

中華大學 資訊安全教育訓練

圖書與資訊處 林肯豐

2026/10/08

資訊安全教育訓練

- 近期資訊安全工作宣導
- 資通安全管理法- 教育體系之法遵說明
- 教育部高教深耕計劃 -資安專章之要求
- 本校高教深耕計劃 -資安專章規劃方案
- 資訊安全內部稽核準備事項

台灣面臨強烈網路威脅

微軟發布2026數位防禦報告，臺灣上半年遭網路威脅影響排名升至全球第4名 | iThome

iThome

新聞

AI

資安

Cloud

CIO

政府

醫療

永續

專題

活動

技術

IT EXPLAINED

搜尋

員工用 AI，企業 Mac 跟上了嗎

天天更新、週週整理、關鍵情報！

10/24-25 台灣最大自造者盛會

新聞

微軟發布2026數位防禦報告，臺灣上半年遭網路威脅影響排名升至全球第4名

微軟揭露最新全球資安態勢，指出臺灣客戶2026年上半年遭受網路威脅影響排名全球第4，佔全球總量的3.9%，去年的1.8%增逾一倍，顯示臺灣在全球受威脅版圖中的相對位置明顯上升

文/ 羅正漢 | 2026-10-05 發表



領先威脅一步

日報

掌握最新漏洞與攻擊

週報

深度解析產業趨勢

iThome 專業編輯團隊，
打造資安人的每日必讀清單。

免費訂閱



社交工程要警覺

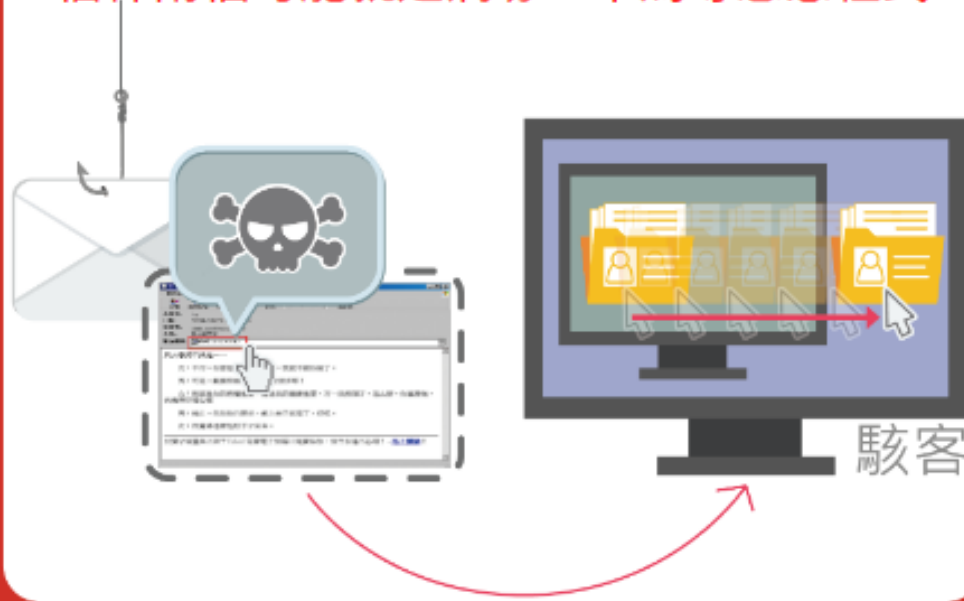
教育部每年4月~11月都會實施社交工程演練，目的是為了模擬駭客寄送各類詐騙信件的手法，測試教職員點選各類誘騙信的比率，以強化教育機構教職員對資安等社交工程的警覺意識。

社交工程是利用人性的弱點進行詐騙，最常利用電子郵件等方式進行。往往駭客最常在這類的信件中藏惡意的軟體或連結，使用者稍不注意點擊或開啟就會讓駭客有機可趁。

駭客會弄個假冒網站來騙取你的帳號密碼



信件附檔可能就是病毒、木馬等惡意程式



收信時必須要注意寄件者的信箱、寄件時間以及信件的主旨還有附加檔案等等..., 發現這些疑點有可能是釣魚郵件就應避免開啟信件附件或點擊信件內的超連結。

寄件人信箱若是.....

- 不認得的人
- 沒有業務往來的人
- 署名某人但他應該不會跟我聯絡的信箱網域名稱蠻可疑的(像某單位的網域又有點不像、或是免費信箱)

收件人群組若是.....

- 還有其他一些不認識收件人
- 看來像是從網站把同頁面的通訊錄都納入收件人名單中

信件內的超連結若是.....

- 滑鼠移到超連結上可看到實際連結的網址與表面上的網址不同
- 超連結網址看得出來是某個已知網站但中間有些微拼錯字的
- 超長的超連結網址就要特別小心

信件內容若是.....

- 不合常理
- 提到為了避免什麼不好的後果
- 提到你中獎了或你獲得什麼好處
- 提到別人或自己可能發生桃色事件或不雅照片等八卦消息
- 內容明顯文法錯誤或錯字不少, 不像是一般人會嚴謹擬訂字句。
- 強調快點擊超連結或開啟附加檔案



寄件時間若是.....

- 不太正常的寄件時間, 像是半夜3點怎麼有人會寄信聯繫業務呢?

信件主旨若是.....

- 主旨看來跟自己無關的
- 主旨與信件內容不相關
- 主旨是回覆什麼, 但之前並未寫信去問過什麼啊!

附加檔案若是.....

- 檔案名稱看起來不應該寄給我的
- 檔案名稱與信件內容不相關
- 署名某人來信, 但應該不會寄這種檔案給自己啊!
- 除了副檔名.txt, 任何檔案都有可能包藏惡意程式在內, 有懷疑的話就開啟前先用防毒軟體掃描較保險。



電腦使用安全宣導



- 個人電腦、伺服器或主機應設定螢幕密碼保護程式，下班時應關閉不需使用之個人電腦。
- 須瞭解「免費軟體」或「共享軟體」相關版權規定，不得任意安裝及散佈未經授權軟體。
- 個人電腦皆須安裝防毒軟體、軟硬體常更新修正程式。
- 物聯網設備要修改出廠預設密碼
- 列表機避免對校外開放連線，不要設定可連線外部的實體IP，以防止遭外部攻擊入侵，列印資料立即取走。

Windows 10 (2025年10月14停止安全性更新)

<https://support.microsoft.com/zh-tw/windows/windows-10-%E6%94%AF%E6%8F%B4%E5%B0%87%E6%96%BC-2025-%E5%B9%B4-10-%E6%9C%88-14-%E6%97%A5%E7%B5%90%E6%9D%9F-2ca8b313-1946-43d3-b55c-2b95b107f281>

 | 支持 Microsoft 365 Office 產品 裝置 帳戶與帳單 資源 [試用 Copilot Chat](#)

Windows 10 支援將於 2025 年 10 月 14 日結束

► 套用到

提醒一下，Windows 10 將於 2025 年 10 月 14 日終止支援。此時將不再提供技術協助、功能更新和安全性更新。如果您有執行 Windows 10 的裝置，建議您將其升級至 Windows 11 - 更現代化、更安全且高效率的運算體驗。如果裝置不符合在 Windows 11 上執行的技術需求，建議您註冊 Windows 10 消費者擴充安全性 匯報 (ESU) 計劃，或將裝置取代為支援 Windows 11 的裝置。

我有哪些選項可以繼續在 Windows 作業系統上受支援？

- **在目前的電腦上安裝 Windows 11** - 如果您的電腦符合 [Windows 11 的最低系統需求](#)，而且符合直接升級至 Windows 11 的資格，您可能已經收到升級的通知。若要檢查您的電腦是否符合免費升級的資格，請前往「開始」>「設定」>「更新」&「安全性」> Windows Update，然後選取「檢查更新」。
- **裝有 Windows 11 的新電腦** - 如果您的電腦不符合資格，或者您想要預先安裝 Windows 11 的新電腦，您可能想要先探索最新的 [Windows 11 電腦](#)。該 [工具](#) 將幫助您根據您的獨特需求找到合適的 PC。
- **ESU 計劃匯報 (擴展安全性)** - 如果您在移至 Copilot+ PC 或其他新的 Windows 11 裝置之前需要更多時間，消費者延伸安全性匯報 (ESU) 計劃可以在 2025 年 10 月 14 日之後的一年內保護您的 Windows 10 裝置。

如果您是 IT 專業人員，請參閱 [ESU 計劃的擴充安全性 匯報 \(以 Windows 10\)](#)。

Windows 10 (請升級至Windows 11)

<https://lis.chu.edu.tw/p/406-1052-37501,r646.php?Lang=zh-tw>

- 參考圖資處網站windows 10升級windows 11 之說明進行升級



隨機版或校園授權版從windows10更新至windows11

校園授權版從windows10更新至windows11

方法1.若您原本已經有可以正常開機的windows10(桌面左下角windows符號是黑白色，win11是藍色且在偏中間)，請先確認您的Office版本是2016或以上版本，請在此處[下載圖資處windows升級壓縮檔](#)，然後用滑鼠右鍵點取此壓縮檔(CHUtoWin11.zip)，再用滑鼠左鍵來解壓縮全部，等它解壓縮完成後，在CHUtoWin11的目錄中會有setup.exe，再用滑鼠右鍵點取此檔案，用系統管理員執行



安裝 Windows 11。

安裝程式將連線以取得更新、驅動程式和選用功能。這些更新將協助安裝順暢地進行，而且可以包含重要修正、更新的設備磁碟機，以及不在安裝媒體上的其他檔案。

WinRAR 資安漏洞



國家資通安全研究院
National Institute of Cyber Security

核心業務 ▾

資安資源 ▾

最新消息 ▾

🏠 > 最新消息 > 公告訊息 > 最新公告 > WinRAR曾遭嚴重零時差攻擊 資安院呼籲民眾立即更新至最新版

最新消息

公告訊息



最新公告

活動訊息

採購公告



人才招募

資訊公開



WinRAR曾遭嚴重零時差攻擊 資安院呼籲民眾立即更新至最新版

2025/9/2 上午 11:15:25

國家資通安全研究院提醒民眾，知名壓縮軟體WinRaR近日嚴重漏洞(CVE-2025-8088)曾在修補程式釋出前遭駭客利用發動「零時差攻擊」。駭客會透過夾帶惡意壓縮檔的電子郵件，引誘收件人解壓縮後觸發惡意程式，進而竊取資料或遠端控制電腦。資安院呼籲民眾務必立即更新至最新版WinRaR(7.13)，並避免在更新前開啟任何RaR壓縮檔，以降低受駭風險。

資安院進一步說明，已經有駭侵組織利用此漏洞製作惡意壓縮檔，將實際藏有惡意程式之壓縮檔命名為「履歷、自傳或職缺說明」，偽裝成求職郵件引誘收件人開啟。一旦收件人解壓縮檔案後，漏洞即被觸發，木馬程式(如SnipBot, RustyClaw及Mythic agent)會直接植入電腦開機目錄，並於每次開機時自動執行。這讓駭客能長期潛伏竊取機敏資料，甚至完全控制電腦。

資產盤點 (2026/10/15 前完成)

