第二期高等教育深耕計畫資安強化專章規劃(草案)

教育部資訊及科技教育司

111年10月21日

大 綱

1. 第二期規劃 - 主冊專章：資安強化
2. 計畫專章撰寫建議方向

1.第二期規劃 - 主冊專章：資安強化

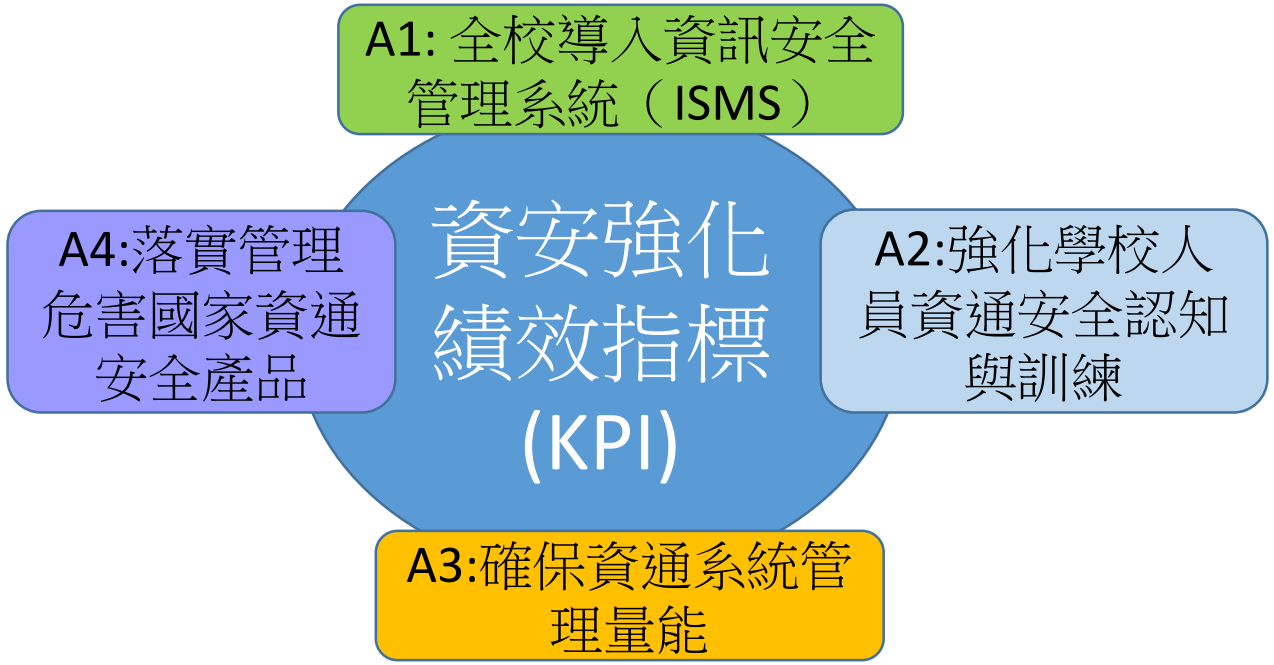
第二期規劃 - 主冊專章：資安強化

- **計劃說明:**
  - 為協助大學建立持續性與永續性的教研環境，不因資安事件受影響而中斷教學與研究，爰規劃資安強化專章，大學可參照資通安全管理法及其子法要求，推動資通安全管理，以資通安全責任等級分級辦法就管理面、技術面及認知與訓練面研提規劃推動之策略及擬定相關績效指標。

2.計畫專章撰寫建議方向

計畫專章撰寫建議方向

- 各校可參考數位發展部資通安全署「資通安全維護計畫範本」撰寫資安強化的各項指標(KPI)要求相關內容，並**提供參考相關文件**(例如:**程序書**或**表單**)



計畫專章撰寫建議方向

- 依本部訂定資安強化(績效指標)提供參考之績效指標(A1~A4)

A1: 全校導入資訊安全管理系統（ISMS）	A2:強化學校人員資通安全認知與訓練	A3:確保資通系統管理量能	A4:落實管理危害國家資通安全產品
K1.資通安全長之配置 K2.資通安全推動組織 K3.資通系統及資訊之盤點 K4.資通安全風險評估 K5.內部資通安全稽核及委外稽核 K6.業務持續運作演練 K7.資訊安全管理系統(ISMS)適用範圍	K1.配置資通安全專職人員 K2.提升資通安全專職人員資安職能 K3.提升教職員資安意識	K1.資通系統集中化管理 K2.適度降低資通系統數量	K1.禁止公務使用大陸廠牌資通訊產品 K2.限制出租場域使用大陸廠牌資通訊產品

計畫專章撰寫建議方向

主項目	次要項目	KPI (學校可依需求自行另訂量化指標)	備註
全校導入資訊安全管理系統（ISMS）	資通安全長之配置	學校置資通安全長，指派主任秘書以上人員兼任。	建議參照主管機關「資通安全維護計畫書」範本，於「伍、資通安全推動組織 一、資通安全長」加入資安具體策略及措施項目
	資通安全推動組織	學校資通安全推動組織由資通安全長召集全校各單位（包含行政單位及系所辦公室）主管或副主管組成，每年至少召開會議1次。	建議參照主管機關「資通安全維護計畫書」範本，於「伍、資通安全推動組織 二、資通安全推動小組」加入資安具體策略及措施項目
	資訊安全管理系統(ISMS)適用範圍	ISMS適用範圍至少包含全校範圍內之核心資通系統、保有個資或防護需求中等級以上之資通系統，及其相關網路與資訊機房活動。	建議參照主管機關「資通安全維護計畫書」範本，於「貳、適用範圍」加入資安具體策略及措施項目

