113 年度義守大學個人資料管理制度內部稽核計畫書

一、 前言

依據「資通安全管理法」、「資通安全責任等級分級辦法」，明確要求各級機關（包括教育單位）應建立資安防護基準，並應依其資通安全責任等級辦理資通安全應辦事項，本校為 C 級單位須導入資訊安全管理系統，為確保符合「資通安全管理法」及「教育體系資通安全管理規範」等，本校自 104 年度起實施專案稽核。

(一)依據「私立專科以上學校及私立學術研究機構個人資料檔案安全維護實施辦法」、「教育體系資通安全暨個人資料管理規範」、「學校財團法人及所設私立學校內部控制制度實施辦法」，擬定個人資料管理制度內部稽核計畫。

(二)資訊安全管理制度(Information Security Management)為組織內部所使用之資訊，進行實施全面性管理，以妥善保護資訊機密性(Confidentiality)、完整性(Integrity)與可用性(Availability)，並且降低資安事件衝擊至可承受範圍(即為風險胃納)，資訊安全管理制度循環分為 PDCA 四大部份，詳如圖 1。

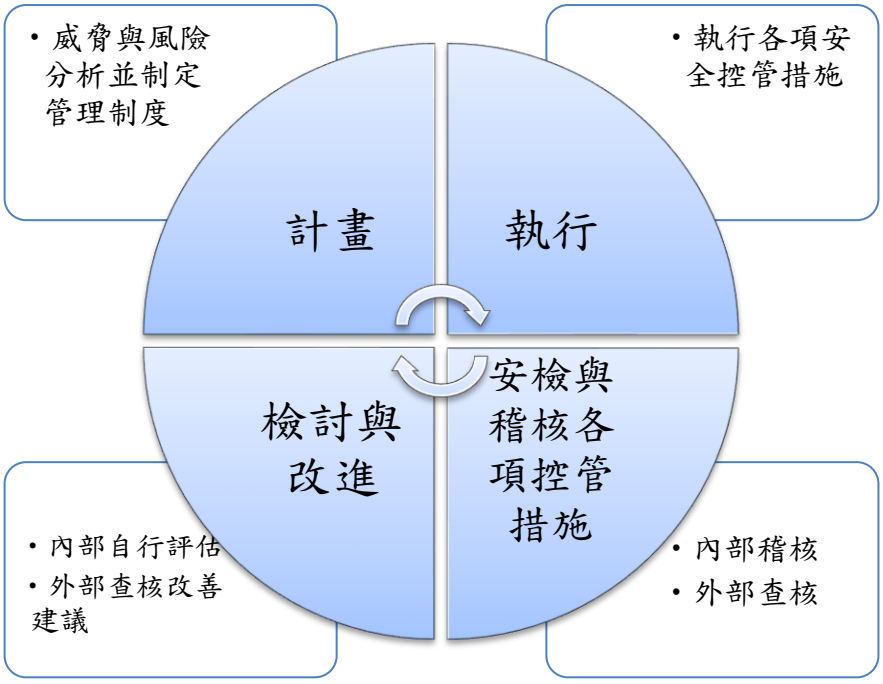

圖 1. 資訊安全管理制度循環

二、 113 年度稽核計畫

(一)依據 112 年 10 月 19 日校長核定「義守大學 113 年度稽核計畫」，113 年 4 月至 8 月實施專案稽核「個人資料管理制度自我檢查(稽核案號 ISU113-AD006)」。

(二)採分權分層負責，資安由業務承辦單位(圖書與資訊處)辦理資通安全檢測項目及

教育訓練等；個資由業務承辦單位(秘書處)辦理個資檢測項目及教育訓練等；全校各單位辦理自評；稽核人員(稽核室)運用問題樹方法建立應稽核項目問卷，外部稽核不列本案查核範圍。

