管理系統文件

文件類別	第二階文件	
文件編號	IMS-P-007	
文件名稱	資安及個資內部稽核作業管理程序書	
發行單位	國立虎尾科技大學	
發行日期	110 年 11 月 01 日	
版次	2.3	
適用單位/範圍	全校 (凡業務涉及個資蒐集、處理、利用之單位皆適用之)	
訂修廢單位	審　　查	核　　准

（原版簽名頁保存於 IMS 推動小組）

訂　　修　　廢　　記　　錄		
版次	發行日期	訂 修 廢 內 容 摘 要
1.0	106/01/11	初版發行
2.0	108/08/21	因應資通安全管理法施行修訂相關用詞及規範。(5.2.4.2.1、5.3.5)
2.1	109/08/12	由於目前 IMS-P-002-03 為 ISMS 有效性測量表，並且沒有「會議紀錄單」，因此修正 5.5。
2.2	110/03/29	1.修訂 1.目的 內文「教版資通安全管理規範」為: 「ISO27001」標準。 2.修訂「3.4 附錄 A 資通安全管理規範」為:「3.4 國際標準資訊安全管理系統(ISO27001：2013)」。 原「3.5 教育體系資通安全暨個人資料管理規範」改為「3.5 英國國家標準個人資訊管理系統(BS10012：2017)」。
2.3	110/11/01	5.4.2.2 原「BS10012:2009」修改為「BS10012:2017」以符合目前現況。

1. 目的

為查驗本校資通安全及個人資料保護管理制度（以下簡稱 IMS）各項作業的控制目標、控制措施、流程及程序是否符合法規、法令、ISO27001 標準、教版個資安全管理規範、BS10012 標準及內部控制要求，以求適時發掘問題，並採取矯正預防及持續改善措施，以確保各項業務能有效運作，特制定本程序書。

2. 適用範圍

凡本校於執行與管理定期或不定期之資安及個資內部稽核作業，均適用本程序書。

2.1 本校資通安全管理制度(ISMS)驗證範圍內之稽核作業。

2.2 本校個人資料管理制度(PIMS)驗證範圍內之稽核作業。

3. 參考文件

3.1. 個人資料保護法。

3.2. 個人資料保護法施行細則。

3.3. 資通安全管理法。

3.4. 國際標準資訊安全管理系統(ISO27001：2013)。

3.5. 英國國家標準個人資訊管理系統(BS10012：2017)」。

3.6. 教育體系資通安全暨個人資料管理規範。

3.7. IMS-P-008 矯正預防及持續改善管理程序書。

4. 名詞定義

4.1 資安及個資內部稽核

對於各項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，並能適切達到管理目標。資安及個資內部稽核，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資安及個資內部稽核。

4.3　不定期稽核

於必要時，對特定單位資通安全及個人資料保護管理制度之運作，所執行之資安及個資內部稽核。

4.4　資安及個資內部稽核人員

4.4.1　由稽核小組召集人遴選適當合格之資安及個資內部稽核人員，依需要進行任務編組以執行資安及個資內部稽核。

4.4.2　受過內外部資通安全安及個人資料保護管理系統條文與資安及個資內部稽核相關課程至少 6 小時（含）以上之專業訓練且領有證書或上課證明者，始得任用為資安及個資內部稽核人員。

4.5　資安及個資內部稽核計畫

稽核人員依據本次稽核目的，並參考前次稽核追蹤事項所製作之工作計畫。

4.6　資安及個資內部稽核報告

為資安及個資內部稽核工作之結果，包括背景描述、稽核期間、稽核項目(範圍)、稽核方法與標準、稽核結果、改進建議等內容。

4.7　資安及個資內部稽核查檢表

稽核人員依稽核計畫實施書面查核或進行實地查核，並確實記錄所發現之情況，以做為稽核之佐證並留下稽核軌跡。

5. 作業內容

5.1　資安及個資保護稽核管理流程圖

作業流程	權責單位	相關表單
稽核計畫擬定	稽核小組組長	資安及個資內部稽核計畫
審核（No / Yes）	執行秘書	資安及個資內部稽核計畫
發出稽核通知	稽核小組	資安及個資內部稽核通知單
召開啟始會議	資通安全長或執行秘書	會議紀錄
執行稽核	稽核小組	資安及個資內部稽核查檢表
撰寫稽核報告	稽核小組	矯正及預防措施處理單
召開總結會議	執行秘書	會議紀錄
執行矯正措施	受稽單位	矯正及預防措施處理單
效果確認（No / Yes）	資安及個資內部稽核人員	
稽核結果彙整	執行秘書	資安及個資內部稽核報告
提報管理審查	執行秘書	資安及個資內部稽核報告 矯正及預防措施處理單
紀錄保存	推動小組	

5.2　稽核人員組成

5.2.1　由校長指派一位委員擔任召集人，各一級單位應派一人參加稽核小組，組成「稽核小組」，以執行資安及個資內部稽核作業。

5.2.2　「稽核小組」召集人遴選本校「內部稽核小組」人員或其他適切人員組成「內部稽核小組」，以執行資安及個資內部稽核作業，並由「稽核小組」召集人擔任或委派其他人員擔任「內部稽核小組組長」。

