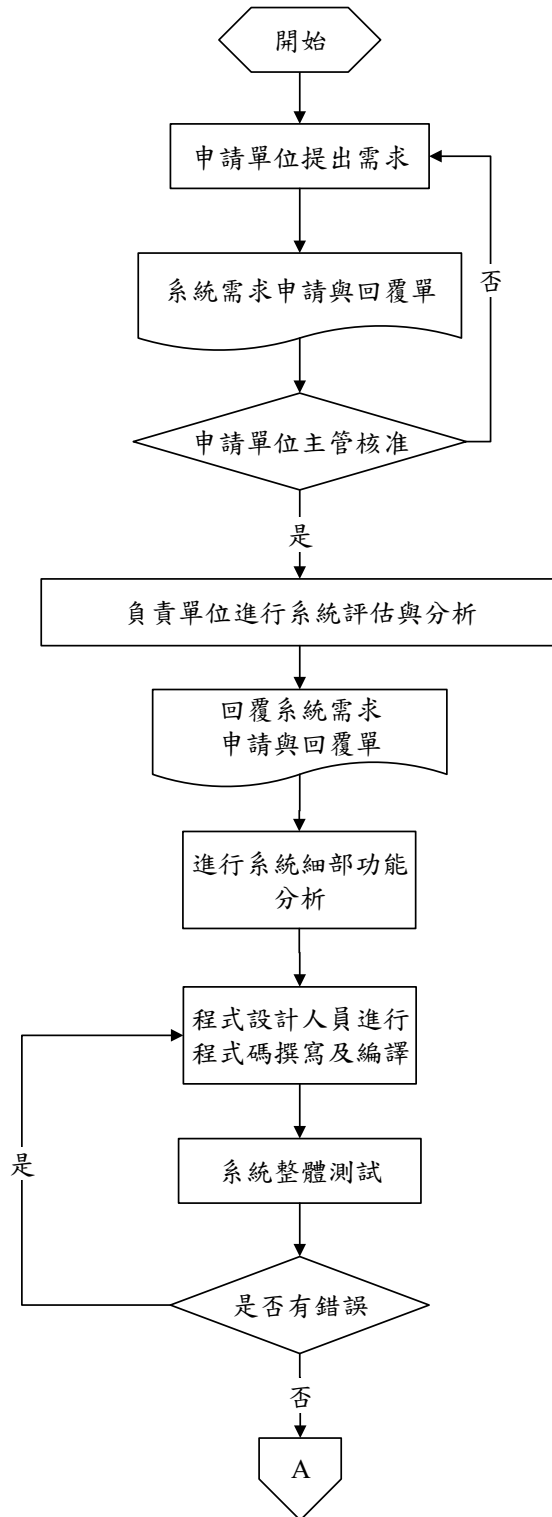


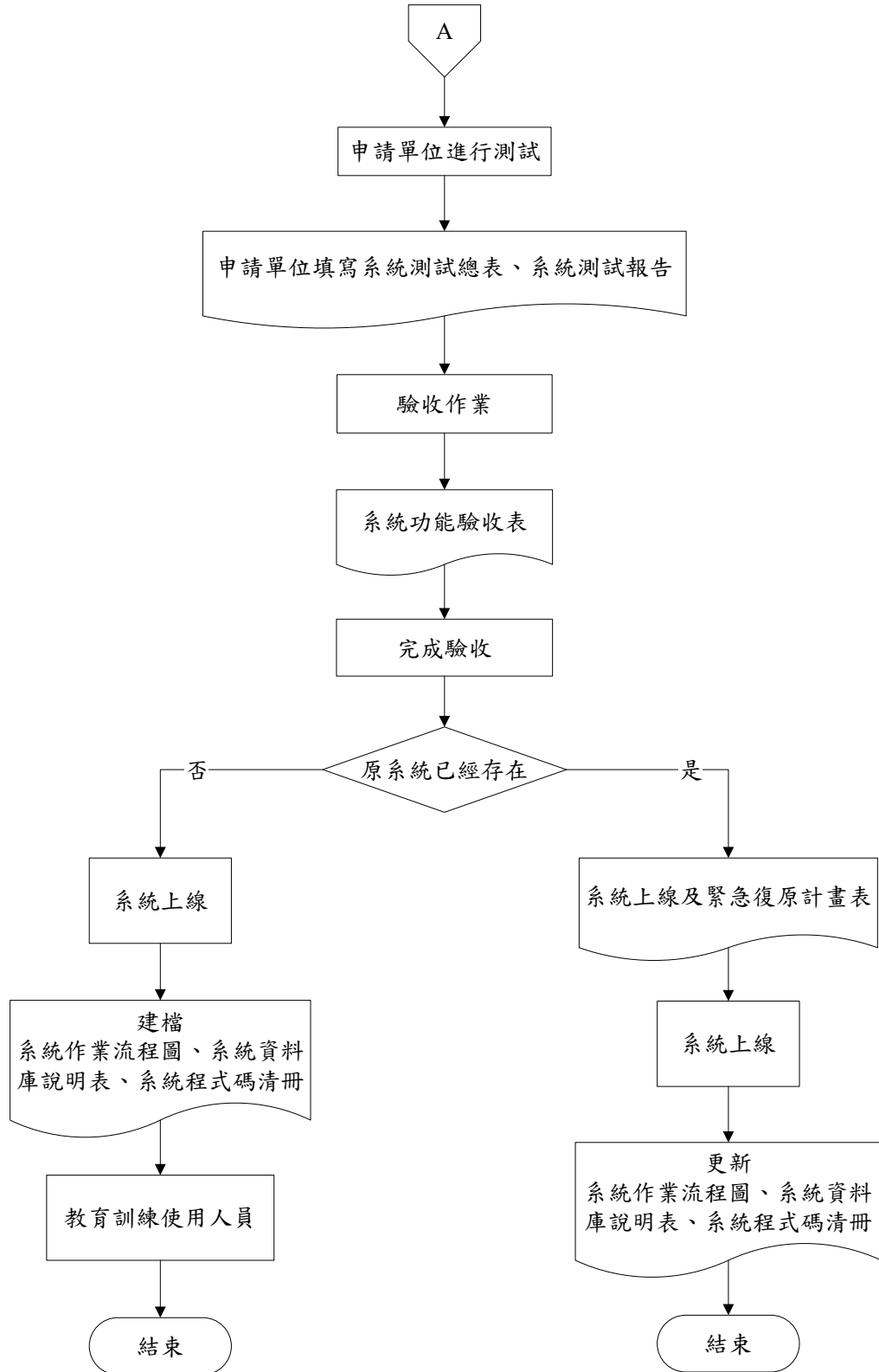
制定單位：秘書室			公布日期：104/12/24		
文件編號	SC 電校 001	版本	01	頁次	1/7
作業名稱	系統開發及程式修改作業				
主要負責單位	圖書與資訊處				
相關法令	教育體系資通安全管理規範				

一、 流程圖：

● 系統開發與維護管理

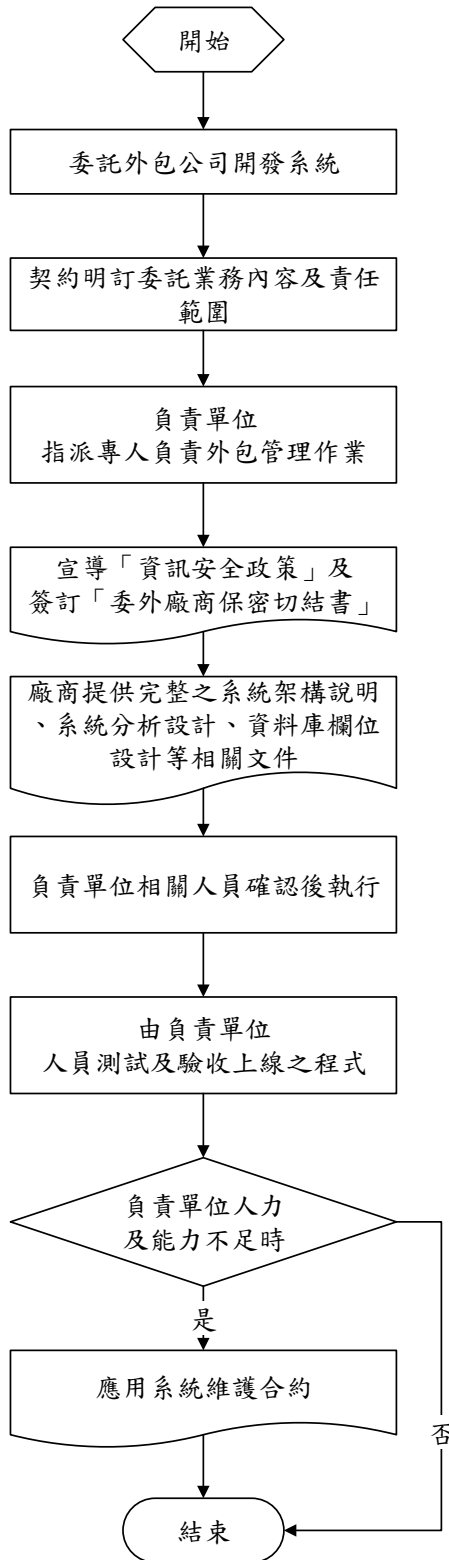


制定單位：秘書室				公布日期：104/12/24	
文件編號	SC 電校 001	版本	01	頁次	2/7
作業名稱	系統開發及程式修改作業				
主要負責單位	圖書與資訊處				
相關法令	教育體系資通安全管理規範				



制定單位：秘書室				公布日期：104/12/24	
文件編號	SC 電校 001	版本	01	頁次	3/7
作業名稱	系統開發及程式修改作業				
主要負責單位	圖書與資訊處				
相關法令	教育體系資通安全管理規範				

● 外包業務管理



制定單位：秘書室				公布日期：104/12/24	
文件編號	SC 電校 001	版本	01	頁次	4/7
作業名稱	系統開發及程式修改作業				
主要負責單位	圖書與資訊處				
相關法令	教育體系資通安全管理規範				

## 二、 作業程序：

### (一)、 應用系統開發及管理制度：

1. 應訂定應用系統開發及管理制度。
2. 系統開發應配合學校整體發展策略。
3. 應用系統發展管理制度應明確規範發展系統之標準流程。

### (二)、 系統計劃、開發及管理：

#### 1. 提案與回覆：

- (1)、 應用系統開發前，應由申請單位提出「系統需求申請與回覆單」，載明系統開發或程式修改等具體需求事項，送交圖書與資訊處進行可行性評估。
- (2)、 承辦人員於完成與申請單位之訪談與系統分析後，於「系統需求申請與回覆單」中回覆評估結果，包含功能細項、預估人力與時程、建議方案等。

#### 2. 系統分析：

- (1)、 系統分析時，應依現況及推展情形由圖書與資訊處指派適當人員專任負責。
- (2)、 系統分析人員於完成系統分析作業後，應對申請單位提出說明，以再次確認系統開發與設計方向之正確性。

#### 3. 系統設計：輸入畫面、檔案結構、輸出報表、處理程序。

### (三)、 系統測試管理：

1. 程式設計初步完成後，準備「系統測試總表」通知申請單位進行聯合測試，並請申請單位於「系統測試總表」中填寫測試結果，測試完成後填寫「系統測試報告」。
2. 程式功能若無法達成申請單位預定需求，則請系統開發人員另行修改程式後，擇期再測試，直至符合預定需求為止。

### (四)、 系統上線與驗收管理：

1. 聯合測試進行順利完成後，進行相關驗收作業，並請申請單位簽收「系統功能驗收表」。
2. 若原系統已經存在，應於系統上線前訂定「系統上線及緊急復原計畫表」，內容包含系統轉換規劃，轉換備援處理等。
3. 系統上線後，程式開發者應將系統設計與功能規格書，內容包含「系統作業流程圖」、「系統資料庫說明表」，以及「系統程式碼清冊」建檔。
4. 系統分析人員會同程式設計人員負責使用人員之教育訓練。

### (五)、 系統維護管理：

1. 經開發使用中之系統，如有修改需求時，應由需求單位主管與圖書與資訊處主管先行研議，並達成共識後，由需求者填具「系統需求申請與回覆單」，經需求單

制定單位：秘書室				公布日期：104/12/24	
文件編號	SC 電校 001	版本	01	頁次	5/7
作業名稱	系統開發及程式修改作業				
主要負責單位	圖書與資訊處				
相關法令	教育體系資通安全管理規範				

位主管核准後，交圖書與資訊處，始得進行修改作業。

2. 原始程式如經修改，應一併修正操作說明等資料。
3. 程式修改完成後，程式設計人員應通知需求單位進行測試，並請申請單位於「系統測試總表」中填寫測試結果，測試完成後填寫「系統測試報告」。
4. 程式經測試結果如已符合使用者之需求後，進行相關驗收作業，並請申請單位簽收「系統功能驗收表」。
5. 後續衍生之修改需求，亦應提出修改申請，交由圖書與資訊處進行評估。

(六)、外包業務管理：

1. 系統開發業務外包，應經過既定程序核准，且所委託業務內容及責任範圍，須明訂於契約。
2. 委外廠商應提供負責系統維護、聯絡窗口及電話詢答服務，並解決系統相關事宜，並配合本處相關程序辦理異常排除及通報事宜，如必要應提供駐點服務。
3. 委外廠商處理個人資料應遵守「個人資料保護法」及本處之相關規定，並簽訂「委外廠商保密切結書」。
4. 由圖書與資訊處指派專人負責外包管理作業。
5. 外雇被委託公司人員至本校時，對其職務種類及業務範圍，應有明確規定。
6. 保固期滿後，圖書與資訊處考量人力及能力狀況，必要時，與外包公司簽訂「應用系統維護合約」。
7. 系統若委由外部廠商開發，廠商應提供完整之系統架構說明、系統分析設計、資料庫欄位設計等相關文件，經由本處相關人員確認後方能執行。
8. 委外廠商應確實控管程式與文件版本之一致性。
9. 委外廠商進行系統開發與維護時，不得任意複製或攜出本處限閱等級（含）以上之業務資料。
10. 委外廠商需針對交付之系統，應保證系統內不含後門程式、隱密通道及特洛伊木馬程式。
11. 若系統、軟體由委外廠商開發者，應由本處人員測試及驗收上線之程式，確定符合相關需求後，方得依照「系統開發及程式修改作業」之程序進行上線。
12. 程式修改與開發需遵守「系統開發及程式修改作業」之規定，若有例外，須經資訊單位主管人員同意以後，方可實施。

三、 控制重點：

(一)、 應用系統開發及管理制度：

1. 是否逐年訂定系統開發策略計劃。

制定單位：秘書室				公布日期：104/12/24	
文件編號	SC 電校 001	版本	01	頁次	6/7
作業名稱	系統開發及程式修改作業				
主要負責單位	圖書與資訊處				
相關法令	教育體系資通安全管理規範				

