離你最近的資安專家

BCCS 漢昕科技

國立臺南大學
115年資通安全及個人資料保護通識教育訓練(含政策宣導)

2026/07/14 (星期二)

主講人：漢昕科技 顧問 王子豪(Sky)

一站式資安防護

AGENDA

1. 本校資安及個資管理政策宣導
2. 資通安全素養
3. 資訊資產盤點說明
4. 個人資料保護認知
5. 個資檔案風險評鑑與衝擊值評估
6. 社交工程防範
7. 保護智慧財產權宣導
8. ODF開放文件應用宣導說明

訓練目的與法規規範

守護校園資訊資產，履行法定防護義務。

- 了解資安與個資保護之重要性。
- 熟悉校內 ISMS 與 PIMS 管理政策。
- 提升日常作業的資安防護意識與應變能力。

依據《資通安全管理法》與《資通安全責任等級分級辦法》，本校一般使用者與主管，每人每年至少須接受 3 小時之一般資通安全教育訓練。

看不見的威脅與真實的代價

看不見問題，並不代表沒有問題。

$19.63 美金
台灣信用卡資料
暗網平均標價

Simulated Web Financial Database

Document Type	Country/Type	Cost on the Dark Web
89. Payment card data	Singapore	$19.73
90. Payment card data	**Taiwan**	**$19.63**
91. Payment card data	Malaysia	$19.43
92. Payment card data	Myanmar	$19.39
93. Payment card data	Oman	$19.31

沒有 100% 絕對安全的系統，防護措施會因時間因素而失能。

便利性與安全性總是相衝突，必須在合理成本下取得最佳平衡。

每位教職員工都是防禦鏈上的關鍵節點，有責任保護業務機密與隱私。

離你最近的資安專家

BCCS 漢昕科技

一站式資安防護

INFORMATION SECURITY & PRIVACY POLICY

本校資安及個資管理政策宣導

資訊安全與個人資料保護管理政策說明

資通安全的基石：CIA 三要素

運用系統化之控制措施（政策、實施、稽核、軟硬體等），確保本校資訊資產受到妥善保護。

[C] 機密性 (Confidentiality)

使資訊不可用或不揭露給未經授權之個人、個體或過程的性質。

(確保只給對的人看)

例如:密封的掛號信

[I] 完整性 (Integrity)

保護資產的準確度 (Accuracy) 和完全性 (Completeness) 的性質。

(確保資料不被竄改)

例如:銀行的匯款單

[A] 可用性 (Availability)

經授權個體因應需求之可存取及可使用的性質。

(確保需要時隨時可用)

例如:家裡的自來水

校內政策概觀：《資通安全管理政策 V7.0》

政策宗旨：「避免因人為疏失、蓄意或自然災害等風險，確保本校資訊資產受到妥善保護，降低風險危害。」

最高指導原則：「所有於本校執行作業之人員、維護廠商、業務往來單位，皆必須確實遵守並配合本政策（ISMS）。」

ISMS 適用範圍 —— 我們的守備半徑

核心系統

本系統涉及之核心業務為「網路應用服務」及「校務資訊系統」。

資訊資產

本校擁有及存放於校內各種資訊資產（紙本/電子）及資料。

實體環境

本校各辦公處所、建築、機房設備及校園網路之設備。

人員與流程

執行作業之人員、委外廠商、系統、手冊、工具與基礎建設。

服務不中斷的承諾：嚴格的可用性目標

網路機房維運

確保核心資通系統網路機房維運服務，
達全年上班時間 96% 以上之可用性。

核心資通系統

本校關鍵業務核心資通系統服務，
達全年上班時間 98% 以上之可用性。

復原時間目標 (RTO)

因資安或異常事件造成服務中斷，每次最長不得超過系統所訂之復原時間目標 (RTO)。

誰來掌舵？—— 最高推動組織架構

召集人：副校長

由副校長親自擔任召集人，展現管理階層對資安之最高重視。

資通安全暨個人資料保護推動委員會

- 負責政策之核定與監督
- 協調資通安全預防工作
- 指導危機處理與應變措施
- 確保 ISMS 實務運作之有效性與安全性

從資安到個資：《個人資料保護管理政策 V2.1》

依據法律規範，建立安全的個資與隱私保護環境，免於竊取、竄改、毀損或洩漏。

全程防護：嚴格保護個資之蒐集、處理、利用、儲存、傳輸與銷毀。

意識提升：透過教育訓練提升同仁對個資保護之安全意識與管理能力。

風險管控：定期進行風險評鑑，降低營運風險。

追求卓越的循環：管理審查與修訂機制

> 資訊安全是一個持續性的工作，防護措施可能會因時間因素而失能，必須透過『管理階層審查』確保 ISMS 的可用性、安全性及有效性。

賦能網路：校內學習與宣導資源 (1/2)

國立臺南大學資通安全宣導網

內容說明：提供 ISMS 規範下載、風險評鑑作業說明、最新資安漏洞通告。

https://isms.nutn.edu.tw/

國立臺南大學個人資料保護宣導網

內容說明：提供 PIMS 政策、個資法條文與相關解釋、個資事件通報流程。

https://pip.nutn.edu.tw/

賦能網路：國家級線上學習資源 (2/2)

國家資通安全研究院 (NICS)

資源內容：資安素養自我評量與委外管理稽核指引。

教育部資訊素養與認知網

資源內容：防範社交工程教學、常見電子郵件詐騙手法 (Top 5) 解析、勒索病毒防範。

經濟部智慧財產局

資源內容：校園影印教科書合理使用界線與智慧財產權保護宣導。

CYBERSECURITY AWARENESS

資通安全素養

提升資通安全意識與防護知能

核心觀念：尋找日常防護的平衡點

沒有 100% 安全的系統

安全設備並非萬能，看不見問題並不代表沒有問題。

集體防禦

資訊安全，人人有責。在網際網路世界中，除了保護自己的系統，也絕不干擾或破壞他人的系統。

便利與安全的取捨

便利性與安全性經常互相衝突，我們必須在日常公務中找到合理的防護平衡點。

人員資通安全守則：核心作業原則

一體適用：本校全體教職員工與委外廠商皆須嚴格遵循資通安全管理規範。

機密保護：妥善保管敏感文件與個人資料，避免未經授權的存取或外洩。

法遵與自律：遵循教育部臺灣學術網路管理規範及相關法律，不從事非法下載或干擾網路運作。

第一道防線：強密碼設定與管理

Password Formula

[8+ 碼] + [Aa 大小寫] + [123 數字] + [@#$ 符號] = 堅不可摧

密碼破解時間表

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	57 minutes	2 hours	4 hours
6	Instantly	46 minutes	2 days	6 days	2 weeks
7	Instantly	20 hours	4 months	1 year	2 years
8	Instantly	3 weeks	15 years	62 years	164 years
9	2 hours	2 years	791 years	3k years	11k years
10	1 day	40 years	41k years	238k years	803k years
11	1 weeks	1k years	2m years	14m years	56m years
12	3 months	27k years	111m years	917m years	3bn years
13	3 years	705k years	5bn years	56bn years	275bn years
14	28 years	18m years	300bn years	3tn years	19tn years
15	284 years	477m years	15tn years	218tn years	1qd years
16	2k years	12bn years	812tn years	13qd years	94qd years
17	28k years	322bn years	42qd years	840qd years	6qn years
18	284k years	8tn years	2qn years	52qn years	463qn years

Time it takes a hacker to brute force your password in 2025

Hardware: 12 x RTX 5090
Password hash: bcrypt (10)

Hive Systems

資料來源： Read more and download at hivesystems.com/password

強密碼檢查清單

- ☑ 長度與複雜度：至少 8 碼（建議 12-16 碼以上）。
- ☑ 定期更換：每 6 個月必須更換一次。

四大禁忌

- ✕ 使用個人資訊（生日、身分證、電話）。
- ✕ 使用連續或重複字元（如 123456, aaaaaa）。
- ✕ 將密碼記錄於明顯處（嚴禁貼在螢幕或寫在白板上）。
- ✕ 與他人共用帳號密碼。