5.2.3　為確保稽核過程的客觀性與獨立性，稽核之執行應由非受稽人員擔任。

5.2.4　資安及個資內部稽核人員之資格

5.2.4.1　基本資格

5.2.4.1.1　資安及個資內部稽核人員應接受與稽核相關之訓練課程至少 6 小時以上，並領有證明者。

5.2.4.1.2　具有基本與正確的稽核認知者，並定期參加與稽核領域相關之訓練，以持續加強稽核專業能力與查核技巧。

5.2.4.2　各管理體系之個別要求

5.2.4.2.1　資通安全管理制度(ISMS)：具有 CISA 或通過 ISO27001 主導稽核員考試並領有證書或資通安全管理法認可專業證照。

5.2.4.2.2　個人資料管理制度(PIMS)：具有 TPIPAS 內評師資格或通過 BS10012 主導稽核員考試，並領有證書者。

5.3　稽核計畫擬訂

5.3.1　由「稽核小組」組長於每次執行資安及個資內部稽核作業前，擬妥「資安及個資內部稽核計畫表」闡明稽核範圍與項目後，經「執行秘書」核准後實施。

5.3.2　排定資安及個資內部稽核計畫時，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。

5.3.3　若稽核計畫有異動時，應由「執行秘書」審核後實施。

5.3.4　稽核頻率

5.3.4.1　定期性

本校資安及個資內部稽核作業，應每年定期執行一次。

5.3.4.2　非定期性

「執行秘書」於下列時機，得隨時召集「稽核小組」，到特定單位或範圍執行非例行性之稽核作業：

5.3.4.2.1　各單位業務重大變動時。

5.3.4.2.2　發生重大資安及個資保護事件時。

5.3.4.2.3　資安及個資內部稽核完畢後之跟催。

5.3.4.2.4　其它需進行非定期性資安及個資內部稽核的時機。

5.3.5　稽核範圍

內部稽核範圍除了包含 ISO27001 所有控制措施要求外，宜包含資通安全維護計畫之實施情況。

5.4　發出稽核通知

5.4.1　「稽核小組」組長應於稽核前召集「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　編寫資安及個資內部稽核檢查表

5.4.2.1　資通安全管理制度(ISMS)

資安及個資內部稽核人員應針對本次負責部分，先了解相關程序及標準，並詳讀上次稽核之缺失報告，以研擬此次稽核之重點，並編寫於「IMS-P-007-02 資通安全內部稽核查檢表」上，呈稽核組長審核。

5.4.2.2　個人資料管理制度(PIMS)

資安及個資內部稽核人員應依據 BS10012:2017 本文要求

項目及個資法規定，研擬此次稽核之重點，並編寫於「IMS-P-007-03 個人資料內部稽核查檢表」上，呈稽核組長審核。

5.4.3 在進行資安及個資內部稽核作業前，應由稽核組長或其指定之人員，通知受稽部門及稽核人員稽核日期，以便做好相關之準備工作。

5.4.4 受稽單位於接獲稽核通知後，應備妥相關文件與紀錄，並安排各受檢項目之對應人員接受稽核。

5.5 召開啟始會議

資通安全長或執行秘書可視需要於稽核開始前，召集「稽核小組」人員及受稽單位召開「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。並由召集人指派特定人員負責紀錄。

5.6 執行稽核

5.6.1 稽核人員依「IMS-P-007-02 資通安全內部稽核查檢表」及「IMS-P-007-03 個人資料內部稽核查檢表」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「V」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　資安及個資內部稽核人員於稽核後應盡可能收集客觀證據，將發現之稽核缺失撰寫於「IMS-P-008-01 矯正及預防措施處理單」，請受稽單位提出矯正預防措施及改善期限，並於簽名確認後呈核。

5.7.2　撰寫稽核紀錄時，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。

5.7.3　「稽核小組」組長應將所有稽核開立之「IMS-P-008-01 矯正及預防措施處理單」彙總成「IMS-P-007-04 資安及個資內部稽核報告」，作為提報管理審查會議中討論改進事宜之用。

5.8　召開總結會議

5.8.1　稽核人員應將稽核結果透過「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。

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，以維持資安及個資保護管理制度正常運作。

5.9.2　各資安及個資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「IMS-P-008-01 矯正及預防措施處理單」中敘述追蹤狀況，並呈「執行秘書」審核。

5.9.3　若追蹤結果仍有問題，亦應將其狀況再度紀錄於「IMS-P-008-01 矯正及預防措施處理單」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「IMS-P-008-01 矯正及預防措施處理單」交「執行秘書」所指定之專人彙總，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，「稽核小組」亦應於每次進行資安及個資保護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	資安及個資內部稽核計畫表	電子計算機中心	至少 3 年
2	資通安全內部稽核查檢表	電子計算機中心	至少 3 年
3	個人資料內部稽核查檢表	電子計算機中心	至少 3 年
4	資安及個資內部稽核報告	電子計算機中心	至少 3 年
5	矯正及預防措施處理單	電子計算機中心	至少 3 年

6. 附件

6.1 IMS-P-007-01 資安及個資內部稽核計畫表。

6.2 IMS-P-007-02 資通安全內部稽核查檢表。

6.3 IMS-P-007-03 個人資料內部稽核查檢表。

6.4 IMS-P-007-04 資安及個資內部稽核報告。

6.5 IMS-P-008-01 矯正及預防措施處理單。