管理系統文件

文件類別	第二階文件	
文件編號	ISMS-P-007	
文件名稱	資訊安全稽核管理程序書	
發行單位	文件管制小組	
發行日期	104年07月06日	
版　　次	A	
訂修廢單位	審　　查	核　　准
資通安全處理小組	資訊網路中心中心主任 陳君毓	行政副校長 翁順祥

（原版簽名頁保存於文件管制小組）

訂　　修　　廢　　記　　錄		
版次	發行日期	訂 修 廢 內 容 摘 要
A	104/07/06	初版發行

1. 目的

為查驗本校資訊安全管理制度（以下簡稱 ISMS）各項作業的控制目標、控制措施、流程及程序是否符合法規、ISO 標準及組織之資訊安全要求，以確保各項業務能有效運作，特制訂本程序書。

2. 適用範圍

凡本校有關作業之內部稽核管理，均適用本程序書。

3. 參考文件

無。

4. 名詞定義

4.1. 內部稽核

對於資訊安全管理制度運作情形予以查驗，以判定系統之各項活動與其相關結果，是否符合預定計畫，及計劃事項是否有效執行，並能適切達到資訊安全目標。內部稽核區分為定期稽核與不定期稽核兩類。

4.2. 定期稽核

依據定期頒布之稽核計畫內容，對各相關單位進行之內部稽核。

4.3. 不定期稽核

於必要時，對特定單位資訊安全管理制度之運作，所執行之內部稽核。

4.4. 內部稽核人員

4.4.1. 由管理代表遴選適當合格之內部稽核人員，依需要進行任務編組以執行內部稽核。

4.4.2. 受過內部稽核人員訓練課程者，含校內及派外訓練得有證書者，始得任用為內部稽核人員。

5. 作業內容

5.1. 資訊安全稽核管理流程圖

作業流程	權責單位	相關表單
稽核計畫擬定	執行秘書	內部稽核計畫單
審核（No）	資訊安全長	內部稽核計畫單
發出稽核通知（Yes）	資安稽核小組	內部稽核檢查單
召開啟始會議	執行秘書	會議紀錄單
執行稽核	資安稽核小組	內部稽核檢查單
撰寫稽核報告	資安稽核小組	矯正及預防處理單
召開總結會議	執行秘書	會議紀錄單
執行矯正措施	受稽單位	矯正及預防處理單
效果確認（No）	資安稽核小組	
稽核結果彙整（Yes）	執行秘書	矯正及預防處理單
提報管理審查	執行秘書	矯正及預防處理單
紀錄保存	資通安全處理小組	

5.2. 稽核人員組成

5.2.1. 由管理代表或權責主管遴選適當合格之內部稽核人員，組成資安稽核小組，以執行內部稽核作業。

5.2.2. 受過內部稽核人員訓練課程者，始得任用為內部稽核人員。

5.3. 稽核計畫擬訂

5.3.1. 定期性

5.3.1.1. 資訊安全內部稽核作業，應每一年執行一次。

5.3.1.2. 排定稽核計畫時，需注意稽核人員與被稽核之單位及作業不應有直接關係，以確保稽核過程的客觀性與獨立性。

5.3.1.3. 由執行秘書或其指定之人員於每次執行前，擬妥「ISMS-P-007-01 內部稽核計畫單」後，經資訊安全長核准後實施。

5.3.1.4. 若稽核計畫有異動時，應由資訊安全長審核後實施。

5.3.2. 非定期性
執行秘書於下列時機，得隨時召集資安稽核小組，到特定單位或範圍執行非例行性之稽核作業：

5.3.2.1. 各單位業務重大變動時。

5.3.2.2. 內部稽核完畢後之跟催。

5.3.2.3. 其它需非定期性稽核時機。

5.4. 發出稽核通知

5.4.1. 執行秘書於稽核前應召集資安稽核小組成員，召開小組準備會議，分派任務、協調分工、說明稽核重點以及訂定稽核時間。

5.4.2. 資安稽核小組所有成員應針對本次負責之部分，先了解各相關規定程序及標準，並詳讀上次稽核之缺點報告，以研擬此次稽核之重點，並編寫於「ISMS-P-007-02 內部稽核檢查單」上，呈核後影印一份給受稽核單位主管，做為對受稽單位稽核通知使用。