2. 系統開發策略管理制度是否完整而明確。
- (二)、系統計劃、開發及管理：
1. 需求提出：開發新程式或更動原程式之前，「系統需求申請與回覆單」是否經權責主管簽核及評估。
  2. 系統分析：
    - (1)、是否指派專人負責進行系統分析作業；設計人員是否與相關單位人員有充份的討論互動。
    - (2)、系統分析人員是否針對開發或修改之系統功能、流程、提高管理品質等進行評估，並向相關人員確認系統開發設計及修改方向之正確性。
  3. 系統設計：
    - (1)、完成系統分析後，於系統正式開發前，是否經相關主管確認。
    - (2)、系統開發作業是否依循程式開發建議書之內容設計。
    - (3)、系統設計是否具整體性規劃，並整合跨單位之需求。
- (三)、系統測試管理：
1. 程式設計、測試過程及系統程式轉換情形是否完整記錄與保存。
  2. 系統測試環境與正式作業環境轉換所發生問題是否經適當解決。
  3. 程式執行異常時，是否依規定之程序回報申請修改。
  4. 圖書與資訊處提供之使用手冊或說明書是否完整。
- (四)、系統上線與驗收管理：
1. 系統分析人員會同程式設計人員負責教育及訓練使用人員操作新系統，並告知注意事項。
  2. 程式經測試結果如已符合使用者之需求後，是否經申請人確認；「系統功能驗收表」是否亦歸檔存查。
- (五)、系統維護管理：
1. 已開發使用中之系統如有修改需求，需求者是否提出修改申請，並陳相關權責主管簽審。
  2. 圖書與資訊處是否對程式修改申請進行評估。
  3. 系統運作使用後，如經大幅修改測試完成時，相關文件是否一併修正或定期更新。
  4. 需求單位是否將修改後程式之測試結果回饋予系統分析人員。
  5. 程式經測試結果如已符合使用者之需求後，是否經申請人確認；「系統功能驗收表」是否亦歸檔存查。
- (六)、外包業務管理：
1. 外包業務之契約內容是否週詳。

制定單位：秘書室				公布日期：104/12/24	
文件編號	SC 電校 001	版本	01	頁次	7/7
作業名稱	系統開發及程式修改作業				
主要負責單位	圖書與資訊處				
相關法令	教育體系資通安全管理規範				

2. 與被委託單位之權責是否劃分詳盡。
3. 委外開發系統是否經過品質測試確認程序。
4. 圖書與資訊處人力及能力不足時，外包時是否與外包公司簽訂「應用系統維護合約」。

四、 使用表單：

- (一)、 系統需求申請與回覆單(CHU-ISMS-D-035)
- (二)、 系統作業流程圖(CHU-ISMS-D-039)
- (三)、 系統資料庫說明表(CHU-ISMS-D-040)
- (四)、 系統程式碼清冊(CHU-ISMS-D-042)
- (五)、 系統測試總表(CHU-ISMS-D-036)
- (六)、 系統測試報告(CHU-ISMS-D-037)
- (七)、 系統功能驗收表(CHU-ISMS-D-038)
- (八)、 系統上線及緊急復原計畫表(CHU-ISMS-D-041)
- (九)、 委外廠商保密切結書(CHU-ISMS-D-022)
- (十)、 應用系統維護合約

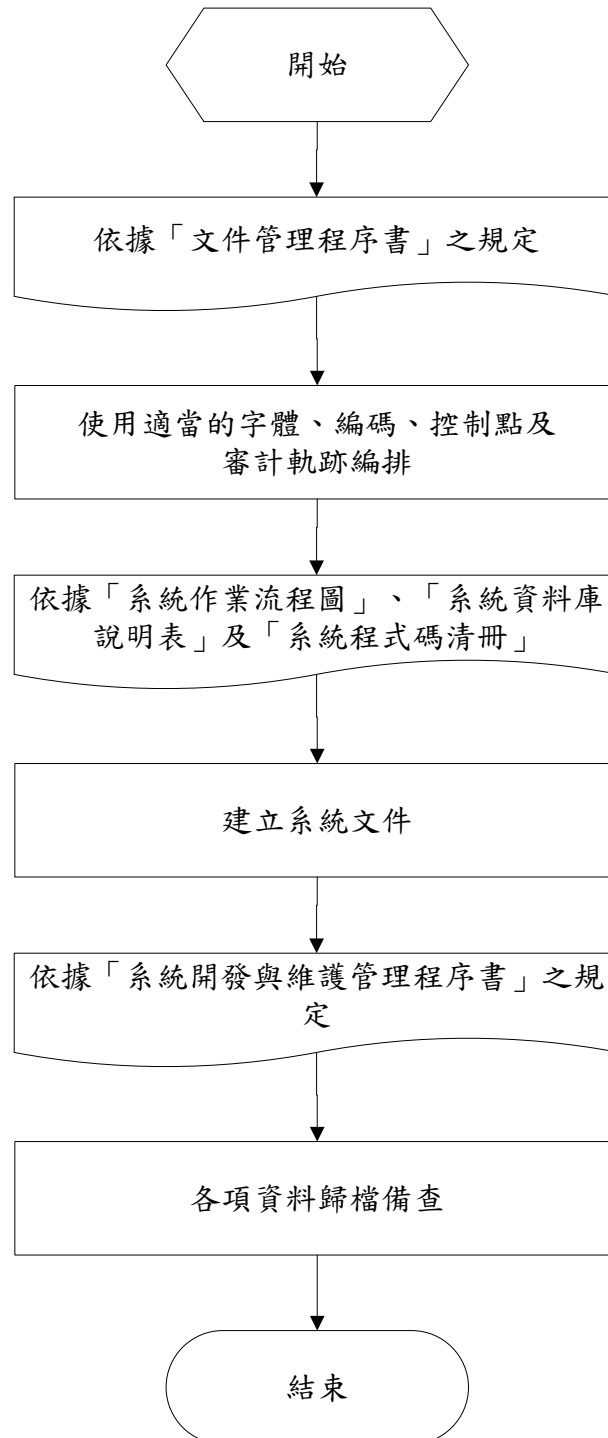
五、 依據及相關文件：

- (一)、 委外管理程序書(CHU-ISMS-B-009)
- (二)、 系統開發與維護管理程序書(CHU-ISMS-B-010)
- (三)、 個人資料保護法

制定單位：秘書室				公布日期：104/12/24	
文件編號	SC 電校 002	版本	01	頁次	1/6
作業名稱	系統文書編製作業				
主要負責單位	圖書與資訊處				
相關法令	教育體系資通安全管理規範				

流程圖：

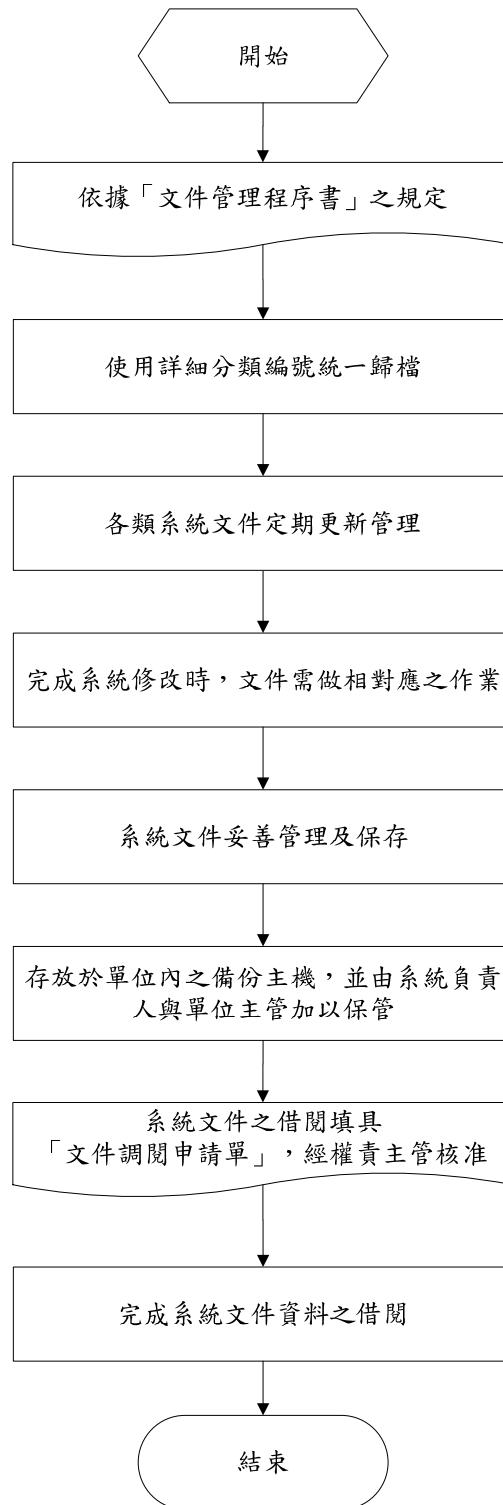
- 系統文件製作





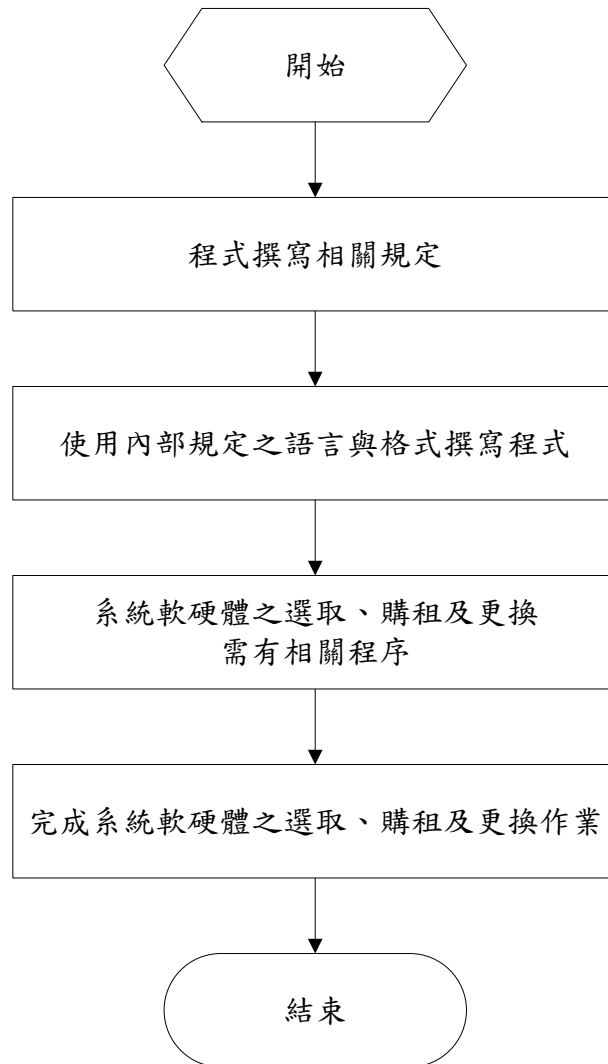
制定單位：秘書室				公布日期：104/12/24	
文件編號	SC 電校 002	版本	01	頁次	2/6
作業名稱	系統文書編製作業				
主要負責單位	圖書與資訊處				
相關法令	教育體系資通安全管理規範				

● 系統文件管理



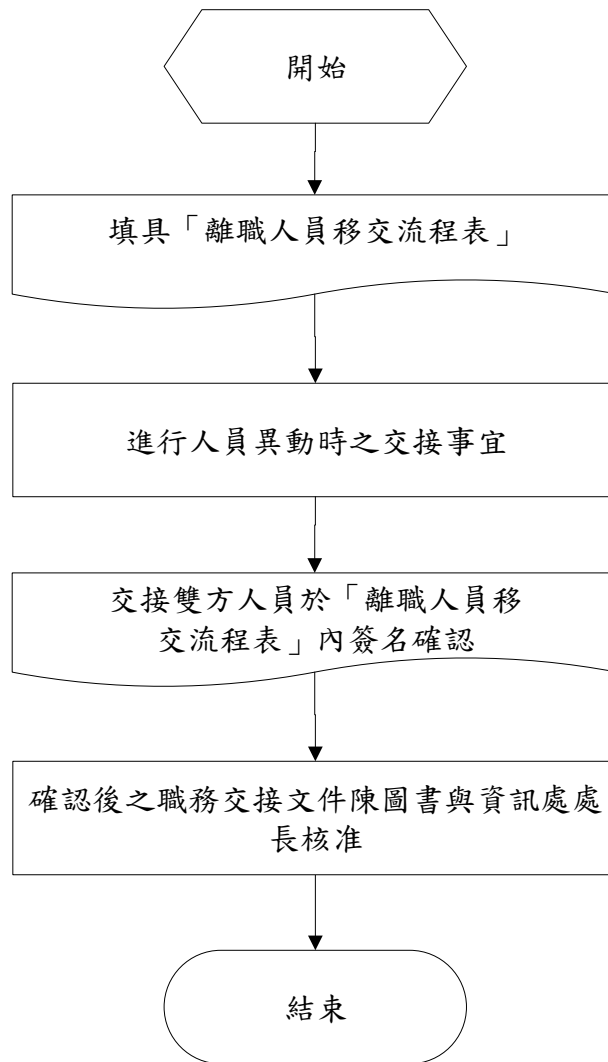
制定單位：秘書室				公布日期：104/12/24	
文件編號	SC 電校 002	版本	01	頁次	3/6
作業名稱	系統文書編製作業				
主要負責單位	圖書與資訊處				
相關法令	教育體系資通安全管理規範				

● 系統標準化管理



制定單位：秘書室				公布日期：104/12/24	
文件編號	SC 電校 002	版本	01	頁次	4/6
作業名稱	系統文書編製作業				
主要負責單位	圖書與資訊處				
相關法令	教育體系資通安全管理規範				

● 圖書與資訊處人員異動



制定單位：秘書室				公布日期：104/12/24	
文件編號	SC 電校 002	版本	01	頁次	5/6
作業名稱	系統文書編製作業				
主要負責單位	圖書與資訊處				
相關法令	教育體系資通安全管理規範				

作業程序：

(一)、系統文件製作：

1. 系統文件可依據「文件管理程序書」之規定，使用適當的字體、編碼、控制點及審計軌跡。
2. 系統文件可依據「系統作業流程圖」、「系統資料庫說明表」及「系統程式碼清冊」加以建立。
3. 系統開發單位可依據「系統開發與維護管理程序書」之規定，完成各項資料歸檔備查。

(二)、系統文件管理：

1. 系統文件可依據「文件管理程序書」之規定，詳細分類編號統一歸檔。
2. 系統修改時，文件應隨之修改，並註明修改時間。
3. 系統文件應備份存放於單位內之備份主機，並由系統負責人與單位主管加以保管。
4. 借閱系統文件資料時，需填具「文件調閱申請單」，經圖書與資訊處主任核准，始得借閱。

(三)、系統標準化管理：

1. 程式撰寫應使用內部規定之語言與格式。
2. 系統軟硬體之選取、購租及更換應透過校內相關程序。

(四)、圖書與資訊處人員異動：

1. 圖書與資訊處人員因故離職或調職時，應確實填具「離職人員移交流程表」，並與職務接任人員辦理交接事宜。
2. 離職或調職人員與職務接任人員於完成交接工作後，雙方均須於「離職人員移交流程表」內簽名確認，並將確認後之職務交接文件陳圖書與資訊處主任核准。

三、 控制重點：

(一)、系統文件製作：

1. 是否依據「文件管理程序書」、「系統作業流程圖」、「系統資料庫說明表」及「系統程式碼清冊」之規定製作系統文件。
2. 是否依據「系統開發與維護管理程序書」之規定覆核系統文件。

(二)、系統文件管理：

1. 系統文件是否依據「文件管理程序書」之規定分類管理。
2. 各類系統文件是否定期更新管理。
3. 系統文件是否妥善管理及保存。

制定單位：秘書室				公布日期：104/12/24	
文件編號	SC 電校 002	版本	01	頁次	6/6
作業名稱	系統文書編製作業				
主要負責單位	圖書與資訊處				
相關法令	教育體系資通安全管理規範				

4. 系統文件之借閱是否填具「文件調閱申請單」，經權責主管核准。

(三)、系統標準化管理：

1. 程式撰寫是否使用內部規定之語言與格式。
2. 系統軟硬體之選取、購租及更換是否有相關程序。

(四)、圖書與資訊處人員異動：

1. 圖書與資訊處人員離職或調職時，是否確實填具「離職人員移交流程表」，並與職務接任人員辦理交接事宜。
2. 「離職人員移交流程表」是否經離職或調職人員及職務接任人員簽名確認，職務交接文件亦是否陳權責主管核准。

