

國立暨南國際大學

南投區域網路中心

資訊安全政策

機密等級：一般

文件編號：NCNU-ISMS-A-001

版 次：2.0

發行日期：107.05.01

資訊安全政策					
文件編號	NCNU-ISMS-A-001	機密等級	一般	版次	2.0

目錄

1	目的	1
2	適用範圍	1
3	目標	2
4	責任	2
5	管理指標	3
6	審查	4
7	實施	4

資訊安全政策					
文件編號	NCNU-ISMS-A-001	機密等級	一般	版次	2.0

1 目的

為確保國立暨南國際大學南投區域網路中心（以下簡稱「本中心」）所屬之資訊資產的機密性、完整性及可用性，以符合相關法令、法規之要求，使其免於遭受內、外部蓄意或意外之威脅，並衡酌本中心之業務需求，訂定本政策。

2 適用範圍

資訊安全管理涵蓋 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，對本中心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(加密控制)。
- 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。

本中心之內部人員、委外服務廠商與訪客皆應遵守本政策。

資訊安全政策					
文件編號	NCNU-ISMS-A-001	機密等級	一般	版次	2.0

3 目標

為維護本中心資訊資產之機密性、完整性與可用性，並保障使用者資料隱私之安全。期藉由本中心全體同仁共同努力以達成下列目標：

- 3.1 保護本中心業務服務之安全，確保資訊需經授權人員才可存取資訊，以確保其機密性。
- 3.2 保護本中心業務服務之安全，避免未經授權的修改，以確保其正確性與完整性。
- 3.3 建立資訊業務永續運作計畫，確保本中心 TANet 與本校核心系統業務活動之持續運作。
- 3.4 本中心 TANet 與本校核心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 本中心應成立資訊安全組織統籌資訊安全事項推動。
- 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訊安全政策。
- 4.4 所有人員有責任報告資訊安全事件和任何已鑑別出之弱點。
- 4.5 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中心之相關規定進行議處。
- 4.6 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訊安全政策。

資訊安全政策					
文件編號	NCNU-ISMS-A-001	機密等級	一般	版次	2.0

5 管理指標

為評量資訊安全管理目標達成情形，本中心特訂定資訊安全管理指標如下：

5.1 定量化指標

5.1.1. 本校每年無發生教職員生密級資料外洩。

5.1.2. 本校每年無發生教職員生資料(如:學生成績或使用者個人資料)遭竄改。

5.1.3. 確保本校關鍵業務系統資訊機房維運服務達全年上班時間96%以上之可用性，並確保：

A. 因資通安全事件、異常事件、其他安全事故造成系統、主機異常而中斷營運服務之情事，每年不得超過8次。

B. 因資通安全事件、異常事件、其他安全事故造成系統、主機異常而中斷營運服務之情事，每次最長不得超過8工作小時。

5.1.4. 本校關鍵業務系統服務達全年上班時間98%以上之可用性，中心關鍵業務系統因資通安全事件、異常事件、其他安全事故造成系統、主機異常而中斷營運服務之情事，每次最長不得超過4工作小時。

資訊安全政策					
文件編號	NCNU-ISMS-A-001	機密等級	一般	版次	2.0

6 審查

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

7 實施

- 7.1 資訊安全政策配合管理審查會議進行資訊安全政策審核。
- 7.2 本政策經「資訊安全委員會」核定後實施，修訂時亦同。