



財團法人高等教育評鑑中心基金會

Higher Education Evaluation and Accreditation Council of Taiwan

資通安全政策

文件編號：ISMS-M-01

機密等級：普通

單位：財團法人高等教育評鑑中心基金會

版次：2.1

發行日期：114年10月31日

[illegible]

目錄

1	目的	1
2	範圍	1
3	目標	1
4	權責	1
5	管理指標	2
6	管理審查	2
7	實施	2

1 目的

財團法人高等教育評鑑中心基金會（以下簡稱本會，英文簡稱 HEEACT）為維持資訊資產正常運作及網路安全，防止資訊遭受不當的讀取、洩漏、竄改、竊取、破壞等情事，透過每年檢視和評估其資通安全規章及程序，以確保其適當性和有效性之目的。

2 範圍

- 2.1 本政策適用範圍為本會之全體同仁、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，包含組織、人員、實體及技術等四大項控制領域，為避免因人為疏失、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，避免對本會造成各種資通安全危害之可能風險。

3 目標

本會資通安全政策為：「**提升資安意識，控制資安風險；落實資通安全，確保持續營運**」。

為維護本會資訊資產之機密性、完整性與可用性，期藉由本政策之實施達成下列目標：

- 3.1 建立安全及可信賴之資訊化作業環境，確保本會資料、系統、設備及網路之安全，以保障本會營運永續運作。
- 3.2 保護本會營運服務之安全，確保資訊需經授權人員才可存取資訊，以確保其機密性。
- 3.3 保護本會營運服務之安全，避免未經授權的修改，以確保其正確性與完整性。
- 3.4 建立本會營運永續運作計畫，以確保本會資通服務之持續運作。
- 3.5 確保本會各項業務服務之執行須符合「資通安全管理法」及其子法，以及相關法令規範之要求。
- 3.6 為保護本會業務及服務相關資料之安全，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 提升對資訊資產及個人資料之保護與管理能力，降低營運風險。

4 權責

- 4.1 本會應成立「資通安全管理委員會」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 本會全體同仁、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 本會全體同仁、委外服務廠商及資料使用者(含保管者)與訪客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、刑事責任，或依本會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，本會應訂定相關管理指標，並定期監控、評估及改善。
- 5.2 應定期審查本會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 應加強本會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，以確保本會資訊資產已受適當之保護。
- 5.7 本會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

本政策應每年至少進行 1 次管理審查，以反映政府法令、技術及業務等最新發展情況，確保本會營運永續運作之能力。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，應列入管理審查會議之討論議題。

7 實施

本政策經本會「資通安全管理委員會」研擬核定後實施，修訂時亦同。