國立清華大學作業程序說明表

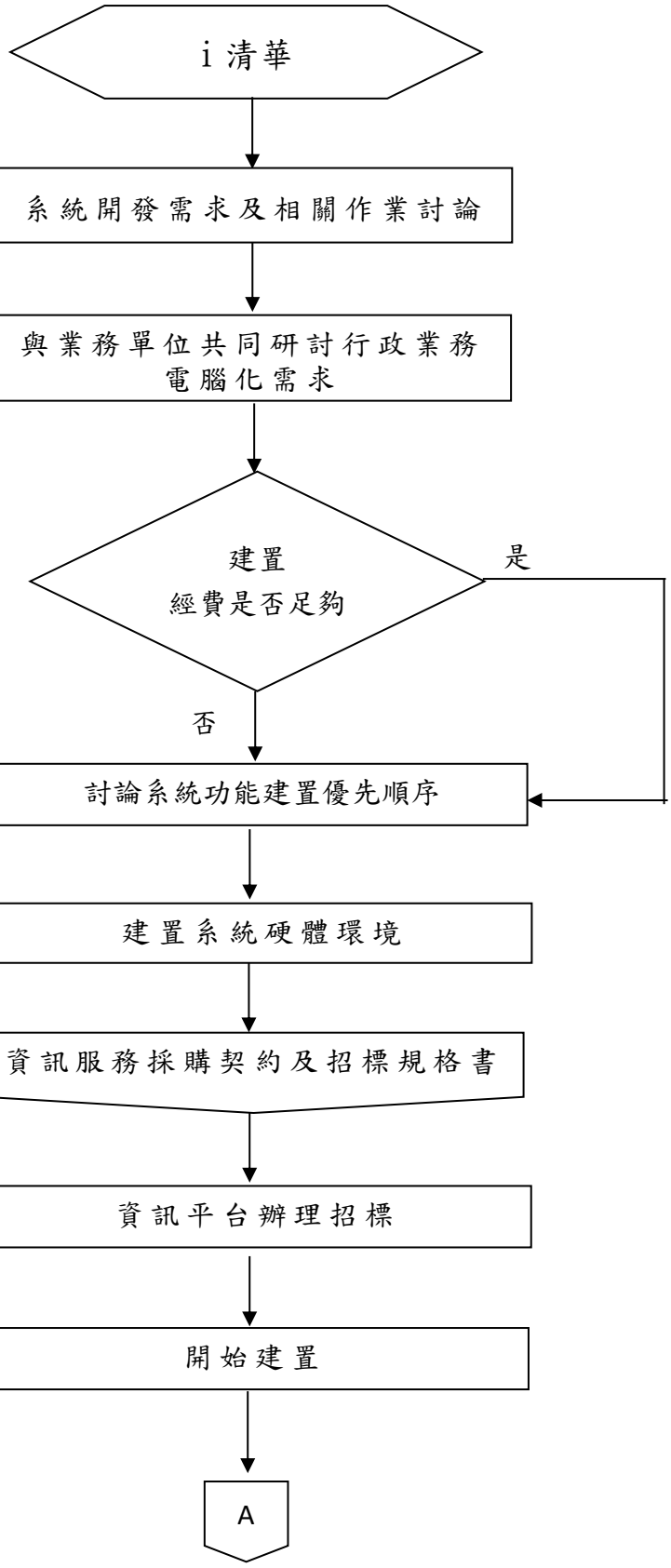
項目編號	113-10
項目名稱	i 清華(原學生資訊平台)作業
承辦單位	學生事務處
作業程序說明	**一、 資訊平台安全管理** (一)系統開發 1.確定欲開發應用系統之預定作業方式、作業項目、作業內容、作業預算及作業時程。 2.與業務單位共同研討、評估業務需求，確定電腦化後之作業方式，依規定呈主管核示後確認作業方式。 3.進行平台招標作業。 4.廠商於開發及設計時應依照本校資訊安全政策及相關管理制度。 5.開發完成平台需通過網站弱點掃描，避免 OWASP TOP10 等安全管理框架之已知弱點。 6.廠商協助平台部屬至伺服器之安全設定，如防火牆控管、防毒軟體、軟體更新。 7.依應用系統分析後之決定按規定程序引進有合法版權之套裝軟體。 (二)行動應用程式發布 1.行動應用程式應於可信任來源之行動應用程式商店或網站發布，且應於發布時說明欲存取之敏感性資料、行動裝置資源及宣告之權限用途。 2.於官網上提供行動應用程式之名稱、版本與下載位置。 (三)系統維護 1.定期網站弱點掃描，避免 OWASP TOP10 等安全管理框架之已知弱點，若校方有發布新的重大網站弱點，應配合更新或修正程式。 2.外包需定期協助平台部屬至伺服器之安全設定。 3.外包廠商協助依照業務單位需求定期備份，每日備份若容量有限至少應維持七天記錄。 4.遵守學校資訊安全政策定期評估，確保資訊安全實務作業之有效性。 5.每年定期取得行動應用 App 資安檢測 MAS 標章，確

