管理系統文件

文件類別	第 一 階 文 件
文件編號	IMS-1-001
文件名稱	資通安全與個人資料保護政策
發行單位	計算機與網路中心
發行日期	114 年 01 月 01 日
版次	1.9

定　　修　　廢　　記　　錄		
版次	發行日期	定 修 廢 內 容 摘 要
1.0	112.01.01	新制定文件
1.9	114.01.01	因應 ISO27001:2022 版本進行轉版，以及與個資政策合併(公告試行)

1. **目的**

為遵循資通安全管理法及其子法、個人資料保護法及其子法等相關法令法規要求，並確保國立臺中教育大學（以下簡稱本校）業務與資訊資產之機密性、完整性及可用性，保有之個人資料皆採取適當安全保護措施，避免因內外部議題，造成核心業務資料與個人資料被竊取、竄改、毀損、滅失、洩漏、不法利用或其他侵害等風險，特制訂資通安全與個人資料保護政策（以下簡稱本政策）。

2. **政策依據/參考標準**

2.1 資通安全管理法第十條及資通安全管理法施行細則第六條。

2.2 個人資料保護法（以下簡稱個資法）及其子法。

2.3 CNS 27001：2023 資訊安全管理系統國家標準。

2.4 CNS 27701：2020 隱私資訊管理系統國家標準。

2.5 ISO 27001：2022 資訊安全管理系統國際標準

2.6 ISO 27701：2019 隱私資訊管理系統國際標準

3. 適用範圍

本政策適用於本校全體同仁及其他得接觸、使用本校資通系統、服務、設備或公務資料之機關(構)、廠商、團體或個人。

4. 政策聲明

資通訊與個人資料是本校有價值的資產，為強調本校落實資通安全管控與善盡個人資料保護之責，特以簡單、容易記憶及符合資通安全與個人資料保護管理為原則，訂定本校之政策聲明為：「資通安全，人人有責」。

5. 管理組織

為落實本政策，本校成立「資通安全暨個人資料保護推動委員會」（以下簡稱委員會），統籌資訊安全管理制度（Information Security Management System，本校四階文件簡稱 ISMS）與個人資料管理制度（Personal Information Management System，本校四階文件簡稱 PIMS)之規劃及推動事宜，其組織架構詳如「IMS-2-003 資通安全及個人資料保護組織管理程序書」。

5.1 管理目標

5.1.1 為確保個人資料與資訊資產之機密性、完整性、可用性（CIA）及遵循性，目標分述如下：

5.1.1.1 機密性（Confidentiality）：不得發生機密資料或個人資料外洩情形。

5.1.1.2 完整性（Integrity）：確保保有之資訊內容正確與完整，避免使用錯誤。

5.1.1.3 可用性（Availability）：確保資訊資產能隨時提供使用。

5.1.1.4 遵循性（Compliance）：遵循資通安全與個人資料相關法令、

主管機關及上級機關要求。

5.1.2 為落實資通安全與個人資料管理目標評核，應依「IMS-2-003 資通安全及個人資料保護組織管理程序書」規定，訂定年度資通安全與個人資料管理具體指標及量測方法，經委員會管理審查會議通過後施行（詳如：IMS-2-004 資通安全及個人資料保護目標管理程序書）。

5.2 管理原則

5.2.1 資安防護原則

5.2.1.1 本校資通安全管理涵蓋 4 項管理事項，為避免因內外部議題，造成核心業務資料與個人資料被竊取、竄改、毀損、滅失、洩漏、不法利用或其他侵害等風險，管理事項為組織控制、人員控制、實體控制、技術控制。

5.2.1.2 資通系統應依「資通安全責任等級分級辦法」規定，資通系統分級及防護基準，於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（IMS-2-010-02 資通系統防護需求分級評估表）；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，完成附表十資通系統防護基準之控制措施（ISMS-2-006-06 資通系統防護基準表）。

5.2.1.3 資料及資通系統管理人應確保資訊資產已盤點造冊並評估 CIA 等級，且持續更新以確保其正確性。

5.2.1.4 使用本校之資料及資通系統，應確實遵守本校相關資通安全要求，且未經授權不得任意複製。

5.2.1.5 具機敏性之資料或具授權軟體之資通系統，宜採取實體銷毀，

或以毀損、刪除或覆寫之技術，使原始資料無法被讀取。

5.2.1.6 資通系統帳號註冊、異動或註銷，應依本校「ISMS-2-005 帳號密碼及存取控制管理程序書」規定申請並經核准後，系統管理者方可開通帳號權限，且應定期清查帳號權限。

