義守大學 111 年度個人資料管理制度內部稽核計畫書

一、 前言

依據 107 年行政院頒布「資通安全管理法」及其子法「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）應建立的資安防護基準，並應依其資通安全責任等級辦理資通安全應辦事項，包含管理面、技術面、認知與訓練，其中資訊安全責任等級分級為 A、B、C 級的單位須導入資訊安全管理系統，係為 CNS/ISO 27001、其他具有同等或以上效因之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，以確保教育體系「資通安全管理法」及「教育體系資通安全管理規範」的完整性及有效性，推動及提升全國大專院校之校園資訊安全。

本校自 104 年度起實施專案稽核，為因應資通訊環境之變化，與考量國際實務標準之發展與普及，並且，配合「個人資料保護法」、「個人資料保護管理政策」及 BS10012:2009 標準之規定與要求，本校持續維護個人資料保護管理系統，遂行推展內部控制、監督管理作業之目的。

(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)本校持續維護個人資料保護管理系統，辦理實質審查，以彰顯執行成效，全案依內部控制制度年度稽核計畫排程，為提高內部稽核之適切性與有效性。

資訊安全管理制度(Information Security Management)係指組織內部所使用之資訊，進行實施全面性之管理，以妥善保護資訊之機密性(Confidentiality)、完整性(Integrity)與可用性(Availability)，並且降低資安事件之衝擊至可承受之範圍(即為風險胃納)，本校資訊安全管理制度循環執行可分為 PDCA 四大部份，詳如圖 1。

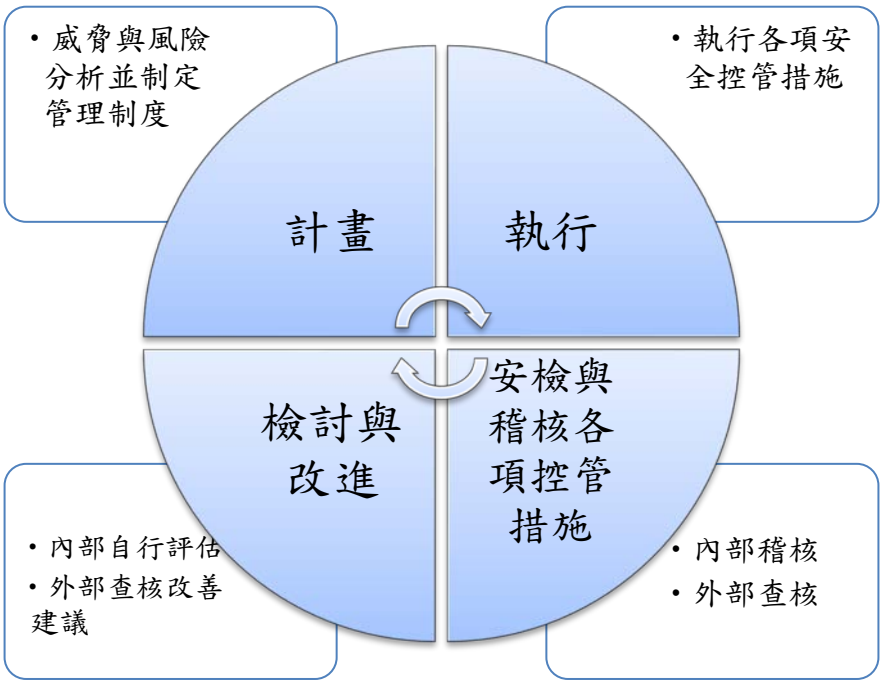

圖 1. 資訊安全管理制度循環

二、 111 年度稽核計畫

(一)依據 110 年 10 月 27 日校長核定「義守大學 111 年度稽核計畫」，次(111)年實施專案稽核「個人資料管理制度自我檢查(稽核案號 ISU111-AD006)」，稽核期間為 111 年 4-8 月，全校各單位為受稽單位，查核範圍為 110 學年度，屬於追蹤回饋期中查核。

(二)本校採分權分層負責，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，同時，為系統化進行稽核，稽核人員(稽核室)運用問題樹方法分析稽核項目，將其整體目的轉換為主要問題，再逐級細分子目的並將其轉換為子問題，藉以臚列主要問題及其子問題之架構，作為後續製作「工作底稿」之基礎，並以查核問卷、查檢表、有效性量測表等方式作為稽核工作底稿，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之價值觀與信念，並增進其相關法律知識。