個人電腦使用守則：建構安全的辦公環境

1 隨手鎖定

離開座位務必登出或鎖定 (Win+L)。螢幕保護程式須設定於 15 分鐘內自動啟動，並需密碼解鎖。

2 即時更新

保持 Windows Update 自動更新，修補系統漏洞。

3 防毒防護

必須安裝防毒軟體，並確保病毒碼為最新狀態。

4 機密資料保護

機密文件須加密或上鎖，廢棄文件須確實銷毀，不得回收再利用。

軟體安裝限制：確保工作環境純淨

✓ 允許安裝

- 合法授權之作業系統與辦公軟體。
- 公務、教學或研究必要之工具軟體。

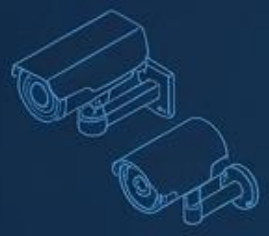
✗ 嚴禁安裝

- 非法下載或破解版軟體（易夾帶木馬或勒索病毒）。
- 與工作無關之娛樂、影音軟體。
- P2P 檔案分享軟體（如 BT，eMule，eDonkey 等）。

原則管制、例外開放：公務若有特殊 P2P 軟體需求，必須填寫申請表，經主管核章並向 圖資處 專案申請後方可使用。

供應鏈安全：禁用大陸廠牌資通訊產品

依國家資安規範，公務環境全面禁止採購及使用大陸廠牌產品（含硬體、軟體及服務）。



影像監控

海康威視 (Hikvision)
大華 (Dahua)
福視寶 (Foscam)

通訊手機

華為 (Huawei)、小米 (MI)
中興 (ZTE)、OPPO
vivo、REALME

網通設備

普聯 (TP-Link)
騰達 (Tenda)
TOTOLINK
水星 (MERCURY)

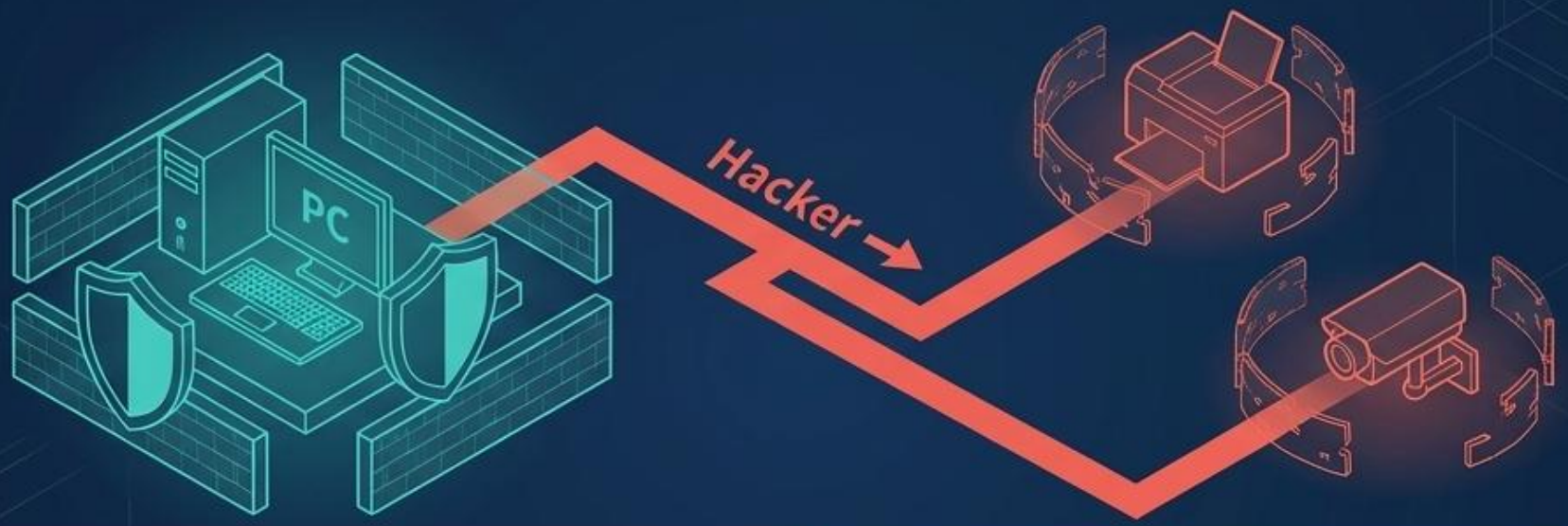
無人機與其他

大疆 (DJI)
海信 (Hisense)

委外規範：學校委外契約或場地租借，必須明訂「不得使用大陸廠牌資通訊產品」，防範廠商貼牌換標。

物聯網 (IoT) 盲區：設備安全管理

聯網設備往往是資安防護的最弱一環。



網路攝影機 (IP Camera)

- 禁止對外開放預設連接埠。
- 必須更改出廠預設密碼。

印表機 / 事務機

- 關閉不必要的網路服務。
- 定期更新韌體。
- 報廢或維修前，須確保清除硬碟中的機密文件留存。

確保所有 IoT 設備納入校園網路管理，隔離於核心網段之外。

實體安全：機房進出與行動設備規範

進出管制

機房為網路心臟，實施嚴格實體存取控制。非授權人員禁止進入；委外廠商須有校內人員陪同並確實填寫進出紀錄。

行動設備嚴格限制

僅限語音通話：於機房內使用智慧型手機，僅允許純語音通話功能。

嚴禁拍照 / 錄影：防止機房配置與設備資訊外洩。

嚴禁網路分享：禁止開啟熱點分享或使用未經授權的網路連線。

新興威脅：生成式 AI 與深偽技術

AI 釣魚攻擊 (AI Phishing)

駭客利用 ChatGPT 等工具，生成毫無文法錯誤、高度客製化的社交工程郵件，降低使用者的戒心。

防護：

絕不點擊未知附件，仔細核對寄件者的「真實網域」。

Deepfake 深偽詐騙

利用 AI 模擬長官或同事的聲音與影像，進行視訊或語音通話，要求緊急匯款或索取機密。

防護：

第二管道查證 (Second Channel Verification)。遇到異常要求，務必掛斷並透過直接回撥分機等實體方式進行身分確認。

離你最近的資安專家

BCCS 漢昕科技

一站式資安防護

營運韌性：對抗勒索病毒的最佳武器 (備份)

黃金 3-2-1 備份原則

3 份備份：保留至少三份資料拷貝 （一份正式工作檔，兩份備份檔）。

2 種媒體：存放於兩種不同的儲存媒體（例如：本機硬碟、外接硬碟、NAS 等）。

1 異地存放：至少一份備份存放在異地或離線環境（防範實體災害與勒索病毒實體災害與勒索病毒同網段感染）。

⚠ **重要或敏感檔案應分開存放，並設定密碼或以加密軟體保護。**

危機處理：資安事件通報與應變

當發現電腦中毒、勒索軟體畫面、或異常網路活動時：

保持冷靜 (Stop)

切勿隨意操作或嘗試自行破解掩蓋。

立即隔離 (Isolate)

迅速拔除實體網路線、關閉 Wi-Fi，防止災情在校園網段擴大。

⚠ *警告：若為勒索軟體，切勿立即關機，以免破壞數位跡證。*

迅速通報 (Report)

