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：**2.1**

發行日期：**107.06.25**

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。
2.0	106.06.01	1~4	王美蘭	修訂 目錄2~7及內文相關資料
2.1	107.06.25	2~4	王美蘭	修訂「資訊安全目標」、「資訊安全管理原則」及「施行」

目錄

資訊安全政策					
文件編號	TSU-ISMS-A-001	機密等級	一般	版次	2.1

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

本校員工、接觸本校業務資料之外機關人員、委外服務提供廠商人員及訪客。

3 名詞定義

3.1 機密性（Confidentiality）：使資訊不可用或不揭露給未經授權之個人、個體或過程的性質。

3.2 完整性（Integrity）：保護資產的準確度（Accuracy）和完全性（Completeness）的性質。

3.3 可用性（Availability）；經授權個體因應需求之可存取及可使用的性質。

3.4 資訊安全：係避免因人為疏失、蓄意或自然災害等風險，運用系統化之控制措施，包含政策、實施、稽核、組織結構和軟硬體功能等，以確保本校資訊資產受到妥善保護。

3.5 資訊資產：凡本校作業流程中使用之資訊資產，如內部人員、外部人員、紙本文件、電子文件、網路服務、電腦應軟體、應用系統、電腦硬體、網路設備、環控系統、建築保護設施與便利設施等皆屬之。

4 權責

設置本校「台灣首府大學資訊安全委員會」，負責政策之核定及監督、資訊

安全預防及危機處理。

5 要求事項

5.1 資訊安全目標

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 資訊安全管理事項

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，對本校帶來各種可能之風險及危害。資訊安全管理應涵蓋 14 項管理事項：

1. 資訊安全政策。
2. 資訊安全組織。
3. 人力資源安全。
4. 資產管理。
5. 存取控制。
6. 密碼學(加密控制)。

7. 實體與環境安全。

8. 運作安全

9. 通訊安全

10. 資訊系統取得、開發及維護。

11. 供應者關係。

12. 資訊安全事故管理。

13. 營運持續管理之資訊安全層面。

14. 遵循性。

5.3 資訊安全管理原則

5.3.1 重要之資訊資產應定期清查、分類分級與進行風險評鑑，並據以實施適當的防護措施。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。

5.3.2 重要資訊資產存取權限應予以區分，考量人員職務授予相關權限，必要時得採行加解密及身分鑑別機制，以加強資訊資產之安全。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。

5.3.3 對於資訊安全事件須有完整的通報及應變措施，以確保資訊系統、業務的持續運作。

5.3.4 相關人員應依規定接受資訊安全教育訓練與宣導，以加強資訊安全認知。

5.3.5 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。

5.3.5 為確保業務資訊之機密性，各項資訊需經權責單位授才可存取，每年發生機密等級資訊外洩之事件不得超過乙次。

5.3.6 為確保本校教職員生資料(如：校園 e 化系統資料庫)之正確性

與完整性，每年發生資料遭未經授權竄改之事件不得超過乙次。

5.3.7 違反本政策與資訊安全相關規範，依相關法規或本校懲戒規定辦理。

6 修訂

6.1 管理階層審查

6.1.1 確保「資訊安全管理系統」實務運作之可用性、安全性及有效性。本政策每年依業務變動、技術發展及風險評鑑的結果或配合政府資訊安全管理要求、法令、技術及最新業務發展現況至少評估或修訂一次。

7 施行

本政策須經「資訊安全委員會」核定後實施，修訂時亦同。本政策公告實施後需以適當方式公告或傳達給本校各單位人員與相關外部單位周知以落實執行運作。