

南部科學園區管理局

資通安全政策

機密等級： 密 內部使用 公開

文件編號：S-101-01

版 本：1.0

施行日期：中華民國 111 年 10 月 5 日

目 次

一、 依據.....	1
二、 目的.....	1
三、 適用範圍.....	1
四、 責任分配.....	1
五、 資通安全目標.....	2
六、 資通安全政策審查.....	3

一、依據

- (一) 資通安全管理法及其施行細則。
- (二) ISO/IEC 27001 國際標準、CNS 27001 國家標準。

二、目的

南部科學園區管理局（以下簡稱本局）為強化資通安全管理，建立安全及可信賴之電子化政府環境，確保資料、資通系統、設備及網路之機密性、完整性與可用性，避免內、外部蓄意或意外之威脅，並提供信賴可靠之資通訊服務，特訂定本政策。

三、適用範圍

- (一) 本政策適用對象為本局任用、聘任、聘用、約僱、駐衛警、技工、工友、臨時人員、計畫助理及派遣人員，接觸本局業務之相關機關（構）、對本局提供服務之廠商及第三方人員。
- (二) 資訊安全管理系統（Information Security Management System，簡稱 ISMS）實施範圍為本局各業務流程衍生之資通安全事項。

四、責任分配

- (一) 應成立資通安全組織，統籌資通安全政策之推動與管理事項。
- (二) 管理階層應積極參與資通安全相關活動，提供對資通安全業務之支持。

- (三) 管理階層對本政策及相關規範負督導執行之責。
- (四) 除員工外，凡接觸業務資料之外部人員、委外服務廠商及訪客亦應遵守本政策及相關規範。
- (五) 員工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資通安全弱點並協助處理。
- (六) 員工應遵守法令法規與本局各項資通安全規定，並有參加本局舉辦各類資通安全教育訓練之義務。
- (七) 任何危及資通安全之行為，將視情節輕重依本局相關規定進行議處。
- (八) 應藉由執行資訊安全管理系統之改善措施，以達到持續改進之目的。

五、資通安全目標

本局資訊安全聲明為：「資訊不外流、資安事件少、服務不中斷」。
資通安全目標為：

- (一) 機密性 (Confidentiality)：確保所欲保護的資訊，避免未經授權的存取，或無意的洩漏。
- (二) 完整性 (Integrity)：確保資訊內容與處理方法為正確與一致性。
- (三) 可用性 (Availability)：確保經授權的使用者在需要時可取得資訊與使用設備。
- (四) 法律遵循性 (Legitimacy)：確保所欲保護的資訊內容，遵循法令法規要求。

六、資通安全政策審查

- (一) 本政策每年審視 1 次，得視需要作調整以因應法令、技術及業務等最新發展現況，確保資通安全實務作業之有效性。
- (二) 本政策經資訊服務、資訊安全暨個資安全委員會召集人或其指定授權代理人核備並經推動處理小組循公文程序簽奉核定，於公告日施行，並以書面、電子或其他方式通知本政策適用人員，修正時亦同。