第一時間通知單位主管，並通報圖資處(或校內資安專責窗口)進行專業處置。

建構南大資安防護網：由您做起

養成好習慣

養成好習慣

- 落實強密碼、定期更新系統、隨手鎖定螢幕。

嚴守紅線規範

嚴守紅線規範

- 禁用大陸廠牌資通訊產品、絕不安裝非法或 P2P 軟體。

保持高度警覺

保持高度警覺

- 防範 AI 深偽詐騙、落實 3-2-1 資料備份與異常通報。

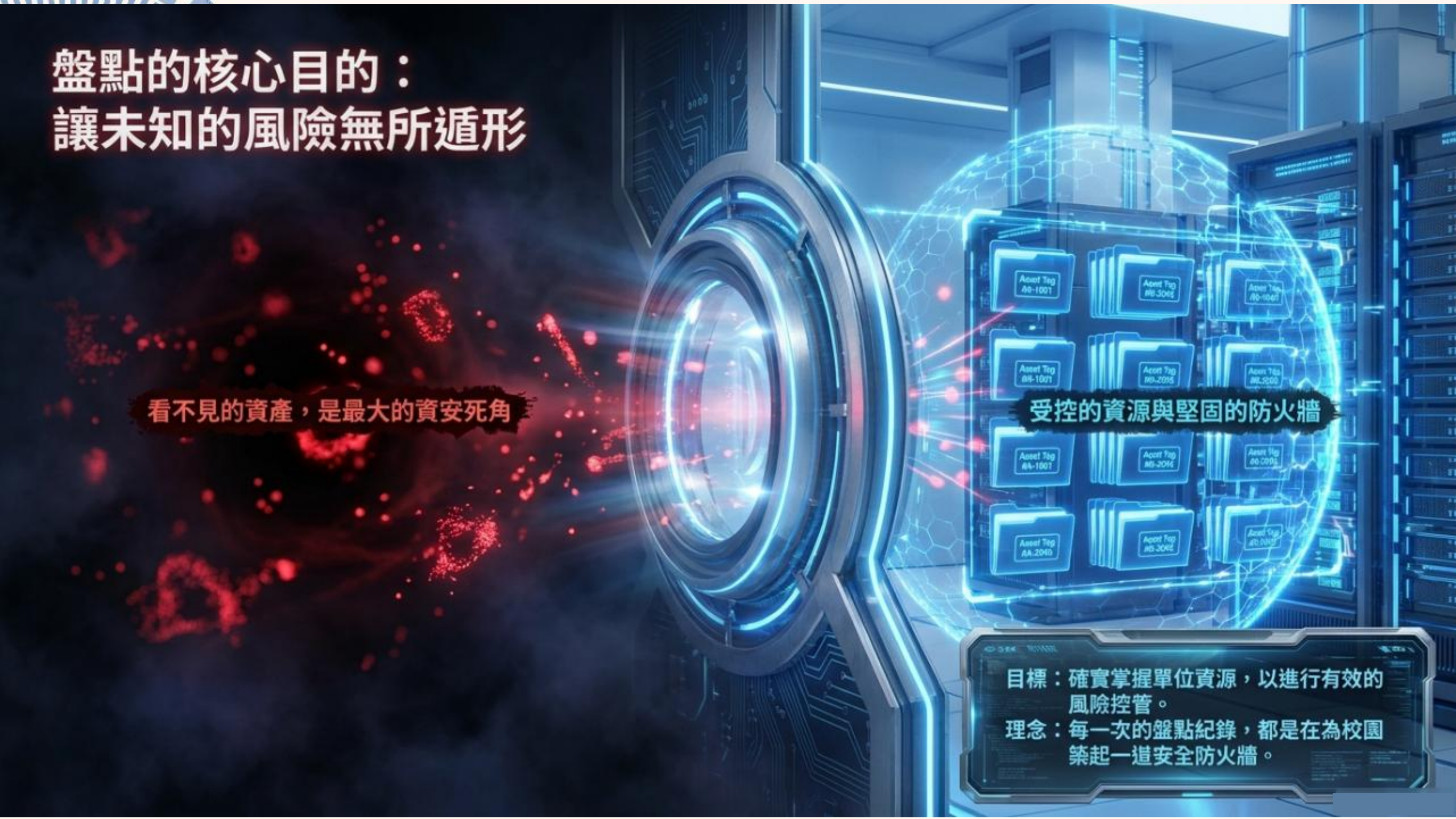
資訊安全不僅是系統與設備的責任，更是全校同仁共同築起的堅固防線。

INFORMATION ASSET INVENTORY

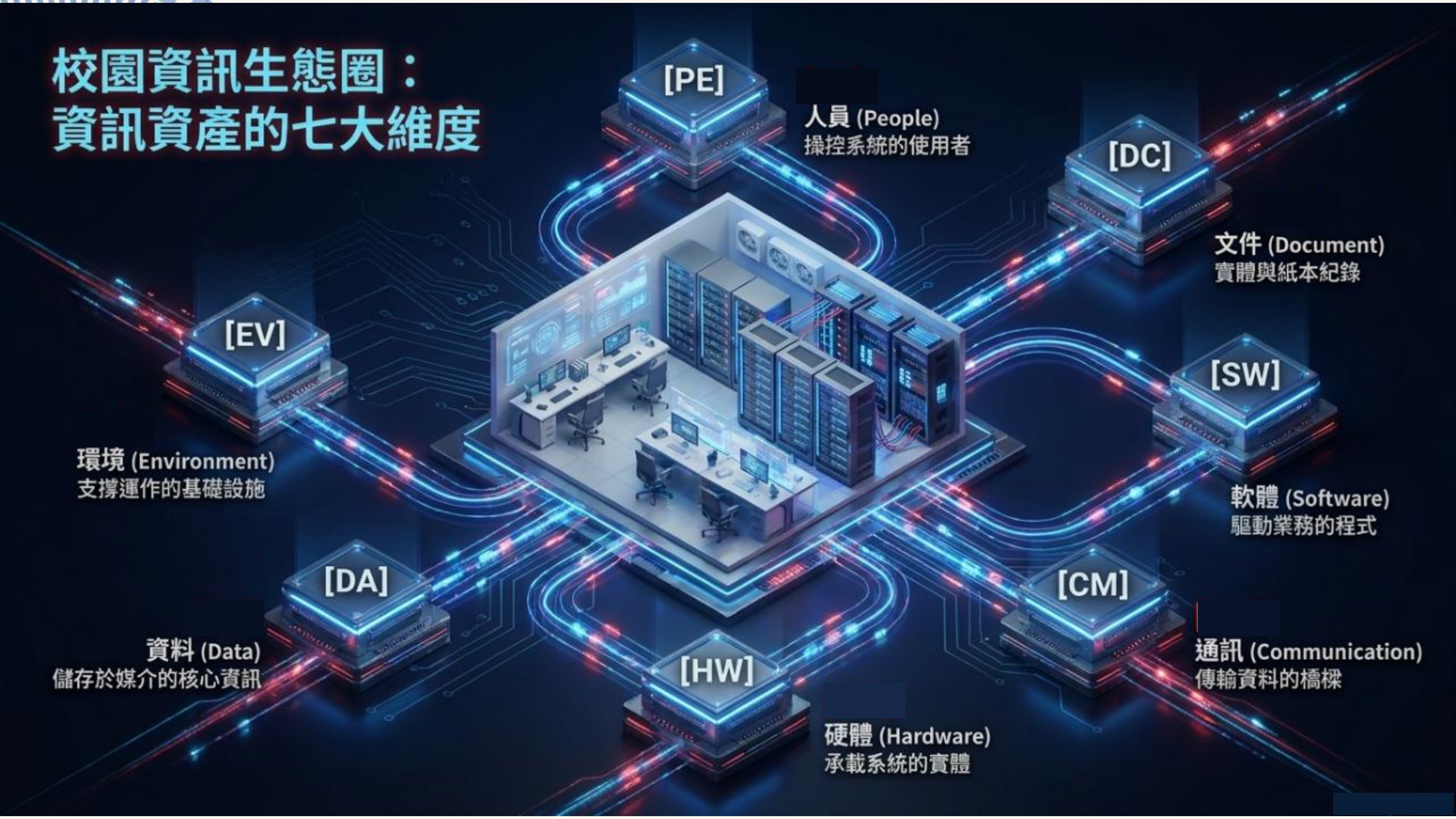
資訊資產盤點說明

資訊資產清查、分類與盤點作業說明

盤點的核心目的：讓未知的風險無所遁形



校園資訊生態圈：資訊資產的七大維度



七大資產圖鑑：盤點目標具體解析

人員 (PE)

資通系統管理維護人員、資訊系統負責人、資安/個資聯絡人、資訊服務委外廠商。

文件 (DC)

