南臺科技大學 高教深耕計畫-資安強化專章執行成果

112-113年執行成果

全校導入資訊安全管理系統

推動項目	成果
資通安全推動組織	● 成立「資通安全暨個人資料保護管理委員會」，主席為校長、校內一級主管為委員、資安長及資料保護長為副校長、執行秘書為計網中心主任，並設有六個工作小組協助推動各項管理制度相關工作。 ● 本校各級主管皆重視資安議題，最近一次會議有八成以上主管親自出席。
資通系統及資訊資產盤點	● 已完成全校行政與學術單位資通系統清查作業，並將每年定期檢視與更新。 ● 持續進行全校資訊資產盤點，至114年7月行政單位已完成盤點，並規劃學術單位115年開始進行，預計115年完成全校盤點。
資通安全風險管理	● 持續進行全校資通安全風險評估作業，至114年7月已完成行政單位風險評估與改善作業，並規劃學術單位115年開始進行。 ● 持續進行資通系統弱掃作業，掃描出之各級弱點皆有進行處理與修正。
內部稽核	● 持續進行全校性資通安全內部稽核，114年完成行政單位內部稽核，學術單位則115年開始進行，預計於116年全數完成。
業務持續運作演練	● 核心資通系統每年皆進行業務持續作演練作業。 ● 演練內容皆納入CIA情境，並會與前年情境不同，以提升演練之有效性。
資訊安全管理系統適用範圍	● 本校「資通安全暨個人資料保護管理政策」施行範圍為全校，內容涵蓋資訊安全管理系統(ISMS)與個人資料管理系統(PIMS)。 ● 除全校性內部稽核外，每年皆會推派不同單位進行第三方外部稽核作業，確保制度於全校範圍有效推行。

112-113年執行成果

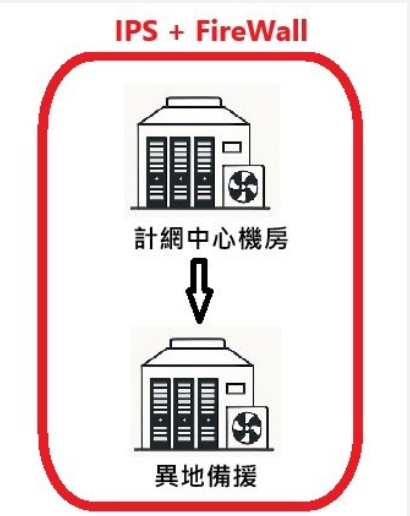
強化人員資通安全認知與訓練

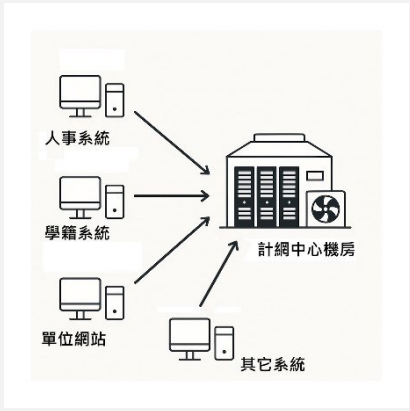
推動項目	成果
全校教職員資安教育訓練達成比率	● 每學期皆會辦理資安通識教育訓練，並進行課後測驗；除實體課程外，也提供線上課程供教職員參與。 ● 每年透過校務會議與行政會議來強化管考各單位教職員工參與訓練之完成度。
新進人員資安認知訓練	● 人事室每學期皆有定期安排新進人員參加相關資安認知訓練課程，未到場者則會列入下一次研習名單中。
社交工程演練被誘騙者加強資安意識措施	● 配合教育部每半年針對教職同仁進行「防範惡意電子郵件社交工程演練」，並針對開啟郵件、點閱郵件附件或連結之人員安排資安教育訓練，並於課程結束後進行測驗，以確認學習效果。
提升系統開發人員資安專業	● 本校已依SSDLC各項要求訂定「系統開發與維護程序書」，程式開發皆依照程序書規範進行並留存紀錄。 ● 程式開發主責單位每年皆在第三方驗證範圍內，驗證開發流程符合ISO27001:2022與本校程序書之要求。 ● 系統開發人員每年皆完成3小時以上資安專業課程訓練。
推動項目	● 每學期皆會辦理資安通識教育訓練，除實體課程外，也提供線上課程供教職員參與。 ● 每年透過校務會議與行政會議來強化管考各單位教職員工參與訓練之完成度。

112-113年執行成果

確保資通系統管理量能

推動項目	成果
重要資通設備設置地點(系統集中化執行率及配套措施)	● 本校核心資通系統皆集中由計網中心管理，全校資通系統約七成已集中於計網中心機房。 ● 計網中心機房設有IPS(入侵防禦系統)與FireWall防護，雲端主機與存儲設備設有異地備援機制，強化資通系統持續運作能力。
遠端維護採「原則禁止例外允許」方式	● 校內網路皆受FireWall保護，外界網路預設無法連入，如廠商有遠端作業需求須照本校「通信與作業管理程序書」規範提出申請，相關權限需經審核通過後才可開通(每次申請開通時間最長為3天)。
日誌內容、記錄時間週期及留存政策(核心系統優先落實但不限)	● 本校各資通系統皆有進行資通系統分級作業，依據分級「普」「中」「高」進行對應之資安防護基準與日誌保存設定作業。 ● 每年皆透過內部稽核與第三方外部稽核來確認各系統之資安防護基準與日誌保存是否合規。

