台灣首府大學

電子計算機中心

資訊安全政策

機密等級：一般

文件編號：**TSU-ISMS-A-001**

版　　次：**1.4**

發行日期：**102.03.05**

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	97.08.06		王美蘭	初版
1.1	98.06.23	2~3	王美蘭	5 管理指標 為評量資訊安全管理目標達成情形，特訂定資訊安全管理指標如下： 5.1 定量化指標 5.1.1 確保本中心資訊維運服務達全年上班時間 95%以上之可用性。 5.1.2 確保因資通安全事件、異常事件、其他安全事故所造成系統、主機異常而中斷營運服務之情事，每季不得超過 7 次。 5.1.3 確保因資通安全事件、異常事件、其他安全事故所造成系統、主機異常而中斷營運服務之情事，每次最長不得超過 4 工作小時。 5.1.4 應適當保護本中心資訊資產之機密性與完整性，每年至少需進行乙次風險評鑑及風險管理。 5.1.5 為確保本中心資訊安全措施或規範符合現行法令、法規之要求，每年至少需稽核乙次。 5.1.6 維護及演練業務永續運作計畫每年至少需進行乙次，以確保本中心資訊業務服務得以持續運作。 5.2 定性化指標 5.2.1 應定期審查本中心資訊安全組織人員執掌，以確保資訊安全工作之推展。 5.2.2 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。 5.2.3 應加強本中心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。 5.2.4 應確保資訊不因傳遞過程，或無意間之行為，透漏給未經授權之第三者。 5.2.5 應加強存取控制，防止未經授權之不當存取，以確保本中心資訊資產已受適當之保護。 5.2.6 本中心資訊系統開發應考量安全需求，並定期稽核安全弱點。 5.2.7 應確保所有資訊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。
1.2	99.09.07		王美蘭	990801 改名大學，修改校名及文件編號英文簡稱。
1.3	100.02.14	2	王美蘭	刪除： 5.1.2 確保因資通安全事件、異常事件、其他安全事故所造成系統、主機異常而中斷營運服務之情事，每季不得超過 7 次。
1.4	102.03.05	2	王美蘭	修訂： 5.1.2 確保因資通安全事件、異常事件、其他安全事故所造成資訊資產價值為 4 之系統、主機異常而中斷營運服務之情事，每次最長不得超過 4 工作小時。

目錄

資訊安全政策					
文件編號	TSU-ISMS-A-001	機密等級	一般	版次	1.4

1 目的

確保台灣首府大學電子計算機中心（以下簡稱本中心）所屬之資訊資產的機密性、完整性及可用性，並符合相關法規之要求，使其免於遭受內、外部的蓄意或意外之威脅。

2 適用範圍

資訊安全管理涵蓋 11 項管理事項，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，對本中心帶來各種可能之風險及危害。管理事項如下：

2.1 資訊安全政策訂定與評估。

2.2 資訊安全組織。

2.3 資訊資產分類與管制。

2.4 人員安全管理與教育訓練。

2.5 實體與環境安全。

2.6 通訊與作業安全管理。

2.7 存取控制安全。

2.8 系統開發與維護之安全。

2.9 資訊安全事件之反應及處理。

2.10 業務永續運作管理。

2.11 相關法規與施行單位政策之符合性。

本中心之內部人員、委外服務廠商與訪客等皆應遵守本政策。

3 目標

維護本中心資訊資產之機密性、完整性與可用性，並保障使用者資料隱私。

藉由全體同仁共同努力來達成下列目標：

3.1 保護本中心業務服務資訊，避免未經授權的存取。

3.2 保護本中心業務服務資訊，避免未經授權的修改，確保其正確完整。

3.3 建立資訊業務永續運作計畫，以確保本中心業務服務之持續運作。

3.4 本中心之業務服務執行須符合相關法令或法規之要求。

4 責任

4.1 本中心管理階層負責本政策之研擬及審查。

4.2 應透過適當的標準和程序以實施本政策。

4.3 所有人員和委外服務廠商均須依照相關安全管理程序以維護本政策。

4.4 所有人員均有責任報告資訊安全事件和任何已鑑別出之弱點。

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中心之相關規定進行議處。

5 管理指標

為評量資訊安全管理目標達成情形，特訂定資訊安全管理指標如下：

5.1 定量化指標

5.1.1 確保本中心資訊維運服務達全年上班時間 95%以上之可用性。

5.1.2 確保因資通安全事件、異常事件、其他安全事故所造成資訊資產價值為 4 之系統、主機異常而中斷營運服務之情事，每次最長不得超過 4 工作小時。

5.1.3 應適當保護本中心資訊資產之機密性與完整性，每年至少需進行乙次風險評鑑及風險管理。

5.1.4 為確保本中心資訊安全措施或規範符合現行法令、法規之要求，

每年至少需稽核乙次。

5.1.5 維護及演練業務永續運作計畫每年至少需進行乙次，以確保本中心資訊業務服務得以持續運作。

5.2 定性化指標

5.2.1 應定期審查本中心資訊安全組織人員執掌,以確保資訊安全工作之推展。

5.2.2 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。

5.2.3 應加強本中心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。

5.2.4 應確保資訊不因傳遞過程，或無意間之行為，透漏給未經授權之第三者。

5.2.5 應加強存取控制，防止未經授權之不當存取，以確保本中心資訊資產已受適當之保護。

5.2.6 本中心資訊系統開發應考量安全需求，並定期稽核安全弱點。

5.2.7 應確保所有資訊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 審查

本政策應每年至少審查乙次,以反映政府法令、技術及業務等最新發展現況，以確保本中心業務永續運作之能力。

7 實施

本政策經「資訊安全委員會」核定後實施，修訂時亦同。