表單	附件 0	流程圖	重要性: ☐ 高 ☒ 中 ☐ 低
一般通知單			
申請單位：	圖書與資訊處教學資源組		
姓名：	陳俞儒		
日期：	2026/10/2		
主旨：	資訊安全工作事項及資安窗口教育訓練通知		
內容：	一、資產盤點及更新資訊資產清單每年一次：請各單位更新「D-008_資訊資產清單」，各單位可參考去年繳交之表單。 二、資訊系統與連網設備(IOT物聯網裝置)之盤點：各單位可參考去年繳交之調查表進行盤點及資料更新(增加今年新購或漏填之連網設備，刪除今年報廢之連網設備)，若為大陸廠牌必須填寫預計汰換的時程。 三、各單位若有建置或委外開發之資通系統，請填寫「D-056_安全等級評估表」、「D-057_資訊系統清冊」、「D-058_資通防護基準控制措施評估表」，填表作業說明請參閱附件【資通系統防護需求分級作業說明】 四、以上資料，請於10/15(四)前完成，電子檔(excel)檔及核章後之電子檔(PDF)檔，請上傳至 https://x.chu.edu.tw/ZCBMD6/，放入至各單位之2026年資料夾中(Teams團隊_資訊安全ISMS團隊)，2025年提供之檔案，也可以於系統中查看。 五、為協助各單位資訊安全工作推行及完成表單之填報，將於10/8(四)上午10:00~11:30於L204電腦教室(一)辦理資訊安全教育訓練，因此項資料需提報高教深耕資安專章中，敬請各單位資通安全保護聯絡窗口人員務必參加。 六、資通安全教育訓練時數，一般人員及主管每年3小時以上之資安通識教育訓練。將另行通知教育訓練研習之時程。		
備註	中華大學短網址轉址服務 https://x.chu.edu.tw/		

資訊安全通識教育訓練 (2026/10/23 前完成)

一般通知單	
申請單位：	人事室
姓名：	葉順琬
日期：	2026/10/2
主旨：	職員工115學年度第1學期第1次資安教育訓練，如說明，請查照。
內容：	一、依資通安全責任等級分級辦法之應辦事項規定，每人每年須接受3小時的資訊安全通識教育訓練，並列為教育部高教深耕計畫資安專章之指標要求。115年度規劃課程為資通安全(通識)【115年資訊安全教育訓練】:認證時數3小時。 二、本次教育訓練採數位線上課程方式辦理(e等公務園+學習平台網址：網頁: https://elearn.hrd.gov.tw/mooc/index.php)，平台操作請參閱附件檔。 三、時間：自即日起至10月23日(五)止期間內撥冗上網觀看，於課程結束後在線上進行測驗，並請將通過測驗所產出之【認證時數證書】(證書需顯示正確中文姓名)之PDF檔於10月23日(五)前上傳至CHUMoodle數位學習平台(https://moodle.chu.edu.tw/mod/assign/view.php?id=189229)即完成參訓。 四、圖資處補充說明： 本課程由臺南市政府e學補給站上架至「e等公務園+學習平台」之開放課程，其中資安政策及部份 訓練內容與本校略有差異處，補充說明如下： 1.本校資安政策公告於本校「資訊安全專區」網頁: https://x.chu.edu.tw/isms 2.資訊安全事件通報流程: 當發現資安事故或異常事件時，請向本校「圖資處教學資源組」通報。 3.校園授權軟體(含防毒軟體)：請至本校網站 https://download.chu.edu.tw 下載安裝。 4. QR Code及短網址管理：建議使用本校自行建置之短網址服務: https://x.chu.edu.tw。 五、本校職員工(含計畫案人員)均需參加。
備註	中華大學短網址轉址服務 https://x.chu.edu.tw/

資訊安全內部稽核 (2026/10/27 ~ 10/28)

中華大學資訊安全內部稽核基本項目查核表

受稽單位：

填表日期：西元 年 月 日

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
1.資通安全政策之推動及目標	1.1 同仁是否知道學校之資通安全政策、目標及應負之責任？				
	1.2 同仁是否知道如何取得學校之資通安全四階文件？				
2.資通安全推動組織	2.1 單位是否已指派人員作為單位內之資安窗口，負責辦理相關資通安全工作？				
	2.2 同仁是否知道單位內之資安窗口人員姓名及聯絡方式？				
3.資訊及資通系統之盤點及風險評估	3.1 是否建立資訊及資通系統資產清單，並每年維護更新？				
	3.2 是否依資訊、資通系統分級與處理之相關規範，進行分級及防護基準評估？				
4 資通安全管理措施之實施情況	4.1 是否定期執行作業系統更新及各項系統漏洞修補程式？				
	4.2 是否全面使用防毒軟體並即時更新病毒碼？				
	4.3 是否定期對電腦系統及資料儲存媒體進行病毒掃描？				
	4.4 電腦是否設定螢幕保護程式並設定密碼保護，並將螢幕保護啟動時間設定為 15 分鐘以內				
	4.5 安裝之電腦軟體是否均有合法授權，符合智慧財產權相關規定？				
	4.6 通行碼是否定期變更(至少每六個月一次)？				
	4.7 通行碼長度是否超過 8 個字元以上？				
	4.8 通行碼是否規定需有大小寫字母、數字及符號組成？				
	4.9 對於敏感性、機密性資訊之傳送是否採取資料加密等保護措施？				
	4.10 公文及儲存媒體在不使用或不在班時是否妥為存放？機密性、敏感性資訊是否妥為收存？				
	4.11 重要的資料及軟體是否定期作備份處理？				
	4.12 設備報廢前是否先將機密性、敏感性資料及版權軟體移除或覆寫？				

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
5 資通安全事件通報及應變之程序及機制	5.1 同仁是否知悉資通安全事件通報應變程序並依規定辦理？？				
	5.2 同仁是否知悉本校資通安全事件發生之通報窗口？				
6 資通安全認知宣導及教育訓練	6.1 同仁是否知悉「人員資訊安全守則」？				
	6.2 同仁是否簽署「保密切結書」？				
	6.3 同仁是否完成 3 小時資通安全通識教育訓練？				
7 落實管理危害國家資通安全產品	7.1 針對公務用之資通訊產品，包含軟體、硬體及服務等，是否已禁止使用大陸廠牌資通訊產品？				
	7.2 委外營運公眾場域之契約或場地使用規定是否已限制使用大陸廠牌資通訊產品？				
8 資訊作業委外安全管理程序	8.1 是否依資訊作業委外安全管理程序，確保委外廠商執行委外作業時，具備完善之資通安全管理措施或通過第三方驗證？				

查核人員：

受稽單位人員：

中華大學 資訊安全專區

中華大學圖書與資訊處

Office of Library & Information Services
Chung Hua University

關於圖資處

資訊服務

圖書服務

圖資服務卡

資訊安全專區

跨域黑客

服務說明

...

首頁 / 資訊安全專區

組織架構

法令規範

四階文件

教育訓練

社交工程

文件下載

資訊安全政策

人員資訊安全守則

資訊安全維護情形

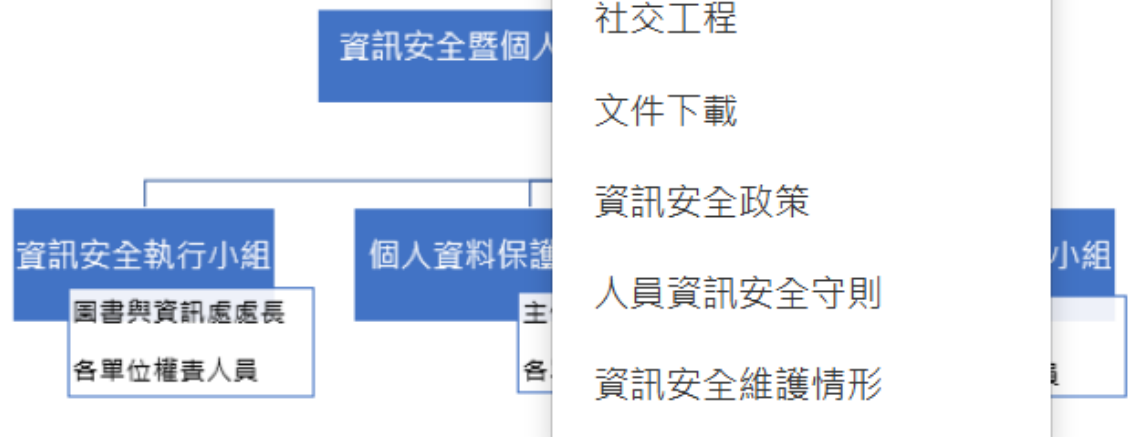


圖 1：資訊安全暨個人資料保護委員會

中華大學圖書與資訊處

Office of Library & Information Services
Chung Hua University

[關於圖資處](#)

[資訊服務](#)

[圖書服務](#)

[圖資服務卡](#)

[資訊安全專區](#)

[服務說明](#)

[首頁](#) / [資訊安全專區](#)

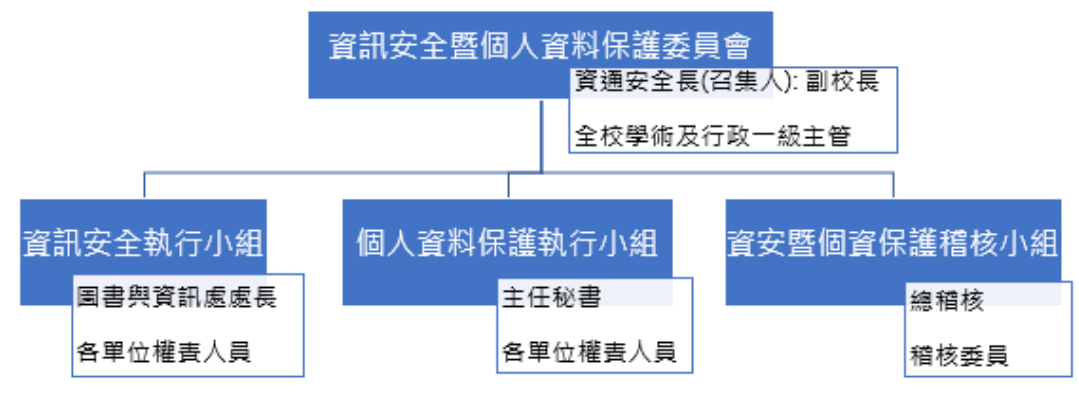


圖 1: 資訊安全暨個人資料保護委員會

[[2015_ISMS證書](#) | [2016_ISMS證書](#) | [2017_ISMS證書](#) | [2019_ISMS證書](#)]

[ISMS文件](#)

[一階文件](#)

[二階文件](#)

[三階文件](#)

[四階文件](#)

[相關文件](#)

[社交工程](#)

