附件1

資通安全政策					
文件編號	HSNU-ISMS-A-001	機密等級	一般	版次	1.0

1 目的

為確保國立臺灣師範大學附屬高級中學（以下簡稱本校）所屬之資通資產的機密性、完整性、可用性及法律遵循性，導入資訊安全管理系統，強化本校資通安全管理，保護資通資產免於遭受內、外部蓄意或意外之威脅，維護資料、系統、設備及網路之安全，提供可靠之資訊服務，訂定本政策。

2 依據

2.1資通安全管理法及子法

2.2個人資料保護法及施行細則

2.3教育體系資通安全暨個人資料管理規範

3 適用範圍

3.1本政策適用範圍為本校之全體人員、委外服務廠商與訪客等。

3.2資通安全管理範疇涵蓋14項領域，避免因人為疏失、蓄意或天然災害等因素，導致資料不當使用、洩漏、竄改、破壞等情事發生，對本校造成各種可能之風險及危害，各領域分述如下：

3.2.1 資通安全政策訂定與評估。

3.2.2 資通安全組織。

3.2.3 人力資源安全。

3.2.4 資產管理。

3.2.5 存取控制。

3.2.6 密碼學(加密控制)。

3.2.7 實體及環境安全。

3.2.8 運作安全。

3.2.9 通訊安全。

3.2.10 系統獲取、開發及維護。

3.2.11 供應者關係。

3.2.12 資通安全事故管理。

3.2.13 營運持續管理之資通安全層面。

3.2.14 法律遵循性。

4 目標

維護本校資通資產之機密性、完整性與可用性，並保障使用者資料隱私。藉由本校全體同仁共同努力來達成下列定性及定量目標：

4.1定性目標：

4.1.1符合政府資通安全相關政策、規定及相關法令要求。

4.1.2適時因應法令與技術之變動，調整資通安全維護之內容，以避免資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性、完整性及可用性。

4.2定量目標：

4.2.1防範惡意電子郵件進行社交工程演練，訂定社交工程郵件開啟率、社交工程郵件點閱率、社交工程郵件附件開啟率。

4.2.2實施資通安全教育訓練。

4.2.3針對非核心且對外服務之資通系統，每年辦理一次備份資料回復測試紀錄（附件12）。

4.3本校完成指標時，考量下列項目：

4.3.1所需配置之人員、預算、設備技術與程序表單。

4.3.2活動或事項負責人員。

4.3.3活動或事項預計完成時間。

4.3.4管理目標是否達成之評估方式。

5 責任

5.1本校依據資通安全組織成立資通安全委員，統籌資通安全事項推動。

5.2 管理階層應積極參與及支持資通安全管理，並授權資通安全組織透過適當的標準和程序以實施本政策。

5.3本校全體人員、委外服務廠商與訪客等皆應遵守相關安全管理程序以維護本政策。

5.4本校全體人員及委外服務廠商均有責任透過適當通報機制，通報資通安全事件或弱點。

5.5任何危及資通安全之行為，將視情節輕重追究其民事、刑事及行政責任或依據本校之相關規定進行議處。

6 審查

本政策應每年至少審查一次，以反映政府法令、技術及業務等最新發展現況及關注方之關注議題，以確保本校資通安全管理運作。

7 實施

本政策經「資通安全委員會」核定後實施，修訂時亦同。