

國立臺灣師範大學資訊中心

資訊安全政策

文件編號：NTNU-ISMS-A-001

機密等級：一般

版 次：1.1

發行日期：103.09.23

本文件為國立臺灣師範大學資訊中心專有之財產，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。

1 目的

為確保國立臺灣師範大學資訊中心（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、委外服務廠商與訪客等。
- 2.2 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：
 - 2.2.1 資訊安全政策。
 - 2.2.2 資訊安全之組織。
 - 2.2.3 人力資源安全
 - 2.2.4 資產管理。
 - 2.2.5 存取控制。
 - 2.2.6 密碼學。
 - 2.2.7 實體及環境安全。
 - 2.2.8 運作安全。
 - 2.2.9 通訊安全。
 - 2.2.10 系統獲取、開發及維護。
 - 2.2.11 供應者關係。
 - 2.2.12 資訊安全事故管理。
 - 2.2.13 營運持續管理之資訊安全層面。
 - 2.2.14 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，期藉由本政策之實施以達成下列目標：

- 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 建立本中心業務永續運作計畫，以確保本中心業務服務之持續運作。
- 3.4 確保本中心各項業務服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 本中心全體人員、委外服務廠商與訪客等皆應遵守本政策。
- 4.4 本中心全體人員及委外服務廠商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

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 定量化指標

5.1.1 確保本中心資訊服務可用性之要求如下：

5.1.1.1 資訊機房維運服務達全年服務時間 97% 以上。

5.1.1.2 關鍵業務系統服務達全年服務時間 98% 以上。

5.1.2 確保因資通安全事件、異常事件、其他安全事故所造成系統、主機異常而中斷營運服務之情事，每年不得超過次數如下：

5.1.2.1 資訊機房維運服務中斷，每季不得超過 3 次。

5.1.2.2 關鍵業務系統服務中斷，每季不得超過 3 次。

5.1.3 確保因資通安全事件、異常事件、其他安全事故所造成系統、主機異常而中斷營運服務之情事，每次最長不得超過工作小時要求如下：

5.1.3.1 資訊機房維運服務中斷，每次最長不得超過 4 工作小時。

5.1.3.2 關鍵業務系統服務中斷，每次最長不得超過 4 工作小時。

6 審查

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情況，確保本中心

業務永續運作之能力。

7 實施

本政策經「資訊安全推動小組」核定後實施，修訂時亦同。