1、 目的

花蓮縣教育處教育網路中心（以下簡稱本中心）為確保資訊資料、系統、設備及網路通訊安全，有效降低因人為疏失、蓄意或天然災害等導致之資通資產遭竊、不當使用、洩漏、竄改或毀損等風險，並建立資通安全管理體系，特訂定資通安全政策(以下簡稱本政策)，本政策未規定事項依政府其他資通安全法規辦理，以達成資通之機密性、完整性與可用性。

2、 依據

依據下列相關法令訂定本政策。

1、 資通安全管理法及其相關子法

2、 個人資料保護法

3、 ISO/IEC 27001 (Information technology, cybersecurity and privacy protection – Information security management systems - Requirements)

4、 CNS 27001 (資訊安全、網宇安全及隱私保護 – 資訊安全管理系統 – 要求事項)

5、 臺灣學術網路管理規範

6、 花蓮縣教育處教育網路中心資訊安全暨個人資料保護政策

7、 花蓮縣教育處教育網路中心資訊安全相關管理規範

3、 實施範圍

本中心資訊安全管理系統(ISMS)之實施範圍為各資通系統之開發、維護及相關機房支援活動的管理」(以下簡稱本範圍)。

4、 政策

1、 確保本範圍內各項資通作業均符合相關法規要求。

2、 確保本範圍內妥適保護所屬資通資產之機密性、完整性及可用性，避免未經授權之存取與修改。

3、 確保本範圍內對外資通相關服務之持續運作。

5、 目標

1、 連線至官網服務之網路維運服務一年不得非預期中斷次數

2、 官網系統維運服務一年不得非預期中斷次數

3、 連線至各資通系統服務之網路維運服務一年不得非預期中斷次數

4、 各資通系統維運服務一年不得非預期中斷次數

5、 資通安全政策審查次數1

6、 資通安全政策宣導次數2

7、 管理審查會議召開次數1

8、 檢查資通安全受訓時數-12小時

9、 資通資產清單已定期更新-半年

10、 定期審查系統存取權限（帳號清查）-1年

11、 檢討營運持續運作計畫演練執行情形

12、 定期執行資安查核次數

13、 矯正措施未於預定時間內改善完成

14、 定期檢視外來文件內容與版本的適用性

6、 控制措施

1、 本範圍內各項資通安全管理規定必須遵守政府相關法規包括但不限於刑法、國家機密保護法、著作權法、個人資料保護法、資通安全管理法等之規定。(外來文件管制表)

2、 由本中心資通安全推動小組負責資通安全制度之建立及推動事宜。(組織人員名冊)

3、 定期實施資通安全教育訓練，宣導資通安全政策及相關實施規定。(每人3小時)

4、 建立資通硬體設施及軟體之管理機制，以統籌分配、運用全單位資源。(資產管理程序規範)

5、 建置新資訊系統前，應將資通安全納入考量因素，防範發生危害系統安全之情況。(資通系統獲取、開發及維護管理程序規範)

6、 建立電腦機房實體及環境安全防護措施，並定期實施相關保養。(機房、設備保養紀錄、維護紀錄)

7、 明確規範資通系統及網路服務之使用權限，防止未經授權之存取動作。(網路安全管理規範、存取控制管理規範)

8、 訂定資通作業安全內部稽核計畫，定期檢視本範圍內人員個人電腦使用情形。(內部稽核計畫、內部稽核報告)

9、 訂定資通作業之災害復原演練計畫並實際演練，確保本中心業務持續運作。(BCP)

10、 本範圍內人員皆有維持資通安全之責任，且應遵守相關之資通安全管理規定。(政策宣導紀錄)

11、 本中心管理階層應積極參與資通安全管理活動，提供對資通安全之支

持及承諾。(管理審查會議)

12、 資通安全政策應定期進行評估修正並頒布實施，以反映政府資通安全管理政策、法令、技術及本中心業務之最新狀況，並確保本中心資通安全實務作業的可行性及有效性。(每年審議紀錄)

7、 修訂與公告

本政策由本中心資通安全推動小組每年定期審議，另組織、業務、關係方之關注、法令或實體環境等因素之變迭時，予以適當修訂。本政策經本中心資通安全管理委員會資通安全長核定後公布施行，修正時亦同。