



---

# 資通安全政策

---

文件編號：NDHU-I-A-01

機密等級：一般

單位：國立東華大學

版次：1.0

發行日期：中華民國 112 年 11 月 20 日



## 目 錄

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

## 1 目的

為確保國立東華大學（以下簡稱「本校」）所屬之資訊資產的機密性、完整性及可用性，以符合「資通安全管理法」等相關法令、法規之要求，使其免於遭受內、外部蓄意或意外之威脅，特訂定本政策。

## 2 適用範圍

- 2.1 本政策適用範圍為本校之全體同仁、委外服務廠商、資料使用者（含保管者）與訪客等。
- 2.2 資通安全管理範疇涵蓋組織、人員、實體及技術等4大領域，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，對本校造成各種可能之風險。

## 3 目標

為維護本校資訊資產之機密性、完整性、可用性與法律遵循性，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 建立安全及可信賴之資通作業環境，確保本校電腦資料、系統、設備及網路之安全，以保障本校業務永續運作。
- 3.2 保護本校業務服務之安全，確保資通系統及相關資訊需經授權人員才可存取資訊，以確保其機密性。
- 3.3 保護本校業務服務之安全，避免未經授權的修改，以確保其正確性與完整性。
- 3.4 建立本校業務永續運作計畫，以確保本校資通業務服務之持續運作。
- 3.5 確保本校各項業務服務之執行須符合相關法令或法規之要求。
- 3.6 為保護本校業務相關個人資料之安全，免於因外在威脅，或內部人員不當之管理與使用，致遭受竊取、竄改、毀損、滅失、或洩漏等風險。
- 3.7 提升對個人資料之保護與管理能力，降低營運風險，並創造可信賴之個人資料保護及隱私環境。

## 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通安全管理制度，並透過適當的標準和程序以實施本政

策。

- 4.3 本校全體同仁、委外服務廠商、資料使用者（含保管者）與訪客等皆應遵守本政策。
- 4.4 本校全體同仁、委外服務廠商及資料使用者（含保管者）均有責任透過適當通報機制，通報資通安全事件或弱點。
- 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「公務機關所屬人員資通安全事項獎懲辦法」及本校之相關規定進行議處。

## 5 管理指標

- 5.1 為評量資通安全管理目標達成情形，本校應訂定相關管理指標，並定期監控、評估及改善。
- 5.2 應定期審查本校資通安全組織人員執掌，以確保資通安全工作之推展。
- 5.3 應符合主管機關之要求，依員工職務及責任提供適當之資通安全相關訓練。
- 5.4 應加強本校資訊資產之環境安全，採取適當之保護及權限控管機制。
- 5.5 應確保資訊不被透漏給未經授權之第三者。
- 5.6 應加強存取控制，防止未經授權之不當存取，以確保本校資訊資產已受適當之保護。
- 5.7 本校資訊系統開發應考量安全需求，並定期稽核安全弱點。
- 5.8 應確保所有資通安全事件或可疑之安全弱點，均依循適當之通報機制向上反應，並予以適當調查及處理。

## 6 管理審查

本政策應每年至少審查 1 次，以反映政府法令、技術及業務等最新發展情況，確保本校業務永續運作之能力。資通安全組織、主管機關（或法令、法規要求）、或專家學者等利害關係人如有資通安全相關回饋事項，應將列入管理審查會議之討論議題。

## 7 實施

本政策經「資通安全管理組織」核定後實施，修訂時亦同。