**113年教育部稽核本校之流程與須請單位配合事項**

管考系統

教育部資安技術稽核(6/6,7)

教育部資安實地稽核(7/9)

管考系統(5/30前繳交資料)

大陸產品去年提報資料

附表3-1,3-2系統清冊

大陸產品去年提報資料整理(如附件)

1. 一、請機關儘速依報廢程序辦理財物報廢事宜，並於報廢前落實資安防護措施(如停用封存、避免與公務環境介接、加強監控、人員離職管理等)。二、報廢作業之依據，可參考行政院秘書長109年12月18日院臺護長字第1090201804A號函辦理。  
   ⏺廠牌/產品 : 華為手機、小米 米家手持無線吸塵器(掃地機器人)、TP-LINK無線路由器(分享器)、大疆 空拍機、OPPO手機、穿戴式心率偵測器(錶) 華為、華為4G路由器
2. 一、請機關解除列管，無須汰換。二、如有其他法規命令限制使用特定產品，則仍須遵循其他相關法規命令。三、機關於辦理資通訊服務採購，如屬具敏感性或國安(含資安)疑慮之業務範疇，應確實於招標文件中載明不允許陸資資訊服務業者參與。  
   ⏺廠牌/產品 : enovo筆記型電腦(ThinkPad T480)

附表3-1,3-2系統清冊整理(如附件)

1.[系統是否備份]為”否” ，則[不符合防護基準項目代碼]應包含[C0301營運持續計畫/系統備份]

2.[是否含若密碼]為”否” ，則[不符合防護基準項目代碼]應包含[C0402 識別與鑑別/身分驗證管理]

3.[系統日誌保存時間是否超過6個月]為”否” ，則[不符合防護基準項目代碼]應包含[C0201事件日誌與可規則性/紀錄事件]

4. [不符合防護基準項目代碼]若填寫，[是否符合防護基準]必須為”部分符合”或”不符合”或”不適用”

教育部資安技術稽核(附件)(5/16前繳交資料)

請參考: 第一梯次受測單位行前說明會\_國立中央大學.pdf

==================  
P1...教育部  
P2...技術檢測行前說明內容

P3...第一天作業

(9:30~10:00)起始會議  
受稽方:電算中心人員  
(10:30~12:00,13:30~16:00)分組檢測  
檢測單位要求到行政單位或系所檢測  
中心會聯絡  
1.SNMG小組成員 或  
2.資安執行與稽核小組成員 或  
3.系所秘書  
連絡上再帶檢測單位過去執行檢測工作  
(16:00~17:00)檢測團隊意見交換  
請受測單位一同參加  
以便於檢測團隊提出檢測缺失時,可以討論+確認缺失,隔天有機會改進並回報

P4...第二天作業

(9:00~12:00,13:30~15:00)分組檢測  
檢測單位要求到行政單位或系所檢測  
中心會聯絡  
1.SNMG小組成員 或  
2.資安執行與稽核小組成員 或  
3.系所秘書  
連絡上再帶檢測單位過去執行檢測工作  
(16:00~17:00)總結會議  
請受測單位(2天)一同參加  
以便於檢測團隊提出檢測缺失時,可以討論+確認缺失

P5...團隊介紹  
P7...4.作業說明

機關自評  
電算中心準備資料  
請全校各單位協助準備資料+電算中心彙整  
5/17+6月陸續提交資料

P8...檢測範圍

全校  
6/6+6/7

P10...技術檢測項目範圍

網路安全  
系統安全  
端點安全  
請各單位提供[使用者電腦清單]+OS版本+[物聯網設備清單]

P11...技術檢測項目範圍及配分  
P12...技術檢測項目  
P13...使用者電腦安全檢測 ─ a.弱點掃描

全單位(Portscan)  
挑選可能存在較高風險之50台使用者電腦進行弱點掃描（ VA）

P15...使用者電腦安全檢測 ─ b.安全防護

依弱點掃描結果，抽樣5-10台較高風險使用者電腦進行深度檢測  
■ 防毒軟體病毒碼更新  
■ 作業系統安全性更新  
■ 應用軟體安全性更新  
■ 瀏覽器安全性更新  
■ 惡意程式檢測

P33...物聯網設備檢測

依單位提供之物聯網設備清單抽選10台； 未列於單位物聯網設備清單中之  
設備抽選10台，總計20台，並從中依風險程度挑選5台進行深度檢測  
■ 物聯網設備軟韌體版本（ 包含是否具有重大CVE風險）  
■ 管理介面存取控制策略  
■ 連線存取控制策略  
■ 加密傳輸保護及管理控制策略

P35...組態設定安全檢測

挑選伺服器主機5台、 使用者電腦5台，總計10台進行檢測。

P44...準備作業配合度

計分範圍：應備文件及相關紀錄完整性

P45...配合事項  
P48...技術檢測

○ 【使用者電腦清單】 ：全機關各單位使用者電腦清單，內容含網路位址、職稱、人員  
姓名、單位名稱、所在地點等，並確保檢測當日電腦為開機狀態。  
○ 【 資安健診結果報告】 ：請提供最近一次資安健診結果報告  
【物聯網設備清單】 ：請提供全機關各單位完整物聯網設備清單。

P52...優先關懷追蹤流程

執行技術檢測作業發現立即性  
風險， 如個資外洩等高風險項目，  
單位需於檢測後一週內提交矯正措  
施及相關佐證紀錄， 安排參與實地  
稽核技術面委員進行審查， 確認後  
即排除風險。

教育部資安實地稽核