資訊安全管理制度四階文件

資訊安全專區

組織架構

法令規範

四階文件

教育訓練

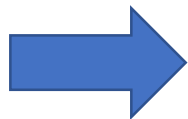
社交工程

文件下載

資訊安全政策

人員資訊安全守則

資訊安全維護情形



首頁 / 資訊安全專區 / 四階文件

一階文件

二階文件

三階文件

四階文件

CHU-ISMS-A-001_資訊安全政策_V5.2

CHU-ISMS-B-001_資訊安全組織程序書_V5.0

CHU-ISMS-B-002_文件管理程序書_V4.0

CHU-ISMS-B-003_資訊資產管理程序書_V4.1

CHU-ISMS-B-004_風險評鑑與管理程序書_V4.1

CHU-ISMS-B-005_人員安全與教育訓練程序書_V5.0

CHU-ISMS-B-006_實體安全管理程序書_V4.0

CHU-ISMS-B-007_通信與作業管理程序書_V4.1

CHU-ISMS-B-008_存取控制管理程序書_V4.1

CHU-ISMS-B-009_委外管理程序書_V5.0

CHU-ISMS-B-010_系統獲取、開發及維護程序書_V4.0

CHU-ISMS-B-011_安全事件管理程序書_V4.0

CHU-ISMS-B-012_業務永續運作管理程序書_V4.1

CHU-ISMS-B-013_資訊安全稽核作業程序書_V4.0

CHU-ISMS-B-014_矯正管理程序書_V4.0

CHU-ISMS-B-015_密碼控制管理程序書_V2.0

CHU-ISMS-C-001_人員資訊安全守則_V5.0

CHU-ISMS-C-002_業務永續運作計畫_V3.0

CHU-ISMS-C-003_關鍵業務障礙偵測與復原作業程序_V4.0

CHU-ISMS-C-004_資訊安全管理制度內部稽核計畫_V5.0

CHU-ISMS-C-005_資訊安全管理制度內部稽核報告_V4.0

CHU-ISMS-C-006_資訊資產異動作業說明書_V4.0

CHU-ISMS-C-007_日常操作管理作業說明書_V3.0

CHU-ISMS-D-001_資訊安全組織成員_V3.0	CHU-ISMS-D-002_外部單位聯絡清單_V1.0
CHU-ISMS-D-003_外來文件一覽表_V3.0	CHU-ISMS-D-004_ISMS有效性量測表_V3.3
CHU-ISMS-D-005_文件調閱申請單_V1.0	CHU-ISMS-D-006_文件修訂建議表_V1.0
CHU-ISMS-D-007_資訊安全管理文件列表_V1.3	CHU-ISMS-D-008_資訊資產清單_V5.1
CHU-ISMS-D-009_威脅及弱點評估表_V1.1	CHU-ISMS-D-010_風險評鑑彙整表_V3.1
CHU-ISMS-D-011_風險改善計畫表_V2.1	CHU-ISMS-D-012_適用性聲明書_V3.0
CHU-ISMS-D-013_保密切結書_V3.3	CHU-ISMS-D-015_人員離職異動移交流程表_V3.2
CHU-ISMS-D-016_教育訓練簽到表_V1.0	CHU-ISMS-D-017_資訊安全管理制度內部稽核自評表_V2.1

CHU-ISMS-D-018_人員進出機房登記表_V1.0

CHU-ISMS-D-019_設備進出紀錄表_V1.2

CHU-ISMS-D-020_機房環境例行性檢查紀錄表_V1.1

CHU-ISMS-D-021_異常事件紀錄表_V1.0

CHU-ISMS-D-022_委外廠商保密切結書_V3.3

CHU-ISMS-D-023_系統與網路檢查紀錄表_V1.6

CHU-ISMS-D-024_防火牆進出規則申請表_V1.0

CHU-ISMS-D-025_防火牆設定備份確認表_V1.0

CHU-ISMS-D-026_授權軟體使用清冊_V1.0

CHU-ISMS-D-029_備份狀況紀錄表_V2.0

CHU-ISMS-D-032_帳號申請表_V1.0

CHU-ISMS-D-033_帳號清查紀錄表_V1.0

CHU-ISMS-D-034_帳號清查結果報告_V1.1

CHU-ISMS-D-035_系統需求申請與回覆單_V1.0

CHU-ISMS-D-036_系統測試總表_V1.1

CHU-ISMS-D-037_系統測試報告_V2.0

CHU-ISMS-D-038_系統功能驗收表_V1.0

CHU-ISMS-D-039_系統作業流程圖_V1.0

CHU-ISMS-D-040_系統資料庫說明表_V1.1

CHU-ISMS-D-041_系統上線及緊急復原計畫表_V1.0

CHU-ISMS-D-042_系統程式碼清冊_V1.0

CHU-ISMS-D-043_資訊安全事件通報與應變作業流程_V2.0

CHU-ISMS-D-044_資訊安全事件報告單_V1.1

CHU-ISMS-D-045_業務永續運作計畫演練活動紀錄_V1.0

CHU-ISMS-D-046_業務流程衝擊分析表_V3.1

CHU-ISMS-D-047_資訊安全管理制度內部稽核表_V2.0

CHU-ISMS-D-048_矯正處理單_V2.0

CHU-ISMS-D-049_資訊資產異動申請表_V1.2

CHU-ISMS-D-051_弱點處理報告單_V1.0

CHU-ISMS-D-053_外部人員保密切結書_V2.3

CHU-ISMS-D-054_資訊安全管理制度內部稽核計畫表_V2.0

CHU-ISMS-D-055_資訊安全管理制度內部稽核報告單_V1.0

CHU-ISMS-D-056「000資通系統」安全等級評估表

CHU-ISMS-D-057_資訊系統清冊

CHU-ISMS-D-058_資通防護基準控制措施評估表_2

CHU-ISMS-D-059_資通系統或服務委外受託者查檢表

CHU-ISMS-D-060_委外廠商資訊安全自評表

CHU-ISMS-D-061_系統開發與維護安全檢核表

資訊安全專區

組織架構

法令規範

四階文件

教育訓練

社交工程

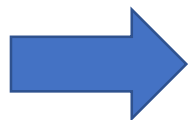
文件下載

文件下載

資訊安全政策

人員資訊安全守則

資訊安全維護情形



首頁 / 資訊安全專區 / 文件下載

資安宣導海報

資安宣導海報

原始檔案放置[雲端連結](#)，請各單位自行下載並張貼於可宣傳區域。

相關下載

單位網站遭竄改緊急應變原則

中華大學_資訊安全內部稽核基本項目查核表_v2.0

資通安全資訊資產清冊_填寫範例

資通安全資訊資產清冊_各欄位填寫內容說明

資訊安全(ISMS)團隊 - MS Teams

貼文區：提供團隊公告、互動討論

The screenshot displays the MS Teams application interface. On the left sidebar, the '資訊安全(ISMS)團隊' (Information Security (ISMS) Team) is selected. The main area shows the '貼文' (Posts) tab, which is highlighted with a red box. The chat history includes two messages from 陳俞儒 (Chen Yurou) dated 2023/12/8.

Message 1: 陳俞儒 2023/12/8 上午 11:05

12/11、12/12將進行資訊安全內部稽核(行政單位)，行政單位稽核時間可看檔案中的20231201的內部稽核計畫表，請資訊安全窗口備妥D-008_資訊資產單、D-013_保密切結書，若有委外系統者，需再備妥與廠商簽訂之合約書及D-022_委外廠商保密切結書、D-056_安全等級評估表、D-057_資訊系統清冊、D-058_資通防護基準控制措施評估表

Message 2: 陳俞儒 2023/12/8 上午 11:14

各單位資通安全及個人資料保護窗口已放入檔案中，若各單位有需更換資訊安全窗口請以公文E化通知圖資處陳俞儒小姐，以利將訊息傳達，謝謝。

資訊安全(ISMS)團隊 - MS Teams

共用(檔案): 提供檔案上傳、文件共享

The screenshot shows the MS Teams interface for the '資訊安全(ISMS)團隊' (Information Security (ISMS) Team). The left sidebar shows the team name and a '主要頻道' (Main Channel) section with a '一般' (General) channel. The main content area is the 'General' channel, which is currently displaying the '已共用' (Shared) tab. A red box highlights the '已共用' tab. Below the tab, a message states: '在 [共用] 索引標籤下，尋找此頻道中所有共用的內容，以及文件庫中的項目。' (Under the [Shared] tab, find all shared content in this channel, as well as items in the library.)

Below the message, there are two buttons: '在文件庫' (In Library) and '在文章中' (In Article). The '在文件庫' button is selected. The main content area shows a list of files in the 'General' group. A red box highlights the first item, a folder named '!資料上傳專區' (Information Security Upload Area). The list of files is as follows:

名稱	修改時間	修改者	標籤設定
!資料上傳專區	9月30日	陳俞儒	
20231019_公文通知_資訊安全教育訓練_各單位填寫資訊安全相關表單	23年12月8日	陳俞儒	
20231122_資安個資委員會會議資料	23年12月27日	林肯豐	
20231201_公文通知_資訊安全內部稽核通知	23年12月8日	陳俞儒	
20231201_公文通知_資訊安全教育訓練_內部稽核前準備工作及查檢...	23年12月8日	陳俞儒	
20231206_公文通知_資訊安全訊息宣導及提供宣導海報下載	23年12月8日	陳俞儒	
20231227-資安個資委員會會議資料	23年12月27日	古佳佳	
20240903_通知_資訊安全工作事項及資安窗口教育訓練	24年9月19日	陳俞儒	

資訊安全(ISMS)團隊 -MS Teams

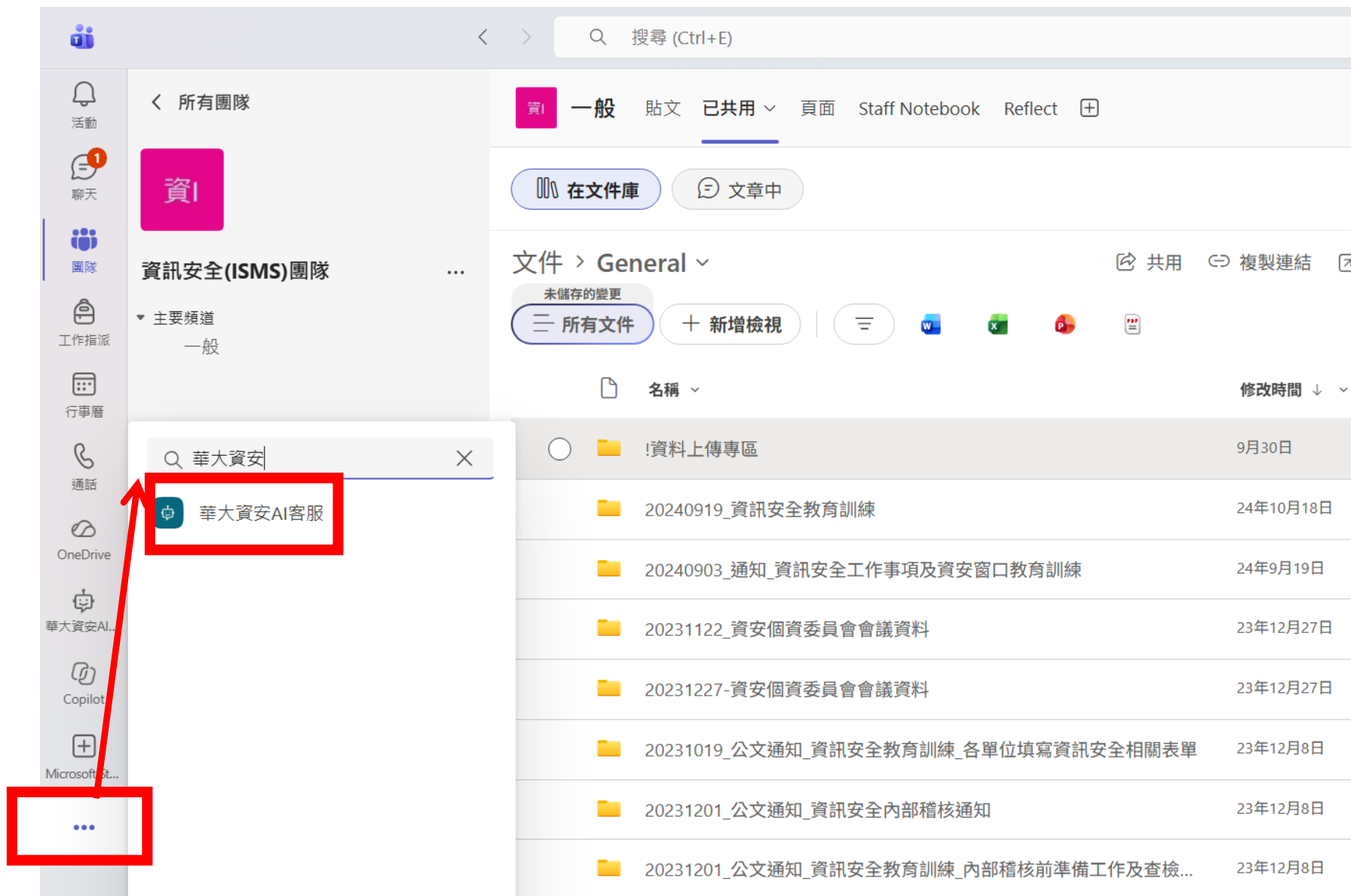
資料上傳專區: 放置各單位上傳的資料

資訊安全(ISMS)團隊

資料上傳專區

名稱	修改時間	修改者	標籤設定	新增欄
人文社會學院_人文社會學院進修學士班	9月30日	陳俞儒		
人文社會學院_行政管理學系	9月30日	陳俞儒		
人文社會學院_語言中心	9月30日	陳俞儒		
人文社會學院_應用日語學系	9月30日	陳俞儒		
人文社會學院_應用外語暨智慧商務學士學位學程	9月30日	陳俞儒		
人事室	9月30日	陳俞儒		
中華書院	10月1日	陳俞儒		
建築與設計學院	10月1日	陳俞儒		
建築與設計學院_土木工程學系	9月30日	陳俞儒		

華大資安AI 客服: 24小時提供資安問答



活動
聊天
團隊
工作指派
行事曆
通話
OneDrive
華大資安AI...
Copilot
Microsoft 365...