四、 使用表單：

- (一)、文件調閱申請單(CHU-ISMS-D-005)
- (二)、離職人員移交流程表(CHU-ISMS-D-015)
- (三)、系統作業流程圖(CHU-ISMS-D-039)
- (四)、系統資料庫說明表(CHU-ISMS-D-040)
- (五)、系統程式碼清冊(CHU-ISMS-D-042)

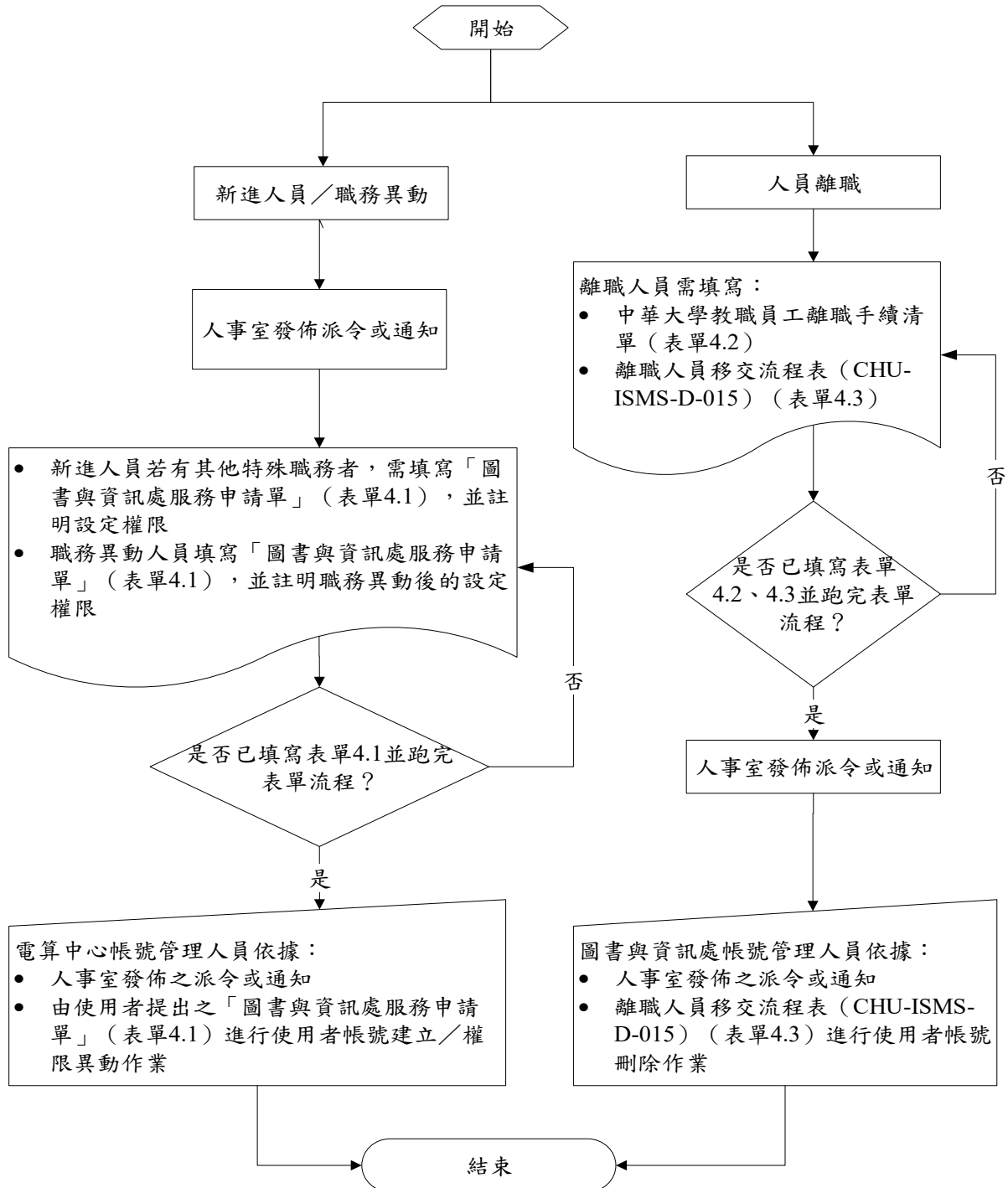
五、 依據及相關文件：

- (一)、文件管理程序書(CHU-ISMS-B-002)
- (二)、系統開發與維護管理程序書(CHU-ISMS-B-010)

制定單位：秘書室				公布日期：104/12/24	
文件編號	SC 電校 003	版本	01	頁次	1/7
作業名稱	程式及資料之存取作業				
主要負責單位	圖書與資訊處				
相關法令	教育體系資通安全管理規範				

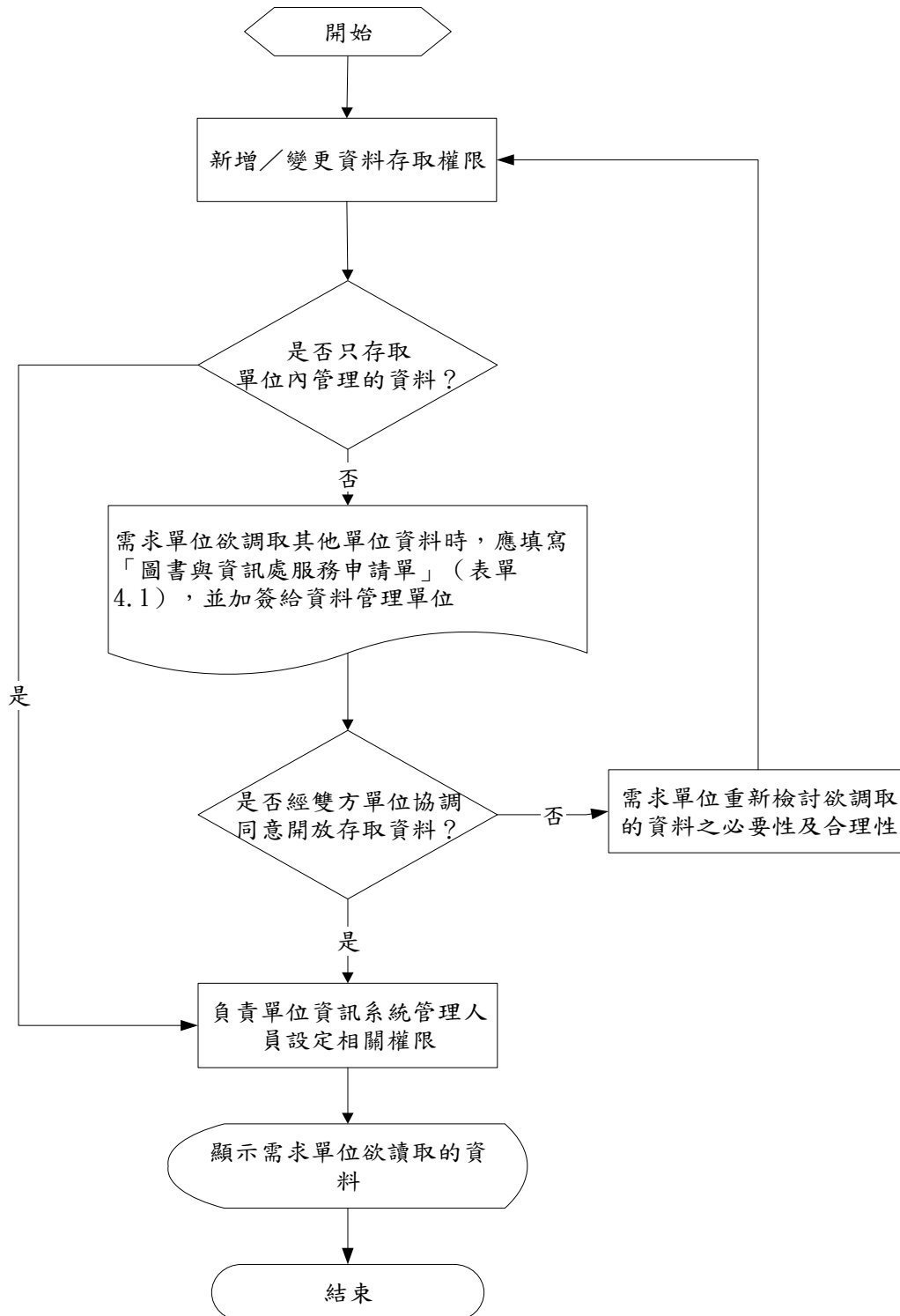
流程圖：

● 使用者權限管理流程圖



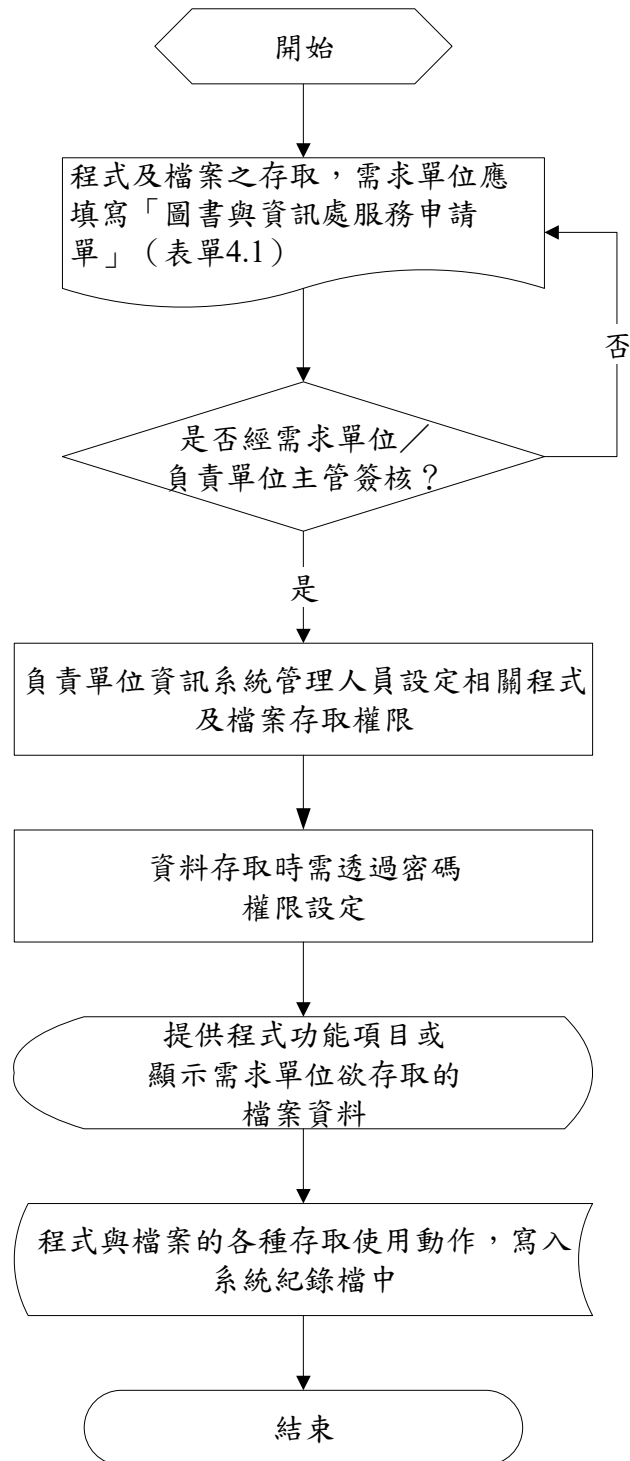
制定單位：秘書室				公布日期：104/12/24	
文件編號	SC 電校 003	版本	01	頁次	2/7
作業名稱	程式及資料之存取作業				
主要負責單位	圖書與資訊處				
相關法令	教育體系資通安全管理規範				

● 資料變更管理流程圖



制定單位：秘書室				公布日期：104/12/24	
文件編號	SC 電校 003	版本	01	頁次	3/7
作業名稱	程式及資料之存取作業				
主要負責單位	圖書與資訊處				
相關法令	教育體系資通安全管理規範				

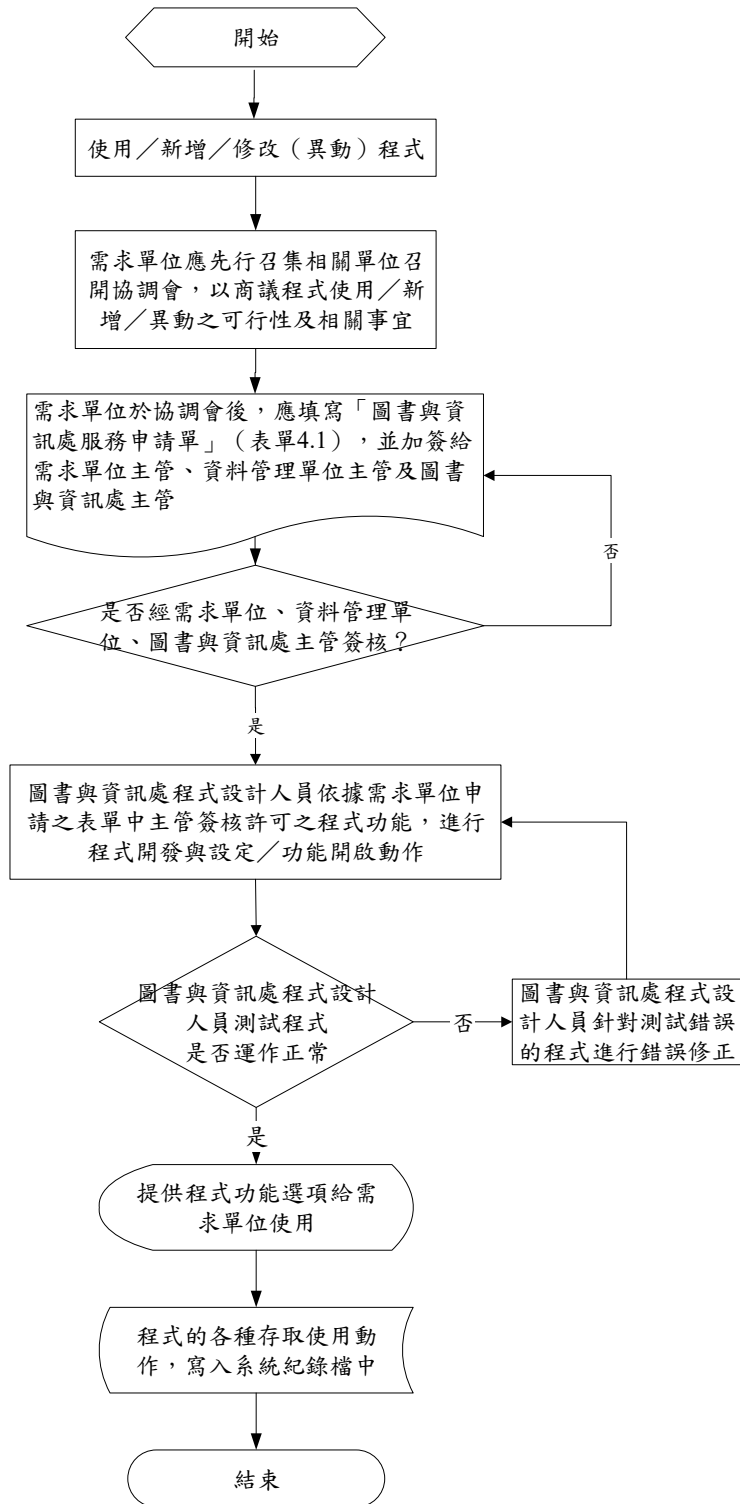
程式及檔案存取流程圖





制定單位：秘書室				公布日期：104/12/24	
文件編號	SC 電校 003	版本	01	頁次	4/7
作業名稱	程式及資料之存取作業				
主要負責單位	圖書與資訊處				
相關法令	教育體系資通安全管理規範				