以紙本形式存在之文書、報表、公文、列印表單、計畫

軟體 (SW)

資通系統、作業系統、應用程式、套裝軟體、資料庫(含自行開發與委外)。

通訊 (CM)

網路設備、網路安全設備、提供資訊傳輸/交換之線路服務。

硬體 (HW)

電腦主機、伺服器、交換器、影印機。

資料 (DA)

儲存於硬碟、磁帶、光碟等媒介之數位資訊。

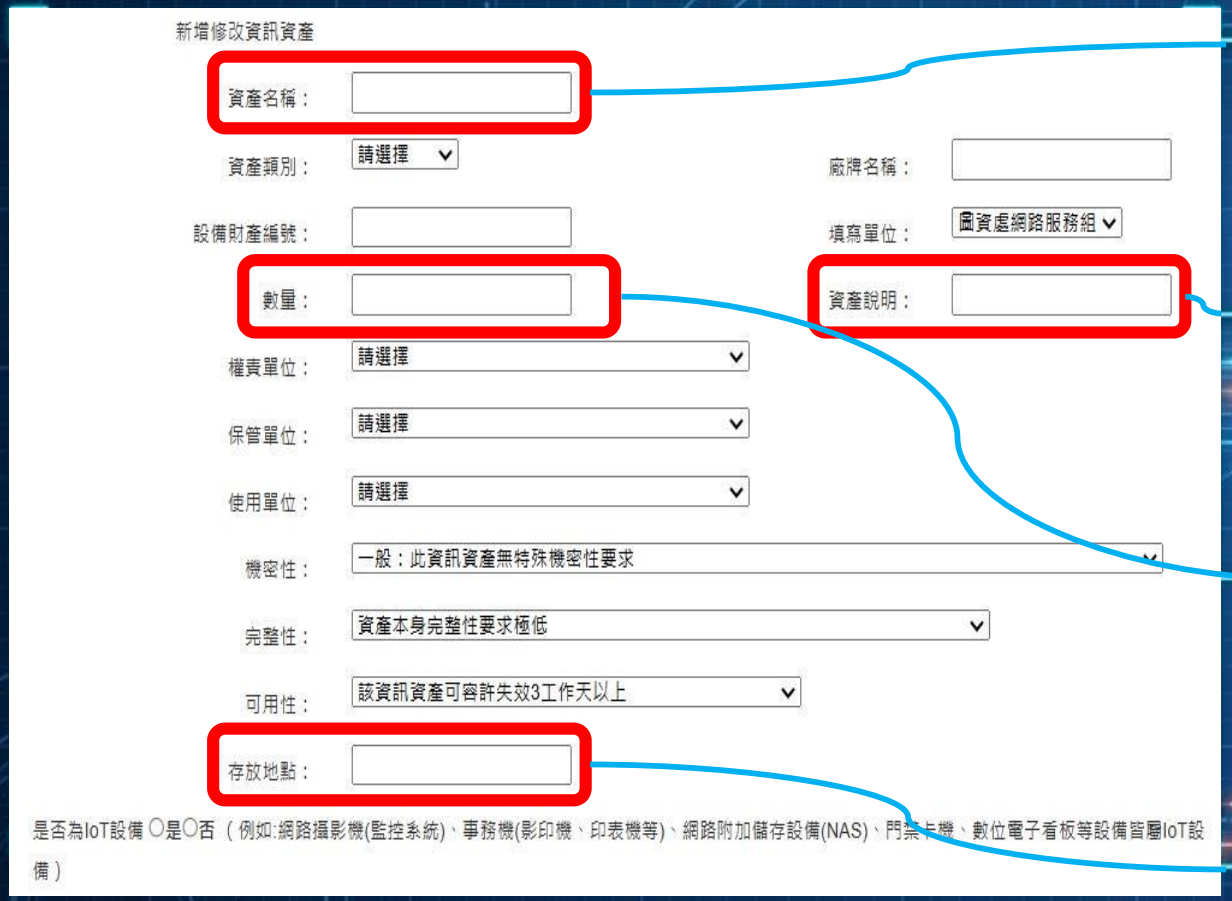
環境 (EV)

辦公室實體、實體機房、電力、滅火器、監視系統、租賃影印機。

資產數位化啟航：填報系統入口

https://system.nutn.edu.tw/formfill/

掌握關鍵細節：清冊核心欄位填寫要點



資產名稱

需具備識別性。舉例：個人電腦、校務行政系統。

資產說明

補充具體用途與細節。舉例：ASUS 廠牌、Windows 10 作業系統。

數量

單位實際保有的精確數量。

存放地點

明確標示實體位置，確保發生事件時能第一時間定位。
舉例：格致樓 C203 辦公室。

衡量資產靈魂：CIA 三維度評分標準

[C] 機密性 (Confidentiality)

4 機密
(Confidential/Top Secret)
此資訊資產所包含資訊為組織或法律所規範的機密資訊

3 敏感
(Sensitive)
此資訊資產僅供內部相關業務承辦人員存取

2 限閱
(Limited Access)
此資訊資產含敏感資訊，但無特殊之機密性要求，且僅供組織內部人員或被授權之外部單位使用

1 一般
(Public/General)
此資訊資產無特殊機密性要求

[I] 完整性 (Integrity)

4 造成業務終止
(Business Termination)
資產具有完整性要求，且完整性被破壞會對組織造成傷害，甚至會造成業務終止

3 傷害不嚴重
(Minor Damage)
資產具有完整性要求，且完整性被破壞會對組織造成傷害，但不至於太嚴重

2 破壞無害
(No Harm)
資產本身具有完整性要求，但是完整性被破壞不會對組織造成傷害

1 要求極低
(Low Requirement)
資產本身完整性要求極低

[A] 可用性 (Availability)

4 僅容許失效 < 4小時
(Tolerance < 4h)
該資訊資產僅容許失效4工作小時

3 失效 4-8小時
(Tolerance 4-8h)
該資訊資產僅容許失效4工作小時以上， 8工作小時以下

2 失效 8小時 - 3天
(Tolerance 8h-3d)
該資訊資產可容許失效8工作小時以上， 3工作天以下

1 容許失效 ≥ 3天
(Tolerance ≥ 3d)
該資訊資產可容許失效3工作天以上

資產價值演算法：取最大值邏輯 (MAX)

[C] 機密性：2 分

[I] 完整性：4 分

[A] 可用性：3 分

系統自動過濾
MAX()

Asset Tag

最終資產價值
= [4]

木桶理論：資產的安全價值取決於最高風險的維度。一旦任一維度達高風險，整體即視為高價值資產，需啟動更高等級防護。

嚴格把關的新陳代謝：異動與報廢決策程序

⚠ 報廢前確認：相關設定與儲存媒體的資料已徹底清除。

徹底終結：儲存媒體的物理銷毀規範

硬碟 (HDD/SSD)

利用消磁機或專業資料清除軟體工具，徹底清除硬碟資料。

光碟 (CD/DVD)

進行實體破壞，將光碟折斷或剪碎，使其無法讀取。

磁帶 (Tape)

以工具破壞實體，使其完全無法使用。

⚠ **絕對底線：價值為敏感級以上的資料，必須反覆確認資料清除後絕對無法還原。**

PERSONAL DATA PROTECTION

個人資料保護認知

個人資料蒐集、處理與利用之保護認知

電子簽章不完善爆糾紛！上海銀行萬筆個資外洩

https://www.youtube.com/watch?v=VTdmS0X7F1E

震撼教育：個資外洩的真實代價

上海商銀等實務案例之鑑

致命疏漏：未訂定密碼規則、未留存存取紀錄。

後果：內部管理輕忽，導致嚴重集體個資外洩事件。

震撼教育：個資外洩的真實代價

行政罰鍰

最高可達 **1,500萬** 元

民事賠償

每人 **500** 至 **2** 萬元，

單一事件最高 **2億** 元

刑事責任

最重可處 **5年** 以下有期徒刑

重新定義：什麼是個人資料？

顯性個資 (直接識別)

