國立臺南大學

資通安全管理政策

機密等級：一般

文件編號：NUTN-ISMS-A001

版　　次：7.0

發行日期：112 年 6 月 12 日

國立臺南大學資通安全管理政策

99.06.08 資訊安全委員會審議通過
99.12.29 資訊安全委員會修正通過
105.12.12 資訊安全委員會修正通過
108.06.10 資通安全委員會修正通過
110.06.07 資通安全委員會修正通過
112.06.12 資通安全暨個人資料保護推動委員會修正通過

1、 目的

國立臺南大學（以下稱本校）為確保及維持資訊資產之機密性、完整性及可用性，依據資通安全管理法及相關子法、ISO/CNS27001、教育體系資通安全暨個人資料管理規範建立資通安全管理制度（以下簡稱 ISMS），落實資通安全防護措施，以符合相關法令規範及內、外部關注方之資通安全期望與要求，特訂定資通安全管理政策（以下簡稱本政策）。

2、 適用人員

本校所有的人員、維護廠商、業務往來者及使用本校服務之使用者，涉及任何資通安全管理系統所涵蓋的範圍，都必須實施或配合這個政策。

3、 範圍

3.1 資通安全管理系統(以下簡稱本系統)，其範圍包括：

3.1.1 本系統涉及之核心業務為「網路應用服務」及「校務資訊系統」。

3.1.2 本校擁有及存放於本校之各種資訊資產及資料。

3.1.3 本校各辦公處所、建築、機房設備及校園網路之設備。

3.1.4 執行作業之人員、系統、手冊、工具、基礎建設。

4、 名詞定義

4.1 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。

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

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

4.4 資通安全：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。

4.5 資訊資產：凡本校作業流程中與資訊及資訊處理設施相關聯之資產，如紙本文件、電子文件、網路服務、電腦應用軟體、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。

5、 權責

5.1 設置本校「資通安全暨個人資料保護推動委員會」，負責政策之核定及監督、資通安全預防及危機處理。

6、 要求事項

6.1 資通安全目標

6.1.1 確保本校核心資通系統網路機房維運服務達全年上班時間 96%以上之可用性。

6.1.2 因資通安全事件、異常事件、其他安全事故造成系統、主機異常而中斷營運服務之情事，每次最長不得超過系統所訂之復原時間目標(recovery time objective, RTO)。

6.1.3 本校核心資通系統服務達全年上班時間 98%以上之可用性，本校~~關鍵業務~~核心資通系統因資通安全事件、異常事件、其他安全事故造成系統、主機異常而中斷營運服務之情事，每次最長不得超過系統所訂之復原時間目標(recovery time objective, RTO)。

6.2 資通安全管理事項

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。資通安全管理應涵蓋下列管理事項：

1.資通安全政策。

2.資通安全組織。

3.人力資源安全。

4.資產管理。

5.存取控制。

6.加密控制(密碼學)。

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.資通安全事故管理。

13.營運持續管理之資通安全層面。

14.遵循性。

6.3 資通安全管理原則

6.3.1 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。

6.3.2 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(例 rar)及身分鑑別機制，以加強資訊資產之安全。

6.3.3 對於資通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。

6.3.4 應訂定營運持續計畫並定期演練，以確保重要系統、業務於資安事故發生時能於預定時間內恢復作業。

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

6.3.6 定期執行資通安全稽核作業，檢視存取權限及資通安全管理制度之落實。

6.3.7 違反本政策與資通安全相關規範者，依相關法規辦理。

6.3.8 本政策每年至少評估一次，依業務變動、技術發展及風險評鑑的結果修訂。

7、 修訂

7.1 管理階層審查

確保「資通安全管理系統」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通安全管理要求、法令、技術及最新業務發展現況至少評估或修訂一次。

8、 施行

8.1 本政策須經「資通安全暨個人資料保護推動委員會」審核，核定後依據「文件管理程序書」公告或傳達給本校各單位人員與相關外部單位實施，修訂時亦同。

9、 相關文件

9.1 國立臺南大學資通安全暨個人資料保護推動委員會設置要點

9.2 風險評鑑與管理程序書

9.3 文件管理程序書