文件編號	NCHU-ISMS-D-023	機密等級	限閱	版本	4.0

國立中興大學
113年度資訊安全內部稽核計畫

中華民國 113 年 5 月 20 日

文件編號	NCHU-ISMS-D-023	機密等級	限閱	版本	4.0

一、稽核目的

國立中興大學(以下簡稱本校)ISMS管理文件之「NCHU-ISMS-B-013　資訊安全稽核管理辦法」5.3點規定, 每兩年至少執行一次內部稽核作業(本校預計於三年內完成全校所有單位(含行政及學術單位)至少一次之內部稽核作業), 以檢視本校各項作業的控制目標、措施、流程及程序是否符合法規、規範、標準及組織之資訊安全法要求。

依據教育部110年12月30日臺教資(四)字第1100179797號函「國立大專校院資通安全維護作業指引」, 分階段規劃辦理內部稽核, 本校內部稽核範圍除計資中心為核心資通系統範圍檢核外, 另以行政單位優先、資通系統(包含單位網站)自行管理優先為原則進行抽查稽核。

二、稽核作業方式

資訊安全稽核小組得於執行稽核計畫前召開行前會議, 依稽核項目性質及受查單位特性選擇稽核方式, 包含檢查、觀察、詢問或查證相關文件等, 並視需要擇定適宜之抽核比率, 以蒐集及查核充分且適切之稽核證據, 並做成稽核報告。

三、稽核對象

本校全部單位。

四、稽核依據

（1） 資通安全管理法、個人資料保護法等相關法規規定。
（2） 教育部「國立大專校院資通安全維護作業指引」。
（3） 教育機構資安驗證中心「各校以全機關為範圍導入ISMS應優先落實的執行策略」(如附件)。

五、權責

依據本校ISMS管理文件之「NCHU-ISMS-B-013　資訊安全稽核管理辦法」設置要點，稽核人員接受過資訊安全稽核相關教育訓練與證照。辦理：
(1) 規劃及執行內部稽核工作，查核前通知受稽核組別。
(2) 受稽核組別於接獲稽核通知後，應配合準備稽核所需相關資料。
(3) 內部稽核發現之缺失與改善建議，並於結束稽核後提交稽核報告。

六、本年度稽核項目

本次內部稽核執行排程為113年5月20日，預計抽查本校20個單位，被抽查之單位於稽核前三個工作日告知，將協同**教育機構資安驗證中心**主導稽核員及本校計算機及資訊網路中心具有資安證照的同仁執行稽核。依據教育機構資安驗證中心及教育部對部署機關構相關作業要求-「各校以全機關為範圍導入ISMS應優先落實的執行策略」，此次稽核重點為一般人員、系統管理人員、委外承辦人員、核心系統管理員、系統開發人員等五大類人員應辦事項進行稽核。同時對照教育部實地稽核採用之「資通安全實地稽核項目檢核表」，此次稽核的重點在於管理面、技術面，如下表所列。

構面	稽核項目	稽核重點說明
管理面	四、資訊及資通系統盤點及風險評估	• 確認資訊資產盤點及相關管理程序 • 確認資訊資產處置規範與異動汰除管控作業 • 確認風險評估、風險處理及後續追蹤情形
	五、資通系統或服務委外辦理之管理措施	• 確認資訊作業委外安全管理程序 • 確認資訊委外資安要求及服務等級協議 • 確認委外人員管理 • 確認委外供應商之管理、監督及稽核
	六、資通安全維護計畫與實施情形之持續精進及績效管理機制	• 確認機關資通安全計畫訂定、修正及實施情形 • 確認內部稽核及後續追蹤

構面	稽核項目	稽核重點說明
技術面	七、資通安全防護及控制措施	• 確認安全性檢測實施情形 • 確認資通安全健診、資通安全防護實施情形 • 確認資通系統及相關設備監控 • 確認使用紀錄管理 • 確認電子資料安全管理機制 • 確認網路規劃及管理 • 確認資料處理、儲存及傳輸安全 • 確認電子資料相關設備管理確認行動裝置安全、軟體使用安全、網路即時通訊安全及電子郵件安全
	八、資通系統發展及維護安全	• 確認資通系統之防護需求 • 確認SSDLC各個階段之安全檢核, 包括系統需求、設計、開發、測試、驗收時應注意之安全措施 • 確認資通系統之變更管制程序
	九、資通安全事件通報應變及情資評估因應	• 確認資安事件通報及應變作業規範及落實 • 確認資安事件改善措施之有效性
策略面	其他	• 核心業務及其重要性 • 資通安全政策及推動組織 • 專責人力及經費配置

七、稽核時程計畫表

本次內部稽核作業由113年5月20日執行資訊安全管理制度符合性稽核。

日期	時　間	項　　目	稽核人員(校外/校內)		地點
5/20	09:00-09:30	啟始會議	楊志強 鍾沛原 劉育彰 陳偉嵩 黃攸德 黃柏森	楊崇誠 呂仲聖 吳秉特 林中義 張博凱 許家蓁 周鎂錡 林怡璇 呂竑邦 陳品澄 曾釋賢 黃惠貞	計資中心
	10:00-12:00	• 資訊及資通系統盤點及風險評估 • 資通系統或服務委外辦理之管理措施 • 資通安全維護計畫與實施情形之持續精進及績效管理機制 • 資通安全防護及控制措施 • 資通系統發展及維護安全 • 資通安全事件通報應變及情資評估因應			各單位
	午 休				
	13:30-15:30	• 資訊及資通系統盤點及風險評估 • 資通系統或服務委外辦理之管理措施 • 資通安全維護計畫與實施情形之持續精進及績效管理機制 • 資通安全防護及控制措施 • 資通系統發展及維護安全 • 資通安全事件通報應變及情資評估因應			各單位
	15:30-16:00	稽核發現彙整			計資中心
	16:00-16:30	結束會議 ※內部稽核抽查單位皆須出席結束會議。			計資中心 致平廳

八、報告撰寫及處理

稽核報告應請受稽核組別代表簽名。受稽核組別於接獲稽核報告後，應依據本校「NCHU-ISMS-B-014　資訊安全矯正與預防管理辦法」規定，兩週內完成缺失分析原因及擬採行矯正預防措施，並經單位主管核定後回覆計資中心。