2. 為落實私立大學校院全面提升教育品質，鼓勵學校健全發展及推動整體特色。

3.配合行政運作考核項目之業務項目(六十三)「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)……」至業務項目(六十八)。

前項措施對照個人資料保護施行細則(105.03.02 修正)，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)主稽核項目與稽核項目所組成的縱向及橫向之循環控制作業，依實際運作狀況查核，包括個人資料管理制度控制循環，如圖 1.控制作業循環路徑圖。

1.主稽核項目:個人資料管理制度自我檢查，自我檢查項目包括：

(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.稽核項目：(1)資訊紀錄管理作業(2)網路安全管理作業(3)資訊系統存取控制管理作業(4)監督管理作業。

3.資安及個資安全稽核管理機制，因應 COVID-19 疫情發展，為避免群聚、降低移

動感染風險，以維護校園環境安全與教職員生健康安全，本校採滾動式防疫措施如採分組遠距(居家)辦公、110 學年度採延後開學等，本案資訊管理循環為內部控制十項循環基礎，啟動稽核應變機制，經風險評估，得採延長稽核期程及彈性調整稽核程序，由受稽單位辦理「書面自評」，稽核室提供書面自評紙本表單，並由稽核室通知查檢抽測佐證資料；以書面自評及實地查核，雙軌進行稽核程序。

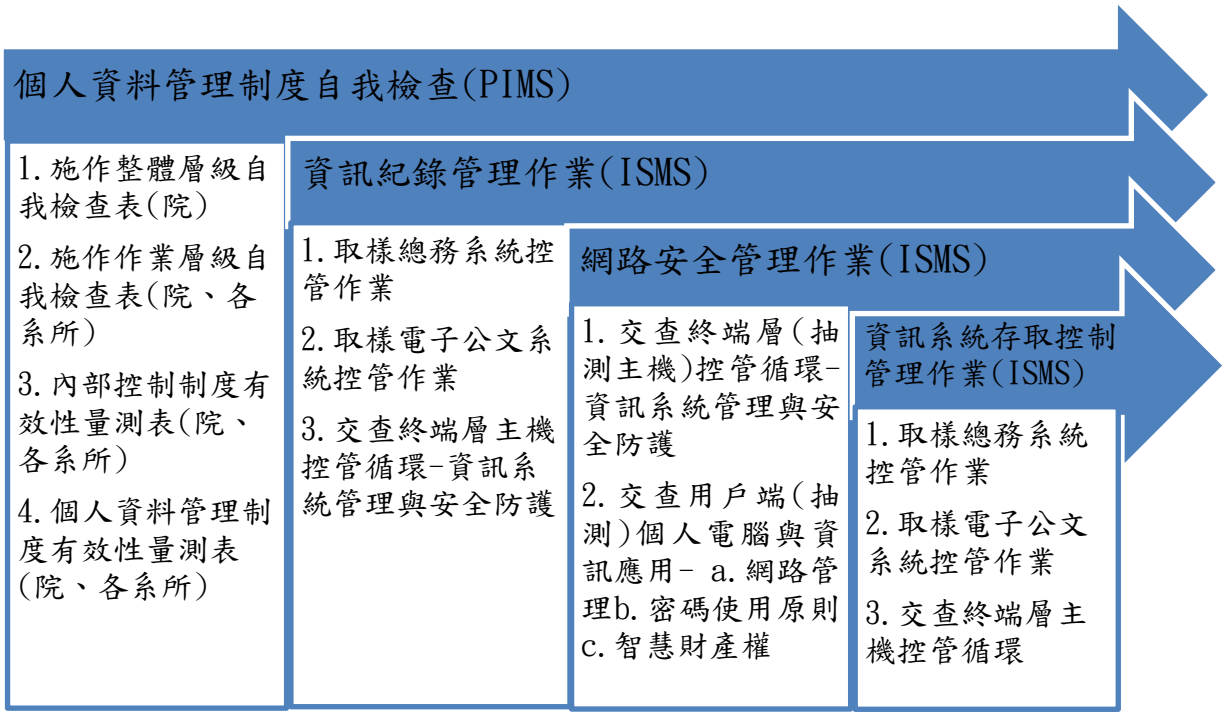

圖 1.控制作業循環路徑圖

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)110 年 10 月 27 日校長核定義守大學 111 年度稽核計畫，於次(111)年實施。

(二)擬送 111 年 1 月 3 日個人資料保護工作小組第 20 次會議備查。