● 程式管理流程圖



制定單位：秘書室				公布日期：104/12/24	
文件編號	SC 電校 003	版本	01	頁次	5/7
作業名稱	程式及資料之存取作業				
主要負責單位	圖書與資訊處				
相關法令	教育體系資通安全管理規範				

一、 作業程序：

(一)、 資訊安全規劃：

1. 圖書與資訊處依據「中華大學資訊安全政策」，以維護本校資訊資產的機密性、完整性及可用性，以及符合相關法令、法規之要求。
2. 經核准人員才能使用資訊系統，處理資料存取等事宜。

(二)、 使用者權限管理：

1. 圖書與資訊處於各項資訊系統使用授權時，應規範使用者帳號及使用者權限之維護程序及責任。
2. 新進人員或職務異動時，應經由人事室發佈派令或通知，或由使用者提出「圖資處服務申請單」，註明設定權限，經部門主管核准後，由帳號管理人員進行使用者帳號建立作業。
3. 人員離職時之使用者權限刪除應併入離職程序。離職人員應填寫「中華大學教職員工離職手續清單」及「離職人員移交流程表」，並以表單知會圖書與資訊處刪除。

(三)、 資料變更管理：

1. 資料為各使用單位所擁有，於建立使用者權限時，可限定資料之存取權限。
2. 若其他單位需調取資料，應由需求單位填寫「圖資處服務申請單」並加簽給資料管理單位。經雙方單位協調同意，並由圖書與資訊處資訊系統管理人員設定權限後，方能讀取資料。
3. 原始資料與電腦輸出資料應可互相勾稽。

(四)、 程式及檔案存取：

1. 程式、檔案之存取使用，由需求單位提出使用申請，並經需求單位主管簽核後轉圖書與資訊處辦理。
2. 程式、檔案之存取使用，均需留下紀錄。
3. 程式之原始式碼及執行檔應分開不同群組存放，且其存取作業亦應分別管制。
4. 系統程式應依業務權責限定程式設計人員之資料存取功能及範圍(如：程式之讀、寫)，並由圖書與資訊處主任評估其作業效益及核准其存取權限。
5. 檔案存取，應僅限預先許可之工作權限。
6. 供稽核使用之程式及檔案，應僅限稽核人員使用。
7. 資料存取應透過密碼權限設定，以杜絕未經授權之存取發生。
8. 程式及檔案應依不同用途存放不同區域。

(五)、 程式管理：

1. 對重要程式非經授權不得使用。

制定單位：秘書室				公布日期：104/12/24	
文件編號	SC 電校 003	版本	01	頁次	6/7
作業名稱	程式及資料之存取作業				
主要負責單位	圖書與資訊處				
相關法令	教育體系資通安全管理規範				

2. 程式之使用在電腦中均應保有紀錄。
  3. 正式程式說明文件之使用，應設權限管控。
  4. 禁止操作員變更程式名稱或編錄程式。
  5. 所有程式修改均應經需求單位填寫「圖資處服務申請單」，並經由需求單位主管、資料管理單位主管與圖資處主管核准，並有相關負責之人員，以杜絕程式未經授權而遭更改之情形。
  6. 有關單位均應參與重要程式修改過程。
  7. 正式程式之修改，需經多次測試以決定其預定結果。
  8. 程式修改時，備用程式、程式列表及其他說明文件亦應隨同更新。
  9. 程式之登錄、刪除或更改，均應在電腦內留存紀錄。
  10. 當程式執行發生錯誤時，應查明執行錯誤原因再予繼續執行。
- (六)、資料檔(庫)管理：資料檔(庫)之管理責任，應與使用此資料檔(庫)之應用程式及作業區隔獨立。

## 二、 控制重點：

- (一)、資訊安全規劃，是否訂定相關偵防措施及管理辦法。
- (二)、使用者權限管理：
  1. 是否訂定資訊安全程序。
  2. 使用者登錄系統帳號及使用權限之維護程序是否依規定辦理。
  3. 本校人員離職或調職時，是否立即註銷或更新使用者帳號、密碼權限。
- (三)、系統資料變更管理，是否以使用者密碼限定資料之存取權限。
- (四)、程式及檔案存取：
  1. 是否確實掌握教職員工及學生使用電腦系統程式及檔案之存取權限。
  2. 經授權使用之個人帳號、密碼權限表格是否特別予以列管保護。
  3. 系統維護人員之程式、檔案存取權限是否明確界定並經核准；於作業時即依授權範圍存取之。
  4. 程式、檔案之存取使用是否留下紀錄，是否定期核驗。
  5. 原始程式及目的程式是否分開存放。
  6. 資料存取方式是否適當，無不當之操作程序。
- (五)、程式錯誤之處理：
  1. 程式各種錯誤訊息是否確實記錄。
  2. 程式設計人員是否針對程式錯誤加以修改，相關之系統程式是否亦一併修改。
  3. 各種錯誤及其處理紀錄是否定期陳送主管核驗。

制定單位：秘書室				公布日期：104/12/24	
文件編號	SC 電校 003	版本	01	頁次	7/7
作業名稱	程式及資料之存取作業				
主要負責單位	圖書與資訊處				
相關法令	教育體系資通安全管理規範				

三、 使用表單：

- (一)、 圖資處服務申請單。
- (二)、 中華大學教職員工離職手續清單。
- (三)、 離職人員移交流程表 (CHU-ISMS-D-015)。

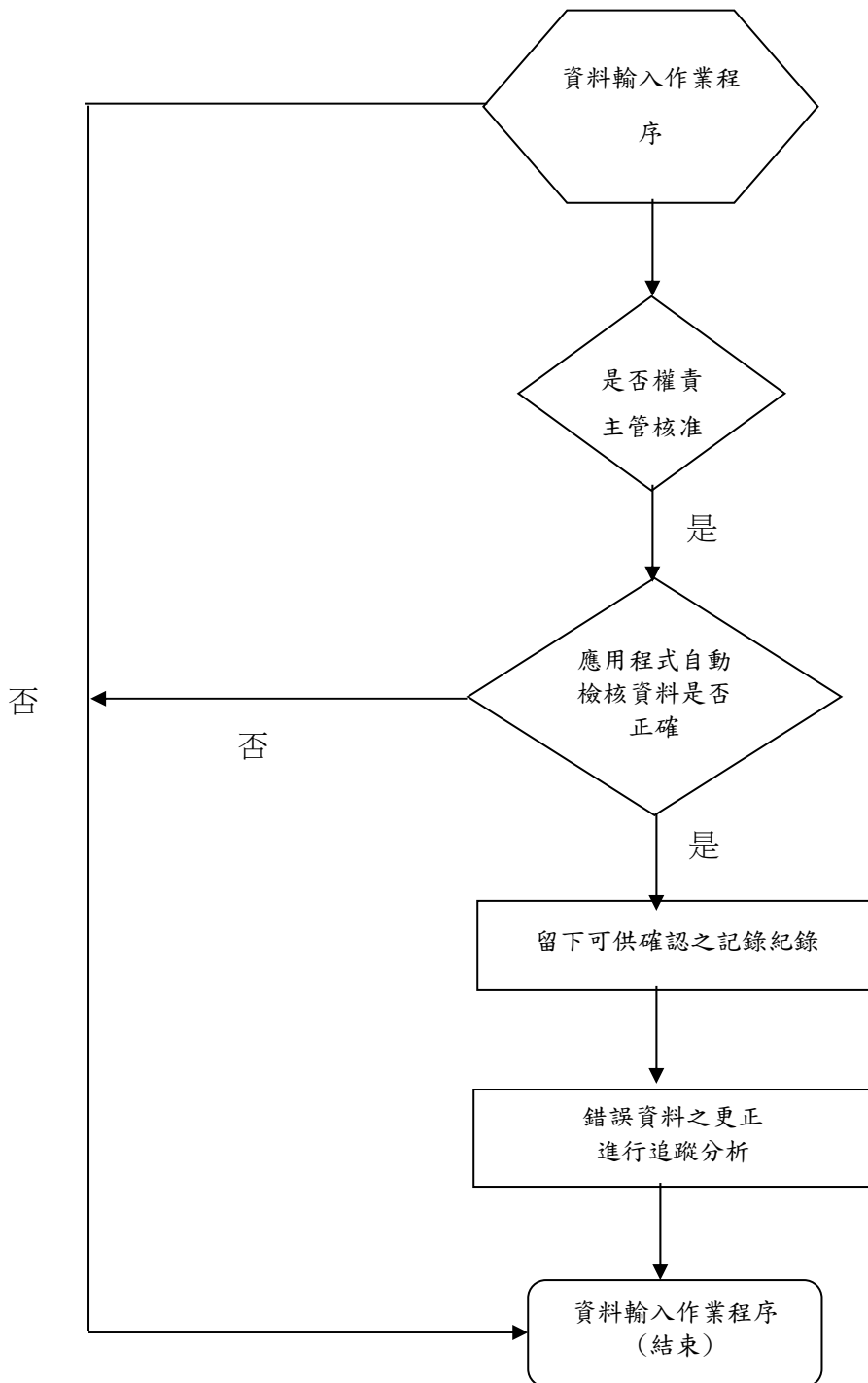
四、 依據及相關文件：

- (一)、 中華大學資訊安全政策 (CHU-ISMS-A-001)。
- (二)、 存取控制管理程序書 (CHU-ISMS-B-008)。
- (三)、 系統開發與維護程序書 (CHU-ISMS-B-010)。
- (四)、 資訊安全稽核作業程序書 (CHU-ISMS-B-013)。
- (五)、 矯正及預防管理程序書 (CHU-ISMS-B-014)。

制定單位：秘書室				公布日期：104/12/24	
文件編號	SC 電校 004	版本	01	頁次	1/4
作業名稱	資料輸出入及處理作業				
主要負責單位	圖書與資訊處				
相關法令	教育體系資通安全管理規範				

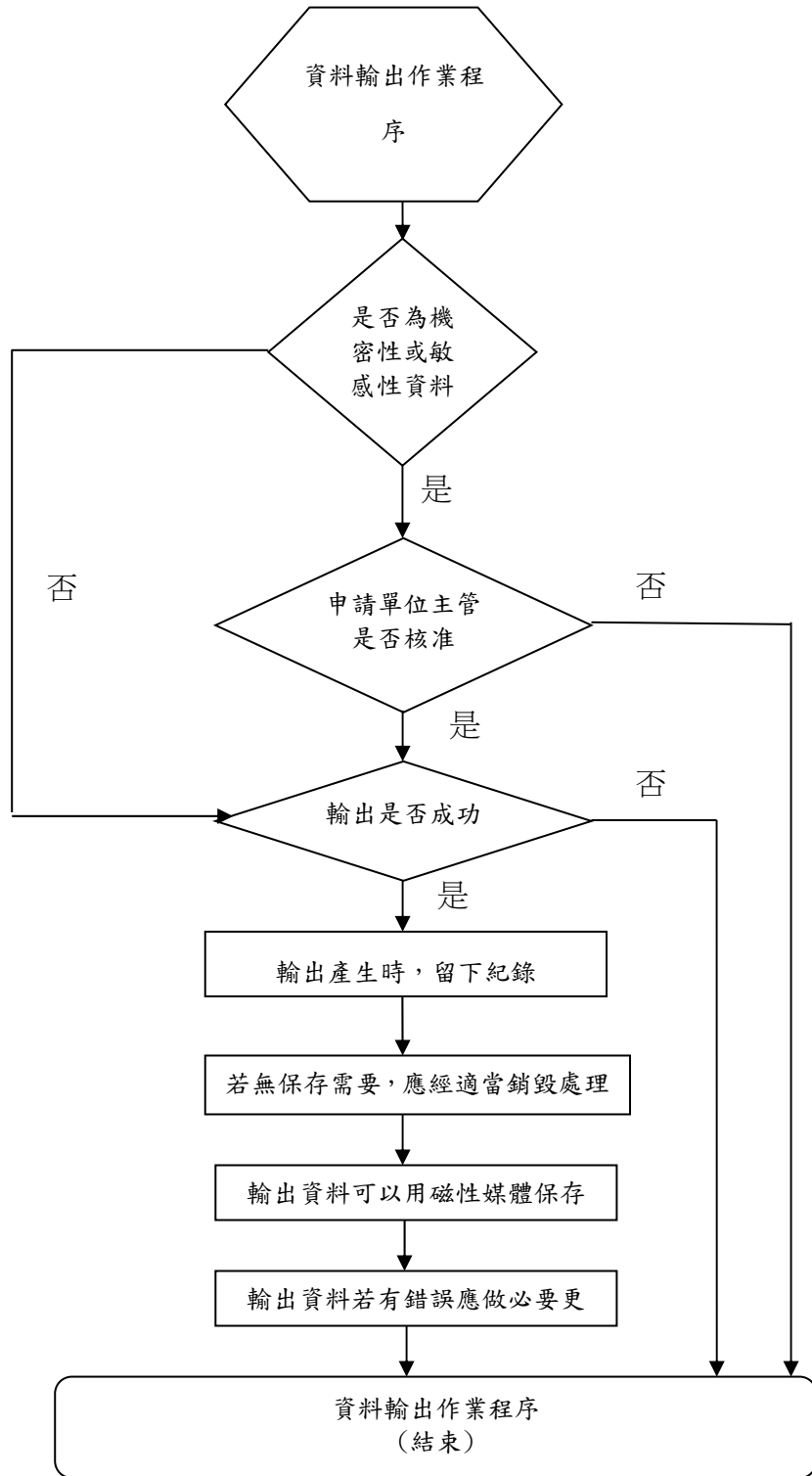
一、 流程圖：

- 資料作業輸入程序



制定單位：秘書室				公布日期：104/12/24	
文件編號	SC 電校 004	版本	01	頁次	2/4
作業名稱	資料輸出入及處理作業				
主要負責單位	圖書與資訊處				
相關法令	教育體系資通安全管理規範				

資料作業輸出程序



制定單位：秘書室				公布日期：104/12/24	
文件編號	SC 電校 004	版本	01	頁次	3/4
作業名稱	資料輸出入及處理作業				
主要負責單位	圖書與資訊處				
相關法令	教育體系資通安全管理規範				

## 二、 作業程序：

### (一)、 輸入：

1. 依據各系統之原始單據執行資料輸入處理。
2. 資料輸入單據或由系統產生之單據應以流水編號加以控管如遇有漏號，應即通知相關單位追蹤處理，以確保資料之完整性。
3. 資料允許輸入方式：
  - (1)、使用單位將資料依設計的輸入格式輸入。
  - (2)、將備份資料回存至主機。
4. 各單位於執行輸入作業前，應先行審核資料內容是否經權責主管核准或已授權，始可輸入，以確保輸入資料的有效性及真確性。
5. 應用程式應設定自動檢核功能或亦可考量由人工執行相關控管措施。如：資料屬性、數值正負號檢查、檢查號核對等。
6. 資料輸入處理應留下可供確認之紀錄。
7. 錯誤資料之更正執行應指派業務所屬單位授權之專人負責。
8. 應針對經常發生錯誤資料之發生原因進行追蹤分析，以期改善，並減少錯誤發生。
9. 當發生錯誤時，應先分析是屬於資料本身錯誤、或主檔錯誤、或程式錯誤，並追究其原因，取不同應變措施。
10. 備份資料回存後，須統計資料之完整性及正確性。

