



國立臺灣科技大學電子計算機中心

資訊安全政策

文件編號：NTUST-IS-A-01

機密等級：公開使用

版 次：1.1

發行日期：102.10.25

目 錄

1 目的.....	1
2 範圍.....	1
3 資訊安全目標.....	1
4 資訊安全要求事項.....	1
5 審查與宣導.....	2
6 施行.....	2

1 目的

本政策遵循本校「國立臺灣科技大學資訊安全政策」，規範國立臺灣科技大學電子計算機中心（以下簡稱「本中心」）資訊安全管理制度，以確保本中心所管理資訊資產之機密性、完整性、可用性及符合相關法規之要求，進而保障全校教職員工生之權益。

2 範圍

本中心教職員工生、接觸本中心業務資料之外機關人員、委外服務提供廠商人員及訪客均適用之。

3 資訊安全目標

3.1 本中心之資訊安全政策包含下列目標：

- 3.1.1 確保本中心所保管校務資料之機密性、完整性與可用性，防止非法使用校務資料。
- 3.1.2 確保本中心所提供資訊服務之完整性與可用性，提供全校師生便利和穩定的資訊服務。
- 3.1.3 確保本中心所提供軟硬體資源之可用性，合法及正確地使用。

4 資訊安全要求事項

- 4.1 確實遵守「個人資料保護法」、「著作權法」、「**電子簽章法**」等資訊安全相關法令。
- 4.2 為能有效確保本中心之資訊安全，應針對各資訊安全領域訂定資訊安全規範。
- 4.3 確實遵守本中心相關資訊安全規定，確保適當使用本中心資源。
- 4.4 遵循本中心資安事件通報機制，通報所發現之資訊安全事件或資訊安全弱點。
- 4.5 對於資訊安全事件須有完整的通報及應變措施，以確保資訊系統及重要業務的持續運作。
- 4.6 進行資訊處理時，若含有個人資料，應依據「個人資料保護法」及相關規定審慎處理，不私自蒐集或洩漏業務資訊，非公務用途嚴禁調閱使用。
- 4.7 領取使用者代碼後應立即自行設定密碼，密碼長度至少應有 7 位數字元組成；密碼複雜度設定至少需由英文、數字或特殊符號的其中二個組成；個人電腦及主機或網路設備之密碼至少 6 個月須更換一次；使用者不得將自己的使用者代碼與密碼交付他人使用。
- 4.8 本中心主管應積極參與資訊安全管理活動，提供對資訊安全之支持及承諾。
- 4.9 依角色及職能為基礎，針對不同層級人員，依據「行政院國家資通安全會報」之規定或實際需要辦理資訊安全教育訓練及宣導，促使全體人員瞭解資訊安全的重要性，各種可能的安全風險，以提高資訊安全意識並熟悉工作中之資訊安全職責，促其遵守資

訊安全規定。

- 4.10 應使用具合法版權軟體，避免上網下載來路不明之軟體。
- 4.11 委外廠商應遵循本政策以及相關程序之規定，不得未經授權使用或濫用本中心之各類資訊資產，若涉及限制使用等級以上業務，應簽署保密切結書。
- 4.12 每年至少召開一次管理審查會議，審核本中心資訊安全業務執行狀況，建立管理指標量測方式與評估管理指標量測結果。
- 4.13 應建立資訊資產風險評鑑機制，每年至少進行一次風險評鑑，並由中心主任決定可接受風險值。
- 4.14 每年應至少進行一次業務永續經營計畫及資安事件通報程序之演練、測試、檢討。
- 4.15 違反本政策與本校之資訊安全相關規範，依相關法規或本校懲戒規定辦理。

5 審查與宣導

- 5.1 為確保資訊安全管理制度實務運作之可用性、安全性及有效性。本政策應每年依業務變動、技術發展及風險評鑑的結果或配合政府資訊安全管理要求、法令、技術及最新業務發展現況至少評估或修訂一次。
- 5.2 本政策得以書面、電子郵件（E-MAIL）、公告於網站、或其他方式公告周知。
- 5.3 本政策經資訊安全長核可後施行，修正時亦同。