國立政治大學

資通安全政策

機密等級：一般

文件編號：NCCU-A-001

版　　次：2.0

發行日期：113/07/30

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	110/09/06	All	郭紫玫	初版 (依資通安全管理法與 ISO 27001 標準要求事項修訂)
1.1	111/09/30	p.2	郭紫玫	依行政院要求，為免影響資安事件通報，勿納入資安事件發生次數，調整為不得發生未通報情形
2.0	113/07/30	All	郭紫玫	1. 因應 ISO 27001 2022 標準，進行內容調整。 2. 調整定量化指標。

資通安全政策					
文件編號	NCCU-A-001	機密等級	一般	版次	2.0

目錄

資通安全政策					
文件編號	NCCU-A-001	機密等級	一般	版次	2.0

1 目的

為確保國立政治大學（以下簡稱本校）所屬之資訊資產的機密性、完整性及可用性，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，並衡酌本校之業務需求，訂定本政策。

2 適用範圍

本政策適用範圍為本校之全體人員、委外服務廠商與訪客等。

3 目標

為維護本校資通業務之機密性、完整性與可用性，保障使用者資料隱私安全，並提升人員安全意識，期藉由本校全體同仁共同努力來達成下列目標：

3.1 保護本校資通業務之安全，避免未經授權的存取，確保其機密性。

3.2 保護本校資通業務之安全，避免未經授權的修改，確保其正確性與完整性。

3.3 建立本校資通業務永續運作計畫，確保業務活動之持續運作。

3.4 確保本校資通業務之執行須符合相關法令或法規之要求。

4 責任

4.1 本校應成立資通安全組織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訊安全管理制度，並透過適當的標準和程序實施本政策。

4.2.1 資訊安全政策範疇，依據 ISO 27001 標準涵蓋四大控制措施領域，分別為組織控制措施、人員控制措施、實體控制措施及技術控制措施，並參考 ISO 27002 發展出各項主題政策，分述如下：

4.2.1.1 存取控制。

4.2.1.2 實體及環境安全。

4.2.1.3 資產管理。

4.2.1.4 資訊傳送。

4.2.1.5 端點裝置之安全組態及處置。

4.2.1.6 連網安全。

4.2.1.7 資訊安全事故管理。

4.2.1.8 備份。

4.2.1.9 密碼技術及金鑰管理。

4.2.1.10 資訊分類分級及處理。

4.2.1.11 技術脆弱性管理。

4.2.1.12 安全開發。

4.3 本校所有人員、委外服務廠商與訪客等皆應遵守本政策。

4.4 本校應考量內、外部議題及利害關係者要求，訂定適當之資訊安全管理制度（ISMS）實施範圍，經由管理階層審核、確認後實行。

4.5 本校所有人員及委外服務廠商均有責任透過適當通報機制，通報資通安全事件或資通安全弱點。

4.6 任何危及資通安全之行為，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懲處。

4.7 本校定期審查資訊安全目標之達成。

5 管理指標

5.1 定量化指標

5.1.1 確保本校核心資通機房維運服務達全年時間 98%(含) 以上之可用性。

5.1.2 確保滿足核心資通系統之服務可用率，扣除因系統維護得停止服務時間，達全年之服務可用率≧99.5%。

5.1.3 發生資通安全事件時，不得有未通報情形。

5.2 定性化指標

5.2.1 定期審查本校資通安全組織人員執掌，以確保資通安全工作之推展。

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通安全相關訓練。

5.2.3 應加強本校核心資通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。

5.2.5 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。

5.2.6 確保所有資通安全意外事故或可疑之安全弱點，都應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

6.1 本政策應至少每年審查乙次，以反映政府法令、技術及業務等最新發展現況，確保維持營運和提供服務之能力。

6.2 資訊安全管理制度（ISMS）實施範圍應定期或不定期視內、外部環境之變更或執行狀況，如：法令法規之要求、組織異動、資安事件發生、管理制度落實狀況等因素，於管理審查會議進行檢視調整。

7 實施

本政策經「資通安全委員會」核定後實施，得以書面、電子或其他方式通知同仁、與本校相關利害關係者及提供資通服務之廠商，修訂（正）時亦同。