國立臺灣大學

教務處 數位學習中心

資訊安全政策

文件編號：1-01-01

版次：1.0

修訂紀錄

版本	修訂日期	修訂頁次	修訂單位	修訂類別				修訂摘要
				增訂作業項目	刪除作業項目	修正控制重點	其他修訂	
1.0								

目錄

壹、 目的

鑑於資訊安全為數位學習中心各項服務安全運作之基礎，為確保臺灣大學教務處之數位學習中心之教學科技組（以下簡稱本單位）所維運之 NTU COOL 平台（以下簡稱數位學習平台或本平台）其相關資訊系統、設備、網路、資料、及相關維運人員之安全，特訂定資訊安全政策（以下簡稱本文件），作為本單位資訊安全管理系統的指導原則。

貳、 目標

本單位資訊安全目標為確保本平台各項服務之機密性(Confidentiality)、完整性(Integrity)、與可用性(Availability)，除遵循臺灣大學之資訊安全目標外，訂定下列資訊安全目標：

一、符合政府法令及上級單位之要求。

二、確保本平台資料之機密性與完整性。

三、確保本平台之可用性。

本單位將訂定系統安全強化標準，並定期定義及量測資訊安全之量測指標，以確認資訊安全管理系統是否達成資訊安全目標。

參、 適用範圍

本單位之數位學習平台，包含實體環境、軟硬體設備、營運資料、管理單位及相關作業流程。

肆、 資訊安全管理系統運作機制

一、資訊安全管理系統運作機制

（一） 計畫 (Plan)

建置風險管理制度，並對影響資訊資產安全之弱點、威脅、及現行控管機制進行風險評估。

（二） 建置 (Do)

依據 ISO27001 的要求，依據風險評估之結果並考量成本效益後，設計、建置/修改、及執行資訊安全控制機制。

（三） 稽核 (Check)

定期或不定期實施資訊安全自行查核，以確保落實資訊安全管理。

（四） 檢討改善 (Act)

根據稽核之結果，執行矯正措施，修改及執行資訊安全控制機制。

二、管理階層責任

管理階層應確保完成下述工作，以表示對資訊安全管理系統之充分支持：

（一） 審查與訂定資訊安全管理系統之相關規範。

（二） 建立資訊安全指標。

（三） 指派資訊安全之執掌與權責。

（四） 宣導遵守本資訊安全政策與法令規定、達成資訊安全指標、及檢討改善之重要性。

（五） 提供資訊安全管理系統之各項作業所需之資源。

（六） 決定風險可接受水準。

（七） 執行資訊安全管理系統之管理審查作業。

（八） 建立與維護資訊安全管理系統，並維持其有效性。

（九） 定期與不定期檢視確認本資訊安全政策與相關管理規範、作業程序符合本單位之營運需求與資安目標。

（十） 確保參與資訊安全管理系統之相關作業之所有人員均具備工作所需之相關職能。

三、文件及紀錄管理要求

資訊安全文件之發行、變更、與管制皆應設計管制機制，資訊安全管理系統運作所產生之表單與紀錄，應指派相關記錄保管人妥善保管，並訂定保存期限與閱覽權限，另應定期追蹤制度執行狀況，以維護管理系統之有效

運作。

四、資訊安全管理系統之稽核

應定期或不定期進行資訊安全管理系統之評估與稽核作業，以評估資訊安全目標、資訊安全政策與相關管理規範、作業程序是否合乎相關標準、法令規定或資訊安全需求，並依規劃落實與有效執行，以持續確保資訊安全管理系統之有效性。

五、矯正措施

稽核所發現之事項，應透過矯正措施採取適當之管控措施，以降低資訊安全管理系統運作過程中不符合資訊安全政策與相關管理規範之情形，並採取控管措施防止不符合事項之再度發生。

六、資訊安全管理體系之管理審查

應落實管理審查制度，以確保資訊安全管理系統與相關制度之持續運作適用性、適切性與有效性。資訊安全管理小組應定期召開會議討論ISO27001與相關規範所要求之審查輸入項目，並產生審查輸出項目。

七、本資訊安全政策應每年至少評估一次，或於重大環境變更時執行變更評估，以有效反應政府法令規範、資訊技術與平台運作環境等最新狀況，確保資訊安全管理系統之有效性。

八、資訊安全目標應每年定期檢視其適切性，並應涵蓋機密性(Confidentiality)、完整性(Integrity)、與可用性(Availability)等目標，以滿足資訊安全政策之要求。

九、本資訊安全政策經資訊安全管理小組核定後實施，修正時亦同。