

# 國立臺灣師範大學心理與教育測驗 研究發展中心

---

## 資訊安全政策

---

文件編號：NACE-ISMS-A-001

機密等級：一般

版 次：3.0

發行日期：106.10.17

本文件為國立臺灣師範大學心理與教育測驗研究發展中心專有之財產，非經書面許可，不得透露或使用本文件，亦不得複印、複製或轉變成任何其他形式使用。

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	102.03.11		NII	初版發行
2.0	103.10.31		NII-吳昭儀	依 ISO 27001:2013 要求，修訂本政策。
2.1	104.01.19	P.2、3	NII-吳昭儀	依 ISO 27001:2013 文件審查之發現事項，修訂本政策。
3.0	106.09.26	P.1、2	周紘正	修訂文件編號及版次，修改 2.2、3.3、5.3 之內容

---

## 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.....	2
7 實施.....	3

## 1 目的

為確保國立臺灣師範大學心理與教育測驗研究發展中心（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

2.1 本政策適用範圍為本中心之全體人員、委外服務廠商、工讀生與訪客等。

2.2 範圍訂定應考量：

2.2.1 背景環境、內外部議題

2.2.2 關注方之要求事項（含法律、法規、合約）

2.2.3 中心及其他單位所執行之活動間的界面及相依性

相關驗證範圍及關注方所關注事項之鑑別結果，展現於 ISMS 驗證範圍核定函，並由召集人核定。

2.3 資訊安全管理範疇涵蓋 14 項領域，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，對本中心造成各種可能之風險及危害，各領域分述如下：

2.3.1 資訊安全政策

2.3.2 資訊安全之組織

2.3.3 人力資源安全

2.3.4 資產管理

2.3.5 存取控制

2.3.6 密碼學

2.3.7 實體及環境安全

2.3.8 運作安全

2.3.9 通訊安全

2.3.10 系統獲取、開發及維護

2.3.11 供應者關係

2.3.12 資訊安全事故管理

2.3.13 營運持續管理之資訊安全層面

2.3.14 遵循性

### 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 確保本中心業務資訊需經權責單位授權才可存取，以維護其機密性。
- 3.2 確保本中心業務資訊之正確與完整，避免被竄改或損壞。
- 3.3 確保本中心資訊服務之持續運作，以維護資訊系統及其相關業務。
- 3.4 確保本中心各項業務之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並支持資訊安全管理制度，並透過適當標準及程序實施本政策。
- 4.3 本中心全體人員、相關教育主管機關、各試務委員會、委外服務廠商、工讀生與訪客等皆應遵守本政策。
- 4.4 本中心全體人員均有責任透過適當通報機制，通報資訊安全事件或弱點。
- 4.5 任何危及資訊安全之行為，將視情節輕重依本中心相關規定進行議處。

### 5 管理指標

為評量資訊安全管理目標達成情形，特訂定資訊安全管理指標如下：

- 5.1 凡本中心機密業務資訊或考生個人資料，須達全年零外洩，以確保本中心相關業務之機密性。
- 5.2 凡本中心業務相關對外公開資訊之完整性，須達 100%，以確保本中心相關業務之完整性。
- 5.3 確保本中心資訊機房維運服務及關鍵業務系統服務之可用性達全年 98% 以上。
- 5.4 為確保本中心資訊安全措施或規範符合現行法令、法規之要求，每年至少需執行兩次內部稽核，須達成 98% 以上，以確保本中心相關業務之適法性。

### 6 審查

- 6.1 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，並確保本中心業務永續運作之能力。
- 6.2 本中心召集人應每年至少審查乙次資訊安全目標達成情形表，以確認資訊安全目標計

---

畫之工作內容、所需資源、負責人員、達成時間及成果評估方式等資訊，以明確展現最高管理者對資訊安全之領導及承諾。

## 7 實施

本政策經國立臺灣師範大學心理與教育測驗研究發展中心資訊安全工作組召集人核定後實施，修訂時亦同。