



文件名稱：系統開發與維護管理程序

文件發行章

文件編號：ISMS-02-013

制定單位：圖資處

申請類別：制定 修訂 廢止

機密等級：一般

NO	修訂日期	頁次	版本	修訂內容摘要
1	2010.08.01		V1.0	新制定
2	2010.11.01	P2	V2.0	5.1.7 補充說明鐘訊同步
		P2		5.1.8 SSL 加密之說明
		P2		5.3.1.1, 5.3.1.2 文字修正
		P4		5.6.3 修正錯字“程式”
		P4		5.6.5 修正為“系統開發組”
		P4		5.7.4 錯字修正
3	2011.07.29	P1	V3.0	因應本校內控文件之編號統一管理，以 ISMS 為文件範圍之識別。
		P5		修改使用表單之文件編號。
4	2011.09.28	P3	V3.1	修改填寫「系統驗收確認單」時機。
5	2012.09.13	P1	V4.0	內文中本中心改為圖資處
		P4		增加資訊系統分類分級與鑑別作業程序說明與表單名稱
6	2013.07.31	P1	V4.1	將全校性網頁開發、維護納入權責
		P2		新增網頁更新異動服務申請作業
		P5		新增網頁更新異動申請單(ISMS-04-057)
7	2015.04.30	P1	V4.2	修訂範圍敘述
		P5		增加 5.8.4 資訊系統分類分級與鑑別作業中「其他」影響構面「個資衝擊風險等級」之定義
8	2015.09.30	P1~P5	V4.3	修訂單位名稱
		P5		明定影響構面衝擊程度與參考法源

未經本校同意禁止複製



# 環球科技大學

文件名稱	系統開發與維護管理程序	版本	5.2
文件編號	ISMS-02-013	發行日期	2019/01/04
		頁次	1 / 6

## 1. 目的：

本程序書制訂之目的在於確保圖書資訊處資訊系統需求、分析設計、開發、測試、上線與維護作業之安全管理。

## 2. 範圍：

資訊系統之程式開發生命周期等相關支援活動，如既有線上系統之測試、修改、維護、上線變更、原始碼之管控與儲存等作業。

## 3. 權責：

圖書資訊處相關資訊系統暨全校性網頁開發、維護人員與委外人員，遵守本程序書之相關規定，以確保圖書資訊處相關軟體與資料等資訊資產之安全。

## 4. 名詞解釋：

無。

## 5. 作業說明：

### 5.1 一般控制措施：

- 5.1.1 當發展新資訊系統，或現有系統功能之強化，於系統規劃需求分析階段，即將安全需求要項納入系統功能。
- 5.1.2 在採購軟體時，視其安全需求，進行分析。除事前經權責單位主管核准外，應避免修改軟體，如需修改應依本程序書之變更作業控制措施加以控管。
- 5.1.3 系統之安全需求及控制程度，應與資訊資產價值相稱，並考量安全措施不足，可能帶來之傷害程度。
- 5.1.4 資訊系統應保護資料，防止洩漏或被竄改。
- 5.1.5 在作業系統上執行應用軟體，應建立控制程序並嚴格執行，為減少可能危害作業系統之風險，應用程式之更新作業應限定只能由授權之管理人員才可執行，可建