### (二)、 輸出：

1. 機密性或敏感性資料之輸出，應有適當管制。
2. 圖書與資訊處人員經圖書與資訊處主任授權，於核准工作權限內始進行資料輸出作業。
3. 輸出產生時，須留下紀錄，並能依使用者工號追蹤查核。
4. 輸出資料使用後若無保存需要，應經適當銷毀處理。
5. 重要資料之查詢須經核准後，始得進行之。
6. 輸出資料若以可攜式電腦儲存媒體，例如：筆記型電腦、隨身碟、外接式硬碟、光碟、磁帶等保存時，應定期檢查，以確定在必要時能以報表方式列印。
7. 輸出資料若發現錯誤，應做必要更正，並重新執行資料處理作業。

## 三、 控制重點：

### (一)、 輸入：

1. 各項資料之輸入是否評估其工作範圍、權責後，始授權執行輸入作業。
2. 單據或系統產生之單據是否以流水編號加以控管。

制定單位：秘書室				公布日期：104/12/24	
文件編號	SC 電校 004	版本	01	頁次	4/4
作業名稱	資料輸出入及處理作業				
主要負責單位	圖書與資訊處				
相關法令	教育體系資通安全管理規範				

3. 對於具影響性之系統操作功能，應有適當安全控管措施，該安全控管措施應考量業務需求及資訊資產之機密性，授與適當之存取權限及有效日期。
4. 資料輸入人員於收到原始單據時，是否審核資料內容經權責主管核准，始可輸入。
5. 應用程式是否設定自動檢核功能。
6. 資料輸入處理是否留下紀錄。
7. 當資料輸入發生錯誤時，是否立即追查原因並處理之。
8. 錯誤資料更正是否依既定程序分析錯誤屬性。

(二)、輸出：

1. 資料輸出是否經過適當之核決程序處理。
2. 資料輸出及其輸出份數是否經適當管制。
3. 當輸出資料不成功或不需時是否經適當銷毀處理。
4. 輸出資料保存是否妥當。

四、 使用表單：

- (一)、 系統需求申請與回覆單 (CHU-ISMS-D-035)
- (二)、 系統功能驗收表 (CHU-ISMS-D-038)

五、 依據及相關文件：

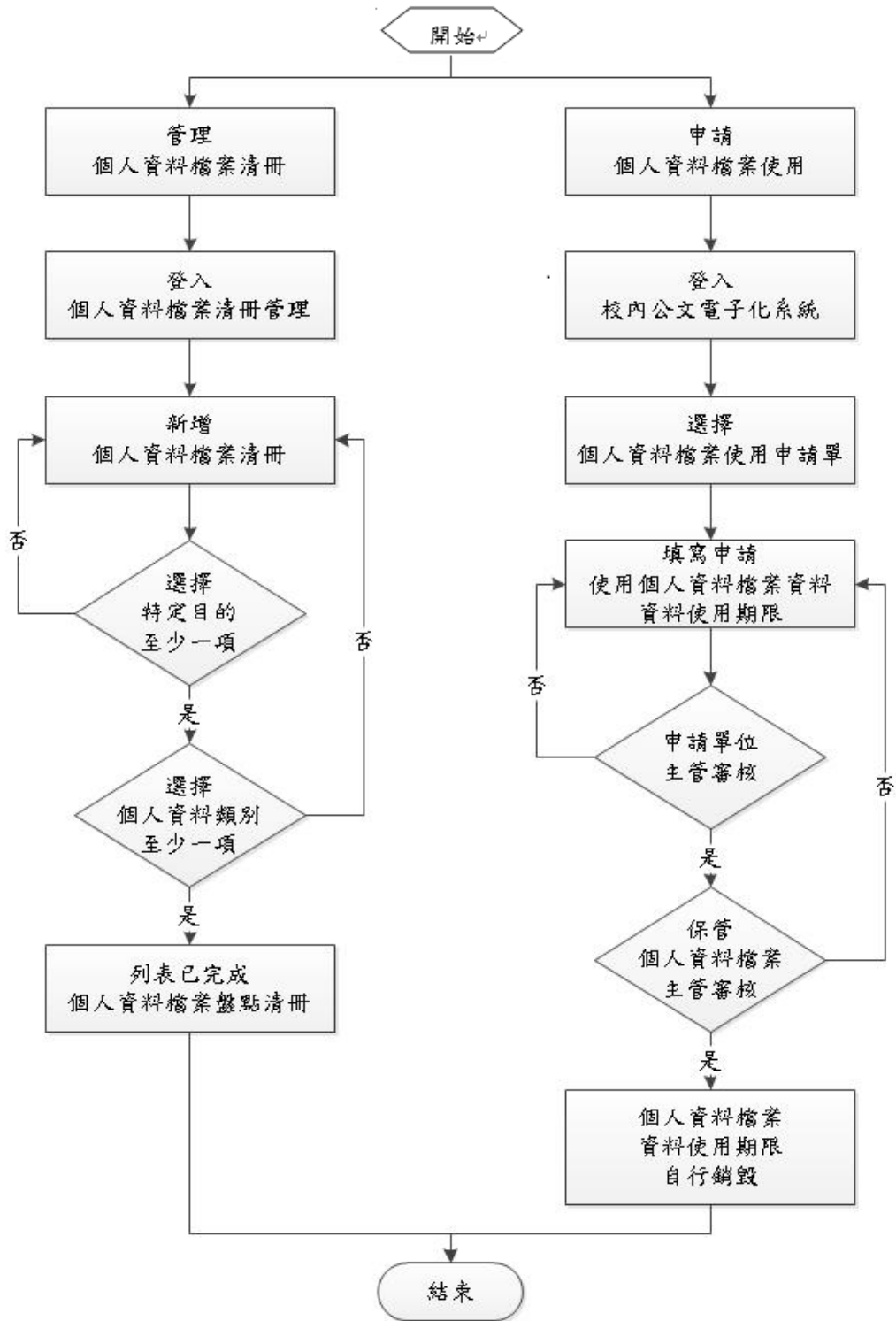
- (一)、 系統開發與維護管理程序書 (CHU-ISMS-B-010)
- (二)、 存取控制管理程序書 (CHU-ISMS-B-008)



制定單位：秘書室				公布日期：104/12/24	
文件編號	SC 電校 005	版本	01	頁次	1/4
作業名稱	個資盤點系統及電子公文個人資料檔案使用申請單作業				
主要負責單位	圖書與資訊處				
相關法令	教育體系資通安全管理規範				

一、 流程圖：

- 個資盤點系統及電子公文個人資料檔案使用申請單作業



制定單位：秘書室				公布日期：104/12/24	
文件編號	SC 電校 005	版本	01	頁次	2/4
作業名稱	個資盤點系統及電子公文個人資料檔案使用申請單作業				
主要負責單位	圖書與資訊處				
相關法令	教育體系資通安全管理規範				

## 二、 作業程序：

### (一)、個人資料保護及安全原則：

1. 本處由資訊安全官擔任機關召集人，統籌決策與執行單位內資訊安全與個資隱私業務之資源整合運用。
2. 本處不另設專人辦理安全維護及保管事項，統一由本校「個資保護聯絡窗口」兼辦專責人員業務。
3. 本處由文管人員擔任「個資保護聯絡窗口」，作為機關學校間個資業務協調聯繫之對口、機關學校本身個資安全事件通報之對口，以及重大個資外洩事件之民眾聯繫單一窗口。圖書與資訊處將「個資保護聯絡窗口」之聯繫方式（如：電話、email）置於圖書與資訊處網站，以便利民眾提出申訴與救濟。
4. 個人資料檔案應定期備份，並防止個人資料被竊取、竄改、毀損、滅失或洩露。個人資料輸入、輸出、存取、更新、更正或註銷等處理行為，宜釐定使用範圍及調閱或存取權限。個人資料檔案之處理行為應設置使用者代碼及通行碼，不得與他人共用並定期更新。另視需要考量採取權限區隔、資料加密機制，或相關核准程序加以控管，並留存使用者身分、識別帳號與其行為紀錄以供事後稽查。
5. 個人資料檔案儲存於個人電腦者，應於該電腦設置可辨識身份之登入通行碼，並視業務及資料重要性，考量其他輔助安全措施。個人資料檔案使用完畢後，應即退出應用程式，不得留置於電腦終端機。
6. 含有個人資料之紙本報表的申請、讀取、列印、使用、存檔、轉交及銷毀等處理及利用行為，宜建立相關之授權、監督及行為記錄機制。
7. 內部傳遞或與其他機關交換個人資料時，應選擇可靠且具備保密機制之傳遞方式，如於實體文件封袋加上彌封、或對資料檔案壓縮加密，並對轉交或傳輸行為加以記錄流向備查。
8. 對於個人資料輸入部分，登入”個人資料檔案清冊管理系統”，將個人資料清冊完整輸入進去。
9. 對於個人資料之調閱透過電子公文系統的”個人資料檔案使用申請單”提出申請並核准，並在資料使用期限過自行銷毀。調閱紀錄可視機關實際需求存檔，以利後續人員查詢及追蹤。
10. 以電腦處理個人資料時，需核對個人資料之輸入、輸出、編輯或更正是否與原件相符。個人資料提供利用時，對資料相符與否如有疑義，應調閱原檔案查核。
11. 本處管理之網站或網頁內容，於確有必要公佈個人資料時，需經所屬單位主管核准，且依相關法律及規範處理，始得公佈。

## 三、 控制重點：

制定單位：秘書室				公布日期：104/12/24	
文件編號	SC 電校 005	版本	01	頁次	3/4
作業名稱	個資盤點系統及電子公文個人資料檔案使用申請單作業				
主要負責單位	圖書與資訊處				
相關法令	教育體系資通安全管理規範				

(一)、處理個資之資訊設備使用注意事項：

1. 處理個人資料檔案之資訊設備，需設置使用者代碼及通行碼。
2. 通行碼至少每六個月更換一次，通行碼長度應至少8碼，且包含文數字。
3. 禁止與他人共用電腦系統帳號。
4. 採取權限區隔，非專責處理特定個人資料者不得具有存取或查閱個人資料之權限。
5. 個人資料檔案應予以加密。
6. 至少每月備份資訊設備內個人資料檔案一次。
7. 個人資料檔案使用完畢後，應立即退出應用程式。
8. 資訊設備應使用螢幕保護程式，設定螢幕保護密碼，並將螢幕保護啟動時間設定為15分鐘以內。
9. 交換個人資料檔案時，應對資料檔案加密，亦或是透過加密通道傳送。
10. 個人資料禁止存放於網路芳鄰分享目錄，並停用Guest帳號。
11. 應避免使用即時通訊軟體傳輸個人資料檔案。
12. 應避免使用外部網頁式電子郵件(Webmail)傳輸個人資料檔案。
13. 禁止使用點對點(P2P)軟體及Tunnel相關工具下載或提供分享檔案。
14. 存放個人資料之資訊設備應與外部網路隔絕（如：防火牆）。
15. 存放個人資料之資訊設備應安裝防毒軟體，除至少每日更新病毒碼外，並應每周執行完整掃描。
16. 存放個人資料之資訊設備應定期檢視、更新作業系統、應用程式漏洞（如：Windows作業系統、Windows Office、Adobe Acrobat等）。

(二)、設備管理注意事項：

1. 由專人負責管理儲存個人資料檔案之資訊設備與其他相關設施等，並檢視、處理其錯誤或異常事件等訊息。
2. 儲存個人資料之資訊設備應置放於實體安全區域（如：門禁控管之辦公區域、機房），避免有心人士或非授權人員存取。
3. 儲存個人資料檔案之磁碟、磁帶，及紙本等相關儲存媒體，由專人管理，並置於實體保護之環境（如：上鎖之防潮箱、書櫃），必要時應建立備份機制，以防止資料損壞、遺失或遭竊取。相關儲存媒體非經權責單位同意並留存紀錄，不得任意攜出或拷貝複製。
4. 外部團體或個人更新或維修電腦設備時，應指派專人在場，確保個人資料之安全及防止個人資料外洩。

制定單位：秘書室				公布日期：104/12/24	
文件編號	SC 電校 005	版本	01	頁次	4/4
作業名稱	個資盤點系統及電子公文個人資料檔案使用申請單作業				
主要負責單位	圖書與資訊處				
相關法令	教育體系資通安全管理規範				

5. 儲存個人資料檔案之電腦或相關設備如需報廢或移轉他用時，應確實刪除該設備所儲存之個人資料檔案。

(三)、人員管理注意事項：

1. 本處應對處理個人資料檔案之人員施予資訊安全與個資隱私保護之教育訓練（內、外訓皆可），並定期於單位內宣導個資隱私保護之重要性。
2. 處理個人資料檔案之人員，其職務如有異動，應將所保管之儲存媒體及有關資料列冊移交，接辦人員除應於相關系統重置通行碼外，應視需要更換使用者識別帳號。
3. 處理個人資料檔案之人員，應簽訂保密切結書，並確認於離職時或合約終止時取消或停用其使用者識別帳號。

(四)、系統開發及委外管理注意事項：

1. 自行開發或委外處理個人資料檔案之資訊系統，應在系統開發生命週期之初始階段，將個人資料檔案的安全需求納入考量（如：邏輯測試）；系統之維護、更新、上線、及版本異動等作業，應予安全管制，避免危害個人資料安全。
2. 宜避免允許維護人員或系統服務廠商以遠端登入方式進行牽涉個人資料的資訊系統維護或其他有關之運作；若需使用遠端登入方式進行維護，則應透過加密通道進行（如：HTTPS、SSH等）。
3. 自行開發或委外處理個人資料檔案之資訊系統，應保護及控制測試資料，且宜避免以真實個人資料進行測試；如需使用，應將可辨識之個人資料修改為無法辨識之模糊資訊（如：虛擬或錯置），並於完成測試作業後迅速移除。
4. 個人資料檔案若委外建檔，應於委外合約中載明所處理之個人資料保密義務、資訊安全相關責任及違反之罰則。

四、 使用表單：

- (一)、個人資料檔案使用申請單(校內電子公文系統)

