國立中央大學附屬中壢高級中學

資通安全政策

機密等級：一般

文件編號：CLHS-A-001

版 次：1.1

發行日期：113.10.01

修 訂 紀 錄				
版次	修訂日期	修訂頁次	修訂者	修訂內容摘要

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

目　錄

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

1 目的

為確保國立中央大學附屬中壢高級中學（以下簡稱本校）所屬之資訊資產的機密性、完整性、可用性及符合相關法規之要求，免於遭受內、外部蓄意或意外之威脅，訂定本政策。

2 依據

2.1 資通安全法(及施行細則)

2.2 個人資料保護法（及施行細則）

2.3 行政院及所屬各機關資訊安全管理要點

2.4 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 資訊安全管理範疇涵蓋 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 資訊安全政策訂定與評估。

3.2.2 資訊安全組織。

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 資訊安全事故管理。

3.2.13 營運持續管理之資訊安全層面。

3.2.14 遵循性。

4 目標

維護本校資訊資產之機密性、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 定期審查本校資通安全組織人員執掌，以確保資通安全工作之推展。

4.1.2 應加強本校網管機房設施之環境安全，採取適當之保護及權限控管機制。

4.1.3 應加強存取控制，防止未經授權之不當存取，以確保本校資通資產受適當的保護。

4.1.4 確保資訊不會在傳遞過程中，或因無意間的行為透露給未經授權的第三者。

4.1.5 確保所有資通安全意外事故或可疑之安全弱點，都依循適當之通報機制向上反應，並予以適當調查及處理。

4.2 定量目標：

4.2.1 確保資訊資產受適當之保護，每年未經授權或因作業疏失導致之資安事故，每年不得超過 3 件。

4.2.2 確保本校機房維運服務達全年上班時間 90%(含)以上之可用性。

4.2.3 確保滿足各關鍵業務系統之服務可用率達全年上班時間之 90%(含)以上。

4.2.4 本校每人每年接受三小時以上之一般資通安全教育訓練比例達 90%以上。

5 責任

5.1 本校應成立資訊安全組織統籌資訊安全事項推動。

5.2 管理階層應積極參與及支持資訊安全管理制度，並授權資訊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，通報資訊安全事件或弱點。

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

6 審查

本政策應每年至少審查乙次，以反映政府法令、技術及業務等最新發展現況，以確保永續運作及提供學術網路服務之能力。

7 實施

本政策經「資通安全委員會」核定後實施，修訂時亦同。