5.2.1.7 資通系統應設置通行碼管理，通行碼設定原則需遵循「ISMS-2-005 帳號密碼及存取控制管理程序書」之要求。使用者應依「ISMS-2-004 網路安全管理程序書」規定之方式存取網路服務，不得於辦公室內私裝電腦及網路通訊等相關設備。

5.2.1.8 依據「ISMS-2-004 網路安全管理程序書」規定，機密或敏感電子資料，於儲存或傳輸時應進行加密保護。

5.2.1.9 依據「ISMS-3-001 一般資通設備安全管理作業標準書」規定，主機與個人電腦應安裝防毒軟體，並隨時進行軟、硬體之必要更新或升級。

5.2.1.10 依據「ISMS-2-003 實體與環境安全管理程序書」規定，資通設備應更新作業系統、應用程式漏洞修補及防毒病毒碼等。

5.2.2 個資保護管理原則

5.2.2.1 應建立負責辦理個人資料保護之管理組織，並訂定個資保護與管理措施。

5.2.2.2 應維護個資檔案清冊之正確性，識別內外部關注方，並考量相關法令法規及作業要求，進行個資之風險評估，採取適當安全維護措施，以確保善盡個資良善管理之責任。

5.2.2.3 應依個資法第 17 條規定，每年至少 1 次於蒐集完成建立或變更後，公告本校「保有個人資料檔案公開項目彙整表」。

5.2.2.4 基於合法蒐集最少之必要個資，非經當事人同意，所有個資不應逾越特定目的之必要範圍。

5.2.2.5 個資蒐集行為（含直接蒐集與間接蒐集），除個資法所列免告知情形外，應依個資法明確告知當事人；若為直接蒐集，亦須告知當事人不提供個資時對其權益之影響。

5.2.2.6 應識別法令法規之各項要求，確保合法處理個資。

5.2.2.7 因業務需求將個人資料提供予外部單位，應告知外部單位本校資通安全及個人資料保護政策（本文件），並要求其採取適當之安全措施，嚴謹處理相關個人資料。

5.2.2.8 個資存取權限之授予應考量業務需求之適當權限，實施職權區隔與獨立性審查。

5.2.2.9 個資之保留期限應符合法令法規要求或本校之業務週期需求，當蒐集之特定目的消失或保留期限屆滿時，應主動或依當事人之請求，刪除、停止處理或利用該個資。

5.2.2.10 因業務需求進行個資國際傳輸時，應考量主管機關之相關規範，並僅在對方有安全保護機制的狀況下，始傳遞出中華民國境外。

5.2.2.11 應建立維護當事人個資權利之作業程序，並提供適當申訴與抱怨之管道。

5.2.2.12 涉及個資業務之委外廠商應瞭解本校個人資料保護管理之要求，並遵循契約中規範雙方之責任與義務。

5.2.2.13 遇個資疑似遭竊取、洩漏、竄改或其他侵害時，應依相關事件管理程序（詳如：IMS-2-009 事件管理程序書），儘速通報並防止事件擴大，並於事後彙整相關資料，作為規劃預防及改

進措施之依據，以達到持續改善之目的。

5.2.3 管理文件體系

為落實資通安全與個人資料保護管理，應發展本校資通安全與個人資料文件體系，訂定政策、相關程序及管理規範等文件，並建立及保存資通安全與個人資料保護管理之各項紀錄。

5.2.4 定期宣導與檢討

5.2.4.1 本政策應以網站公告、書面、電子郵件或其他方式宣導，以提供個資蒐集處理利用或資通服務之單位共同遵行。

5.2.4.2 本政策每年應定期檢討評估 1 次，以符合政府法令、技術及業務等最新發展現況，確保資通安全與個人資料保護實務作業之可行性及有效性。

5.2.4.3 本政策經檢討評估後，當本校決定需要對資通安全與個人資料保護管理制度變更時，應考量整體性，並以專案規畫方式執行變更。

5.2.5 不定期宣導與審查

當本校面臨下列狀況時，應針對資通安全與個資保護政策進行檢討與審查。

5.2.5.1 適用法令、法規或標準發佈、異動或廢止。

5.2.5.2 本校營運策略發生重大變更。

5.2.5.3 利害相關人對資通安全與個人資料保護需求改變。

5.2.5.4 發生重大資通或個人資料安全事故。