

中國文化大學

資訊中心

資訊安全政策

機密等級：公開

文件編號：PCCU-S-A-001

版次：1.3

## 1. 依據

為確保中國文化大學資訊中心(以下簡稱本中心)所屬資訊資產之機密性、完整性及可用性，並符合相關法令、法規之要求，使其免於遭受內、外部蓄意或意外之威脅，爰依據「行政院及所屬各機關資訊安全管理要點」、「行政院及所屬各機關資訊安全管理規範」、「教育部所屬機關及各級公私立學校資通安全工作事項」及「個人資料保護法」等相關法令與法規，並衡酌本中心之業務需求，訂定資訊安全政策。

## 2. 目標

為確保本中心相關資料、資訊系統、設備及網路安全，同仁應於現有預算經費及人力資源下，共同達成資訊資產之機密性、完整性與可用性之資訊安全管理目標，以符合資訊安全管理制度有效性之量測。

## 3. 適用範圍

3.1 本政策適用範圍包括本中心之員工、工讀生及委外服務廠商。

3.2 資訊安全管理之範疇含括 14 個領域，避免因人為疏失、蓄意或天然災害等因素，對本中心造成各種可能之風險及危害，各領域分述如下：

3.2.1 資訊安全政策。

3.2.2 資訊安全之組織。

3.2.3 人力資源安全

3.2.4 資產管理。

3.2.5 存取控制。

- 3.2.6 密碼學。
- 3.2.7 實體及環境安全。
- 3.2.8 運作安全。
- 3.2.9 通訊安全。
- 3.2.10 系統獲取、開發及維護。
- 3.2.11 供應者關係。
- 3.2.12 資訊安全事故管理。
- 3.2.13 營運持續管理之資訊安全層面。
- 3.2.14 遵循性。

#### **4. 資訊安全管理責任**

- 4.1 本中心應成立資訊安全組織，統籌資訊安全事項之推動與管理。
- 4.2 管理階層應積極參與及承諾持續改善資訊安全管理制度及相關活動，提供對資訊安全之支持。
- 4.3 管理階層須對本政策及相關規範負督導執行之責。
- 4.4 中心之員工、工讀生及委外服務廠商，應遵守本政策及相關規範，並恪盡保護本中心資訊資產安全之責。
- 4.5 中心之員工、工讀生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資訊安全弱點。
- 4.6 任何危及資訊安全之行為，將視情節輕重依本校之相關規定進行議處或追究其行政、民事及刑事責任。

## 5. 資訊安全政策之審查及實施

本政策應每年定期審查，遇組織、業務、法令或環境等因素之更迭，予以適當修訂，經中心主任核定後公告施行，以確保資訊安全管理制度運作之有效性。