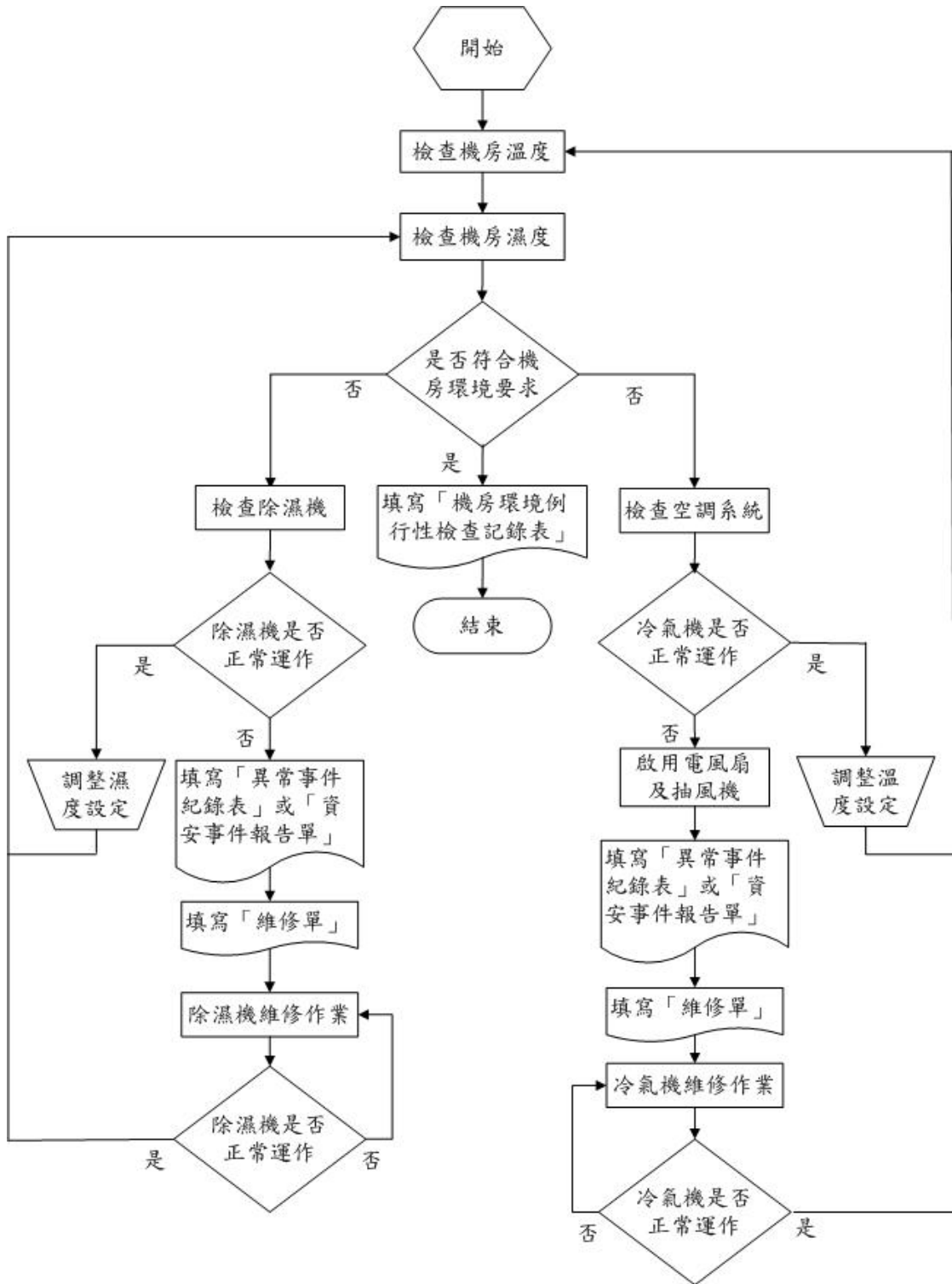
五、 依據及相關文件：

- (一)、個人資料保護程序書（CHU-ISMS-B-015）
- (二)、個人資料保護法
- (三)、教育體系資通安全管理規範
- (四)、個人資料保護檢核表（CHU-ISMS-D-052）
- (五)、保密切結書（CHU-ISMS-D-013）

制定單位：秘書室				公布日期：104/12/24	
文件編號	SC 電網 001	版本	01	頁次	1/5
作業名稱	檔案及設備之安全作業				
主要負責單位	圖書與資訊處				
相關法令	教育體系資通安全管理規範				

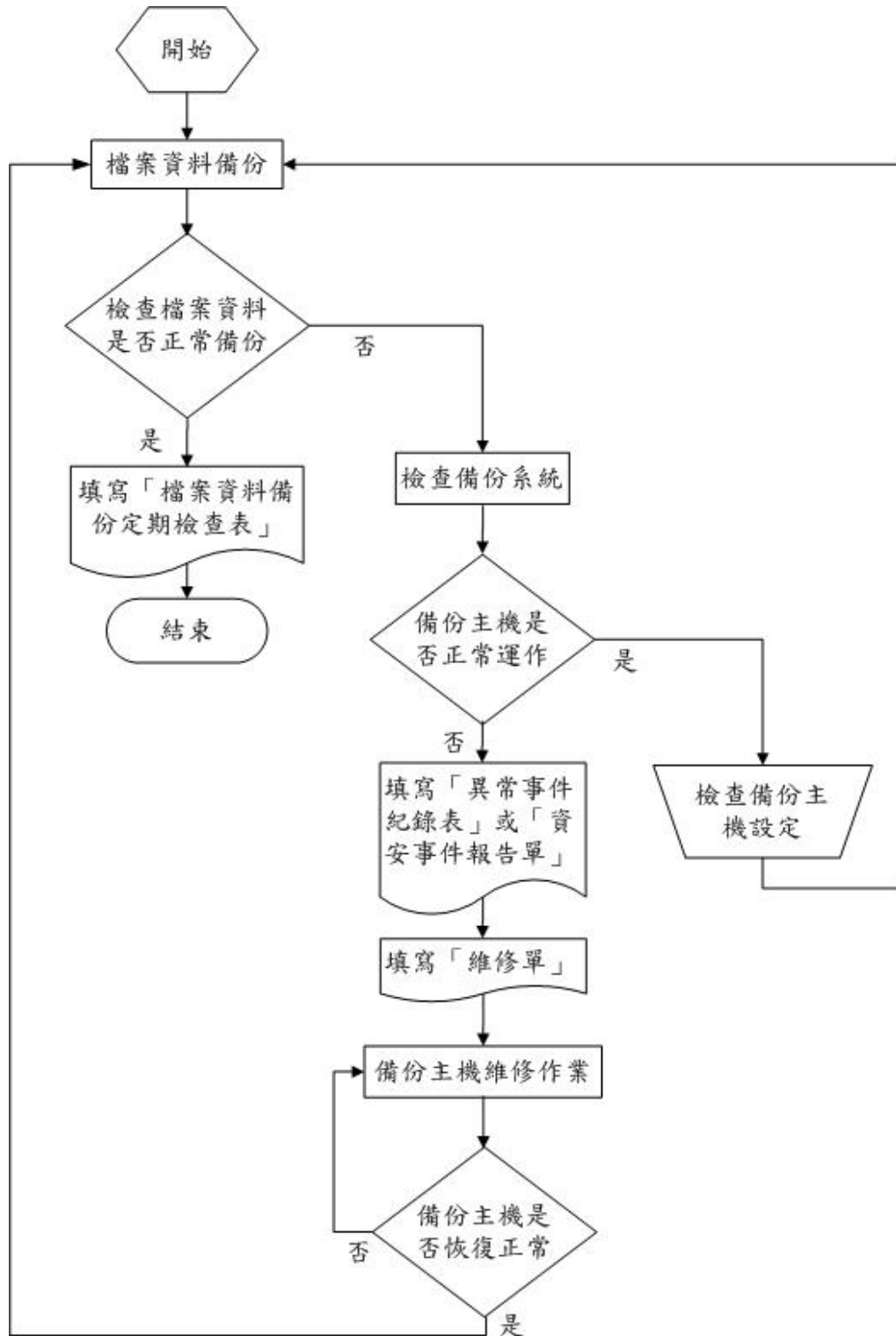
一、 流程圖：

● 機房環境例行性檢查：



制定單位：秘書室				公布日期：104/12/24	
文件編號	SC 電網 001	版本	01	頁次	2/5
作業名稱	檔案及設備之安全作業				
主要負責單位	圖書與資訊處				
相關法令	教育體系資通安全管理規範				

● 檔案備份：



制定單位：秘書室				公布日期：104/12/24	
文件編號	SC 電網 001	版本	01	頁次	3/5
作業名稱	檔案及設備之安全作業				
主要負責單位	圖書與資訊處				
相關法令	教育體系資通安全管理規範				

## 二、 作業程序：

### (一)、 機房管理：

1. 機房溫度應維持在27 °C以下，相對濕度應維持在60%RH以下，並填寫於「機房環境例行性檢查紀錄表」中，且須有防火設備以及門禁管制裝置。
2. 重要資訊設備應放置於機房內防護，對於人員的進出須有門禁紀錄及錄影設備控管，未經授權者不得擅自進入，若外部人員或本處未具機房進出權限之人員，因執行業務需求進入機房時，必須由儀器設備權責單位或保管單位，指派人員隨行並填寫「人員進出機房登記表」後方可進出機房，並遵守相關設備管理之規定。
3. 機房應設置足量之不斷電系統（UPS），供應重要資訊設備電源之使用，以保障資訊設備之正常作業，並填寫於「機房環境例行性檢查紀錄表」中。
4. 機房內應保持整齊清潔，並嚴禁吸菸、飲食、堆置易燃物或爆裂物等危險物品，且須設置滅火設備，並定期檢測其有效使用期間。
5. 資訊設備保管單位應每日檢查設備機房運作的情形，並填寫於「機房環境例行性檢查紀錄表」，發現異常時，應填寫「異常事件紀錄表」並進行必要之處置。
6. 電力、網路、通信設備應予以保護，以防止遭有心人士截取或破壞。
7. 機房應設置專用空調設備以維持電腦主機正常運作，並對空調設備進行定期維護、檢修。
8. 重要電腦主機之資訊設備、監視系統及警報系統等應定期檢修測試。
9. 資訊設備專用電源插座，不得使用於資訊及空調設備以外之設備，以免耗用電源，發生跳電當機情形，影響正常作業。

### (二)、 檔案備份：

1. 系統業務之負責人員，應依「通訊與作業管理程序書」及「日常操作管理作業說明書」進行備份，並於「備份狀況記錄表」做備份記錄，以確認主機檔案備份是否完整。
2. 檔案備份過程中發現異常，應於「異常事件紀錄表」或「資安事件報告單」上記錄發生原因及排除方法。
3. 檔案備份除了備份於機房實體主機外，重要系統資料應考量置放於安全且獨立於機房外之處所。
4. 檔案備份資料應定期清除備份資料，以及定期盤點備份資料。
5. 檔案備份資料，應依「通信與作業管理程序書」測試其回存之可用性。

### (三)、 安全管理：

1. 電腦使用區域之家具設備、地板等宜不易燃。

制定單位：秘書室				公布日期：104/12/24	
文件編號	SC 電網 001	版本	01	頁次	4/5
作業名稱	檔案及設備之安全作業				
主要負責單位	圖書與資訊處				
相關法令	教育體系資通安全管理規範				

2. 逃生出口應保持乾淨暢通，逃生路線應明確並有緊急照明裝置。
3. 設置二氧化碳滅火器因應突發狀況。
4. 對進出電腦使用區域之敏感地區宜有足夠之管制措式。

### 三、控制重點：

#### (一)、機房管理：

1. 是否制訂完整之機房管理制度。
2. 機房是否依據實體安全管理程序書妥善管理。
3. 機房是否具有足量之不斷電系統（UPS）。
4. 機房是否嚴禁擺置易燃或爆裂物等危險物品；滅火設備是否定期檢測有效使用期間。
5. 重要電腦及通訊設備是否特別防護；人員進出機房之控管，是否亦經核准。
6. 每日機房設備運作情形，是否確實檢查並作成記錄。

#### (二)、檔案備份：

1. 檔案備份是否依「通訊與作業管理程序書」及「日常操作管理作業說明書」進行備份，是否確實記錄於「備份狀況記錄表」。
2. 檔案備份作業發現異常時，是否於「異常事件紀錄表」或「資安事件報告單」上記錄發生原因及排除方法。
3. 檔案備份資料是否置放於安全又獨立於機房外之處所。
4. 檔案備份資料是否定期清除及定期盤點。
5. 檔案備份資料是否定期測試其回存之可用性。

#### (三)、安全管理：

1. 電腦使用區域之辦公設備、地板等，是否具不易燃燒且防火功能之材質。
2. 逃生出口是否保持乾淨暢通、逃生路線是否明確標示，並有緊急照明裝置。
3. 是否設置二氧化碳滅火器因應突發狀況。
4. 對進出電腦使用區域之敏感地區是否有足夠的管制措式。

### 四、使用表單：

- (一)、機房環境例行性檢查紀錄表 (CHU-ISMS-D-020)
- (二)、備份狀況記錄表 (CHU-ISMS-D-029)
- (三)、異常事件紀錄表 (CHU-ISMS-D-021)
- (四)、資安事件報告單(CHU-ISMS-D-044)
- (五)、人員進出機房登記表 (CHU-ISMS-D-018)



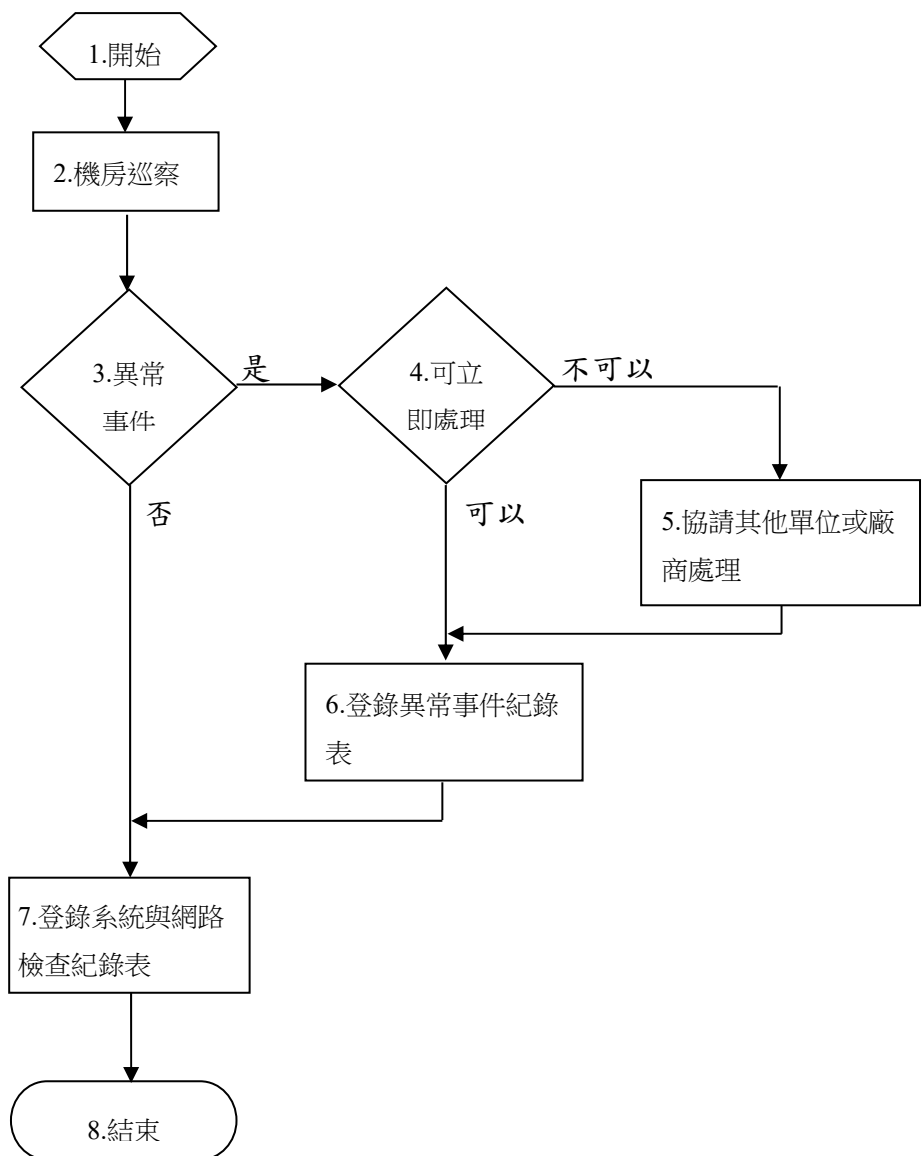
制定單位：秘書室				公布日期：104/12/24	
文件編號	SC 電網 001	版本	01	頁次	5/5
作業名稱	檔案及設備之安全作業				
主要負責單位	圖書與資訊處				
相關法令	教育體系資通安全管理規範				