所有團隊

資訊安全(ISMS)團隊

主要頻道
一般

資訊

搜尋 (Ctrl+E)

一般 貼文 已共用 頁面 Staff Notebook Reflect

在文件庫 文章中

文件 > General

未儲存的變更

所有文件 新增檢視

名稱 修改時間

名稱	修改時間
!資料上傳專區	9月30日
20240919_資訊安全教育訓練	24年10月18日
20240903_通知_資訊安全工作事項及資安窗口教育訓練	24年9月19日
20231122_資安個資委員會會議資料	23年12月27日
20231227-資安個資委員會會議資料	23年12月27日
20231019_公文通知_資訊安全教育訓練_各單位填寫資訊安全相關表單	23年12月8日
20231201_公文通知_資訊安全內部稽核通知	23年12月8日
20231201_公文通知_資訊安全教育訓練_內部稽核前準備工作及查檢...	23年12月8日



華大資安AI客服

圖資處

新增

適用於

概觀 權限

中華大學 - 資訊安全AI客服

提供中華大學教職員本校資安相關規定諮詢

應用程式功能

Bot

使用提示完成工作、尋找資訊和聊天

建立者: [圖資處](#)

版本 1.0.3

權限

此應用程式將擁有下列權限:

- 接收我所提供給它的訊息與資料。
- 將訊息和通知傳送給我。



華大資安AI客服

成功新增!

您今天想如何使用此應用程式?

開啟

或選擇要使用應用程式的位置

搜尋頻道、聊天或會議

選取會議

[檢視更多](#)



2024中華大學-微軟Copilot研習



中華大學 生成式AI的教與學系列工作坊-Microsoft Copilot

華大資安AI 客服: 24小時提供資安問答



< > 🔍 搜尋 (Ctrl+E)

... 👤 中華大學 林

— 📄 ✕



活動



聊天



團隊



工作指派



行事曆



通話



OneDrive



華大資安AI...

...



應用程式



華大資安AI客服

聊天 已共用

...

1/5 下午 02:38

中華大學資訊安全要求的密碼原則為何?

華大資安AI客服 (AI 生成的) 1/5 下午 02:38



中華大學資訊安全要求的密碼原則如下：

1. 密碼最短使用期限：1天

2. 密碼最長使用期限：180天

3. 密碼必須符合複雜性要求：啟用

4. 強制密碼歷史：3次

5. 密碼長度最小值：8碼

這些原則旨在確保使用者的密碼具有足夠的安全性，防止未經授權的存取。若您需要設定或修改密碼，請依照上述原則進行。

AI-generated content may be incorrect

◎ 您對此次回答的評分？

★

★★

★★★

★★★★

★★★★★

1/5 下午 02:38

★★★★★

輸入訊息



活動

1

聊天

團隊

工作指派

行事曆

電話

OneDrive

Copilot

華大資安AI...

...

應用程式

華大資安AI客服

聊天 檔案

華大資安AI客服 下午 01:28

請問還有什麼可以為您服務的嗎？

下午 01:36

請問Windows 11如何設定密碼原則？

華大資安AI客服 AI生成時 下午 01:36

要在Windows 11中設定密碼原則，請按照以下步驟進行：

1. 開啟本機群組原則編輯器：

• 按下 **Win + R** 鍵，輸入 **gpedit.msc**，然後按下 **Enter** 鍵。

2. 導航至密碼原則設定：

• 在本機群組原則編輯器中，依次展開 **電腦設定** > **Windows 設定** > **安全設定** > **帳戶原則** > **密碼原則**。

3. 設定密碼原則：

• 在右側窗格中，您可以看到多個密碼相關的設定項目。根據本校的密碼原則，您需要設定以下項目：

• 密碼最短使用期限：雙擊 **密碼最短使用期限**，設定為 **1** 天。

• 密碼最長使用期限：雙擊 **密碼最長使用期限**，設定為 **180** 天。

• 密碼必須符合複雜性要求：雙擊 **密碼必須符合複雜性要求**，選擇 **已啟用**。

• 強制密碼歷史：雙擊 **強制密碼歷史**，設定為 **3** 次。

• 密碼長度最小值：雙擊 **密碼長度最小值**，設定為 **8** 碼。

4. 應用設定：

• 完成上述設定後，點擊 **確定** 或 **應用** 以保存變更。

5. 重新啟動電腦：

• 為確保設定生效，建議重新啟動電腦。

這樣就完成了在Windows 11中設定密碼原則的步驟。如果有任何問題或需要進一步的協助，請隨時告訴我。 AI-generated content may be incorrect

• 您對此次回答的評分？

★

★★

★★★

★★★★

★★★★★

下午 01:37

★★★★★

華大資安AI客服 下午 01:37

請問還有什麼可以為您服務的嗎？

輸入訊息

資通安全管理法- 教育體系之法遵說明

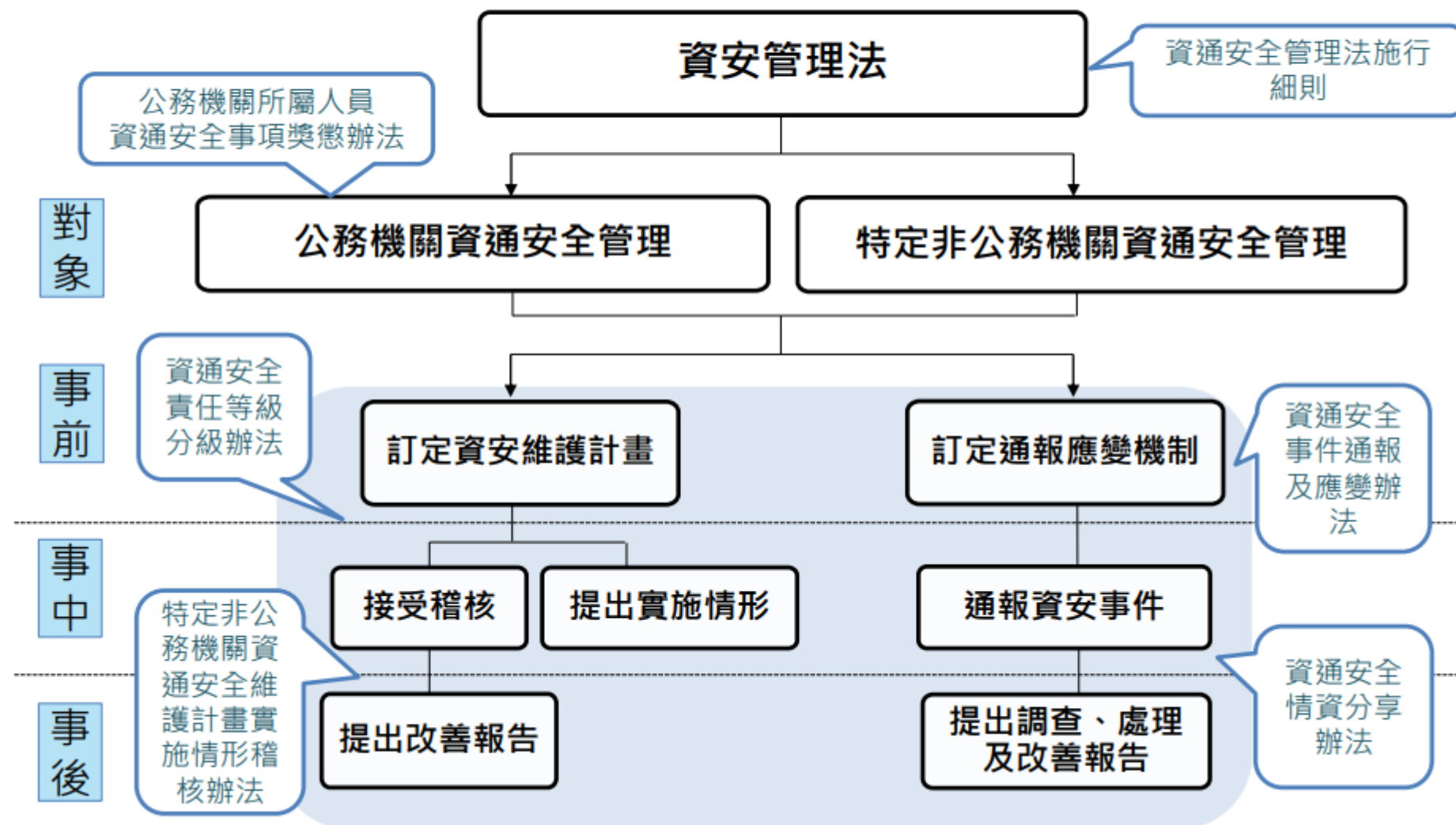


資通安全管理法

- 總統107年6月6日公布資通安全管理法。
- 行政院107年11月21日發布相關子法：
 - 資通安全管理法施行細則
 - 資通安全責任等級分級辦法
 - 資通安全事件通報及應變辦法
 - 特定非公務機關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
 - 公務機關所屬人員資通安全事項獎懲辦法
- 行政院107年12月05日函定自**108年1月1日施行**。