姓名、身分證字號、護照號碼、出生年月日、聯絡方式、財務情況、婚姻與家庭、教育與職業

隱性個資 (間接識別與數位軌跡)

網路平臺帳號、IP 位址、Cookie、社會活動軌跡、GPS 定位紀錄

任何「得以直接或間接方式識別該個人之資訊」，皆受法律絕對保護！

絕對紅線：特種個人資料

原則上「不得蒐集、處理或利用」，除非具備嚴格法定例外條件！

- 病歷
- 醫療
- 基因
- 性生活
- 健康檢查
- 犯罪前科

實務提醒：校園問卷或活動報名表，若非絕對必要，嚴禁要求填寫此類資料（如：辦理一般講座不得要求提供詳細病歷或血型）。

行事準則：蒐集、處理與利用之基本原則

誠實信用

不得以詐欺或隱瞞方式取得。必須光明正大、尊重權益。

特定目的

為了什麼事蒐集，就只能用在那件事。嚴禁擅自挪作他用。

最小化原則

只蒐集「絕對必要」的資料。不得過度蒐集（例如：僅需聯絡方式時，不應索取身分證字號）。


公務機關蒐集要件 (決策檢核圖)
業務需求：是否符合「特定目的」？
是
執行法定職務必要範圍內？
(如：依學籍規定處理成績)
經當事人書面同意？
(如：自願參加校外活動之保險資料)
對當事人權益無侵害？
(如：不涉及隱私之去識別化統計)
合法蒐集

必須說清楚：個資告知義務清單

依據個資法第8條，蒐集前必須明確告知當事人以下事項：

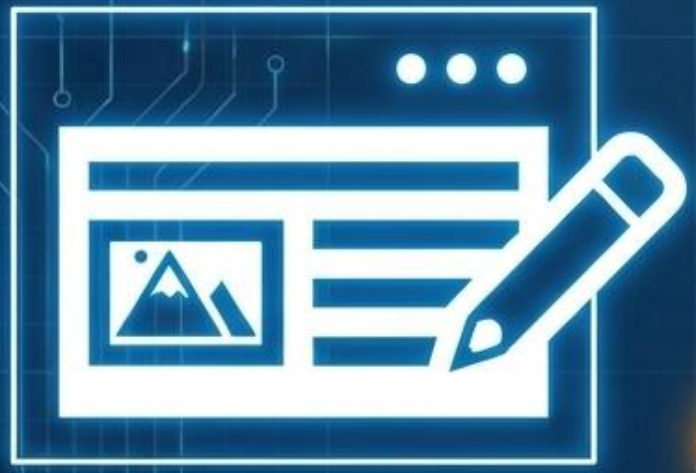
個人資料蒐集告知事項

- ☑ 【機關名稱】蒐集資料的單位是誰？
- ☑ 【蒐集目的】為什麼要蒐集這些資料？
- ☑ 【個資類別】具體涵蓋哪些資料項目？
- ☑ 【利用規範】資料利用的期間、地區、對象及方式？
- ☑ 【當事人權利】當事人可以行使哪些權利？
- ☑ 【不提供之影響】若當事人選擇不提供，對其權益有何影響？

掌控權在誰手裡？當事人的五大權利

實務提醒：本校於合法範圍內，必須受理當事人填具「個人資料使用資訊服務申請表」行使上述權利。

實戰避雷 (一)：校園雲端服務陷阱



情境痛點：校園辦理活動報名、問卷調查、滿意度回饋，最常使用雲端表單服務。

危機所在：雲端表單設定不慎，等同於將全校師生個資直接公開上網！

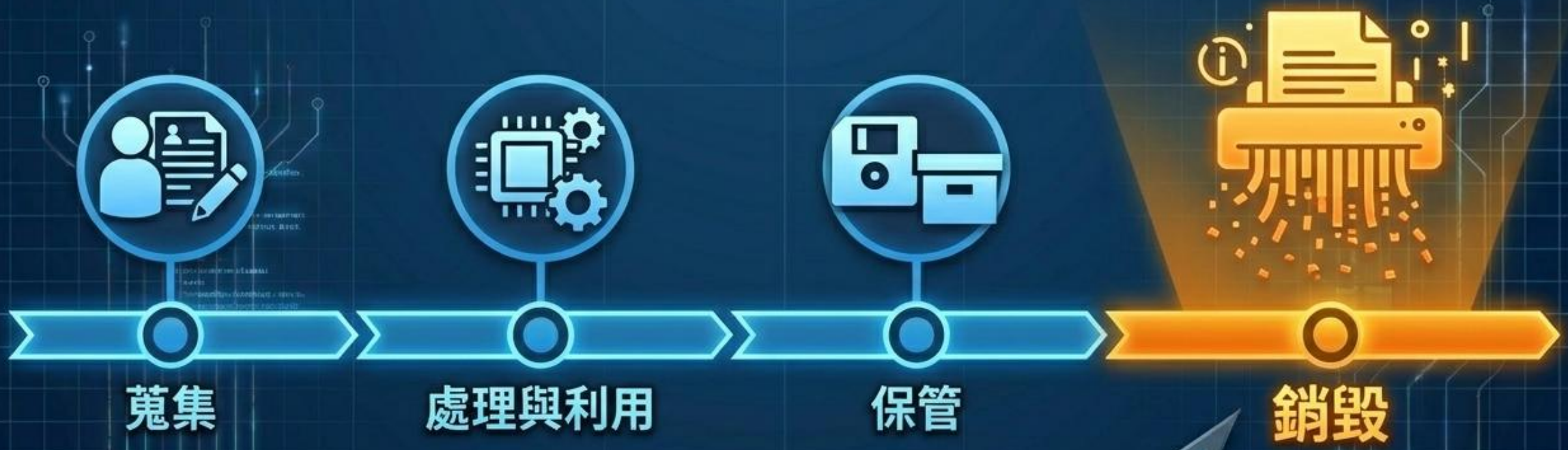
防護對策：
1. 嚴格落實存取控制 (Access Control)。
2. 再三確認分享對象與檢視權限。
3. 公務處理完畢，應及時關閉表單存取。

實戰避雷 (二)：雲端表單防護關鍵設定

災難後果：一旦勾選此功能，所有填表人（包含先前的作答者）的姓名、電話、甚至身分證字號，將被後續作答者全部看光，造成不可挽回的集體個資外洩！

正確作法：確保僅有「表單擁有者 / 授權之共同編輯者」能夠檢視後台原始資料。

有始有終：個資生命週期管理



核心觀念：

- 必須為每一份個資訂定「保存期限」。
- 特定目的消失、業務終止或保存逾期後，不得繼續「留著備用」。
- 實體文件應妥善碎紙，數位檔案應確實刪除銷毀，並留存軌跡紀錄。

總結昇華：個資保護最高原則

找不到
(隱匿性)
無關人員與外部搜尋引擎無法找到機敏資料。

進不來
(存取控制)
設下嚴格的帳號密碼與權限門檻，阻擋未授權存取。

看不懂
(加密化)
即使資料遭竊，經過遮蔽或加密處理也只是亂碼。

帶不走
(防外洩機制)
限制異常下載、關閉未授權列印與隨身碟存取。

臺南大學的防護網與支援資源

遇到個資疑慮？我們在這裡協助您！

- 本校個資保護宣導網
  網址：https://pip.nutn.edu.tw
- 標準告知聲明
  辦理活動或發送表單時，請至網站下載並引用本校標準同意聲明書。
- 申訴與諮詢窗口
  如有任何個資疑慮，請聯繫本校專責單位。秘書室專門委員電子郵件：pims@mail.nutn.edu.tw