(三)稽核目的

1.強化校園師生尊重個人資料價值觀與信念，並增進其相關法律知識。

2.配合行政運作考核項目「學校應依教育部與所屬機關(構)及學校資通安全責任等級分級作業規定，導入資訊安全管理制度(ISMS)」等。

對照個人資料保護施行細則，得包括下列事項，並以與所欲達成之個人資料保護目的間，具有適當比例為原則。

1.配置管理之人員及相當資源。

2.界定個人資料之範圍。

3.個人資料之風險評估及管理機制。

4.事故之預防、通報及應變機制。

5.個人資料蒐集、處理及利用之內部管理程序。

6.資料安全管理及人員管理。

7.認知宣導及教育訓練。

8.設備安全管理。

9.資料安全稽核機制。

10.使用紀錄、軌跡資料及證據保存。

11.個人資料安全維護之整體持續改善。

(四)個人資料管理制度自我檢查(含資安)稽核項目所組成之循環控制，各單位自評(表單電子化)、稽核室實地抽測查核，雙軌進行稽核程序，包括個人資料管理制度控制循環(含資安)，以完備資料安全及個資安全稽核管理機制，如圖1.控制作業循環路徑圖。

1.個資稽核項目

(1)個人資料檔案管理安全、個人資料業務委外情形等。

(2)校園保護智慧財產權與資訊安全(含個資保護)，包含本校個人資料檔案安全維護計畫措施自我檢查。

2.資安稽核項目

(1)資訊管理循環(含監督管理)

(2)資訊紀錄管理

(3)網路安全管理

(4)資訊系統存取控制管理

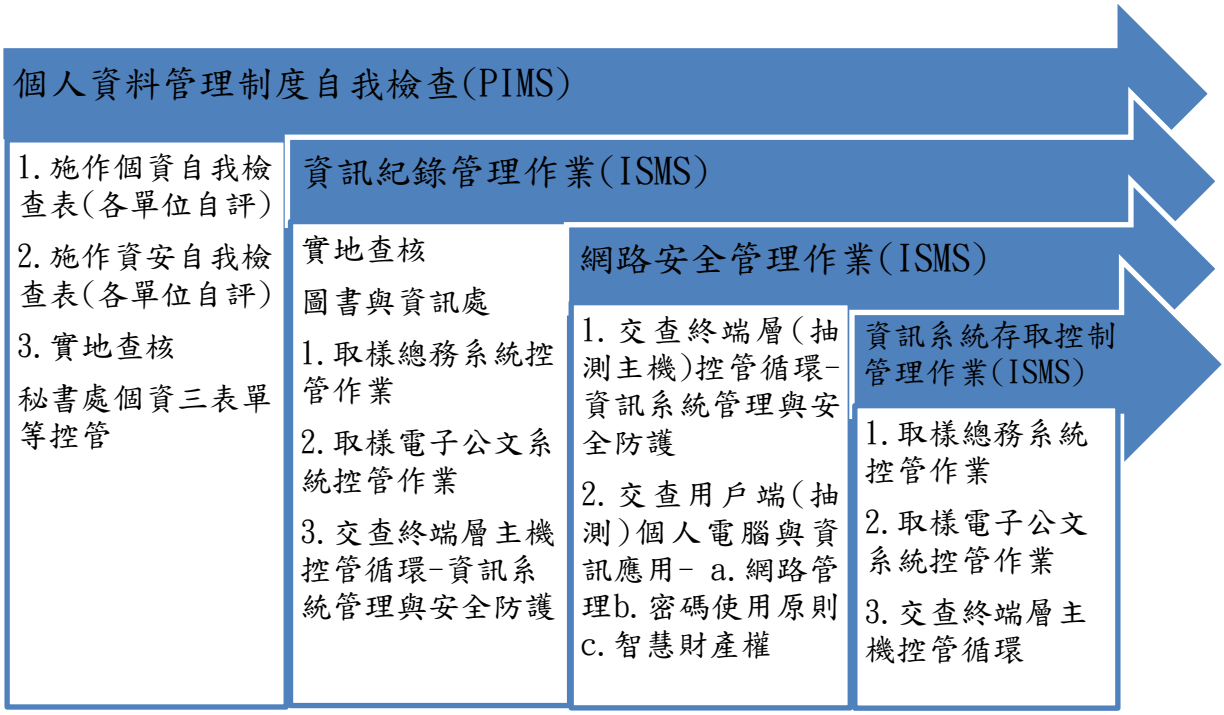

圖 1.控制作業循環路徑圖

註：(1)個人資料管理系統(Personal Information Management System，簡稱 PIMS)、
(2)資訊安全管理系統(Information Security Management System，簡稱 ISMS)。

三、計畫審查及執行

(一)112 年 10 月 19 日校長核定義守大學 113 年度稽核計畫，於次(113)年實施。

(二)113 年 1 月 4 日「112 學年度第一學期第 1 次個人資料保護工作小組會議」備查。