國立臺北商業大學
National Taipei University of Business

資通安全暨個資保護政策

文件編號：A-A-01
使用範圍：一般

頒行日期：112 年 10 月 01 日

修 訂 紀 錄			
版次	修訂日期	主要修訂摘要	簽核人
1.0	112/10/1	新發行	資安長 黃焜煌
1.1	113/6/13	調整資安目標	資安長 黃焜煌
2.0	114/7/17	配合本年度所有資安與個資管理制度文件整體架構大改版，故版次直接升級大版次為 2.0。	資安長 黃焜煌

目錄

1. 目的

為遵循資通安全管理法及其子法、個人資料保護法（以下簡稱個資法）及施行細則等相關法令法規要求，並確保國立臺北商業大學（以下簡稱本校）業務與資訊資產之機密性、完整性及可用性，保有之個資皆採取適當安全保護措施，避免因內外部議題，造成核心業務資訊與個資被竊取、竄改、毀損、滅失、洩漏、不法利用或其他侵害等風險，特制訂資通安全暨個資保護政策（以下簡稱本政策）。

2. 適用範圍

本政策適用於本校全體同仁及其他會接觸本校資通系統、資通服務、設備或公務資訊之機關(構)、廠商、團體或個人。

3. 權責

本校全體同仁（本校教職員、與本校有雇傭關係之人員及與本校無雇傭關係之人員）及相關供應商與受託單位，均應遵守本政策之相關規定。

4. 管理組織

為落實本政策，本校成立資通安全暨個資保護管理委員會（以下簡稱本委員會），統籌資通安全暨個資保護管理制度之規劃及推動事宜，其組織架構請參考「A-B-01 組織管理程序」。

5. 管理目標

5.1 為確保資訊資產與個資之機密性、完整性、可用性及法律遵循性，目標分述如下：

5.1.1 機密性：不得發生機密資訊或個資外洩情形。

5.1.2 完整性：確保保有之資訊內容正確與完整，避免資訊使用錯誤。

5.1.3 可用性：核心系統執行正常運作，中斷次數不可超過績效指標定義之次數。

5.1.4 法律遵循性：遵循主管機關及資安暨個資保護相關法令要求。

5.2 為落實資安暨個資保護管理目標評核，應依「A-B-01 組織管理程序」規定，訂定年度資安暨個資保護管理具體指標及量測方法，經本委員會會議通過後施行。

6. 管理原則

6.1 資安防護原則

6.1.1 資通系統應依「資通安全責任等級分級辦法」附表九之規定完成系統防護需求分級，依分級之結果，完成附表十中資通系統防護基準要求。

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

6.1.3 使用本校之資訊及資通系統，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資訊。

6.1.4 具機敏性之資訊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，使原始資訊無法被讀取。

6.1.5 資通系統帳號註冊、異動或註銷，應依本校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。

6.1.6 資通系統應設置通行碼管理，使用者應依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。

6.1.7 機密或敏感電子資訊，於儲存或傳輸時應進行加密保護。

6.1.8 主機與個人電腦應安裝防毒軟體，並隨時進行軟、韌、硬體之必要更新或升級。

6.1.9 資通設備應定期更新作業系統、應用程式漏洞修補及病毒碼更新等。

6.1.10 依「各機關對危害國家資通安全產品限制使用原則」，公務用之資通訊產品（含軟體、硬體及服務）不得使用大陸廠牌，且不得安裝非授權軟體。

6.2 個資保護管理原則

6.2.1 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。

6.2.2 應維護個資檔案清冊之正確性，識別內外部利害關係人，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。

6.2.3 應依個資法第 17 條規定，每年或不定期於蒐集完成建立或變更後，公告本校保有個資檔案公開項目。

6.2.4 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。

6.2.5 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。

6.2.6 應識別法令法規之各項要求，確保合法處理個資。

6.2.7 因業務需求將個資提供予外部單位，應告知外部單位本政策，並要求其採取適當之安全措施，嚴謹處理相關個人資訊。

6.2.8 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。

6.2.9 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。

6.2.10 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。

6.2.11 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。

6.2.12 涉及個資業務之委外廠商應瞭解本政策之要求，並遵循契約中規範雙方之責任與義務。

6.2.13 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，儘速通報並防止事件擴大，並於事後彙整相關資訊，作為規劃預防及改進措施之依據，以達到持續改善之目的。

7. 管理文件體系

為落實本政策，應發展本校資安暨個資保護文件體系，訂定與本政策相關之程序及管理規範等文件，並建立及維持資安暨個資保護管理之各項紀錄。

8. 實施

8.1 本政策應以網站公告、書面、電子郵件或其他方式宣導，以提供資通安全施作及個資之蒐集、處理、利用之單位共同遵行。

8.2 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，確保資安暨個資保護實務作業之可行性及有效性。