掃描立即前往

PERSONAL DATA RISK ASSESSMENT

個資檔案風險評鑑與衝擊值評估

個人資料風險評鑑與衝擊值評估作業說明

資訊安全的雙重防護機制

第一層：堡壘的建造者

透過個資檔案盤點與風險衝擊評估，
找出系統性弱點並加固城牆。

第二層：堡壘的守門人

當攻擊者試圖繞過城牆直接欺騙人類時，
我們必須具備識破社交工程的心理素質。

第一道防線：精準盤點你的資訊資產

防禦的前提是「知道你擁有什麼」。依據個資法，我們必須從三大維度全面鑑別與清查：

1. 法令法規要求
依據法律規定必須保有之資料。

2. 組織業務分析
從單位既有文件與特定業務需求中判別。

3. 作業流程 (SOP)
從日常行政與教學處理流程中盤點。

完整個資檔案清單

個資的校園旅行：盤點系統軌跡圖

*國立臺南大學各單位保有個人資料檔案清查盤點系統，依國立臺南大學個人資料檔案清冊需求開發，填報順序依序為P1名稱、P2目的、P3蒐集、P4處理、P5利用、P6保存、P7銷毀、P8揭露、P9重要性：

名稱 > 目的 > 蒐集 > 處理 > 利用 > 保存 > 銷毀 > 揭露 > 重要性

起點站

系統登入
(使用校務系統帳號密碼登入)

站點一：蒐集 (P3)

(資料從何而來？)

站點二：處理 (P4) / 利用 (P5)

(我們如何使用這些資料？)

站點三：保存 (P6)

(資料存放在哪裡？期限多久？)

終點站：銷毀 (P7)

(到期後如何安全抹除？)

⚠ 完整掌握資料在 P1（名稱）至 P9（重要性）的每一個環節，才能建立有效的控制措施。

測量風險深度：衝擊值評估矩陣

評估時，須同時考量**財務影響**與**當事人損害程度**，並取其**最大值 (MAX)** 作為最終衝擊值。

啟動風險計算引擎

風險值 = 個資資產價值 × 衝擊值(MAX) × 可能性值

⚠ 風險值並非只是一個數字。根據計算結果的高低，各單位必須建立對應的「風險處理計畫」，優先分配資源修補最脆弱的環節。

當防線被突破：個資事件應變協議

1.查明與阻斷

確認遭惡意破壞或不慎洩漏的範圍，立即執行緊急因應措施。

2.通知當事人

查明後應儘速以適當方式通知受影響之當事人。

3.向上通報

依本校「個人資料保護緊急應變處理作業說明書」通報程序，並至國家資通安全通報應變網站進行通報。

SOCIAL ENGINEERING DEFENSE

社交工程防範

社交工程攻擊辨識與防範作業說明

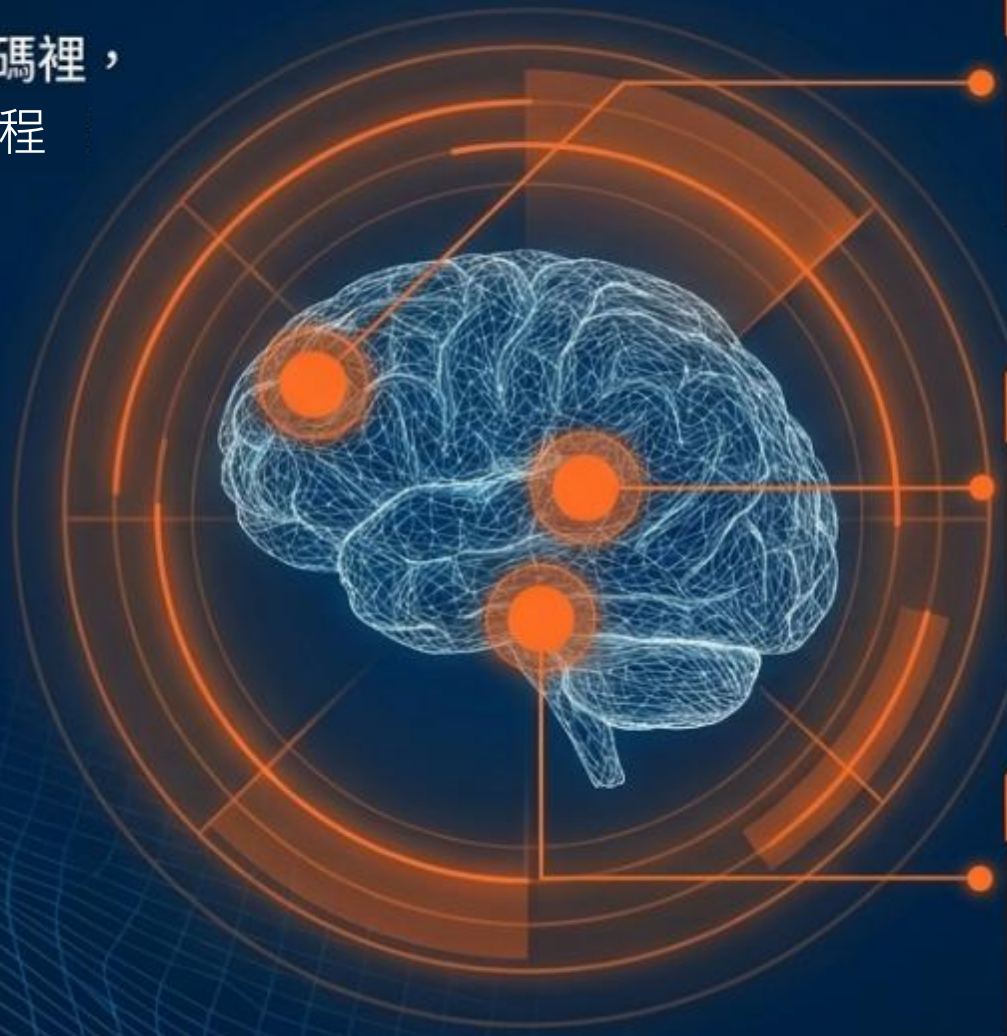
離你最近的資安專家

BCCS 漢昕科技

一站式資安防護

第二道防線：駭客的心理操縱術

最危險的漏洞不在系統程式碼裡，
而在人類的大腦裡。社交工程
不駭電腦，他們「駭人」。



貪婪與好奇 (Curiosity)

對應手法 → 下餌攻擊（如：丟棄在路邊的惡意 USB）、引誘性主旨。

信任與服從 (Trust)

對應手法 → 假托冒名、CEO詐騙（假冒長官指令）、水坑攻擊。

恐懼與急迫 (Fear)

對應手法 → 恐嚇軟體（警告帳號即將被停權）。

無孔不入的釣魚陷阱：特徵解剖

1. 惡意簡訊 (Smishing)

偽裝成快遞包裹異常或罰單未繳的短網址連結。

2. QR Code 詐騙 (Quishing)

覆蓋在實體海報或停車單上的偽造二維碼，掃描即竊取憑證。

3. 搜尋引擎釣魚

偽裝成官方網站的「Google 惡意贊助商廣告」，引導至釣魚登入頁。

4. 引誘性電子郵件

教育部演練常見的高點擊率主旨（如：ChatGPT帳號異常、加薪調薪通知、Me Too事件等時事熱點)。

眼見不一定為憑：進階欺騙技術

BEC
(商業電子郵件詐騙)

長期潛伏於郵件系統中，觀察並模仿長官或合作廠商的語氣，在關鍵時刻（如：匯款、變更帳號）發出偽造指令。

Deepfake
(深偽技術)

結合 AI 技術，不只文字造假，更能「複製聲音」甚至「偽造視訊影像」。

核心觀念：當高階主管透過語音或視訊提出異常的「緊急資金調度」或「機敏資料索取」要求時，極有可能是 AI 生成的陷阱。

詐團"AI變臉"假傳匯款指令 跨國企業被坑8億

https://www.youtube.com/watch?v=QG_JM64kYVw

人類防火牆的啟動密碼：停、看、聽

停 (Stop)

克制點擊衝動。面對帶有「急迫性」或「強烈誘惑」的信件，絕不立刻點擊不明連結或下載附件。

看 (Look)

仔細檢查破綻。檢視寄件者的「完整電子郵件地址」（非僅看顯示名稱）、查驗網址是否有拼字錯誤，並留意用語是否符合常理。

聽 (Listen)

