中華大學

資訊安全政策

機密等級：一般

文件編號：CHU-ISMS-A-001

版　　次：5.1

發行日期：2023/11/22

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	2009/3/4		資訊安全執行委員會	初版
1.1	2009/5/11		資訊安全執行委員會	字詞修訂
1.2	2009/8/19	2	資訊安全執行組	經管審會決議，資訊安全組織名稱由「資訊安全執行委員會」變更為「資訊安全執行組」
1.3	2010/4/12	2	資訊安全執行組	修訂政策目標含定性化(3.1)和定量化(3.2)兩大目標
1.4	2010/9/13	1	資訊安全執行組	依據 2010/8/11 資訊安全小組會議建議，新增個人資料保護相關規定，經管審會決議通過
1.5	2011/4/19	2	資訊安全執行組	經管審會決議，修訂政策目標(3.2)定量化目標
1.6	2011/8/17	1	資訊安全執行組	依據管審會決議廢止個人資料保護程序書修訂 2.2.12
1.7	2012/4/16	2	資訊安全執行組	依據擴增認證範圍的需要，增訂條文 3.2.2 和修訂條文 3.2.4 內容，經管審會決議通過
1.8	2013/4/15	3	資訊安全執行組	經管審會決議，修訂 4.4 之通報程序

1.9	2014/5/12	1	資訊安全執行組	經管審會決議，增訂 2.2.12 個人資料保護。
2.0	2014/8/11	1	資訊安全執行組	經管審會決議，修訂 1 說明和刪除 2.2.12 項目。
3.0	2016/3/8	本文件	資訊安全小組	因單位組織異動名稱變更，原「電子計算機中心」變更為「圖書與資訊處」，原「電算中心」變更為「本處」，原「本中心」變更為「本處」。
3.1	2017/3/30	2,3	資訊安全執行組	經本次管審會決議，將認證範圍界定為本處資訊服務之相關人員，未含圖書與資訊組的同仁。
4.0	2018/8/20	本文件	資訊安全執行組	依據 2016 年版教育體系資通安全規範修訂本資安政策，並經管審會決議通過。
5.0	2023/6/9	本文件	資訊安全執行小組	資安管理制度擴展至全校，修正相關適用範圍及說明。
5.1	2023/11/22	本文件	資訊安全暨個人資料保護委員會	修訂目的及實施方式，本政策經資訊安全暨個人資料保護委員會審議通過

				後公告實施 修訂定性化及定量化目標之核心業務新增核心字句及資通系統

目錄

資訊安全政策					
文件編號	CHU-ISMS-A-001	機密等級	一般	版次	5.1

1 目的

為確保中華大學（以下簡稱「本校」）所屬之資訊資產的機密性、完整性及可用性，遵循中華民國「資通安全管理法」及相關法令規定，使其免於遭受內、外部蓄意或意外之威脅，並衡酌本校之業務需求，訂定本校資訊安全政策（以下簡稱「本政策」）。

2 適用範圍

2.1 本政策適用範圍為本校資訊服務之內部人員、委外服務廠商與訪客等相關人員。

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，對本校造成各種可能之風險及危害，各領域分述如下：

2.2.1 資訊安全政策訂定與評估。

2.2.2 資訊安全組織。

2.2.3 人力資源安全與教育訓練。

2.2.4 資訊資產分類與管制。

2.2.5 存取控制安全。

2.2.6 密碼學(加密控制)。

2.2.7 實體與環境安全。

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

為維護本校資訊資產之機密性、完整性與可用性，並保障使用者資料隱私之安全，藉由本校資訊服務之相關人員共同努力達成下列目標：

3.1 定性化目標

3.1.1 保護本校核心業務服務之安全，確保資訊經授權人員才可存取，以確保其機密性。

3.1.2 保護本校核心業務服務之安全，避免未經授權的修改，以確保其正確性與完整性。

3.1.3 建立本校核心業務永續運作計畫，以確保本校核心業務服務之持續運作。

3.1.4 確保本校各項核心業務服務之執行符合相關法令或法規之要求。

3.1.5 確保所有資安事件、意外事件或可疑之安全弱點，都應依循適當通報機制向上反應，予以適當調查及處理。

3.1.6 定期審查本校資訊安全組織人員執掌，以確保資訊安全工作之推展。

3.1.7 應符合主管機關之要求，依員工職務及責任提供適當之資訊安全相關訓練。

3.1.8 應加強本校資訊機房設施之環境安全，採取適當之保護及權限控管機制。

3.1.9 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受適當的保護。

3.1.10 確保資訊不會在傳遞過程中，或因無意間的行為透露給未經授權的第三者。

3.2 定量化目標

3.2.1 確保核心系統機房內核心系統電力、空調服務達到全年 97% 以上之可用性，可用性計算公式為 $\frac{365\text{天}\times 24\text{時}-\text{中斷服務時數}}{365\text{天}\times 24\text{時}}$。

3.2.2 確保核心系統網路通訊服務達到全年 95% 以上之可用性，可用性計算公式為 $\frac{365\text{天}\times 24\text{時}-\text{中斷服務時數}}{365\text{天}\times 24\text{時}}$。

3.2.3 確保核心系統業務服務達到全年 95% 以上之可用性，可用性計算公式為 $\frac{365\text{天}\times 24\text{時}-\text{中斷服務時數}}{365\text{天}\times 24\text{時}}$。

3.2.4 確保核心系統業務服務中斷(如人員操作錯誤、病毒攻擊、硬體故障和程式錯誤)每年發生次數低於 8 次。

3.2.5 為確保本校資訊安全措施或規範符合現行法令、法規之要求，每年至少需執行內部稽核乙次。

3.2.6 應適當保護本校資訊資產之機密性與完整性，每年至少需進行資訊資產盤點及資通系統風險評鑑作業乙次。

3.2.7 為確保本校資訊業務服務得以持續運作，每年至少需執行核心業務永續運作計畫演練乙次。

4 責任

4.1 本校設立資訊安全暨個人資料保護委員會統籌資訊安全事項推動。

4.2 本校各級主管應積極參與及支持資訊安全管理制度，並透過所制訂的相關標準和程序來達成本政策。

4.3 本校資訊服務之相關人員、委外服務廠商與訪客等皆應遵守本政策。

4.4 本校資訊服務之相關人員及委外服務廠商發現資安事件時，應通報本校資安連絡人，並副知本校資訊安全執行小組執行秘書，再由資安連絡人透過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 審查

本政策每年至少應審查一次，以反映政府法令、技術及業務等最新發展現況，並確保本校業務永續運作之能力。

6 實施

本政策經資訊安全暨個人資料保護委員會審議通過後公告實施，修訂時亦同。