（學校名稱）
高等教育深耕計畫第二期
專章—資安強化
第一階段（112至113年）成果報告暨
第二階段（114至116年）計畫書
（撰寫架構）

（封面可自行設計）

1.請以A4紙張、直式橫書、14號字、固定行高21點方式雙面列印裝訂，毋須目次頁，以5頁為限（不含封面、附表）。
2.請於113年12月5日（星期四）下午5時前，將紙本及光碟（含計畫書電子檔WORD檔及PDF檔）之各1份，函報本部資訊及科技教育司（寄送達，非以郵戳為憑）；公文副本知會資安專章計畫辦公室（10025臺北市中正區濟南路一段321號（國立臺北商業大學資訊與網路中心）），同時檢附紙本1份。
3.並於113年12月5日（星期四）下午5時前至資安強化專章執行成果填報平臺（https://sproutsec.moe.edu.tw/）填報附表1-2，紙本免附。

中華民國113年　月　日

一、執行成效說明**(112**至**113**年**)**

二、目前遭遇困難與建議解決方式

三、推動策略及預期效益**(114**至**116**年**)**

（1）基本資訊:

1. 學校單位數量(行政、教學與研究單位):

2. 教師及職員數量:

3. 資通系統數量:

4. 委外系統數量:

5. 大陸廠牌資通訊產品數量:

（2）學校推動資訊安全強化預計投入經費(附表1-1)。

（3）績效指標與執行說明(附表1-2)。

附表**1-1 主冊專章-推動資訊安全強化預計投入之經費**

單位:元

推動資訊安全強化預計投入經費				
項目 年度	人事費	業務費	設備費	總計
114年				
115年				
116年				

3年度總計				

附表**1-2**績效指標與執行說明

項目	推動策略	評核指標	未來3年績效指標			落實執行之規劃說明
			114年	115年	116年	
1.全校導入資訊安全管理系統ISMS	1.1資通安全長之參與	1.1.1資安長參與支持之相關記錄				
	1.2資通安全推動組織	1.2.1由全校一級單位主管或副主管組成委員會並出席相關會議				
		1.2.2落實管理審查(八大議題的納入)				
		1.2.3利害關係人關注與回應處置				
	1.3資通系統及資訊之盤點	1.3.1資訊資產清冊持續推動全校盤點、更新	%	%	%	
		1.3.2全校範圍系統持續完整盤點				
		1.3.3全校範圍IoT持續完整盤點及安全管控	%	%	%	
	1.4資通安	1.4.1全校執行風險評	%	%	%	

項目	推動策略	評核指標	未來3年績效指標			落實執行之規劃說明
	全風險管理	估				
		1.4.2系統主機弱掃/網站弱掃、滲透測試、資安健診執行規劃				
		1.4.3安全檢測結果修補管控制度及執行成效				
		1.4.4防毒、防火牆等防護措施				
	1.5內部稽核	1.5.1持續推動並完成全校內部稽核作業	%	%	%	
	1.6委外資安要求	1.6.1委外招標案納入資安規範				
		1.6.2委外承辦人及廠商資安教育訓練				
		1.6.3委外廠商作業及維護流程資安檢視				
	1.7業務持續運作演練	1.7.1核心系統BCP(完備C.I.A.演練情境)				
		1.7.2重要資料異地備份及回復測試(至少全	%	%	%	

項目	推動策略	評核指標	未來3年績效指標			落實執行之規劃說明
		部核心系統)				
	1.8資訊安全管理系統(IS MS)適用範圍	1.8.1以全校為範圍訂定資安目標及其達成之量測				
2.強化學校人員資通安全認知與訓練	2.1提升教職員資安意識	2.1.1全校教職員資安教育訓練達成比率	%	%	%	
		2.1.2新進人員資安認知訓練				
		2.1.3社交工程演練被誘騙者加強資安意識措施				
		2.1.4資安事件通報校內程序宣導及演練				
	2.2提升系統開發人員資安專業	2.2.1開發及維護系統符合資通系統防護基準執行控制措施				
		2.2.2落實SSDLC				

項目	推動策略	評核指標	未來3年績效指標			落實執行之規劃說明
3.確保資通系統管理量能	3.1資通系統集中化管理	3.1.1重要資通設備設置地點(系統集中化執行率及配套措施)	%	%	%	
		3.1.2遠端維護採「原則禁止例外允許」方式				
		3.1.3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)				
4.落實管理危害國家資通	4.1禁止公務使用大陸廠牌資通產品	4.1.1禁止採購大陸廠牌資通產品作法及教育訓練宣導				
		4.1.2全校範圍既有列冊管理及管控措施、汰除				
	4.2限制出租場域使用大陸廠牌資通產品	4.2.1出租場域禁用規定及教育訓練宣導				

項目	推動策略	評核指標	未來3年績效指標			落實執行之規劃說明
安全產品						
5.學校資安額外作為	5.1創新或創意的規劃作為	*可自行增列指標				
		*可自行增列指標				
		資安額外作為建議可先考慮: • 「資通安全責任等級分級辦法」應辦事項，如:資通安全弱點通報機制(VANS)導入、端點偵測及應變機制(EDR)導入、政府組態基準(GCB)導入、資通安全威脅偵測管理機制(SOC)建置、入侵偵測及防禦機制(IDS/IPS)建置、應用程式防火牆(WAF)建置、進階持續性威脅攻擊防禦措施(APT)建置、擴大弱點掃描/滲透測試實施範圍、配置其他資安專責人員。 • 或「資通系統防護基準」做法，如:高級系統異地備份機制、中/高級系統備援機制、對外服務系統傳輸之機密性與完整性全面改善(啟用HTTPS、TLS等安全傳輸協定)。 • 或113年實地稽核新增查核項目，如:雲端服務應用資安防護、公務使用即時通訊軟體管控措施。				