切換管道查證。若收到涉及機敏資訊、金流或帳號密碼重設的通知，應透過「信件以外」的管道（如：撥打已知的分機電話）向本人或官方確認。

技術武裝：阻斷惡意程式的兩大設定

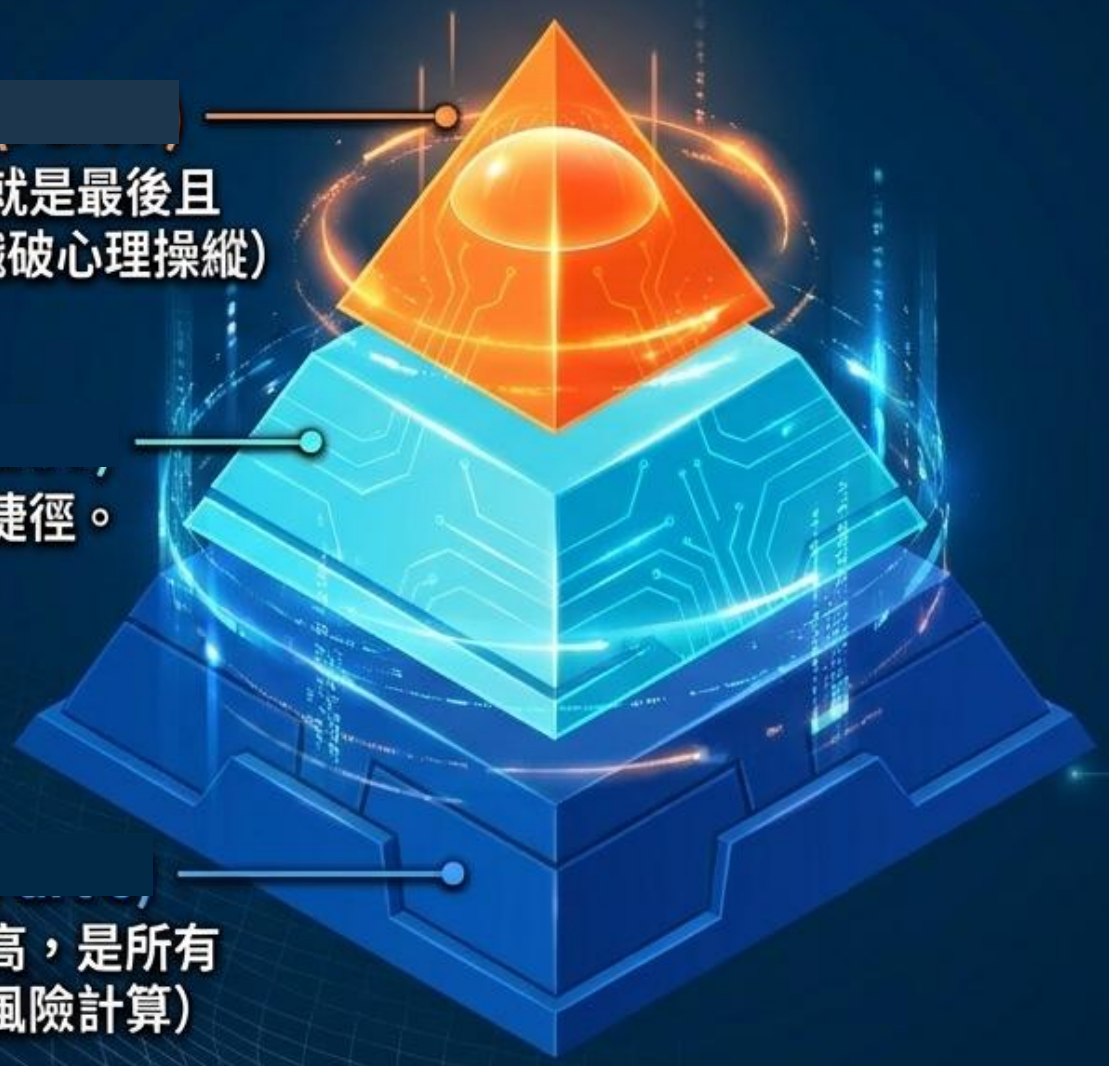
防線一：關閉信件「預覽」功能

為什麼？
預覽信件在某些軟體中等同於「開啟信件」，可能直接觸發夾帶在信件中的惡意程式或追蹤碼。

防線二：優先以「純文字模式」開啟郵件

為什麼？
取消 HTML 格式顯示，能讓隱藏在圖片或按鈕底下的 真實網址無所遁形，剝除駭客的視覺偽裝。

打造國立臺南大學的零信任資訊堡壘



塔尖守門人：人類警覺

當一切系統失效，您的大腦就是最後且最強大的防線。（停看聽、識破心理操縱）

中層屏障：系統設定

利用軟體設定剝奪攻擊者的捷徑。（關閉預覽、純文字模式）

底層結構：盤點與評估

知道資料在哪裡、風險有多高，是所有防禦的基石。（個資盤點與風險計算）

臺南大學的防護網與支援資源

- 本校電子郵件社交工程演練資訊網
https://www.nutn.edu.tw/cc/emailse/index.htm

- 國立臺南大學115年防範惡意電子郵件社交工程認知素養線上評量
- 國立臺南大學115年防範惡意電子郵件社交工程演練宣導資料
- 教育部115年度臺灣學術網路防範惡意電子郵件社交工程演練服務計畫

