影響等級說明

影響等級		評估類別 - 機密性	評估類別 - 完整性	評估類別 - 可用性
輕微	1級	屬「普通」等級資料遭洩漏	非核心業務系統或資料遭竄改	非核心業務運作遭影響或短暫停頓
	2級	屬「內部使用」等級業務資料遭洩漏	核心業務系統或資料遭輕微竄改	核心業務運作遭影響或系統效率降低，於可容忍中段時間內回復正常運作
嚴重	3級	屬「密」等級資料遭洩漏	核心業務系統或資料遭嚴重竄改	核心業務運作遭影響或系統停頓，無法於可容忍中段時間內回復正常運作
	4級	屬「密」等級資料遭洩漏	本校重要資訊基礎建設系統或資料遭竄改	本校重要資訊基礎建設遭影響或系統停頓，無法於可容忍中段時間內回復正常運作



資訊安全及個人資料保護注意事項 (一) & (二)



資料與設備 (Data & Devices)

防毒軟體病毒碼更新
重要資料定期備份 (一份離線保存)
共用電腦勿存機敏資料並裝防毒



密碼規則 (Password Rules)

主機登入密碼強度要求 (英數字、大小寫、符號、非英文單字、至少 8 碼)



數位平台 (Digital Platforms)

單位網站定期檢查上傳內容避免被搜尋引擎索引
數位學習平台上傳文件審慎檢查權限 (避免侵權或個資外洩)



通訊與活動 (Comms & Events)

避免在 Line 群組發佈當事人個資
辦理活動依目的合法蒐集處理個資 (敏感文件、隨身碟謹慎處理)

資訊安全及個人資料保護注意事項 (三), (四) & (五)

委外與採購

系統維護/採購事先
與資網中心聯繫討論

廠商合約需納入資安
與個資規範及責任
歸屬

主機與遠端

架設主機或申請VM
需定期變更密碼提高
複雜度

遠端登入連線需遵守
防火網管制措施

勒索軟體威脅

駭客透過遠端或惡意
程式取得最高權限進
行加密勒索

強調平時定期離線備
份的重要性 (沒有備
份恐影響業務)

電腦本機安全性原則

- ✓ 密碼最小長度：至少8字元
- ✓ 密碼有效期：180天

- ✓ 密碼最小長度：至少8字元
- ✓ 密碼有效期：180天
- ✓ 密碼複雜性：英文、數字、特殊符號
- ✓ 桌面鎖定：10分鐘

電腦安全設定措施

✓ 必需安裝防毒

↻ 定期更新OS與軟體



開啟本機防火牆



設定鐘訊同步(NTP)



不可使用未授權軟體



不可使用未授權無線網路



不可使用未授權無線網路

IoT設備使用注意事項

種類：印表機、監控設備、PLC等.

預設禁止主動對外連線

必需變更預設密碼

建議啟用存取控制

建議啟用存取控制
僅配發私有IP網段.

資通系統集中化管理

採集中化管理於資網中心IDC機房 (專業維運)
建置伺服器需填防火牆開埠申請，設備集中管理
善用校網頁公用平台，避免自行架站

遠端維護規定

採「**原則禁止、例外允許**」
遠端桌面(RDP)、SSH、VNC開埠申請必須
限制存取來源IP.

落實管理危害國家資通安全產品

禁止公務及限制出租場域使用大陸廠牌資通訊產品 (具連網功能設備)