5.4.3. 受稽單位於接獲稽核通知後，應配合準備稽核所需之相關資料。

5.5. 召開啟始會議

執行秘書可視需要於稽核開始前，召集資安稽核小組及受稽單位召開「啟始會議」，說明稽核方式、範圍、時程、配合事項以及進行其他事前溝通。此啟始會議由執行秘書指派特定人員負責紀錄，並填寫於「ISMS-P-002-03 會議紀錄單」。

5.6. 執行稽核

5.6.1. 稽核人員依「ISMS-P-007-02 內部稽核檢查單」上之查檢項目，先實地檢查作業狀況及書面資料，再與經辦人員面談實際作業狀況。

5.6.2. 稽核時，稽核人員應秉持公正、謹慎客觀、友善之態度進行查核工作，並且以協助者態度發現缺點，不任意批評而以客觀建議方式要求修正。

5.6.3. 稽核人員於稽核時，應依抽樣之原理收集足夠之客觀證據，研判該稽核項目是否符合相關規範，稽核時應保存適當的稽核軌跡，其稽合結果可分符合、不符合、不適用三種。

5.6.3.1. 符合：以「○」符號表示，表實際作業確實符合稽核要項之規範、要求。

5.6.3.2. 不符合：以「╳」符號表示，表實際作業完全或部份未達稽核要項之規範、要求。

5.6.3.3. 不適用：以「＼」符號表示，表實際作業未發生稽核要項之規範、要求或時間點未到，以致稽核時無法確認、判斷。

5.6.4. 受稽單位應尊重及支持稽核人員，誠實答覆稽核人員所提問題，並接受調閱相關的紀錄、報告及文件資料。

5.7. 撰寫稽核報告

5.7.1. 內部稽核人員於稽核後應盡可能收集客觀證據，將發現之缺失及與受稽單位研討之改善措施撰寫於「ISMS-P-008-01 矯正及預防處理單」，請受稽單位提出改善期限並簽名確認後呈核。

5.7.2. 記錄時，應盡可能將相關之人、事、時、地、物以及違反之規定或條款填寫清楚，以利日後之追溯。

5.8. 召開總結會議

5.8.1. 稽核人員應將稽核結果透過資安稽核小組內部會議討論、彙整後由執行秘書提出稽核報告。

5.8.2. 執行秘書應於稽核完成後，召開「總結會議」，說明稽核結果及發現，並對各項疑義進行澄清。此總結會議由執行秘書指派特定人員負責紀錄，並填寫於「ISMS-P-002-03 會議紀錄單」。

5.9. 執行矯正措施

5.9.1. 各受稽單位應於改善期限前完成矯正措施，以維持資訊安全管理制度正常運作。

5.9.2. 各內部稽核人員應於改善期限後追蹤確認缺點之改善情形，於「ISMS-P-008-01 矯正及預防處理單」中敘述追蹤狀況，並呈執行秘書、資訊安全長。

5.9.3. 若追蹤結果仍有問題，亦應將其狀況再度紀錄於「ISMS-P-008-01 矯正及預防處理單」呈核加以追蹤，直至改善完成為止。

5.10. 提報管理審查

稽核人員於稽核完成後，應將「ISMS-P-008-01 矯正及預防處理單」交執行秘書彙總，以提報管理審查會議。

5.11. 相關法令之要求

本校執行業務時，應遵守相關法令、法規之要求，資安稽核小組亦應於每次進行資安稽核時檢視其符合性。

5.12. 紀錄保存

相關業務承辦人員應參照如下規範，妥善保存各項紀錄。

編號	表單名稱	保存地點	保存期限
1	內部稽核計畫單	資網中心	至少 1 年
2	內部稽核檢查單	資網中心	至少 1 年

6. 附件

6.1. ISMS-P-007-01 內部稽核計畫單。

6.2. ISMS-P-007-02 內部稽核檢查單。

6.3. ISMS-P-002-03 會議紀錄單。

6.4. ISMS-P-008-01 矯正及預防處理單。