# 環球科技大學

文件名稱	系統開發與維護管理程序	版本	5.2
文件編號	ISMS-02-013	發行日期	2019/01/04
		頁次	2 / 6

立應用程式之更新稽核紀錄。

5.1.6 系統若需委外建置或維護，請參考「委外資訊服務管理程序」之相關管理規範。

5.1.7 系統相關主機應進行時鐘同步，以維繫日誌資訊記錄在時間上的可靠性。

5.1.8 系統被評估為高敏感性資料，可使用 SSL 憑證進行加密，以確保資料傳輸之機密性與完整性，申請憑證時依系統安全需求設定加密金鑰長度。

## 5.2 軟體控制措施：

5.2.1 作業系統變更時，應審查與測試重要營運系統，以確保對組織作業或安全無不利之衝擊。

5.2.2 系統軟體應由系統負責人進行安裝，安裝時應視狀況通知相關技術人員支援或通知使用者，以避免資訊服務中斷或影響業務。

5.2.3 軟體正式上線測試由系統負責人辦理，測試時應事先通知協調相關人員支援。系統負責人應通知相關人員及使用者以避免資訊服務中斷或影響業務。

5.2.4 系統軟體更新系統負責人須定期檢視更新系統安全修補、防毒軟體及防毒碼，以維持系統正常運作。

5.2.5 各資訊設備內安裝之套裝軟體，應具期限內之合法版權。

## 5.3 軟體增修作業控制措施：

### 5.3.1 提案申請作業：

5.3.1.1 如增需作業為全新的作業或服務時，需求提案單位應先填具「資訊系統需求提案單」提出系統需求，並經該單位一、二級主管核准確認後始得送交圖書資訊處。

5.3.1.2 如增需作業為資料查詢，資料、報表、程式修正時，需求提案單位應先填具「資訊系統問題反應/協助單(MR 單)」提出系統需求，並經該單位一、二級主管核准確認後始得送交圖書資訊處。