資通安全管理法架構



附表六 資通安全責任等級 C 級之特定非公務機關應辦事項修正規定

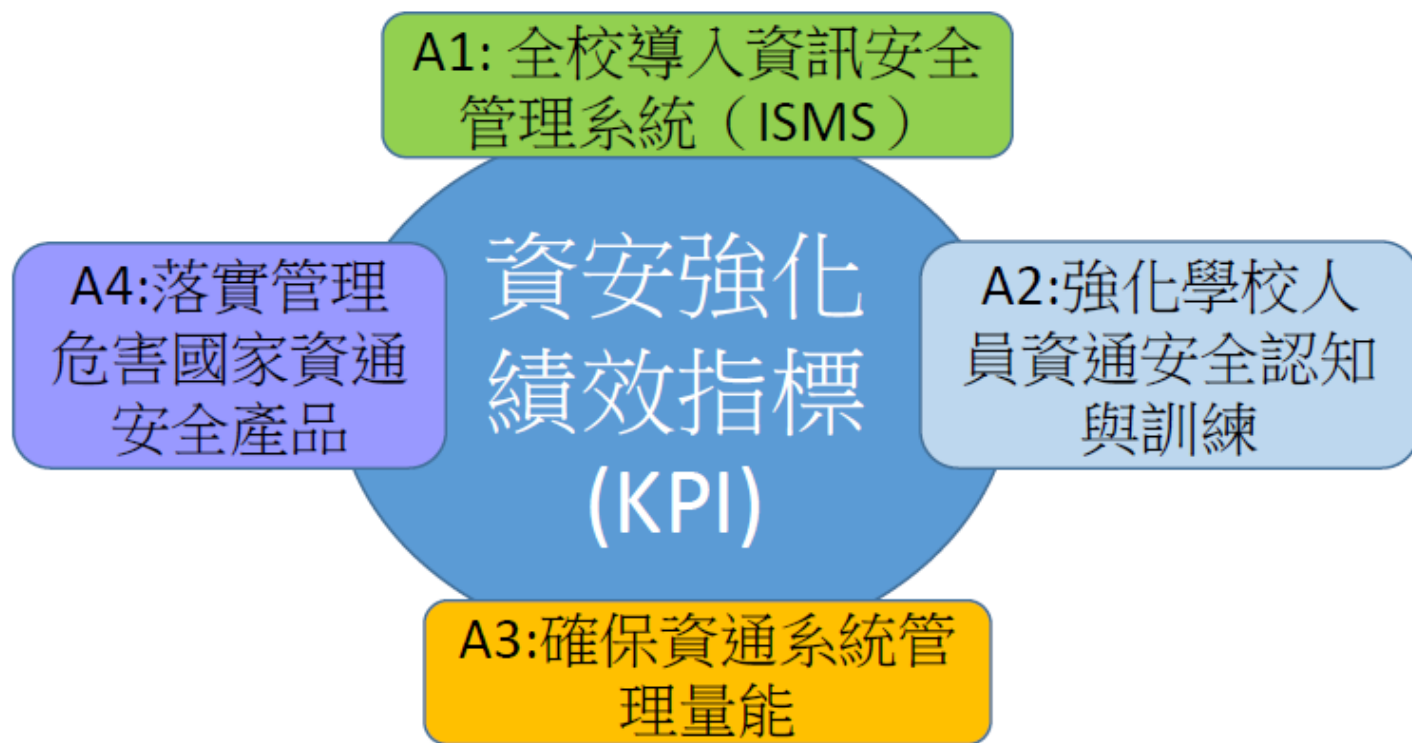
制度面向	辦理項目	辦理項目細項	辦理內容
管理面	資通系統分級及防護基準		初次受核定或等級變更後之一年內，針對自行或委外開發之資通系統，依附表九完成資通系統分級；其後應每年至少檢視一次資通系統分級妥適性；並應於初次受核定或等級變更後之二年內，完成附表十之控制措施。
	資訊安全管理系統之導入		初次受核定或等級變更後之二年內，全部核心資通系統導入 CNS 27001 或 ISO 27001 等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，並持續維持導入。

教育部高教深耕計劃 - 資安專章之要求



計畫專章撰寫建議方向

- 各校可參考數位發展部資通安全署「資通安全維護計畫範本」撰寫資安強化的各項指標(KPI)要求相關內容，並提供參考相關文件(例如:程序書或表單)





計畫專章撰寫建議方向

- 依本部訂定資安強化(績效指標)提供參考之績效指標(A1~A4)

A1: 全校導入資訊安全管理系統 (ISMS)

- K1.資通安全長之配置
- K2.資通安全推動組織
- K3.資通系統及資訊之盤點
- K4.資通安全風險評估
- K5.內部資通安全稽核及委外稽核
- K6.業務持續運作演練
- K7.資訊安全管理系統(ISMS)適用範圍

A2:強化學校人員資通安全認知與訓練

- K1.配置資通安全專職人員
- K2.提升資通安全專職人員資安職能
- K3.提升教職員資安意識

A3:確保資通系統管理量能

- K1.資通系統集中化管理
- K2.適度降低資通系統數量

A4:落實管理危害國家資通安全產品

- K1.禁止公務使用大陸廠牌資通訊產品
- K2.限制出租場域使用大陸廠牌資通訊產品

本校高教深耕計劃 - 資安專章規劃方案

1. 推動組織

本校設置「資訊安全暨個人資料保護委員會」作為資通安全推動組織(如圖 1)，由資通安全長召集全校學術及行政一級主管等組成，每年至少召開會議一次。本委員會下設「資訊安全執行小組」、「個人資料保護執行小組」及「資安暨個資保護稽核小組」。「資訊安全執行小組」統籌並執行各項資訊安全相關事宜，由圖書與資訊處處長擔任該小組執行秘書。「個人資料保護執行小組」統籌並執行各項個人資料保護相關事宜，由主任秘書擔任該小組執行秘書。「資安暨個資保護稽核小組」統籌各項資安暨個資保護稽核事宜，由本校總稽核擔任該小組執行秘書。各項資安暨個資保護作業與執行由本校各行政單位及教學單位推派人員擔任該小組成員或由執行秘書指定之。

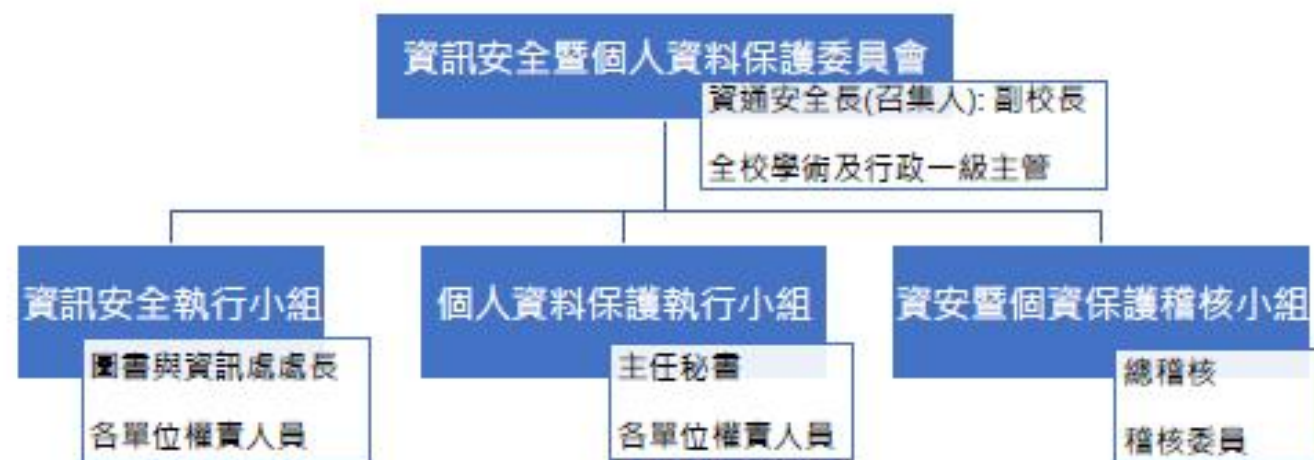


圖 1: 資訊安全暨個人資料保護委員會

2. 計畫架構

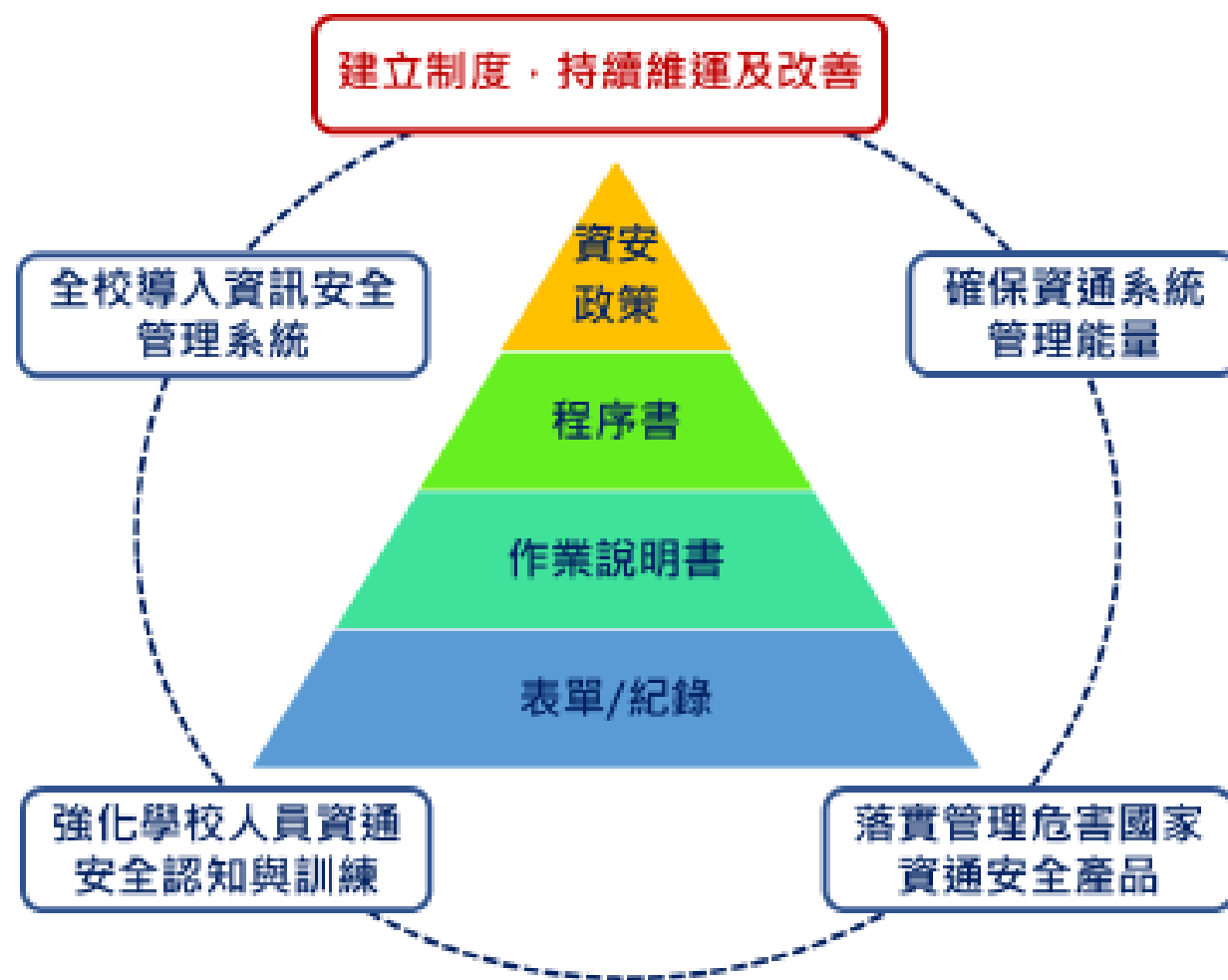


圖 2: 資訊安全強化計畫架構

全校導入資訊安全管理系統

資通安全長之配置：本校「[資訊安全暨個人資料保護委員會設置辦法](#)」，明訂由副校長擔任「資通安全長」，以落實推動及監督校內資通安全相關事務。

資通安全推動組織：本校設置「[資訊安全暨個人資料保護委員會](#)」作為資通安全推動組織，由資通安全長召集全校學術及行政一級主管等組成，每年至少召開會議一次，並得視業務推動之需要，不定期召開會議。

資訊及資通系統之盤點：

- ◆參照本校資訊安全管理系統(ISMS)「[CHU-ISMS-B-003_資訊資產管理程序書](#)」每年辦理資訊及資通系統資產盤點，各資訊資產權責單位應鑑別所管轄之資訊資產，並建立「資通系統資產清冊」，依管理責任指定對應之資產管理人，並依資產屬性進行分類，分別為：人員(People/PE)、文件(Document/DC)、軟體(Software/SW)、通訊(Communication/CM)、硬體(Hardware/HW)、資料(Data/DA)、環境 (Environment/EV) 等 7 類。
- ◆資訊及資通系統之盤點範圍包含全校各單位。每年提交之「[資通系統資產清冊](#)」包含落於本校 IP 網段內、或使用本校網域名稱之資通系統，「[物聯網設備管理清冊](#)」包含學校採購、公務使用之物聯網設備。
- ◆本校為私立大學，將依照「資通安全責任等級 C 級特定非公務機關應辦事項」之規定，針對全校自行或委外開發之資通系統，依資通系統防護需求分級原則完成資通系統分級，其後每年至少檢視一次資通系統分級妥適性，並完成資通系統防護基準之控制措施，依據教育體系資通安全暨個人資料管理規範，將全部核心資通系統導入資訊安全管理系統並持續維持導入。

