XXXX學校

資訊安全稽核作業程序書

機密等級：一般

文件編號：XXXX-B-013

版　　次：1.0

發行日期：109.XX.XX

修　訂　紀　錄				
版次	修訂日期	修訂頁次	修訂者	修訂內容摘要

目錄

1　目的

建立XXXX學校（以下簡稱「本校」）獨立稽核之規範，以判斷各項作業的控制目標、措施、流程及程序是否符合法規及組織之資訊安全要求。

2　適用範圍

本校承辦相關資訊業務之資訊安全稽核作業管理。

3　權責

3.1　資訊安全委員會

3.1.1指派資訊安全稽核小組組長及組員。

3.1.2負責督導資安稽核作業。

3.2　資訊安全稽核小組

3.2.1辦理稽核作業相關事宜。

3.2.2稽核缺失定期追蹤改善情形並加以記錄。

3.3　資訊安全稽核小組組長

3.3.1確保稽核業務依本程序書確實執行。

3.3.2協調提供稽核所需資源。

3.3.3編製資訊安全稽核計畫。

3.3.4召開資訊安全稽核小組準備會議。

3.3.5召開稽核啟始及結束會議。

3.3.6負責報告稽核執行情形及成果。

3.3.7列管「資訊安全管理制度內部稽核報告」及所附相關查核資料。

3.4　資訊安全稽核小組組員：配合資訊安全稽核小組組長指示，執行稽核作業、完成各項紀錄及查證矯正與預防措施執行情形。

3.5　受稽部門：受稽部門之主管於稽核期間應指派人員接受稽核，並協助調閱有關紀錄、報告或文件。對於稽核發現缺失應提出並執行矯正與預防措施。

4　名詞定義

4.1　資安稽核：一種有系統且獨立的資訊安全檢查，以決定各項活動及相關結果是否與所計畫的安排相符，以及安排是否有效執行及達成目標。

4.2 稽核類別：

4.2.1內部稽核：由資訊安全稽核小組針對組織之資訊安全控制、風險評鑑與業務永續運作計畫等作業，進行定期查核，以確保其成效。

4.2.2外部稽核：由本校以外單位所進行的資訊安全稽核。

4.2.3專案稽核：專案稽核得視特定目的需求（例如：資訊安全事件調查），以不定期之專案方式進行。

5 作業說明

5.1 稽核頻率

5.1.1每年定期辦理資訊安全內部稽核作業。

5.1.2視需要不定期執行專案稽核。

5.2 稽核人員之要求

資訊安全稽核小組之組長與組員由資訊安全委員會指派。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稽核員。稽核人員資格要求如下：

5.2.1資訊安全稽核小組組長：須由接受資安相關稽核訓練者擔任。

5.2.2資訊安全稽核小組組員：須由接受資安相關稽核訓練者擔任。

5.3 稽核計畫

為達稽核之有效性，稽核小組組長應事前規劃並編製「資訊安全管理制度內部稽核計畫」，以作為執行稽核指導綱要，內容應包括：稽核範圍、項目、人員、時程、程序等，並經資訊安全委員會核准後執行。

5.4 稽核準備

5.4.1資訊安全稽核小組組長應研擬規劃「資訊安全管理制度內部稽核表」，並召開小組準備會議，提示稽核要點、協調分工及排定時程。

5.4.2資訊安全稽核小組組長需於查核前通知受稽部門。

5.4.3受稽部門於接獲稽核通知後，應配合準備稽核所需相關資料。

5.5 稽核執行

5.5.1資訊安全稽核小組組長應於稽核前，召集資訊安全稽核小組、受稽

單位召開啟始會議，說明稽核範圍、時程、配合事項等。

5.5.2資訊安全稽核小組組員於稽核時，應依抽樣之原理收集足夠之客觀證據，以研判該稽核項目與相關規範之符合性。稽核時應保存適當之稽核軌跡。

5.5.3資訊安全稽核小組組員依「資訊安全管理制度內部稽核表」執行稽核，逐項填寫稽核結果。「資訊安全管理制度內部稽核表」內容若須增修，需經資訊安全稽核小組組長同意。

5.5.4受稽部門應尊重及支持資訊安全稽核小組，誠實答覆稽核人員所提問題，並接受調閱有關紀錄、報告及文件。

5.6 稽核報告

5.6.1資訊安全稽核小組組長應於稽核完成後召開稽核結束會議，由資訊安全稽核小組組長報告稽核發現，並對受稽單位所提出之疑義進行澄清。

5.6.2資訊安全稽核小組應召開內部會議討論及彙整稽核發現，於五個工作天內由資訊安全稽核小組組長提出「資訊安全管理制度內部稽核報告」，並請受稽單位代表簽名。

5.6.3受稽部門於接獲稽核報告後，應依據「矯正及預防管理程序書」之規定，最遲於十個工作天內將該單位之缺失分析原因及擬採行之矯正與預防措施填列於「矯正與預防處理單」內，經主管核定後回覆資訊安全稽核小組。

5.7 矯正及預防措施

稽核缺失之後續追蹤應依據「矯正及預防管理程序書」辦理。

5.8 稽核技巧與工具保護

5.8.1系統稽核工具（如：弱點掃描系統等）之存取應由授權的人員於授權範圍內操作，並留有存取、操作紀錄，以防止任何可能之誤用或破解。

5.8.2系統稽核工具應由專人保管，以防止不當操作造成其他系統之損害。

5.9 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。資訊安全稽核小組亦應於每次進行資安稽核時檢視其符合性。

6 相關文件

6.1 資訊安全管理制度內部稽核報告

6.2 資訊安全管理制度內部稽核計畫

6.3 資訊安全管理制度內部稽核表

6.4 矯正及預防管理程序書

6.5 矯正與預防處理單