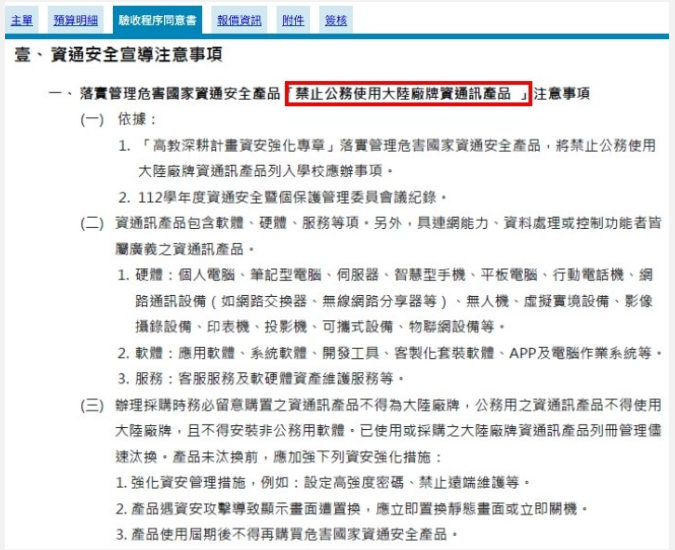




112-113年執行成果

落實管理危害國家資通安全產品

推動項目	成果
禁止公務使用大陸廠牌資通產品	● 本校採購系統已明定禁止採買大陸廠牌之規則，如為大陸廠牌則無法驗收。 ● 進行資通安全內稽工作時，也會對受稽單位所使用資通產品之廠牌進行檢核。 ● 部份大陸廠牌資通訊產品暫無法汰除，皆有進行管控措施降低風險並呈報汰換時程，經資安長核可後才允許暫時使用。
限制出租場域使用大陸廠牌資通產品	● 本校已於出租場域合約明訂不可使用大陸廠牌相關規範。 ● 已訂定「出租場域資通安全暨個人資料保護作業說明書」，以規範出租場域相關作業活動。 ● 每年度皆會對校內出租場域進行抽樣稽查，確保承租方遵守相關規範。



主單　預算明細　驗收程序同意書　報價資訊　附件　簽核

壹、資通安全宣導注意事項

一、落實管理危害國家資通安全產品「禁止公務使用大陸廠牌資通訊產品」注意事項

(一) 依據：

1. 「高教深耕計畫資安強化專章」落實管理危害國家資通安全產品，將禁止公務使用大陸廠牌資通訊產品列入學校應辦事項。
2. 112學年度資通安全暨個保護管理委員會議紀錄。

(二) 資通訊產品包含軟體、硬體、服務等項。另外，具連網能力、資料處理或控制功能者皆屬廣義之資通訊產品。

1. 硬體：個人電腦、筆記型電腦、伺服器、智慧型手機、平板電腦、行動電話機、網路通訊設備（如網路交換器、無線網路分享器等）、無人機、虛擬實境設備、影像攝錄設備、印表機、投影機、可攜式設備、物聯網設備等。
2. 軟體：應用軟體、系統軟體、開發工具、客製化套裝軟體、APP及電腦作業系統等。
3. 服務：客服服務及軟硬體資產維護服務等。

(三) 辦理採購時務必留意購置之資通訊產品不得為大陸廠牌，公務用之資通訊產品不得使用大陸廠牌，且不得安裝非公務用軟體。已使用或採購之大陸廠牌資通訊產品列冊管理儘速汰換。產品未汰換前，應加強下列資安強化措施：

1. 強化資安管理措施，例如：設定高強度密碼、禁止遠端維護等。
2. 產品遇資安攻擊導致顯示畫面遭置換，應立即置換靜態畫面或立即關機。
3. 產品使用屆期後不得再購買危害國家資通安全產品。

114-116年未來規劃

持續強化各項資安作為

推動項目	說明
全校導入資訊安全管理系統ISMS	● 除全校性ISMS制度教育訓練外，推動小組也將至單位進行實地訪談與溝通，協助各單位落實ISMS制度各項作業。
資通安全風險管理	● 除核心資通系統完成弱點掃描/滲透測試/資安健檢外，校內個資數量較多之重要系統也計畫進行弱點掃描/滲透測試。 ● 重要業務承辦人員電腦導入EDR(端點偵測及應變機制)
重要資通設備設置地點(系統集中化執行率及配套措施)	● 校內核心資訊系統與個資量較多之重要系統導入VANS（資通安全弱點通報機制）。
禁止公務使用大陸廠牌資通產品	● 每年編列全校性固定經費，逐步淘汰校內舊有大陸廠牌資通產品
委外資安要求	● 本校已依據「資通安全管理法施行細則」訂定資通訊服務「委外管理程序書」，將持續於行政會議及資安相關教育訓練進行宣導。 ● 將與本校採購/驗收主責單位配合，協助審核委外系統開發/全校性資訊設備維護採購案，確保採購案與合約符合資安法及本校「委外管理程序書」要求，並留存相關審核紀錄。