資通安全風險評估：

- ◆參照本校資訊安全管理系統(ISMS)「[CHU-ISMS-B-004_風險評鑑與管理程序書](#)」，依據資通安全責任等級分級辦法之規定，分別就機密性、完整性、可用性、法律遵循性等構面評估資通系統防護需求分級，以該規定之分級結果，作為資通系統的風險評鑑等級。
- ◆依據前項資通安全風險評估結果、「資通安全責任等級 C 級特定非公務機關應辦事項」及核心資通系統之防護基準，選取適當安控措施，進行相關之防護及控制措施。

內部資通安全稽核及委外稽核：參照本校資訊安全管理系統(ISMS)「[CHU-ISMS-B-013_資訊安全稽核作業程序書](#)」，每年辦理內部資通安全稽核，稽核範圍除了本校以往已通過驗證之範圍：包含網路與資訊機房及部份核心資訊系統(人事室人事管理系統及教務處成績績管理系統)，再加以擴大至全校各單位。根據資通系統（保有個人資料）風險高低、教學單位特性評估，規劃辦理內部資通安全稽核及委外服務供應商之稽核，並明訂於資通安全維護計畫，稽核結果提交至資訊安全管理審查會議，確認資通安全維護計畫之實施情形，確保其持續適切性、合宜性及有效性並持續改善。

業務持續運作演練：參照本校資訊安全管理系統(ISMS)「[CHU-ISMS-B-012_業務永續運作管理程序書](#)」針對核心資通系統制定業務持續運作計畫，辦理核心資通系統之業務持續運作演練。

資訊安全管理系統(ISMS)適用範圍：盤點資訊及資通系統後，將資訊安全管理系統(ISMS)適用範圍擴大至全校範圍內之核心資通系統、保有個資或防護需求中等級以上之資通系統，及其相關網路與資訊機房活動。

強化學校人員資通安全認知與訓練

配置資通安全專職人員：本校圖書與資訊處已有 3 位通過 ISO27001 主導稽核員證照之資安專業人員，具備所須之專業職能，其中一位担任本校資安專責人員，除具備 ISO27001 主導稽核員專業證照之外，同時也擁有 CEH v11 證照。

提升資通安全專責人員及資訊人員資安職能：本校配合竹苗區網中心及相關單位開設之教育訓練課程，安排資通安全專責人員及資訊人員，參照本校資訊安全管理系統 (ISMS)「[CHU-ISMS-B-005_人員安全與教育訓練程序書](#)」，遵循「資通安全責任等級 C 級特定非公務機關應辦事項」之規定，每二年接受三小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受三小時以上之資通安全通識教育訓練。

提升教職員資安意識：規劃運用「e 等公務園+學習平臺」及「教育機構資安驗證中心數位課程」等線上課程，以及邀請資安專業人員來辦理相關教育訓練，並將資通安全通識教育訓練納入人事室每年要求全校職員工必須完成之教育訓練時數、另外也規劃於全校導師會議及行政主管會議的時段，安排全校教師及主管參與資安相關訓練，以達成全校教職員每人每年接受三小時以上之資通安全通識教育訓練。

確保資通系統管理能量

資通系統集中化管理：本校大部份校務資訊系統均由本校圖書與資訊處自行開發及維護管理，少部份外購的資通系統也是由圖書與資訊處資訊專業人員集中管理，剩餘少數由其它單位建置之資訊系統將造冊列管，協助進行安全防護設定及弱點掃描並加強內部稽核。

適度降低資通系統數量：本校網站採用內容管理平台(黑快馬公司之校園階層式網站平台)，可集中由圖書與資訊處資訊專業人員集中管理以降低自行架設網站伺服器及資通系統的數量。其餘少數因應臨時需求建置之網站將造冊列管，協助進行安全防護設定及弱點掃描並加強內部稽核，依其專案需求於預定之期限後下架或限制存取。

落實管理危害國家資通安全產品

禁止公務使用大陸廠牌資通訊產品：盤點全校資通訊產品（含軟體、硬體及服務）屬大陸廠牌者，列出清單造冊列管，協助進行安全防護設定，並於經費許可下儘速汰換。目前已知有少數無人機及小米手機為大陸廠牌之資通訊產品，將要求使用單位不得連接校內核心資訊系統及相關公務用途並儘速汰換。

限制出租場域使用大陸廠牌資通訊產品：於學校委外契約或場地租借使用規定，明訂不得使用危害國家資安之產品（如大陸廠牌軟體、硬體及服務），要求租用廠商盤點大陸廠牌資通訊設備，列出清單並儘速汰換。

資訊安全內部稽核準備事項

中華大學資訊安全內部稽核基本項目查核表

編號：

填表日期： 年 月 日

受稽單位名稱：

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
1.資通安全政策之推動及目標	1.1 同仁是否知道學校之資通安全政策、目標及應負之責任？	☐	☐	☐	
	1.2 同仁是否知道如何取得學校之資通安全四階文件？	☐	☐	☐	
2.資通安全推動組織	2.1 單位是否已指派人員作為單位內之資安窗口，負責辦理相關資通安全工作？	☐	☐	☐	
	2.2 同仁是否知道單位內之資安窗口人員姓名及聯絡方式？	☐	☐	☐	
3.資訊及資通系統之盤點及風險評估	3.1 是否建立資訊及資通系統資產清單，並每年維護更新？	☐	☐	☐	
	3.2 是否依資訊、資通系統分級與處理之相關規範，進行分級及防護基準評估？	☐	☐	☐	

4 資通安全管理措施之實施情況	4.1 是否定期執行作業系統更新及各項系統漏洞修補程式？	☐	☐	☐	
	4.2 是否全面使用防毒軟體並即時更新病毒碼？	☐	☐	☐	
	4.3 是否定期對電腦系統及資料儲存媒體進行病毒掃描？	☐	☐	☐	
	4.4 電腦是否設定螢幕保護程式並設定密碼保護，並將螢幕保護啟動時間設定為 15 分鐘以內？	☐	☐	☐	
	4.5 安裝之電腦軟體是否均有合法授權，符合智慧財產權相關規定？	☐	☐	☐	
	4.6 通行碼是否定期變更(至少每六個月一次)？	☐	☐	☐	
	4.7 通行碼長度是否超過 8 個字元以上？	☐	☐	☐	
	4.8 通行碼是否規定需有大小寫字母、數字及符號組成？	☐	☐	☐	
	4.9 對於敏感性、機密性資訊之傳送是否採取資料加密等保護措施？	☐	☐	☐	
	4.10 公文及儲存媒體在不使用或不在班時是否妥為存放？機密性、敏感性資訊是否妥為收存？	☐	☐	☐	
	4.11 重要的資料及軟體是否定期作備份處理？	☐	☐	☐	

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
	4.12 設備報廢前是否先將機密性、敏感性資料及版權軟體移除或覆寫？	☐	☐	☐	
5 資通安全事件通報及應變之程序及機制	5.1 同仁是否知悉資通安全事件通報應變程序並依規定辦理？	☐	☐	☐	
	5.2 同仁是否知悉本校資通安全事件發生之通報窗口？	☐	☐	☐	
6 資通安全認知宣導及教育訓練	6.1 同仁是否知悉「人員資訊安全守則」？	☐	☐	☐	
	6.2 同仁是否簽署「保密切結書」？	☐	☐	☐	
	6.3 同仁是否完成 3 小時資通安全通識教育訓練？	☐	☐	☐	
7 落實管理危害國家資通安全產品	7.1 針對公務用之資通訊產品，包含軟體、硬體及服務等，是否已禁止使用大陸廠牌資通訊產品？	☐	☐	☐	
	7.2 委外營運公眾場域之契約或場地使用規定是否已限制使用大陸廠牌資通訊產品？	☐	☐	☐	
8 資訊作業委外安全管理程序	7.3 是否依資訊作業委外安全管理程序，確保委外廠商執行委外作業時，具備完善之資通安全管理措施或通過第三方驗證？	☐	☐	☐	

資通安全政策之推動及目標

- 同仁應知道學校的資通安全政策、目標及應負之責任
- 同仁應知道如何取得學校之資通安全四階文件

lils.chu.edu.tw/p/412-1052-2773.php?Lang=zh-tw

學校首頁 新聞網 招生資訊 Language ▼ ▼

中華大學圖書與資訊處

Office of Library & Information Services
Chung Hua University

關於圖資處 資訊服務 圖書服務 圖資服務卡 服務說明

圖資長
業務職掌
樓層介紹
開放時間
空間介紹
政策文件與表單
資訊安全專區
圖資處活動行事曆
會議紀錄
聯絡我們

```
graph TD; A[資訊安全暨個人資料保護委員會] --> B[資訊安全長(召集人): 副校長]; A --> C[全校學術及行政一級主管]; A --> D[資訊安全執行小組]; A --> E[個人資料保護執行小組]; A --> F[資安暨個資保護稽核小組]; D --> G[圖書與資訊處處長]; D --> H[各單位權責人員]; E --> I[主任秘書]; E --> J[各單位權責人員]; F --> K[總稽核]; F --> L[稽核委員];
```

圖 1: 資訊安全暨個人資料保護委員會

[2015_ISMS證書 | 2016_ISMS證書 | 2017_ISMS證書 | 2019_ISMS證書]

ISMS文件 一階文件 二階文件 三階文件 四階文件 相關文件 社交工程

資通安全推動組織

- 單位應指派人員作為單位內之資安窗口，負責辦理相關資通安全工作
- 同仁應知道單位內之資安窗口人員姓名及聯絡方式

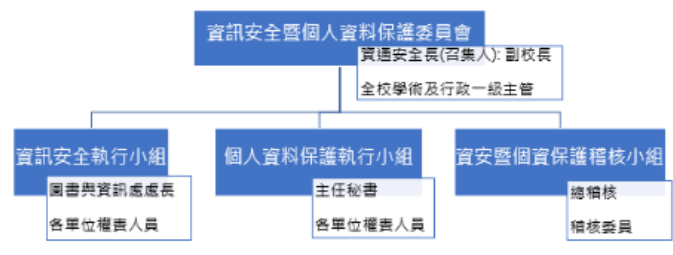
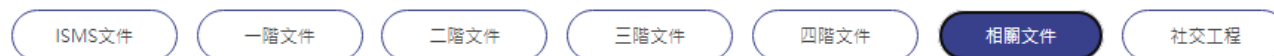


圖 1: 資訊安全暨個人資料保護委員會

[2015_ISMS鑑書 | 2016_ISMS鑑書 | 2017_ISMS鑑書 | 2019_ISMS鑑書]



