國立宜蘭大學

資通安全政策管理程序

文件編號：	I-01-01
版　　次：	1.4
實施日期：	114 年 3　月 27　日
機密等級：	公開

文件制/修訂履歷

制/修訂版次	制/修訂日期	制/修訂說明	制/修訂者	備註
1.0	110/07/30	初版發行	吳玉玲	
1.1	111/08/11	修訂	鄭賀元	刪除陸.一. 行政院及所屬各機關資通安全管理要點
1.2	112/07/04	修訂	邱月娥	原作者字樣改為制/修訂者
1.3	113/05/17	修訂	鄭賀元	修正陸.二：國家標準 CNS27001 名稱為「資訊安全、網宇安全及隱私保護」
1.4	114/03/27	修訂	卓美涓	刪除陸.一行政院國家資通安全會報..

目　　錄

壹、目的

資通安全與個人資料管理委員會（以下稱本委員會）為推動國立空中大學(以下稱本校)資訊安全管理制度，建立安全及可信賴之資訊環境，確保資訊資產之機密性、完整性及可用性，由本校訂定之資通安全政策管理程序，以為適從。

貳、適用範圍

本校各單位與委外服務供應商。

參、定義

無。

肆、權責

一、本委員會資通安全執行組(以下稱資安組)透過標準和程序以實施此政策。

二、本校各單位和委外服務供應商(以下稱所有人員)均須依照本安全管理程序以維護本校資通安全政策。

三、所有人員有責任報告資通安全事件和任何已鑑別出之弱點。

四、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。

伍、作業程序

一、制訂

每年應針對本校資通安全政策及其他相關管理政策共同討論、編制、確認各項政策內容，並依權責提請本委員會審查及核准。資通安全政策與資通安全目標如下：

(一). 資通安全政策

確保本校資通安全，防範資安攻擊事件。

增進校務運作效能，達成永續發展目標。

(二). 資通安全目標

1 確實遵守「資通安全管理法」、「個人資料保護法」、「著作權法」、「電子簽章法」等資通安全相關法令。

2 為能有效確保本校資通安全，應針對各資通安全領域訂定資通安全規範。

3 遵循本校資安事件通報機制，通報所發現之資通安全事件或資通安全弱點。

4 對於資通安全事件須有完整的通報及應變措施，以確保資通系統及重要業務的持續運作。

5 進行資訊處理時，若含有個人資料，應依據「個人資料保護法」及相關規定審慎處理，不私自蒐集或洩漏業務資訊，非公務用途嚴禁調閱使用。

6 本委員會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。

7 依角色及職能為基礎，針對不同層級人員，依據「資通安全管理法」之規定或實際需要辦理資通安全教育訓練及宣導，促使全體人員瞭解資通安全的重要性，各種可能的安全風險，以提高資通安全意識並熟悉工作中之資通安全職責，促其遵守資通安全規定。

8 應使用具合法版權軟體，避免上網下載來路不明之軟體。

9 委外廠商應遵循本政策以及相關程序之規定，不得未經授權使用或濫用本委員會之各類資訊資產，若涉及限制使用等級以上業務，應簽署保密切結書。

10 每年至少召開一次管理審查會議，審核本校資通安全業務執行狀況，建立管理指標量測方式與評估管理指標量測結果。

11 應建立資訊資產風險評鑑機制，每年至少進行一次風險評鑑，並由資安組執行長決定可接受風險值。

12 每年應至少進行一次業務永續經營計畫及資安事件通報程序之演練、測試、檢討。

13 違反本政策與本校之資通安全相關規範，依相關法規或本校懲戒規定辦理。

二、審查

(一). 資通安全政策審查

資通安全政策由資安長或其授權對象(如:資安組執行長)審查及核准。審查形式可由資安組擬定後送請審閱並核定；或經資安長或其授權對象審議。

三、發布、傳達與宣導

資通安全政策及相關政策依權責核定後，應對所有人員及相關外部關注者公布及傳達。資安組統籌規劃政策之溝通於年度教育訓練計畫中，透過教育訓練的方式，使內部及外部關注者全盤了解本政策。可將資通安全政策政策張貼於布告欄及會議室中，確保所有人員知悉。

四、修訂

本政策應至少每年檢討一次，於年度中如有法令或上級主管機關之相關命令發布實施，得：

(一). 由承辦單位發起召開臨時會議，或

(二). 於本委員會工作會議中，

針對法令或上級主管機關之相關命令進行討論，以確認是否需修訂本校各項資通安全政策或其他管理政策，以符合政府法令之要求，並反映資訊科技發展趨勢，確保本校資通安全管理作業之有效性。

陸、參考文件

一、國家標準 CNS 27001 資訊安全、網宇安全及隱私保護－資通安全管理系統－要求事項

二、資通安全管理法及其子法

柒、使用表單

無