掃描立即前往

INTELLECTUAL PROPERTY PROTECTION

保護智慧財產權宣導

智慧財產權保護觀念與著作權法遵循宣導

數位時代下，南大人的三項核心修煉

尊重 (Respect)
保護智慧財產

劃清合理使用與侵權的界線。

平權 (Openness)
擁抱 ODF 開放格式

打破軟體綁架，實現跨機關資訊平權。

守護 (Vigilance)
堅守資安核心

化知識為行動，落實年度防護義務。

基石一：創新與分享的底線

保護智慧財產權，從守護學術倫理開始。

臺灣學術網路資源的「綠燈與紅燈」

綠燈區 - 鼓勵與允許

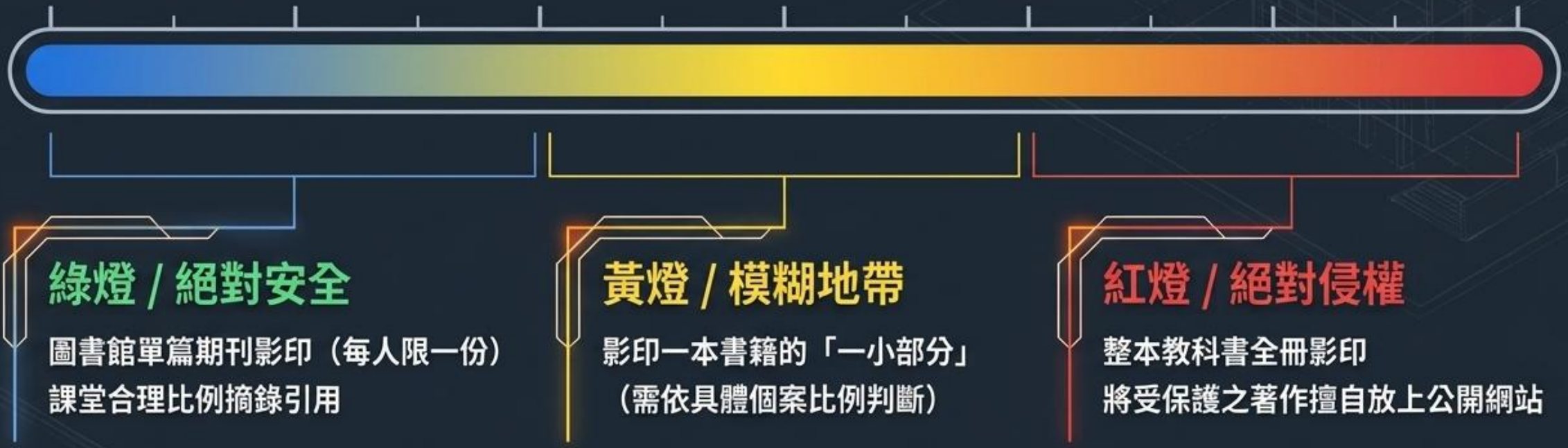
專供「教學」與「學術研究」
之正當目的使用。

紅燈區 - 嚴格禁止

1. 使用未經授權軟體或違法下載
   （如 P2P 盜版下載）。
2. 從事非教學研究之營利或商業活動。
3. 發送惡意攻擊封包或大量垃圾郵件。

違規代價：經查證屬實，將面臨 3 日至最長 30 日之網路停權處分，並自負相關法律責任。

影印教科書的侵權風險光譜



綠燈 / 絕對安全

圖書館單篇期刊影印（每人限一份）
課堂合理比例摘錄引用

黃燈 / 模糊地帶

影印一本書籍的「一小部分」
（需依具體個案比例判斷）

紅燈 / 絕對侵權

整本教科書全冊影印
將受保護之著作擅自放上公開網站

> 智財局核心觀念：書籍價格昂貴不能作為『重製無罪』的理由，整本影印絕對構成侵權！

參考資料：經濟部智慧財產局 校園影印教科書問題之說明 https://www.tipo.gov.tw/tw/copyright/701-21229.html

遇到版權疑慮？校內資源為您導航

資源一：本校智慧財產權宣導網

匯集最新校園網路規範、著作權法規與爭議案例指引。

國立臺南大學 智慧財產權宣導作業管理系統
https://system.nutn.edu.tw/copyright/index.htm

資源二：線上檢核系統

提供教育部網路智財權指引與智財局「教師授課著作權錦囊」。

經濟部智慧財產局 著作權主題網 教師授課著作權錦囊
https://www.tipo.gov.tw/tw/copyright/701-21243.html

建議將此網站加入書籤，作為課程教材準備的首要檢核點。

OPEN DOCUMENT FORMAT

ODF 開放文件應用宣導

ODF 開放文件格式應用與政府文件標準宣導

基石二：打破格式綁架的 ODF 運動

ODF 開放文件格式宣導，實踐跨越世代的資訊平權。

為什麼政府全面推動 ODF 格式？

專屬商業格式

- 需持續花費預算購買軟體授權
- 軟體版本更新後容易跑版不相容
- 剝奪無預算購買軟體者的閱讀權力

ODF 開放格式

- 符合 CNS 15251 國家標準，免費平權
- 無軟體授權綁架，跨機關無礙流通
- 保證政府與學術檔案能永久保存與讀取

南大 ODF 的推動里程碑與現行規範

106 年起 (公文系統)

本校公文系統全面限制。

可編輯之附件檔案，**強制須使用 ODF 格式**上傳。

107 年起 (網頁表單)

全校表單格式更新。

各單位網站之可編輯文件與舊有表單，
均需轉換為 **ODF 格式**。

政府文件流通最高準則：可編輯 ➡ 用 ODF (.odt / .ods / .odp) ｜ 不可編輯 ➡ 用 PDF

對應 MS Word/Excel/PowerPoint

實戰指南：無痛轉換 ODF 格式

數位發展部 ODF文件應用工具
https://moda.gov.tw/digital-affairs/digital-service/app-services/248


基石三：
化知為行的資安承諾
從意識到行動，築起南大的最終防線。

守護校園資產的「五大核心防護盾」

您的年度法定資安任務

依法落實資安教育訓練

依據《資通安全管理法》，本校一般使用者者與主管，每人每年應接受 3 小時以上之一般資通安全教育訓練。

掌握最新防護資源

善用「國立臺南大學資通安全宣導網」與「個人資料保護宣導網」獲取最新教材與法規更新。

堅實的後盾：諮詢與支援網絡

系統與資安技術支援

圖資處 **網路服務組**

王元良 技士

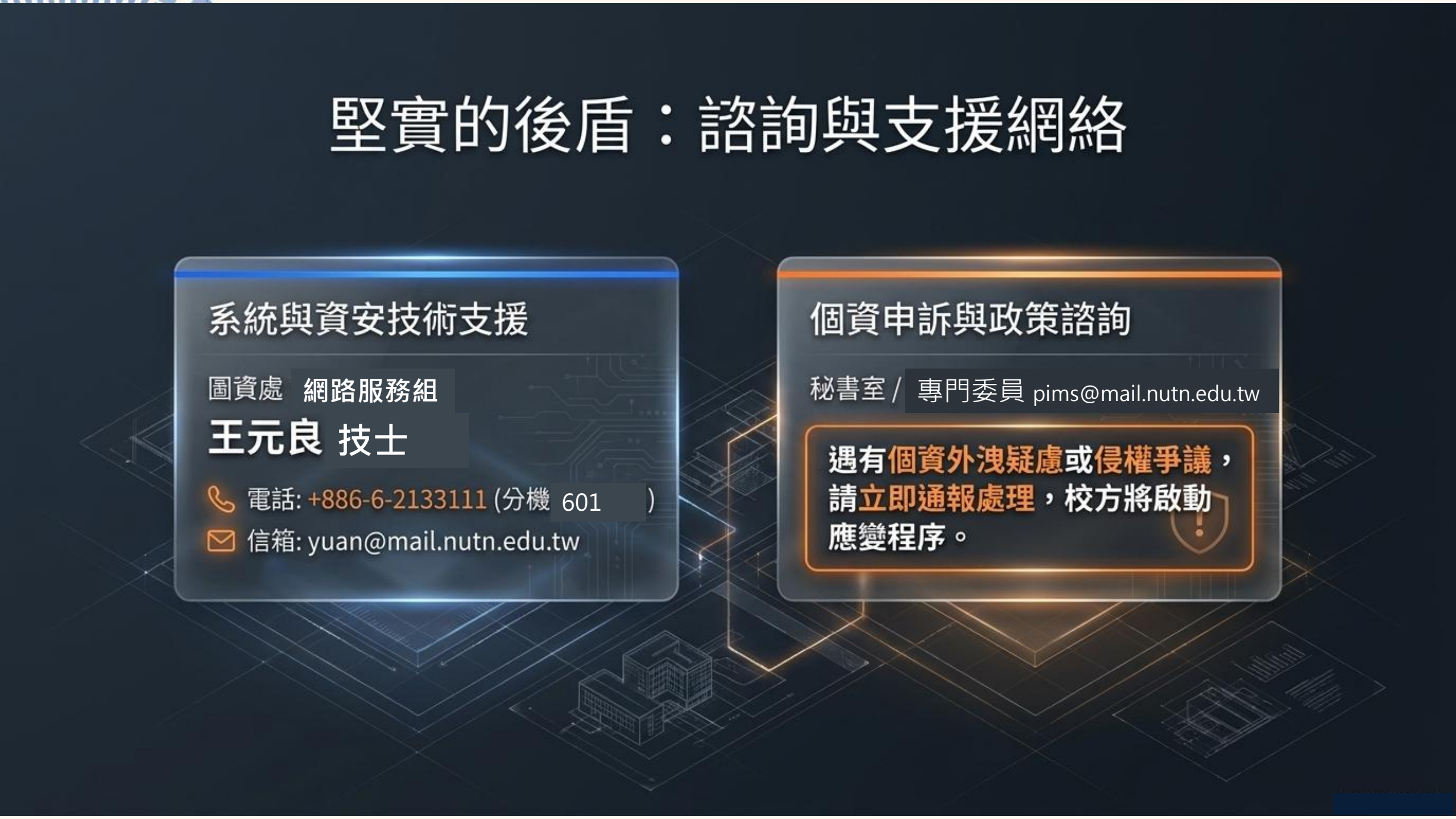
電話: +886-6-2133111 (分機 601)

信箱: yuan@mail.nutn.edu.tw

個資申訴與政策諮詢

秘書室 / 專門委員 pims@mail.nutn.edu.tw

遇有個資外洩疑慮或侵權爭議，請立即通報處理，校方將啟動應變程序。



離你最近的資安專家

BCCS 漢昕科技

課後評量

一站式資安防護

BCCS 漢昕科技

- 離你最近的資安專家 -

Thank you

FOR YOUR ATTENTION

Get in touch:

雲安維運　聯防設備　風險檢測　顧問諮詢　資安學苑