計畫專章撰寫建議方向

主項目	次要項目	KPI (學校可依需求自行另訂量化指標)	備註
全校導入資訊安全管理系統（ISMS）	資通系統及資訊之盤點	學校辦理資通系統及資訊之盤點，盤點範圍包含全校各單位。 1.資通系統資產清冊至少包含落於各校IP網段內、或使用各校網域名稱之資通系統。 2.物聯網設備管理清冊包含學校採購、公務使用之物聯網設備。	建議參照主管機關「資通安全維護計畫書」範本，於「柒、資訊及資通系統之盤點 一、資訊及資通系統盤點」加入資安具體策略及措施項目
	資通安全風險評估	分析全校資訊資產及個人資料檔案可能面臨的風險，並選取適當安控措施。	建議參照主管機關「資通安全維護計畫書」範本，於「捌、資通安全風險評估」加入資安具體策略及措施項目

計畫專章撰寫建議方向

主項目	次要項目	KPI (學校可依需求自行另訂量化指標)	備註
全校導入資訊安全管理系統（ISMS）	內部資通安全稽核及委外稽核	1.學校辦理內部資通安全稽核，稽核範圍包含全校各單位。 2.內部資通安全稽核結果需提報管理審查。 3.學校定期稽核委外服務供應商，以確保資訊作業委外安全。	建議參照主管機關「資通安全維護計畫書」範本，於「壹拾伍、資通安全維護計畫及實施情形之持續精進及績效管理機制」加入資安具體策略及措施項目
	業務持續運作演練	1.針對核心資通系統制定業務持續運作計畫，並定期辦理全部核心資通系統之業務持續運作演練。 2.將行政單位、系所網頁遭竄改納入業務持續運作演練情境。	建議參照主管機關「資通安全維護計畫書」範本，於「玖、資通安全防護及控制措施 五、業務持續運作演練」 加入資安具體策略及措施項目

計畫專章撰寫建議方向

主項目	次要項目	KPI (學校可依需求自行另訂量化指標)	備註
強化學校人員資通安全認知與訓練	配置資通安全專職人員	資通安全專職人員指全職執行資通安全業務者，並依其專業技能給予適當薪資。	建議參照主管機關「資通安全維護計畫書」範本，於「陸、專職(責)人力及經費配置」加入資安具體策略及措施項目
	提升資通安全專職人員資安職能	1.資通安全專職人員各自持有1張以上資通安全專業證照，及1張資通安全職能訓練證書或通過教育體系資通安全專業課程評量。 2.資通安全專責人員以外之資訊人員各自持有1張以上資通安全職能訓練證書或通過教育體系資通安全專業課程評量。	建議參照主管機關「資通安全維護計畫書」範本，於「陸、專職(責)人力及經費配置」加入資安具體策略及措施項目
	提升教職員資安意識	全校教職員每年完成3小時以上資通安全通識教育訓練。	建議參照主管機關「資通安全維護計畫書」範本，於「壹拾參、資通安全教育訓練」加入資安具體策略及措施項目

計畫專章撰寫建議方向

主項目	次要項目	KPI (學校可依需求自行另訂量化指標)	備註
確保資通系統管理量能	資通系統集中化管理	資通系統資安管理作業，原則集中至學校資訊(安)單位或其他具備資通安全專業能力之團隊統籌辦理，並因應集中化管理需求增聘適當人力。	建議參照主管機關「資通安全維護計畫書」範本，於「玖、資通安全防護及控制措施〇(新增)、確保資通系統管理量能」，加入資安具體策略及措施項目
	適度降低資通系統數量	汰換、整併校內資通系統網站，以降低資通系統數量。加強閒置網站（指使用率不高者）及因應臨時需求建置網站（如活動專用網站）之資安管理措施，依其專案需求下架或限制存取。	建議參照主管機關「資通安全維護計畫書」範本，於「玖、資通安全防護及控制措施〇(新增)、確保資通系統管理量能」加入資安具體策略及措施項目

計畫專章撰寫建議方向

主項目	次要項目	KPI (學校可依需求自行另訂量化指標)	備註
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	依行政院政策要求，公務用之資通訊產品（含軟體、硬體及服務）不得使用大陸廠牌，已列管者儘速汰換。	建議參照主管機關「資通安全維護計畫書」範本，於「玖、資通安全防護及控制措施○(新增)、落實管理危害國家資通安全產品」加入資安具體策略及措施項目
	限制出租場域使用大陸廠牌資通訊產品	依行政院政策要求，針對學校出租場域，於學校委外契約或場地租借使用規定，明訂不得使用危害國家資安之產品（如大陸廠牌軟體、硬體及服務）。	建議參照主管機關「資通安全維護計畫書」範本，於「玖、資通安全防護及控制措施○(新增)、落實管理危害國家資通安全產品」加入資安具體策略及措施項目

格式

- 專章計畫提報之頁數以5頁為限（不含封面、毋須目次頁）、A4大小、14號字、雙面列印。
- 計畫書內容：
  - 1.計畫推動策略(可就全校導入資訊安全管理系統(ISMS)、強化學校人員資通安全認知與訓練、確保資通系統管理量能、落實管理危害國家資通安全產品等面向自行調整或增列)
  - 2.五年(112年至116年)總體目標
  - 3.各年度(112年至116年)目標值
  - 4.經費規劃

報告完畢