五、依據及相關文件：

- (一)、實體安全管理程序書(CHU-ISMS-B-006)
- (二)、通訊與作業管理程序書(CHU-ISMS-B-007)
- (三)、日常操作管理作業說明書(CHU-ISMS-C-007)

制定單位：秘書室				公布日期：104/12/24	
文件編號	SC 電網 002	版本	01	頁次	1/3
作業名稱	硬體及系統軟體之使用及維護作業				
主要負責單位	圖書與資訊處				
相關法令	教育體系資通安全管理規範				

一、 流程圖：  
硬體設施管理流程



二、 作業程序：

(一)、 硬體設施管理：

1. 電腦機房重要裝置或設施之運轉及故障情形均須記錄於「系統與網路檢查紀錄表」，每月送資訊安全官簽核。

制定單位：秘書室				公布日期：104/12/24	
文件編號	SC 電網 002	版本	01	頁次	2/3
作業名稱	硬體及系統軟體之使用及維護作業				
主要負責單位	圖書與資訊處				
相關法令	教育體系資通安全管理規範				

2. 各設備裝置故障之原因經分析後，均應採取適當整復措施，且其處理情形亦應紀錄於異常事件紀錄表。
3. 重要裝置應定期辦理預防性維護並作成紀錄。
4. 設備維護應與廠商訂定書面契約以確定維護內容。
5. 啟動機器時，對各種裝置應注意其正常運轉。

(二)、可攜式媒體管理：

1. 磁帶、磁片、光碟、隨身碟及記憶卡等媒體，均應確實管理。
2. 存放重要資料之媒體不使用時，應妥善收存歸位，並置於安全位置區。
3. 儲存媒體之報廢，請詳「資訊資產異動作業說明書」，且須經核准。

(三)、智慧財產權之管理：

1. 本校應使用合法作業系統與應用軟體。
2. 圖書與資訊處不定期實體稽查及程式軟體稽查是否有使用未經授權之軟體及其他不當之軟體。

(四)、軟硬體採購管理：

1. 硬體及系統軟體選購：
  - (1)、電腦設備之採購以預先編列之學年度預算為標準。
  - (2)、電腦設備採購應考慮本校整體短、中、長期策略與發展方向。
  - (3)、電腦軟硬體之採購方法，應遵循中華大學請購單作業及流程。
2. 硬體及系統軟體之安裝：
  - (1)、硬體及系統軟體在使用之前應予以綜合廣泛地測試。
  - (2)、應確定安裝軟體之前所有已知的問題已經評估解決。
  - (3)、進行安裝時，應遵循書面程序。
3. 應限制只有經過授權之人員才可存取系統軟體及相關文件。

三、 控制重點：

(一)、硬體設施管理：

1. 硬體故障是否經適當處理、故障原因是否經評估分析、所有故障異常情形是否完整記錄，並有專人保管、紀錄之核閱亦是否確實。是否評估簽訂硬體維護合約。
2. 是否評估簽訂適當適額之保險契約。

(二)、可攜式媒體管理：

1. 磁帶、磁片、光碟、隨身碟及記憶卡等媒體，是否確實管理。
2. 可攜式媒體，是否置於安全位置區。
3. 可攜式媒體廢棄時，資料是否經銷毀，以使其不得再度使用。

制定單位：秘書室				公布日期：104/12/24	
文件編號	SC 電網 002	版本	01	頁次	3/3
作業名稱	硬體及系統軟體之使用及維護作業				
主要負責單位	圖書與資訊處				
相關法令	教育體系資通安全管理規範				

(三)、智慧財產權之管理：

1. 各單位是否定期稽查未經授權使用之軟體及其它不當軟體。
2. 圖書與資訊處是否不定期實體稽查及程式軟體稽查，有無使用未經授權之軟體及其他不當之軟體。

(四)、軟硬體採購管理：

1. 電腦軟硬體採購是否編列學年度預算。
2. 電腦軟硬體採購是否考慮本校整體短、中、長期策略與發展方向。
3. 電腦設備採購是否依據中華大學請購單作業及流程辦理。

四、 使用表單：

- (一)、系統與網路檢查紀錄表 (CHU-ISMS-D-023)。
- (二)、異常事件紀錄表 (CHU-ISMS-D-021)。

五、 依據及相關文件：

- (一)、資訊資產異動作業說明書 (CHU-ISMS-C-006)。
- (二)、中華大學請購單作業及流程。

制定單位：秘書室				公布日期：104/12/24	
文件編號	SC 電網 003	版本	01	頁次	1/2
作業名稱	系統復原計畫及測試作業				
主要負責單位	圖書與資訊處				
相關法令	教育體系資通安全管理規範				

一、 流程圖：

無。

二、 作業程序：

(一)、 復原措施：

1. 成立緊急應變小組，由不同單位人員共同參與，並加強訓練緊急事故之應變能力。
2. 各種故障等級，應訂有允許復原時間。
3. 硬體或軟體發生故障異常時，使用者應立即登錄電子公文系統填具維修申請(硬體：圖資處電腦設備修繕申請單、軟體：圖資處服務申請單)，通報圖書與資訊處人員進行了解並提供處理建議；維修人員經適當授權後始執行修復作業，且將處理情形回覆至電子公文系統通知使用者修復狀況，並保留維修紀錄。
4. 系統經外力破壞造成無法運作或損毀時，應立即通知維護合約廠商進行修復。
5. 硬體或軟體發生嚴重故障損壞無法回復正常運作時，應詢求備品急用之支援設備暫時使用，回存本校備份資料，以確保系統仍可正常運作。
6. 判定硬體或軟體故障原因。如是硬體設備發生問題，應洽廠商進行檢測維修，並於修復完成後，針對復原之硬體設備進行測試驗收；如是軟體設備發生問題，應與相關單位探討問題發生原因，並追查是否屬人為疏失，必要時應洽廠商或圖書與資訊處人員重新安裝軟體。
7. 對備援設備應不定期檢測，測試其可用性。

(二)、 復原結果測試：

1. 重置後之硬體或軟體，於執行測試作業程序後，應將暫存於其他系統之資料回存，並於完成回存作業及確認資料回存之完整性後，將暫存資料予以銷毀。
2. 測試人員應將測試結果詳述說明，呈原軟硬體購置單位一級主管核示後建檔。

三、 控制重點：

(一)、 復原措施：

1. 是否成立緊急應變小組，且由不同單位人員共同參與，並加強訓練緊急事故之應變能力。
2. 各種故障等級，是否訂有允許復原時間(「業務流程衝擊分析表」)。
3. 是否制訂完整且可行之復原計畫(「關鍵業務障礙偵測與復原作業程序」)。
4. 是否不定期測試及演練復原計畫，以確保硬體或軟體復原計畫之適用性及支援運作能力。

制定單位：秘書室				公布日期：104/12/24	
文件編號	SC 電網 003	版本	01	頁次	2/2
作業名稱	系統復原計畫及測試作業				
主要負責單位	圖書與資訊處				
相關法令	教育體系資通安全管理規範				

5. 當硬體或軟體發生異常時，是否依系統復原作業程序處理。
6. 硬體或軟體復原後，是否追查其故障原因，研討解決之道，避免類似狀況發生。
7. 對於人為破壞或不可抗力因素所造成之系統毀損，是否立即與廠商協商，取得暫時替代之軟、硬體供即時性資料處理之用，避免本校系統運作中斷。

(二)、復原結果測試：

1. 重置後之硬體或軟體，是否依測試作業程序執行測試。
2. 重置後之硬體或軟體，是否已將暫存於其他系統之資料回存，是否於完成回存作業及確認資料回存之完整性後，將暫存資料予以銷毀。
3. 測試人員是否詳述說明測試結果，呈原軟硬體購置單位一級主管核示後建檔。
4. 重置後之硬體或軟體，於執行測試作業程序後，應將暫存於其他系統之資料回存，並於完成回存作業及確認資料回存之完整性後，將暫存資料予以銷毀。

四、 使用表單：

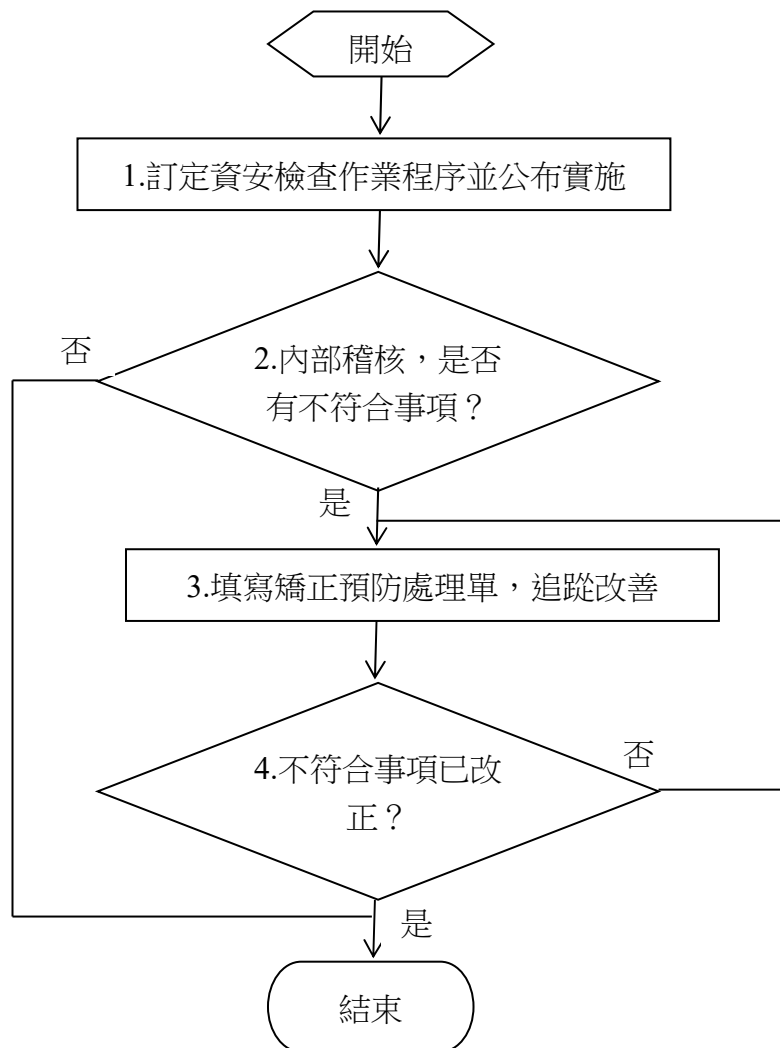
- (一)、 關鍵業務障礙偵測與復原作業程序(CHU-ISMS-C-003)。
- (二)、 業務流程衝擊分析表(CHU-ISMS-D-046)。

五、 依據及相關文件：

- (一)、 業務永續運作計畫(CHU-ISMS-C-002)。

制定單位：秘書室				公布日期：104/12/24	
文件編號	SC 電教 001	版本	01	頁次	1/2
作業名稱	資訊安全之檢查作業				
主要負責單位	圖書與資訊處				
相關法令	教育體系資通安全管理規範				

一、 流程圖：



二、 作業程序：

- (一)、 圖書與資訊處負責訂定校園網路管理規範(中華大學圖書與資訊處校園網路管理辦法)，執行網路管理工具之設定與操作，確保系統與資料的安全性與完整性。
- (二)、 使用單位電腦及網路系統伺服器，應具備病毒掃瞄軟體，並且定期掃瞄電腦病毒與更新病毒碼。
- (三)、 資料經由電子郵件傳送或接收時，應於電腦系統設置防火牆及防毒軟體，以防止

制定單位：秘書室				公布日期：104/12/24	
文件編號	SC 電教 001	版本	01	頁次	2/2
作業名稱	資訊安全之檢查作業				
主要負責單位	圖書與資訊處				
相關法令	教育體系資通安全管理規範				

駭客或電腦病毒之侵害。

- (四)、員工非經權責主管授權，禁止將本校相關資料經由電子郵件對外傳送。
- (五)、禁止教職員工及學生透過網路收發或下載與未經授權使用之軟體及其它不當軟體，以避免佔用本校網路資源及電腦病毒感染機會。
- (六)、重要軟體及檔案應加密處理，避免遭挪用或剽竊。
- (七)、使用單位之重要伺服器主機及網路系統資料，應定期備份重要檔案及資料。
- (八)、每年應配合內部稽核作業，針對本作業之各項控制重點項目進行檢核，若有未符合作業程序之事項，應填寫矯正與預防處理單，進行追蹤改善。

### 三、 控制重點：

- (一)、是否建立電腦網路系統的安全控管機制，以確保網路傳輸資料的安全性，防止未經授權的系統存取。
- (二)、使用單位電腦及網路系統伺服器，是否具備病毒掃描軟體。
- (三)、本校郵件伺服器是否設置防火牆及防毒軟體，以防止駭客或電腦病毒之侵害。
- (四)、是否教育教職員工及學生正確使用合法軟體之概念。
- (五)、圖書與資訊處人員是否定期檢視郵件伺服器上郵件收發情形，若有異常狀況是否陳報權責主管處理。
- (六)、機密檔案是否以予加密保護。
- (七)、使用單位之重要伺服器主機及網路系統資料，是否定期備份檔案及資料。

### 四、 使用表單：

- (一)、資訊安全管理制度內部稽核自評表(CHU-ISMS-D-017)。
- (二)、資訊安全管理制度內部稽核表(CHU-ISMS-D-047)。
- (三)、矯正與預防處理單(CHU-ISMS-D-048)。

### 五、 依據及相關文件：

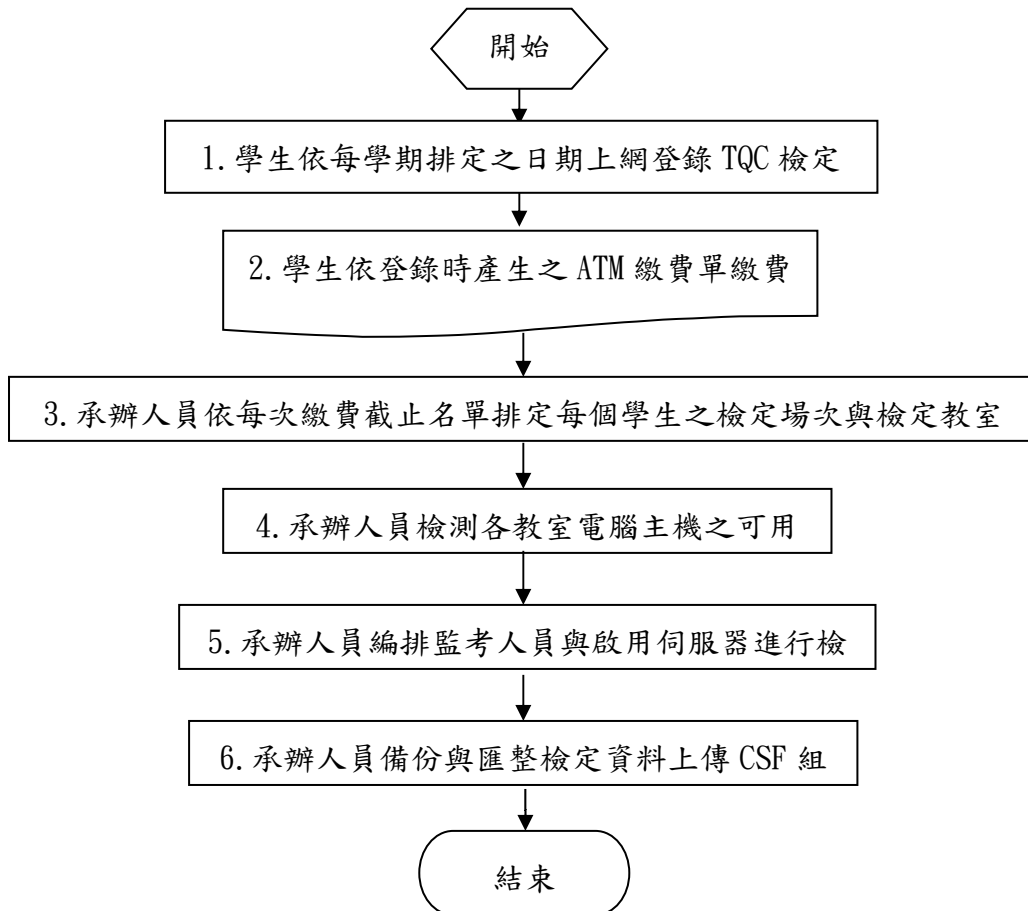
- (一)、中華大學圖書與資訊處校園網路管理辦法。
- (二)、資訊安全稽核作業程序書(CHU-ISMS-B-013)。
- (三)、矯正及預防管理程序書(CHU-ISMS-B-014)。
- (四)、資訊安全管理制度內部稽核計畫(CHU-ISMS-C-004)。
- (五)、資訊安全管理制度內部稽核報告(CHU-ISMS-C-005)。