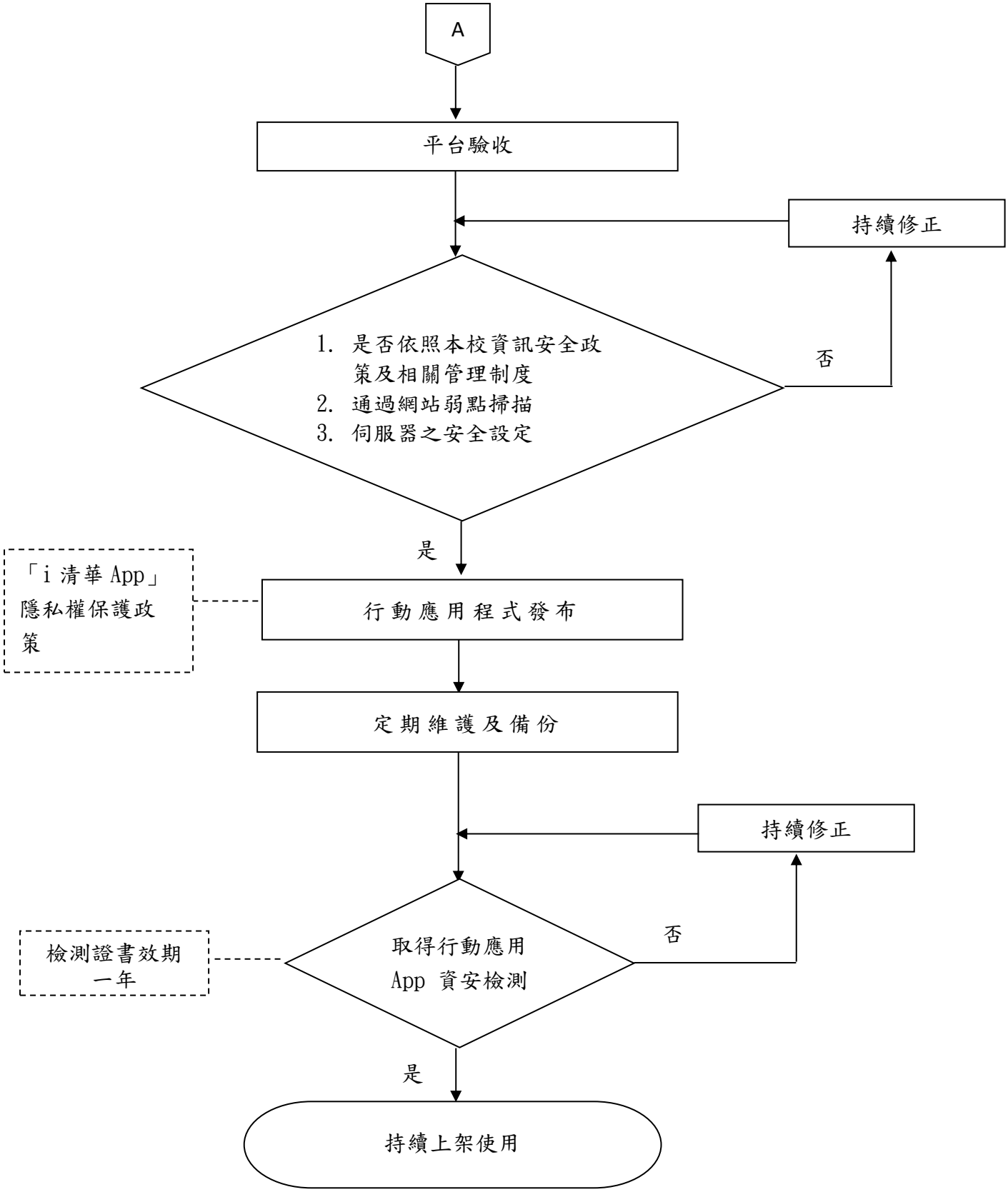
	保資安零風險。 **二、 重要經驗** (一)需確認建置預算成本及相關軟硬體環境是否足以支持平台運作。 (二)因查詢功能可能具有敏感度較高資料，需做適當的資料隱密。 (三)上架國家應避免容易被駭客攻擊的區域及部分敏感國家。 **三、 注意事項** (一)定期配合校方資通系統盤點及防護評估作業。 (二)每年定期取得行動應用 App 資安檢測 MAS 標章。
控制重點 【預定完成日期】 【可量化標示】	一、 定期網站弱點掃描，並配合應配合更新或修正程式。 二、 每年定期取得行動應用 App 資安檢測 MAS 標章，確保資安零風險。 三、 定期配合學校資通系統盤點及防護基準檢核。
法令依據	一、 教育部-國立大專校院資通安全維護作業指引 二、 資通系統防護基準驗證實務 三、 行動應用 App 基本資安檢測基準
使用表單	一、 採購申請表 二、 行政業務電腦化需求提案單 三、 資通系統防護基準檢核表 四、 行動應用 App 資安檢測委託測試接收單