**杭州海康威視 (Hikvision)、華為 (Huawei)、深圳大疆創新
科技公司 (DJI)、普聯技術公司 (TP-Link)、廣東歐加控股公
司 (OPPO)、小米集團 (MI)、浙江大華技術公司 (Dahua)**

資通安全教育訓練時數要求

資通安全專責人員

- ➡ 每人每年至少接受 12 小時以上之資通安全專業課程或職能訓練。

資通安全專責人員以外之資訊人員

- ➡ 每人每二年至少接受 3 小時專業/職能訓練，且「每年」接受 3 小時以上通識教育訓練。

一般使用者及主管

- ➡ 每人每年接受 3 小時以上之資通安全通識教育訓練。

Drill Mechanics & Rules

測試對象：

校長、副校長、主管及一般行政人員
(每人 10 封測試信)。

不植入後門、不讀取資料、不影響公務。

寄件人名稱均為偽造，測試辨識能力
(提示：善用滑鼠游標顯示連結內容)。

演練失敗人員須接受資訊安全講習。

Targets & Execution

教育部年度防制目標

開啟率

< 10%

點閱率

< 6%

時程：

- 第1次集中演練 (4月~7月) /
第2次集中演練 (8月~11月)。

偽冒類型：

- 公務/個人/公司名義；政治/公務/健康/旅遊主題。

觸發條件：

- 點擊連結、開啟附檔、或「自動預覽功能」開啟。

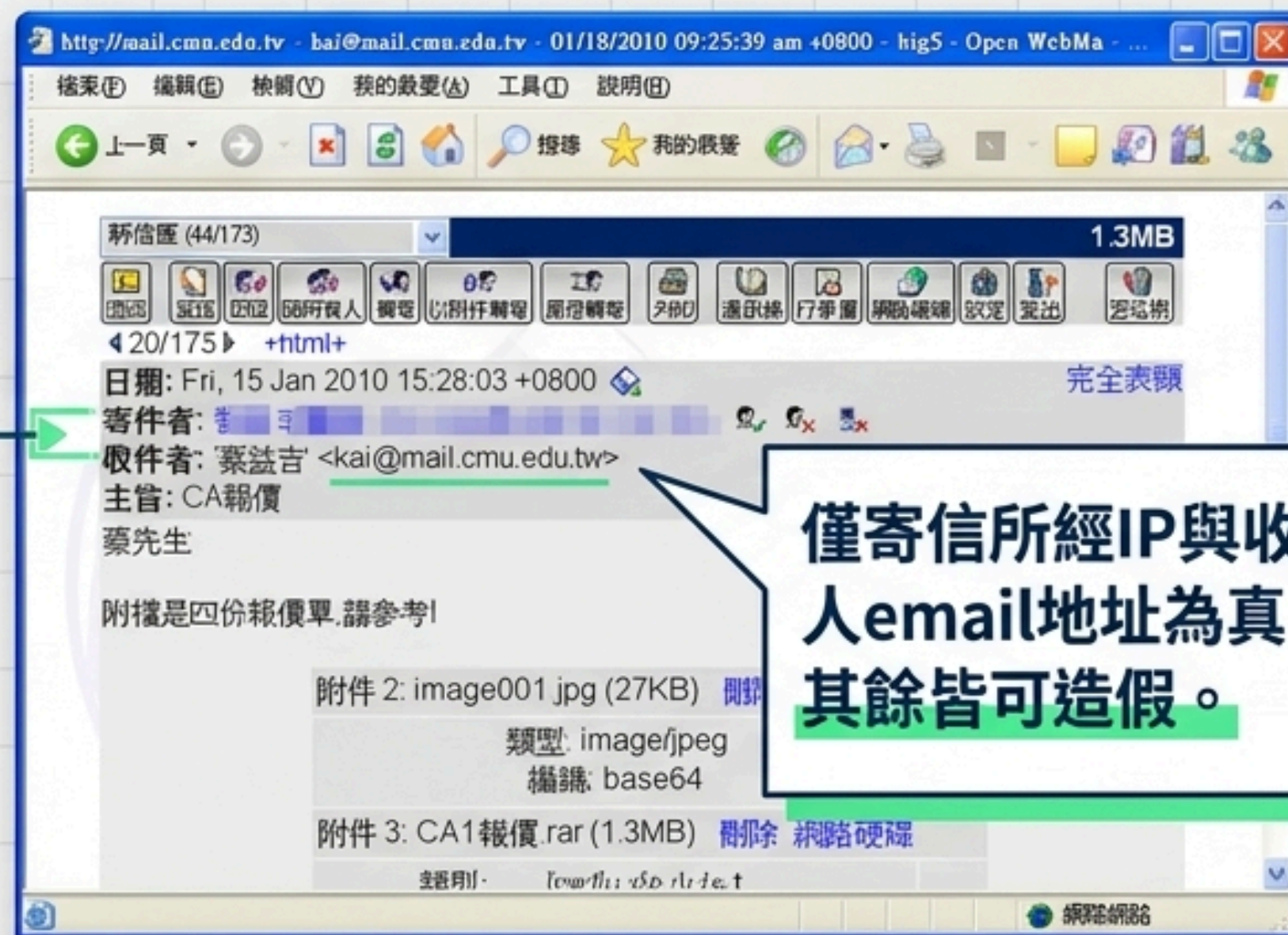
識別威脅：一封電子郵件僅有二處為「真」

Physical Metaphor: Visual Trickery



你能相信這封信嗎？

Digital Technical Example



僅寄信所經IP與收件人email地址為真，其餘皆可造假。

**不點擊：不隨意點擊夾帶網址
(先移動滑鼠檢查來源)**

113年演練信件主旨

真實的惡意電子郵件



關閉郵件預覽功能

環境設定



回信時加入原信:	☒ 加入 ☐ 不加入
保存寄出的信件至寄件備份中:	☒ 儲存 ☐ 不儲存
離開系統時清空垃圾筒:	☒ 清空 ☐ 不清空
離開系統時清空廣告信件匣:	☐ 清空 ☒ 不清空
展開資料夾:	☒ 展開 ☐ 不展開
設定字型大小:	☐ 較小的 ☒ 預設值 ☐ 較大的 ☐ 最大的
撰寫信件時是否另開視窗:	☒ 使用 ☐ 不使用
聯給人快捷功能:	☒ 啟用 ☐ 隱藏
信件預覽功能:	☐ 啟用 ☒ 隱藏
預覽視窗位置:	☒ 下方 ☐ 右方
設定寄件者名稱:	林楷哲
設定底圖:	不使用 ▾
延遲傳送郵件分鐘數:	0
每頁信件數:	40 ▾
請系:	繁體中文 ▾
儲存 取消	

本校網路服務應用系統

無線網路網卡註冊系統(MAC認證):

<https://wifi.ltu.edu.tw>

網路位址註冊系統(DHCP):

<http://ipms.ltu.edu.tw>

名稱解析伺服器(DNS):

192.192.100.2 / 192.192.100.18

網路校時伺服器(NTP):

ntp.ltu.edu.tw

防垃圾郵件過濾伺服器(SPAM):

<https://imss.ltu.edu.tw>