

國立暨南國際大學

教育大數據系統服務中心、人工智慧應用研發
中心及國立臺灣大學教育資料庫專案辦公室

「資訊安全管理系統」
資訊安全政策

發行單位：ISMS 推動小組之綜合業務組

發行日期：2024.08.01

版 次：3.0

使用本程序書前，請先與文件管理者確認版次。

本文件歷次變更紀錄：

| 版次 | 發行日 | 撰擬者或單位 | 說 明 | 核准者 |
|-----|------------|---------------------|--|-------------------|
| 1.0 | 2016.08.10 | ISMS 推動小組 之綜合業務組 | 初次發行 | ISMS 推動小組 之召集人 |
| 1.1 | 2017.07.31 | ISMS 推動小組 之綜合業務組 | 調整資訊安全管理系統 範圍，移除「海外聯合招 生委員會」 | ISMS 推動小組 之召集人 |
| 1.2 | 2017.08.31 | ISMS 推動小組 之綜合業務組 | 依據資訊安全管理系統 範圍，調整「參、適用範 圍」 | ISMS 推動小組 之召集人 |
| 2.0 | 2019.08.31 | ISMS 推動小組 之綜合業務組 | 依據行政院資通安全處 「資通安全維護計畫範 本」，修訂資安政策目 的、新增政策宣導 | ISMS 推動小組 之召集人 |
| 2.1 | 2020.08.31 | ISMS 推動小組 之綜合業務組 | 參考 NIST CSF，新網路 服務安全政策 新增柒、四 | ISMS 推動小組 之召集人 |
| 2.2 | 2021.09.10 | ISMS 推動小組 之綜合業務組 | 配合中心系統名稱變更 以及因應未來核心系統 擴大驗證，修改適用範圍 | ISMS 推動小組 之召集人 |
| 2.3 | 2022.07.01 | ISMS 推動小組 之綜合業務組 | 配合中心組織架構調 整，調整組織名稱與驗證 範圍 | ISMS 推動小組 之召集人 |
| 2.4 | 2022.09.08 | ISMS 推動小組 之綜合業務組 | 因應 TUV 預評意見 修改政策目標 | ISMS 推動小組 之召集人 |
| 3.0 | 2024.08.01 | ISMS 推動小組 之綜合業務組 | 因應組織名稱架構調整 | ISMS 推動小組 之召集人 |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

本政策由 ISMS 推動小組之綜合業務組負責維護。

目 錄

壹、 目的 1

貳、 依據 1

參、 適用範圍 1

肆、 定義 1

伍、 權責 2

陸、 政策目標 2

柒、 資安政策聲明內容 2

捌、 資訊安全目標有效性量測 3

玖、 宣導 3

壹拾、 修訂 3

壹拾壹、 相關文件 3

壹、目的

國立暨南國際大學教育大數據系統服務中心、人工智慧應用研發中心及國立臺灣大學教育資料庫專案辦公室（以下簡稱本組織）為推動資訊安全管理系統，建立安全及可信賴之資訊環境，防止資訊或資通系統受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，並確保其機密性（Confidentiality）、完整性（Integrity）及可用性（Availability）與適法性(Legality)，特訂定本資訊安全政策（以下簡稱本政策），以為遵循。

貳、依據

本政策係依據本組織掌理事項及相關法規訂定之。

參、適用範圍

本組織資訊系統之開發、操作與維護，以及單位網路管理、機房與相關支援活動。

肆、定義

- 一、資訊安全：應用管理程序及安全防護技術於各項資訊作業，包含作業執行時所使用之各項資訊系統軟、硬體設備、存放各種資訊及資料之檔案媒體及經由列表機所列印之各式報表，俾能在資訊蒐集、處理、傳送、儲存及流通之過程中，確保資訊資產之完整性、可用性與機密性。
- 二、機密性(Confidentiality)：確保只有經過授權的人才能存取資訊資產。
- 三、完整性(Integrity)：確保資訊資產的完整性(Completeness)及其處理方法的準確性。

本資料非經書面許可，不准洩露或變更使用，亦不准複印、複製或轉成其他形式使用。

四、可用性(Availability)：確保授權的使用者在需要時，可以使用資訊資產。

五、適法性(Legality)：符合國家相關法令規範。

伍、權責

一、ISMS 推動小組之召集人

- 統籌資訊安全政策、計畫、資源調度等事項之協調審議。

二、ISMS 推動小組之綜合業務組

- 政策之修訂與公告。

陸、政策目標

一、保護機密性資料，避免資料遭受非法存取或竊取。

二、確保資料完整性，確保系統程式不被未經授權修改。

三、落實系統可用性，保持系統維持服務運作水準。

四、符合法規遵循性，力求管理制度與系統安全符合規範。

柒、資安政策聲明內容

一、成立「ISMS 推動小組」確認資訊安全管理運作之有效性。

二、應建立資通安全風險管理機制，定期因應內外資通安全情勢變化，檢討資通安全風險管理之有效性。

三、應保護機敏資訊及資通系統之機密性與完整性，避免未經授權的存取與竄改。

四、維持網路服務之完整性、可用性及機密性，確保有效運用與管理網路及資訊設備以及防範駭客入侵與違規使用系統資源。

五、訂定業務持續運作計劃，定期演練，並配合業務發展與組織現況持續調整更新。

六、定期實施資訊安全教育訓練，宣導資訊安全政策及相關實施規定。

七、訂定資訊安全內部稽核計畫，定期執行內部稽核活動。

八、本組織員工、本組織辦公場所以外之系統連線使用者及承接本組織業務之廠商，應遵循本組織資訊安全管理規定。

九、有關個人資料保護管理相關作業，應參照「個人資料保護法」辦理。

捌、資訊安全目標有效性量測

相關資訊安全目標達成有效性之測量項目與方法，需經本組織 ISMS 或資訊安全相關會議討論訂定，並留存相關測量結果記錄。

玖、宣導

一、本政策及目標應每年透過教育訓練、內部會議、張貼公告等方式，向本組織內所有人員進行宣導。

二、應每年向利害關係人(例如 IT 服務供應商、與本組織連線作業有關單位)傳達資安政策及目標宣導。

壹拾、修訂

本政策應至少每年評估一次，以符合政府法令、法規之要求，並反映資訊科技發展趨勢，確保本組織資訊安全管理作業之有效性。

壹拾壹、相關文件

無