國立清華大學作業流程圖

i 清華(原學生資訊平台)作業

113-10




A
平台驗收
持續修正
1. 是否依照本校資訊安全政策及相關管理制度
2. 通過網站弱點掃描
3. 伺服器之安全設定
否
是
「i 清華 App」隱私權保護政策
行動應用程式發布
定期維護及備份
持續修正
檢測證書效期一年
取得行動應用 App 資安檢測
否
是
持續上架使用

國立清華大學內部控制自行評估表
113 年度

自行評估單位：學生事務處

作業類別(項目)：i 清華作業

評估期間：112 年 8 月 1 日至 113 年 7 月 31 日

評估日期：113 年 8 月 6 日

評估/控制重點	自行評估情形				
	落實	部分落實	未落實	不適用	其他
一、作業流程有效性 (一)作業程序說明表及作業流程圖之製作是否與規定相符。 (二)內部控制制度是否有效設計及執行。	V				
二、i 清華作業 (控制重點條列) (一)是否詳細評估業務需求。	V				
(二)是否詳細評估軟硬體作業環境。	V				
(三)是否依照本校資訊安全政策及相關管理制度。	V				
(四)是否定期進行網站弱點掃描	V				
(五)是否定期確認伺服器安全設定。	V				
(六)是否定期取得行動應用 App 資安檢測。	V				
改善措施欄：					
填表人：　　複核：　　一級主管：					

註：1. 機關得就 1 項作業流程製作 1 份自行評估表，亦得將各項作業流程依性質分類，同 1 類之作業流程合併 1 份自行評估表，就作業流程重點納入評估。

2. 各機關依評估結果於評估情形欄勾選「落實」、「部分落實」、「未落實」、「不適用」或「其他」；其中「不適用」係指評估期間法令規定或作法已修正，但控制重點未及配合修正者；「其他」係指評估期間未發生控制重點所規範情形等，致無法評估者；遇有「部分落實」、「未落實」或「不適用」情形，於改善措施欄敘明需採行之改善措施。

國立清華大學作業層級自行評估表

113 年度

評估單位：學生事務處

評估期間：112 年 8 月 1 日至 113 年 7 月 31 日

評估日期：113 年 8 月 6 日

評估重點	評估情形					部分落實/未落實/不適用情形說明	改善措施/興革建議
	落實	部分落實	未落實	未發生	不適用		
一、 評估機關目標無法達成之風險，並決定須優先處理之風險項目，以及定期滾動檢討風險評估，因應內部及外部環境之改變。	V						
二、 依據各項業務性質與時俱進檢討不合時宜之控制作業及作業流程，並落實執行各項控制作業。	V						
三、 建立檢討主管法令規定機制，並針對外界意見或執行缺失部分即時檢討相關法令規定。	V						
四、遵循相關法令規定或契約。	V						
五、 就涉及人民權利或義務之主管業務建立適當之檢核、審查、追蹤、管制或考核等管理機制，並除依法公開外，另依風險評估結果，推動其行政作業流程透明措施，以利外部監督及形塑廉能政府。	V						
六、 就主管業務對相關機關或單位善盡監理、督導或輔導等責任。	V						
填表人： 複核： 一級主管：							

註：

1. 各單位除上列必要評估重點外，另得視業務性質及外部意見等調整增列評估重點項目，並依評估結果於評估情形欄勾選「落實」、「部分落實」、「未落實」、「未發生」或「不適用」；其中「未發生」係指有評估重點所規範之業務，但評估期間未發生，致無法評估者；「不適用」係指評估期間法令規定或作法已修正，但評估重點未及配合修正者，或無評估重點所規範之業務等。
2. 「評估期間」係指本項作業自行評估所涵蓋之期間；「評估日期」指執行該項評估之日期。
3. 該評估重點係由稽核評估職能單位及負責內部控制或內部稽核業務幕僚單位自行填寫依其相關法令規定應辦理之工作，如施政績效管考、資訊安全稽核、政風查核(含廉政風險評估)、政府採購稽核、工程施工查核、國家關鍵基礎設施安全防護、人事考核(含考核工作績效及獎懲)、內部審核、事務管理工作檢核及定期檢討內部控制機制等工作。
4. 本表及其佐證資料等，應自辦理自行評估工作結束日起，以書面文件或電子化型式至少保存五年。