國立高雄師範大學資訊安全稽核作業要點

113 年 5 月 8 日 113 學年度資安暨個資保護管理審查會議通過
113 年 9 月 25 日 113 學年度第 1 次行政會議通過
114 年 5 月 21 日資安、個資暨智財保護管理審查會議修正通過
114 年 9 月 17 日 114 學年度第 1 次行政會議修正通過

一、 為維護本校資訊設備、網路、系統及資料使用安全，並落實執行資訊機密維護及資訊安全稽核工作，特依據「國立高雄師範大學內部稽核管理作業程序書」及「國立高雄師範大學資通安全維護計畫」訂定本要點。

二、 本校各單位辦理資訊安全稽核相關作業依本要點之規定；本要點未規定者，準用行政院及所屬各機關資訊安全管理要點之規定。

三、 資訊安全稽核區分如下：

（一）外部稽核：指由機關或單位委託專家、學者或專業資安稽核廠商之公正第三方規劃辦理之稽核作業。

（二）內部稽核：指由本校對內部單位自行規劃辦理之稽核作業。

四、 資訊安全稽核頻率如下：

（一）「外部稽核」得視本校資安業務實際需求定期或不定期辦理。

（二）「內部稽核」作業次數，依據本校內部稽核管理作業程序書規定每 2 年辦理 1 次，必要時可視需求不定期辦理，並就本校資通系統（保有個人資料）風險高低、教學單位特性訂定先後順序，規劃全校各單位分年分階段執行內部稽核。

五、 各單位應指派資訊安全管控人員一至二名，作為所屬單位資訊安全稽核及其他應辦事項之聯繫與維護窗口。

六、 各受稽核單位於稽核前均須填列資安稽核相關表單，並備妥相關文件，以利稽核；且實施稽核作業時，得調閱受稽單位有關資料、實地測試及檢查資訊軟、硬體設備使用情形。必要時，得由資訊相關人員或資訊安全稽核人員提供說明及專業諮詢意見。

七、 資訊安全稽核作業實施範圍，應以系統存取控制管理為主，參酌本校資訊現況，針對下列事項，稽核其系統存取有無異狀及實施情形是否符合相關法令之規定：

（一）資產管理。

（二）人力資源安全。

（三）實體與環境安全。

（四）通訊與作業安全。

（五）存取控制。

（六）其他資訊安全管理事項。

八、 資訊安全稽核作業程序如下：

（一）綜合分析機關資訊系統特性、系統存取政策、系統異常存取狀況及授權規定或其他使用管理規定，據以研（修）訂稽核項目，擬訂稽核計畫經管理審查會議通過後實施。

（二）計畫內容包括：計畫目的、稽核日期與行程、稽核範圍、稽核對象、稽核項目、稽核作業方式、評核原則與報告撰寫及處理等。

（三）依據稽核結果就優缺點及改進措施提出書面報告，陳報資安長，並協調缺失單

位確實檢討改進，必要時得實施複查。

（四）前款報告內容包括：稽核時間、受稽核單位、稽核結果處理及建議事項等。

九、本要點經資訊安全、個人資料暨智慧財產權保護管理審查會及行政會議通過，報請校長核定後實施，修正時亦同。