國立中山大學

資通安全政策

機密等級：一般

文件編號：NSYSU-I-A-001

版　　次：3.0

發行日期：110.09.17

修　訂　紀　錄				
版次	**修訂日期**	**修訂頁次**	**修訂者**	**修訂內容摘要**
1.0	97.5.21		資安小組	初版
1.1	97.8.26	封面、P1、P2	資安小組	1. 單位銜稱由「計算機與網路中心」更改為「圖書與資訊處」 2. 本「中心」改為本「處」
1.2	98.5.13	各頁頁首	資安小組	去除「草案」兩字。
2.0	106.12.04	P1~4	資安小組	配合教育體系資通安全暨個人資料管理規範(2016 年版)，修訂本政策
3.0	110.09.17	封面、各頁頁首、P1~3	資通安全暨個人資料保護工作圈執行小組	配合資通安全管理法、ISO27001:2013 國際標準要求，修訂本政策以適用全校。

目錄

1 目的 1

2 適用範圍 1

3 目標 1

4 責任 2

5 管理指標 2

6 審查 3

7 實施 3

資通安全政策					
文件編號	NSYSU-I-A-001	機密等級	一般	版次	3.0

1 目的

為確保國立中山大學（以下簡稱本校）所屬之資訊資產的機密性、完整性及可用性，並符合相關法規之要求，使其免於遭受內、外部的蓄意或意外之威脅，並衡酌本校之業務需求，特訂定資通安全政策（以下簡稱本政策）。

2 適用範圍

本政策適用範圍為本校全體人員、約聘（僱）人員及臨時人員、委外服務廠商與訪客等。

資通安全管理涵蓋 14 項管理事項,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，對本校帶來各種可能之風險及危害。管理事項如下：

2.1 資訊安全政策（訂定與評估）。

2.2 資訊安全組織。

2.3 人力資源安全。

2.4 資產管理。

2.5 存取控制。

2.6 密碼學。

2.7 實體與環境安全。

2.8 運作安全。

2.9 通訊安全。

2.10 資訊系統取得、開發及維護。

2.11 供應者關係。

2.12 資訊安全事故管理。

2.13 營運持續管理之資訊安全層面。

2.14 遵循性。

3 目標

為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之安全，期藉由本校全體同仁共同努力來達成下列目標：

3.1 保護 TANet 服務與本校資通系統業務活動資訊，避免未經授權的存取，確保其機密性。

3.2 保護 TANet 服務與本校資通系統業務活動資訊，避免未經授權的修改，確保其正確性與完整性。

3.3 建立資訊業務永續運作計畫，確保 TANet 服務與本校資通系統業務活動之持續運作。

3.4 TANet 服務與本校資通系統之業務活動執行須符合相關法令或法規之要求。

4 責任

4.1 本校應成立資通安全組織統籌資通安全事項推動。

4.2 管理階層應積極參與及支持資訊安全管理制度，並透過適當的標準和程序予以實施本政策。

4.3 所有人員和委外服務廠商均須依照相關安全管理程序以維護資通安全政策。

4.4 所有人員有責任報告資通安全事件和任何已鑑別出之弱點。

4.5 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本校之相關規定進行議處。

5 管理指標

依據「資安管理指標暨有效性量測表」定期審查資訊安全管理制度之有效性。

6 審查

6.1 本政策應至少每年經資通安全暨智財權保護委員會審查乙次，以反映政府法令、技術及業務等最新發展現況，以確保本校永續運作及提供學術網路服務之能力。

6.2 本校應考量內、外部議題及利害相關者要求，訂定適當之資訊安全管理制度實施範圍，經由管理階層審核、確認後實行。

7 實施

本政策經資通安全暨智財權保護委員會審查後，經資通安全長核定後實施，得以書面、電子或其他方式通知全體人員、與本校連線作業之有關機關(構)及提供資訊服務之委外廠商，修正時亦同。