

國立彰化高級中學資訊安全管理政策

111.10.17資通安全管理審查會議通過

文件機密等級：一般

1 目的

為確保國立彰化高級中學（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，導入資訊安全管理系統，強化本校資訊安全管理，保護資訊資產免於遭受內、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，避免因人為疏忽、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 確保相關資通安全措施或規範符合政策與現行法令的要求每二年至少進行一次內部稽核。
- 4.1.2 每年至少進行一次業務持續計畫之測試或檢核。

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對資產所造成的損害 0 件。
- 4.2.2 確保所有資通安全事件或可疑之安全弱點，每年不依適當通報程序反應，並予以適當的調查及處理 0 件。
- 4.2.3 符合政府資通安全相關政策、規訂及相關法令要求。
- 4.2.4 定期實施資通安全教育訓練。

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及關注方之關注議題，以確保本校資訊安全管理制度之運作。

7 實施

本政策經「資通安全委員會」核定後實施，修訂時亦同。