【本校各單位資通安全保護聯絡窗口】

資訊及資通系統之盤點及風險評估

- 建立資訊及資通系統資產清單，並每年維護更新
- 依資訊、資通系統分級與處理之相關規範，進行分級及防護基準評估

ISMS文件

一階文件

二階文件

三階文件

四階文件

相關文件

社交工程

CHU-ISMS-B-001_資訊安全組織程序書_V4

CHU-ISMS-B-002_文件管理程序書_V4

CHU-ISMS-B-003_資訊資產管理程序書_V4

CHU-ISMS-B-004_風險評鑑與管理程序書_V4

ISMS文件

一階文件

二階文件

三階文件

四階文件

CHU-ISMS-D-008_資訊資產清單

CHU-ISMS-D-056_安全等級評估表

CHU-ISMS-D-057_資訊系統清冊

CHU-ISMS-D-058_資通防護基準控制措施評估表

資訊及資通系統之盤點及風險評估

- 建立資訊及資通系統資產清單，並每年維護更新
- 依資訊、資通系統分級與處理之相關規範，進行分級及防護基準評估

ISMS文件

一階文件

二階文件

三階文件

四階文件

相關文件

社交工程

【本校各單位資通安全保護聯絡窗口】

資通安全資訊資產清冊_各欄位填寫內容說明

資通安全資訊資產清冊_填寫範例

資通系統防護需求分級作業說明

資通系統防護需求分級_安全等級評估表_填寫範例

資通安全管理措施

- 定期執行作業系統更新及各項系統漏洞修補程式
 - 作業系統更新：Windows 10 , Windows 11, Linux , ...
 - 其它系統漏洞修補(包含自行安裝的應用程式)
 - 瀏覽器: Google Chrome , Microsoft Edge , FireFox ,...
 - 其它應用程式:
 - 如果有安裝 Adobe Reader 請定期更新
 - 如果有安裝 JAVA 請定期更新
 - 如果有安裝其它軟體，請定期更新

資通安全管理措施

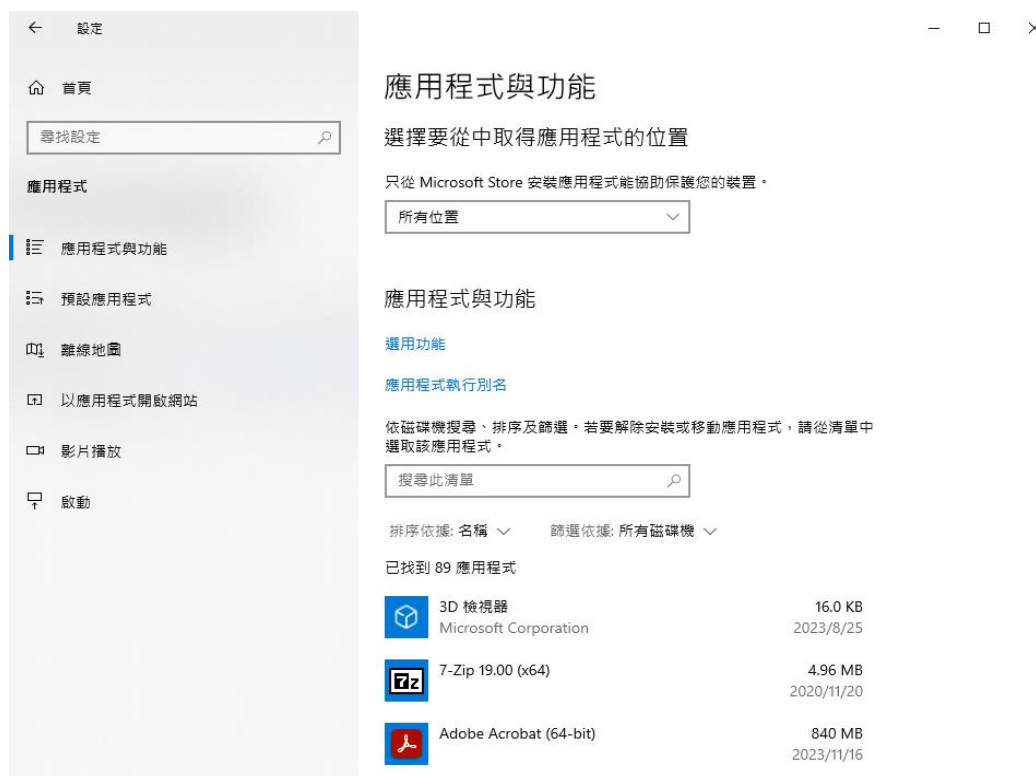
- 全面使用防毒軟體並即時更新病毒碼
- 定期對電腦系統及資料儲存媒體進行病毒掃描
 - 若有安裝Symantec 防毒軟體, 則作Symantec 更新及掃描,
 - 若未安裝則設定內建的Windows Defender 進行防毒更新及掃描

資通安全管理措施

- 電腦是否設定螢幕保護程式並設定密碼保護，並將螢幕保護啟動時間設定為**15**分鐘以內

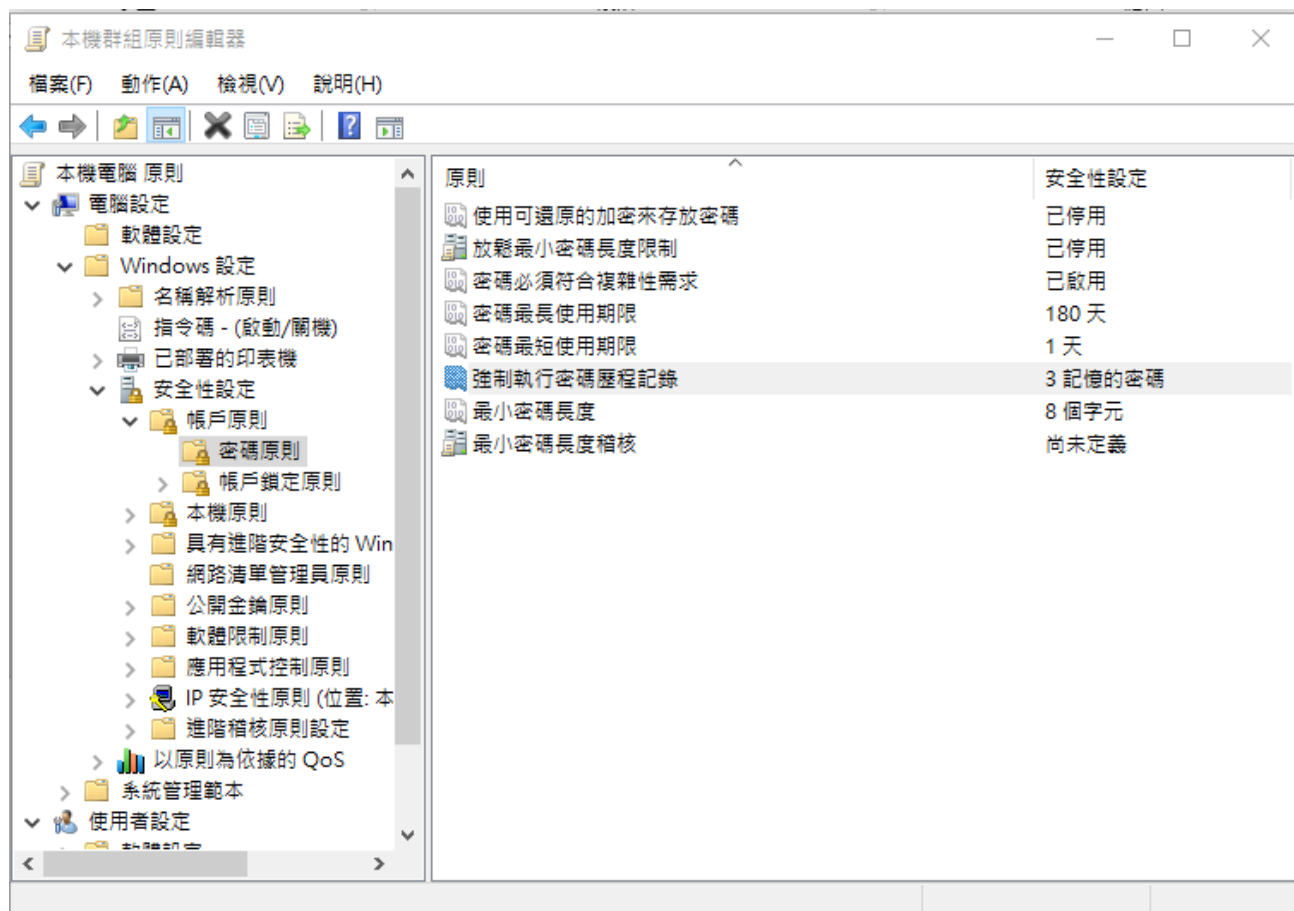
資通安全管理措施

- 安裝之電腦軟體是否均有合法授權，符合智慧財產權相關規定
 - 學校授權軟體下載: <https://download.chu.edu.tw>
 - 自行安裝非學校授權軟體，須取得合法授權證明



資通安全管理措施

- 通行碼是否定期變更(至少每六個月一次)
- 通行碼長度是否超過8個字元以上
- 通行碼是否規定需有大小寫字母、數字及符號組成



資通安全管理措施

- 通行碼是否定期變更(至少每六個月一次)
 - 作業系統密碼變更
 - 各類資訊系統密碼變更
 - 校務資訊系統(教職員系統/CHUMoodle/.... 等資訊系統之密碼)
 - 電子公文
 - 電子郵件
 - 物聯網設備密碼變更： 必須將廠商預設密碼變更為安全的密碼
 - 無線路由器(IP 分享器)
 - 網路多功能事務機/印表機
 - 網路攝影機

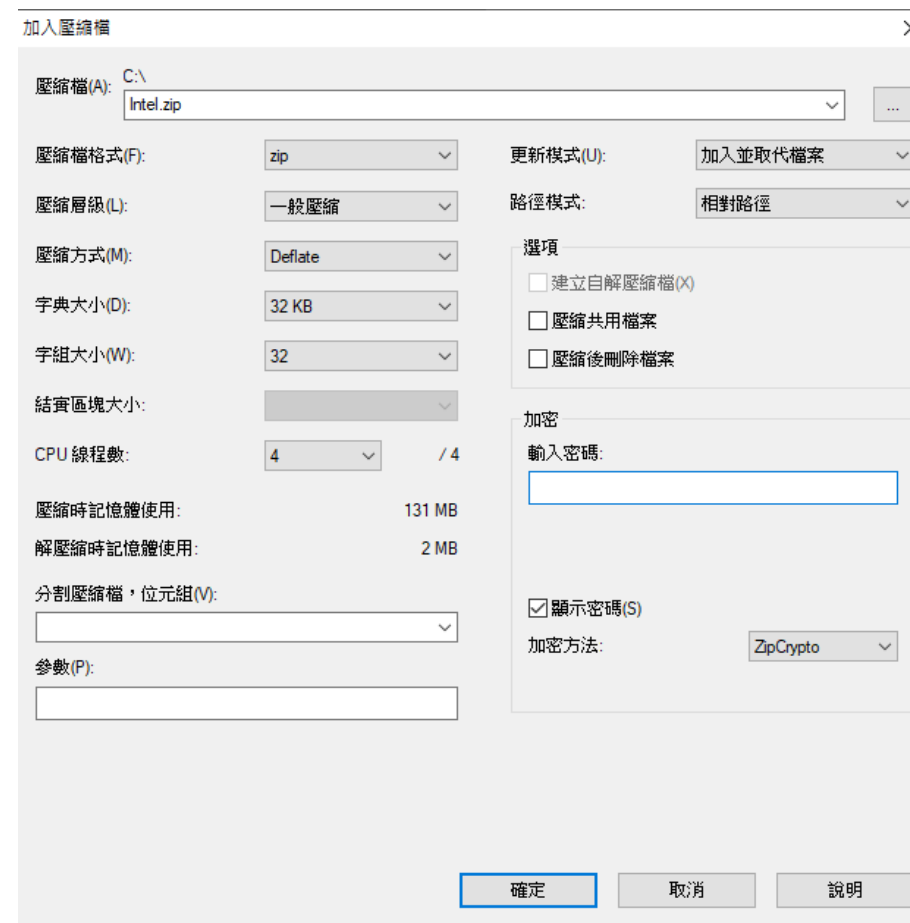
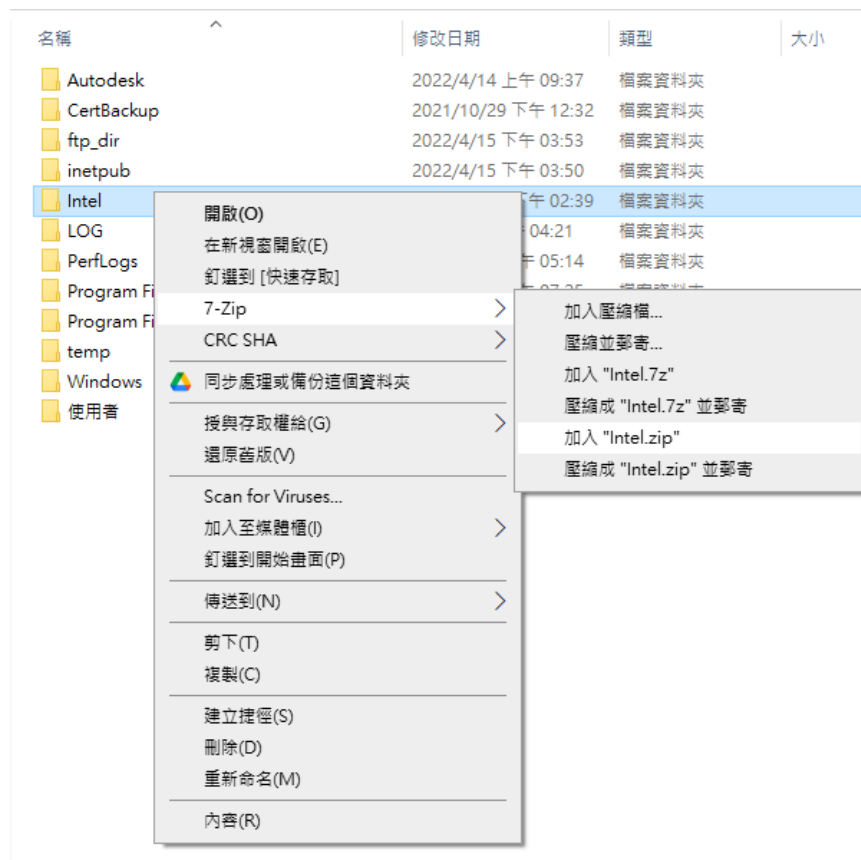
資通安全管理措施