5.3.1.3 如需網頁更新異動服務時，需求提案單位應先填具「網頁更新/異動申請單」提出系統需求，並經該單位一、二級主管核准確認後始得送交圖書資訊處。

# 環球科技大學

文件名稱	系統開發與維護管理程序	版本	5.2
文件編號	ISMS-02-013	發行日期	2019/01/04
		頁次	3 / 6

## 5.3.2 申請審查及回覆：

5.3.2.1 系統開發組組長接受需求後，進行審查作業，並決定接受此申請，或修改範圍過於複雜，需討論再議，並於申請表單中詳述待處理之原因。

5.3.2.2 審查完成後，將申請文件回覆提案單位，由系統開發組組長指派處理人員，於申請表單中，並將申請文件影本指派處理人員。

5.3.2.3 資訊系統開發審核，其硬體的需求審核藉由預測軟、硬體使用狀況及未來需求，可行時如系統容量發展預測、電腦計算能力的負載評估以及骨幹網路的負載需求。

5.3.2.4 申請審查時，須將系統安全需求納入考量。

5.3.2.5 視需求申請需求之要求，必要時由圖書資訊處召開系統需求分析會議，並將系統安全需求納入考量。

5.3.3 如系統增修作業需委外執行時，需參照「委外資訊服務管理程序」執行委外作業。

## 5.4 程式撰寫：

5.4.1 程式開發者應於程式開發前進行系統分析，系統分析時應將系統安全需求納入考量。

5.4.2 輸入應用系統之資料，應檢查主要欄位或資料檔案的內容，以確保資料的安全性、有效性及真確性。

5.4.3 對高敏感性的輸入資料，必要時應採用資料保密機制，在傳輸或儲存過程中應採加密方法保護。

5.4.4 輸出之資料，應於輸出之前，確認其正確性；對於系統內之訊息，則需保護其完整性。

## 5.5 系統測試與驗收：

### 5.5.1 系統測試：

5.5.1.1 系統增修作業完成後，處理人員須進行測試，測試作業須於測試專用電腦上執行，不可於正式環境中進行測試。

5.5.1.2 測試專用電腦需置於機房內，以保全測試資料，如於處理人員的電腦上做

# 環球科技大學

文件名稱	系統開發與維護管理程序	版本	5.2
文件編號	ISMS-02-013	發行日期	2019/01/04
		頁次	4 / 6

測試時，須由處理人員建立虛擬資料。

5.5.1.3 程式功能若無法達成申請單位預定需求，則系統開發人員另行修改程式後，再測試，直至符合預定需求為止。

5.5.1.4 若為系統新增功能，測試完成後需填寫「系統驗收確認單」，交申請單位執行驗收。

5.5.2 系統驗收：

5.5.2.1 申請單位需執行驗收應用系統的資料輸出之正確性與適當性。

5.5.2.2 申請單位驗收無誤後，需於「系統驗收確認單」上簽名確認，並將「系統驗收確認單」交還圖書資訊處。

5.6 原始程式庫資源之存取控制

5.6.1 原始程式庫的存取必須採取嚴格的控制措施，避免在存取原始程式庫的程序中，造成原始程式庫的損毀。

5.6.2 應用程式原始碼資料庫應不可存放在作業系統的檔案中。

5.6.3 應用程式原始碼由程式撰寫人專人控管。

5.6.4 發展中或是維護中的應用程式，應與實務作業之程式原始碼資料庫區隔，不可放置在一起。

5.6.5 系統開發組需建立原始程式之「系統程式碼清冊」。

5.7 系統程式版本與變更管理：

5.7.1 系統正式上線後，系統維護所需之相關軟體及文件應進行版本控管。

5.7.2 對於保存相關軟體及文件電子檔之環境，應進行權限控管與防毒等管制，以防止資料被盜用、誤用、未授權之無意或惡意竄改、受病毒破壞等事件發生，對資料亦應進行備份。對於紙本形式之相關維護文件，亦應進行存取及防護之管制。

5.7.3 系統程式或文件進行變更

5.7.3.1 需求單位於「資訊系統問題反應協助單(MR單)」填寫現況及變更需求，由開發單位評估同意後，主管核准後通知系統開發人員或委外廠商進行處理。

5.7.3.2 應用系統變更如以遠端連線方式進行，則須依「委外服務管理程序」之規

# 環球科技大學

文件名稱	系統開發與維護管理程序	版本	5.2
文件編號	ISMS-02-013	發行日期	2019/01/04
		頁次	5 / 6

範開啟網路通道，在系統負責人之監控下進行系統變更。

5.7.3.3 應用系統變更前，須進行系統備份，降低系統變更失敗時對業務運作之影響，以利進行復原。

5.7.3.4 應用系統變更前，開發單位應評估對各使用單位之影響並通告各相關單位協調系統變更時間，以降低對業務運作之影響。

5.7.3.5 應用系統變更前，變更項目應先行由修改人員進行適當之驗證與測試。

5.7.3.6 完成變更作業後，應更新相關系統文件。

5.7.4 對於因緊急維護狀況需變更之系統，應於事後將相關資料補齊，以利追蹤與查核。

5.7.5 如系統維護作業是根據操作人員問題提報而執行，於維護完成後，由系統維護人員將結果回報給原問題提出人員。

5.8 資訊系統分類分級與鑑別作業：

5.8.1 依「資訊系統分級與資安防護基準作業規定」鑑別資訊系統之安全等級，採行適當安全控制措施，確保資訊系統之安全防護水準。

5.8.2 業務承辦人依其處理資料之性質對資訊系統識別資訊類別，並設定影響構面等級，區分出安全等級以評估影響構面衝擊程度。

5.8.3 依資訊系統服務之業務屬性分為行政與業務二類。

5.8.4 參考機密性、完整性、可用性、法律遵循性四大影響構面衝擊程度等級之定義，於「其他」影響構面訂定「個資衝擊風險等級」，若個資數量未達 20 筆(團體訴訟不成立)列為「普」級、20 筆~40 萬筆(團體訴訟二億元上限)列為「中」級、超過 40 萬筆則列為「高」級。

5.8.5 由圖書資訊處綜整各項資訊系統「安全等級評估表」，並製作「資訊系統清冊」，最後由資安長核定資訊系統安全等級。

6. 參考文件：

6.1 委外服務管理程序(ISMS-02-005)

6.2 資訊系統分級與資安防護基準作業規定

## 環球科技大學

文件名稱	系統開發與維護管理程序	版本	5.2
文件編號	ISMS-02-013	發行日期	2019/01/04
		頁次	6 / 6

### 7.使用表單：

- 7.1 資訊系統需求提案單(ISMS-04-038)
- 7.2 資訊系統問題反應/協助單(MR 單) (ISMS-04-039)
- 7.3 系統驗收確認單(ISMS-04-040)
- 7.4 系統程式碼清冊(ISMS-04-048)
- 7.5 安全等級評估表(ISMS-04-055)
- 7.6 資訊系統清冊(ISMS-04-056)
- 7.7 網頁更新異動申請單(ISMS-04-057)

未經本校同意禁止複製