資通安全政策及目標

一、資通安全政策

為使本校業務順利運作，防止資訊或資通系統受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，並確保其機密性（Confidentiality）、完整性（Integrity）及可用性（Availability），特制訂本政策如下，以供全體同仁共同遵循：

1. 建立資通安全風險管理機制,定期因應內外在資通安全情勢變化,檢討資通安全風險管理之有效性。
2. 保護機敏資訊及資通系統之機密性與完整性，避免未經授權的存取與竄改。
3. 因應資通安全威脅情勢變化，辦理資通安全教育訓練，以提高本校同仁之資通安全意識，本校同仁亦應確實參與訓練。
4. 針對辦理資通安全業務有功人員應進行獎勵。
5. 勿開啟來路不明或無法明確辨識寄件人之電子郵件。
6. 禁止多人共用單一資通系統帳號。
7. 機密資料檔案的讀取及複製，須符合本校各業務單位的規定，並經該單位主管或其授權人員核可。
8. 本政策每年應至少評估檢討一次，以反映本校資訊安全需求、政府法令法規、外在網路環境變化及資訊安全技術等最新發展現況,以確保其對於維持營運和提供適當服務的能力。
9. 本政策如遇重大改變時應立即審查，以確保其適當性與有效性。必要時應告知相關單位及委外廠商，以利共同遵守。

本政策經資通安全長核准，於公告日施行，並以書面、電子或其他方式通知員工及與本校連線作業之有關機關（構）、委外廠商，修正時亦同。

二、資通安全目標

(一) 量化型目標

1. 知悉資安事件發生,能於規定的時間完成通報、應變及復原作業。
2. 電子郵件社交工程演練之郵件開啟率及附件點閱率分別低於 5%及 2%。(請機關自行設定指標)
3. 資安事件通報時間(含演練)超過一小時次數≤2 次。
4. 校園電腦防毒軟體 100%啟用，並持續使用及適時進行軟、硬體之必要更新或升級。
5. 每人每年接受三小時以上之一般資通安全教育訓練。

(二) 質化型目標

1. 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。
2. 達成資通安全責任等級分級之要求，並降低遭受資通安全風險之威脅。
3. 提升本校人員資安防護意識，防止發生中毒或入侵事件。

三、資通安全政策及目標之核定程序

資通安全政策由本校簽陳資通安全長核定。

四、資通安全政策及目標之宣導

1. 本校之資通安全政策及目標應每年透過教育訓練、內部會議、張貼公告等方式，向機關內所有人員進行宣導，並檢視執行成效。
2. 本校應每年向利害關係人(例如 IT 服務供應商、與機關連線作業有關單位）進行資安政策及目標宣導，並檢視執行成效。

五、資通安全政策及目標定期檢討程序

資通安全政策及目標應定期於資通安全管理審查會議中檢討其適切性。