- 對於敏感性、機密性資訊之傳送應採取資料加密等保護措施
 - Office 檔案(設定密碼)



資通安全管理措施

- 對於敏感性、機密性資訊之傳送應採取資料加密等保護措施
 - 將檔案加入有設定密碼的壓縮檔 (以免費軟體 7-zip 為例)

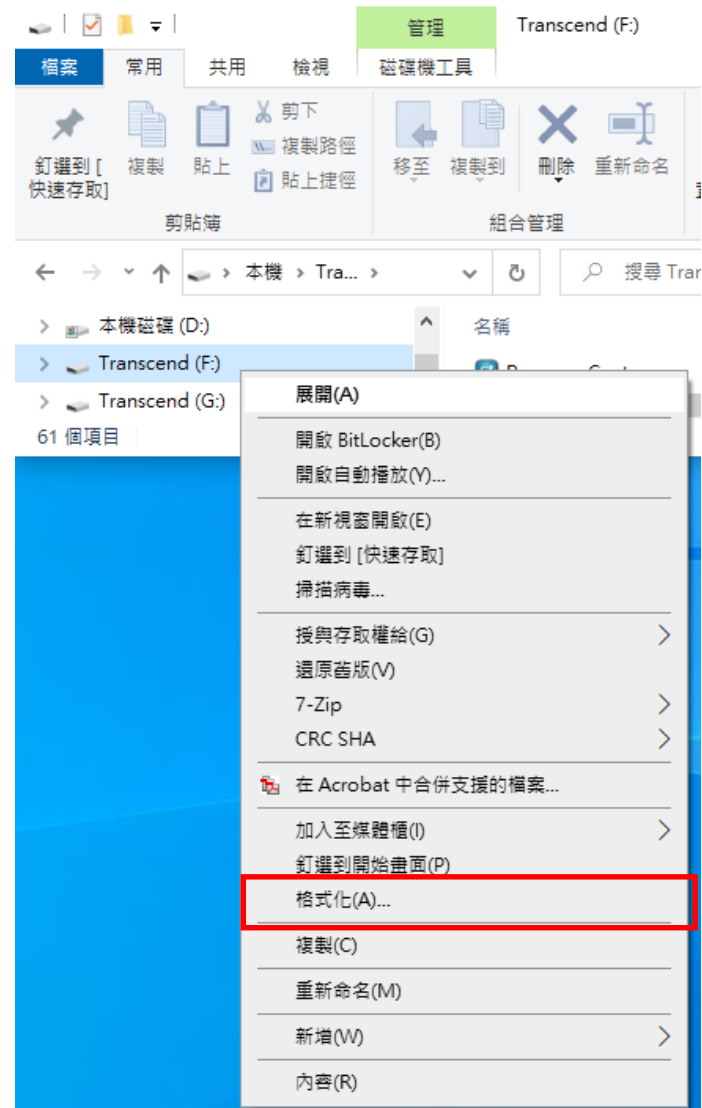
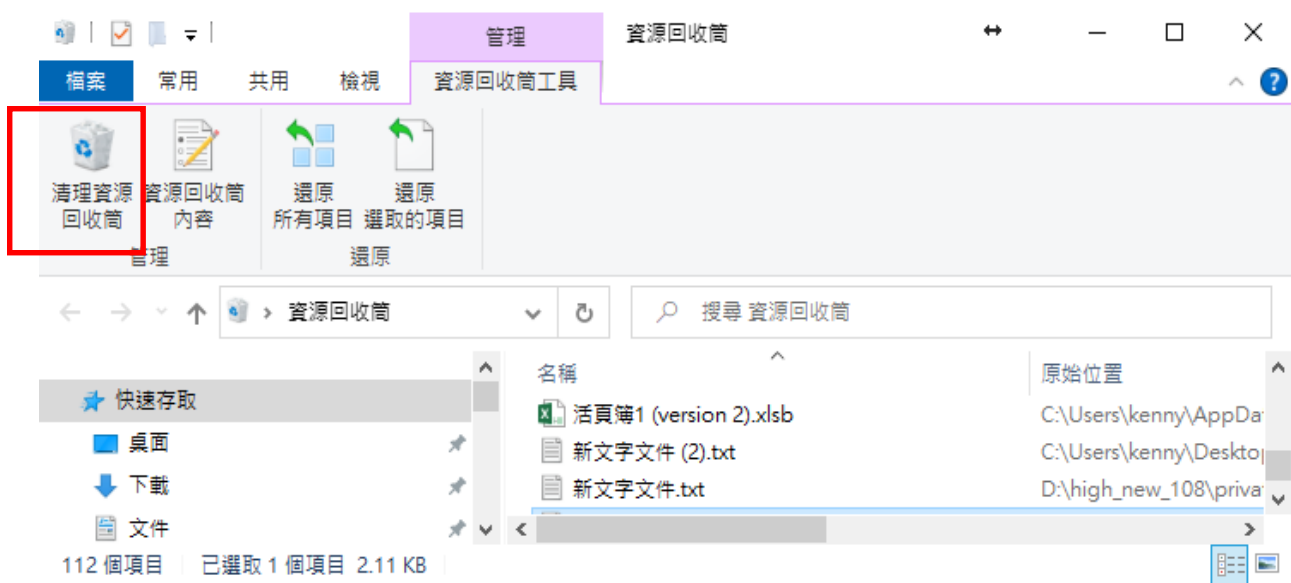


資通安全管理措施

- 公文及儲存媒體在不使用或不在班時應妥為存放(機密性、敏感性資訊應妥為收存)
- 重要的資料及軟體定期作備份處理

資通安全管理措施

- 設備報廢前先將機密性、敏感性資料及版權軟體移除或覆寫
 - 資料夾及檔案清除：
 - (1)將資料夾及檔案刪除並清空資源回收桶
 - (2) 鍵盤同時按下 **[Shift] + [Del]** 鍵 進行刪除
 - 整個硬碟清除：在磁碟機按**右鍵**選[格式化]



資通安全事件通報及應變之程序及機制

- 同仁應知悉資通安全事件通報應變程序並依規定辦理
- 同仁應知悉本校資通安全事件發生之通報窗口
 - 資通安全事件通報
 - 安全事件管理程序書（CHU-ISMS-B-011）
 - 資訊安全事件通報與應變作業流程（CHU-ISMS-D-043）
 - 資訊安全事件報告單（CHU-ISMS-D-044）
 - 資安事件：如單位網頁被置換、帳號被盜用、系統被駭、中毒、機敏資料外洩...
 - 資通安全事件發生之通報窗口：
 - 圖資處教學資源組 江先生(分機6233)

資通安全認知宣導及教育訓練

- 同仁應知悉「人員資訊安全守則」：CHU-ISMS-C-001_人員資訊安全守則
- 同仁應簽署「保密切結書」：CHU-ISMS-D-013_保密切結書
- 同仁應完成3小時資通安全通識教育訓練

教育部高教深耕計畫資安專章之指標要求，每人每年須完成3小時資訊安全通識課程教育訓練

115年度規劃課程如下：

資通安全(通識)【115年資訊安全教育訓練】：認證時數3小時

[e等公務園+學習平臺- 115年資訊安全教育訓練](#)

本課程由臺南市政府e學補給站上架至「e等公務園+學習平台」之開放課程，其中資安政策及部份訓練內容與本校略有差異處，補充說明如下：

1.本校資安政策公告於本校「資訊安全專區」網頁：

<https://x.chu.edu.tw/isms>

2.資訊安全事件通報流程：當發現資安事故或異常事件時，請向本校「圖資處教學資源組」通報。

3.校園授權軟體(含防毒軟體)：請至本校網站

<https://download.chu.edu.tw> 下載安裝。

4. QR Code及短網址管理：建議使用本校自行建置之短網址服務：

<https://x.chu.edu.tw>。

115年資訊安全教育訓練

報名期間：從 2026-01-01 到 2026-12-31

上課期間：從 2026-01-01 到 2026-12-31

資安海報張貼

與我共用 > 資安專章 > 資安宣導海報 ▾



類型 ▾ 使用者 ▾ 上次修改日期 ▾

檔案

↑ 上次修改時間 ▾



https://drive.google.com/drive/folders/1X6vdulMcPIFEAOZDGB7G_hQ3Nf6LXAWI

落實管理危害國家資通安全產品

- 針對公務用之資通訊產品，包含軟體、硬體及服務等，應禁止使用大陸廠牌資通訊產品
- 委外營運公眾場域之契約或場地使用規定應限制使用大陸廠牌資通訊產品
- 大陸品牌認定清單(參考來源 <https://pims.site.nthu.edu.tw/p/405-1095-219536,c18713.php?Lang=zh-tw>)
 - 海康威視(Hikvision),華為(Huawei),歐家控股(OPPO),小米(MI),海信
 - vivo,魅族,努比亞,大華技術(Dahua Technology),普聯（TP-Link）,
 - 大疆(DJI),REALME,TotoLink,Tenda,中興通訊,Foscam

資訊作業委外安全管理程序

- 依資訊作業委外安全管理程序，確保委外廠商執行委外作業時，具備完善之資通安全管理措施或通過第三方驗證
 - 委外管理程序書 (CHU-ISMS-B-009)
 - 委外廠商保密切結書 (CHU-ISMS-D-022)

參考連結

- 中興大學
- <https://sites.google.com/email.nchu.edu.tw/nchu-isms/%E6%95%99%E8%82%B2%E8%A8%93%E7%B7%B4>
- 成功大學
- <https://cc.ncku.edu.tw/p/412-1213-17354.php?Lang=zh-tw>