資安專章附錄

附表 1-2 主冊專章-推動大學資訊安全強化績效指標

一、 教育部要求大學推動資安之重點工作項目表

主項目	編號	次要項目	執行策略與方法
全校導入資訊安全管理系統（ISMS）	1-1	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。
	1-2	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，每年召開會議 1 次。
	1-3	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。 3.每年度製作「資訊資產清單」，並請資安長審查。 4.各單位管理之資訊或資通系統如有異動，更新「資訊資產清單」。
	1-4	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。 各單位依據資通系統盤點結果，評估風險值，並制定相關控制措施，降低、避免、轉移、接受風險後，送資安長審查。
	1-5	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。
	1-6	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，並每二年辦理一次核心資通系統持續運作演練。

			2. 官網網頁遭竄改納入業務持續運作演練情境。
	1-7	資訊安全管理系統（ISMS）適用範圍	1.ISMS 適用範圍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。 2.核心系統依法規執行相關安全檢測。 3.網路與資訊機房活動進行定期資安健診。 4.導入 VANS 弱點通報系統。 5.驗證資網中心 ISMS。
強化學校人員資通安全認知與訓練	2-1	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。
	2-2	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每 2 年完成 3 小時以上資通安全專業課程教育訓練。 3.建立校園資安種子人員網絡、強化組織不斷常新與精進能力。
	2-3	提升教職員資安意識	每年完成 3 小時以上資通安全通識教育訓練。
確保資通系統管理量能	3-1	資通系統集中化管理	1.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。 2.推展主機虛擬化以有效納管各單位之系統。
	3-2	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。
落實管理危害國家資通安全產品	4-1	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。 持續宣導不購買使用大陸廠牌資通訊產品資通訊產品。

	4-2	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）。