### 流程圖：

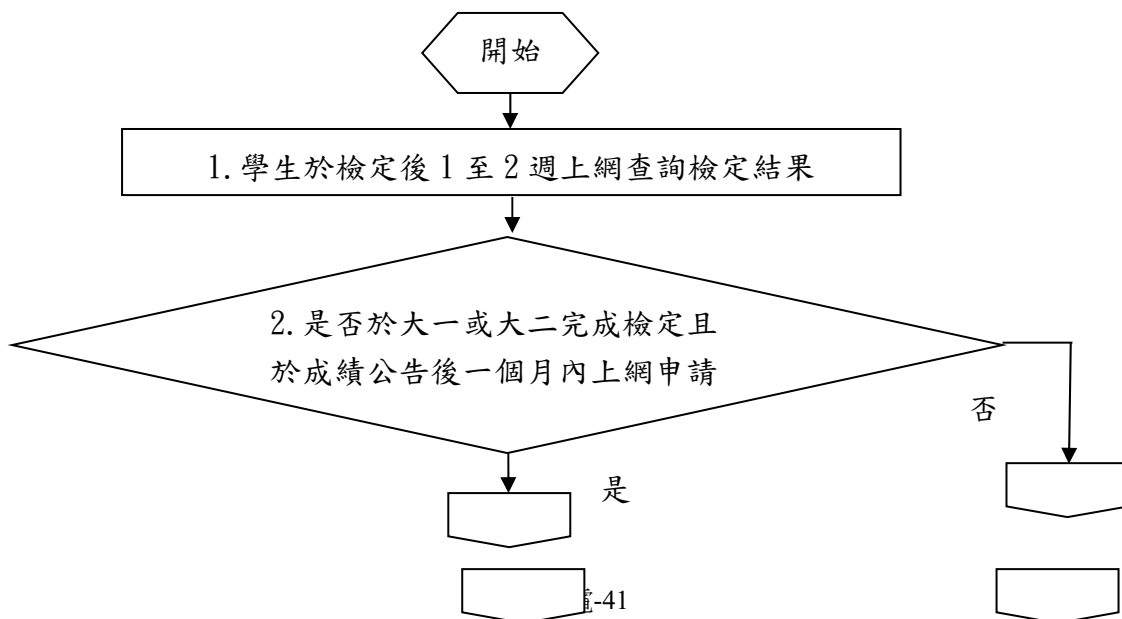


制定單位：秘書室				公布日期：104/12/24	
文件編號	SC 電教 002	版本	01	頁次	1/5
作業名稱	資訊應用能力檢定作業				
主要負責單位	圖書與資訊處				
相關法令	教育體系資通安全管理規範				

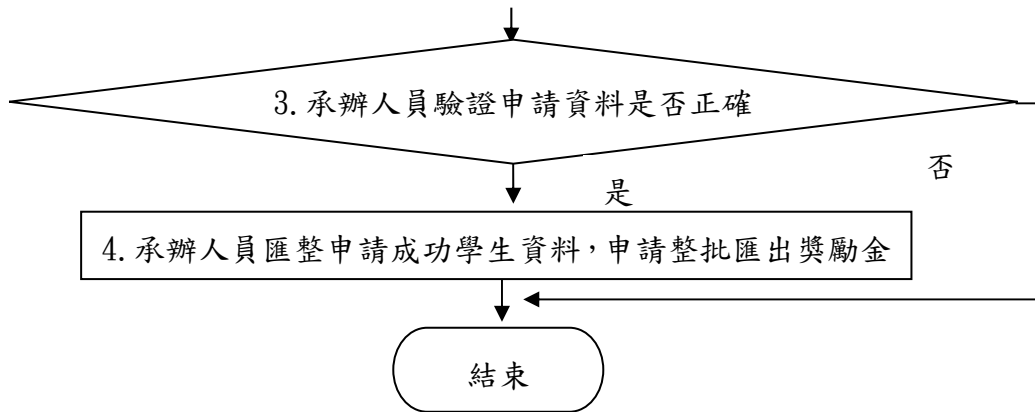
● 校內檢定作業



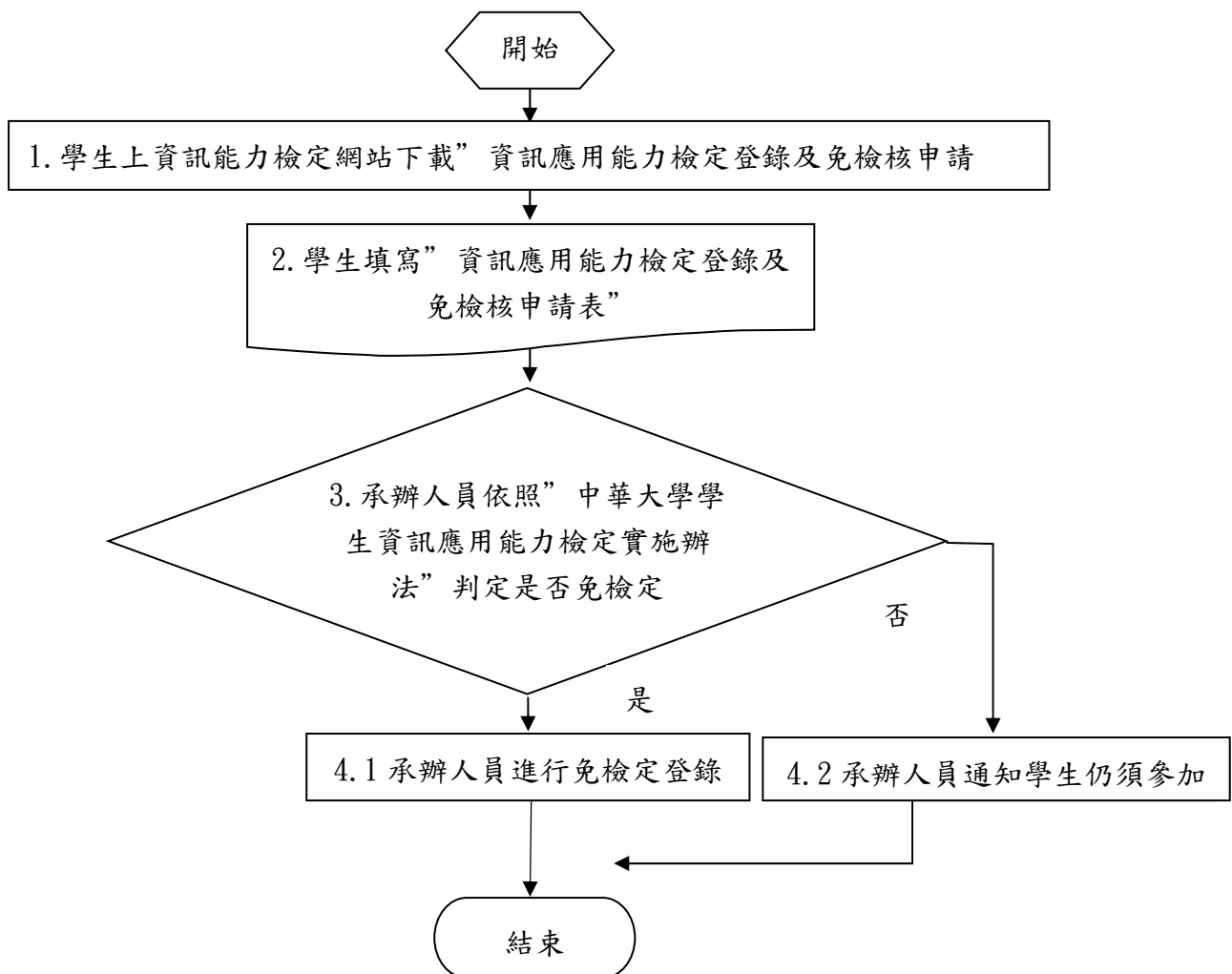
● 獎勵金申請作業



制定單位：秘書室			公布日期：104/12/24		
文件編號	SC 電教 002	版本	01	頁次	2/5
作業名稱	資訊應用能力檢定作業				
主要負責單位	圖書與資訊處				
相關法令	教育體系資通安全管理規範				

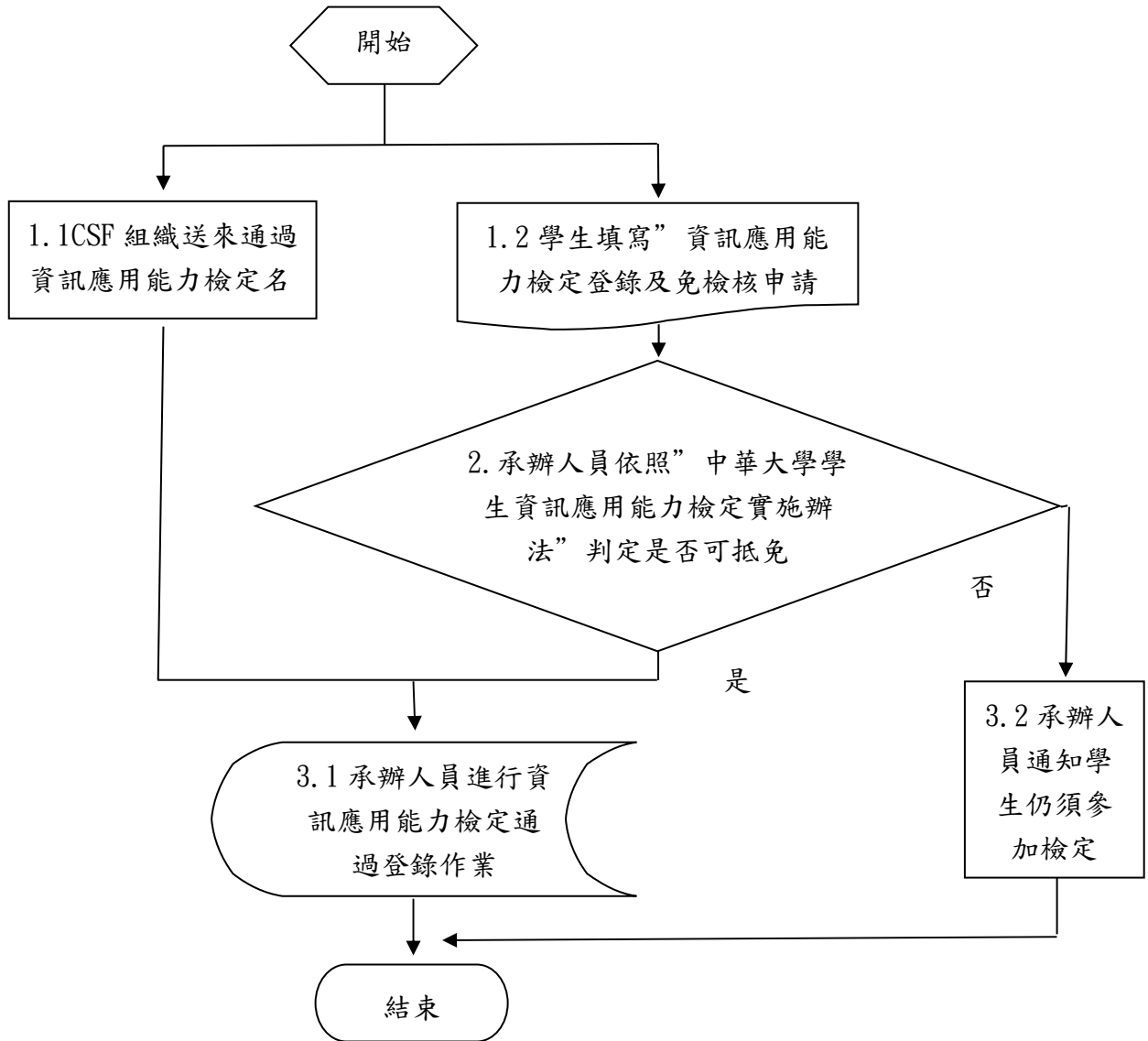


● 免檢核作業



制定單位：秘書室				公布日期：104/12/24	
文件編號	SC 電教 002	版本	01	頁次	3/5
作業名稱	資訊應用能力檢定作業				
主要負責單位	圖書與資訊處				
相關法令	教育體系資通安全管理規範				

通過檢定登錄作業



制定單位：秘書室				公布日期：104/12/24	
文件編號	SC 電教 002	版本	01	頁次	4/5
作業名稱	資訊應用能力檢定作業				
主要負責單位	圖書與資訊處				
相關法令	教育體系資通安全管理規範				

## 二、 作業程序：

### (一)、 學生資訊應用能力檢定制度：

1. 應訂定學生資訊應用能力檢定制度。
2. 學生的資訊應用能力應配合學校整體發展策略。
3. 學生資訊應用能力檢定制度應明確規範發展系統之標準流程。

### (二)、 校內檢定作業：

1. 圖書與資訊處依各學期行事曆排定數次的檢定考試，學生依每學期排定之日期上網登錄TQC檢定。
2. 學生依登錄時產生之ATM繳費單繳費。
3. 承辦人員依每次繳費截止名單排定每個學生之檢定場次與檢定教室。
4. 承辦人員備份與匯整檢定資料上傳CSF組織。

### (三)、 獎勵金申請作業：

1. 學生於檢定後1至2週上網查詢檢定結果。
2. 確認大一或大二完成檢定且於成績公告後一個月內上網申請獎勵金
3. 承辦人員驗證申請資料是否正確
4. 承辦人員匯整申請成功學生資料，申請整批匯出獎勵金

### (四)、 免檢核作業：

1. 學生上資訊能力檢定網站下載”資訊應用能力檢定登錄及免檢核申請表”。
2. 學生填寫”資訊應用能力檢定登錄及免檢核申請表”。
3. 承辦人員依照”中華大學學生資訊應用能力檢定實施辦法”判定是否免檢定。
4. 承辦人員進行免檢定登錄作業。

### (五)、 通過檢定登錄作業：

1. 學生填寫”資訊應用能力檢定登錄及免檢核申請表”或CSF組織送來通過資訊應用能力檢定名單。
2. 承辦人員依照”中華大學學生資訊應用能力檢定實施辦法”判定是否可抵免。
3. 承辦人員進行資訊應用能力檢定通過登錄作業或通知學生仍須參加檢定。

## 三、 控制重點：

### (一)、 學生資訊應用能力檢定制度：

1. 是否每年檢討學生資訊應用能力檢定制度。
2. 學生資訊應用能力檢定制度是否完整而明確。

### (二)、 校內檢定作業：

1. 參與檢定的學生是否已經繳費。
2. 檢定後的匯整與上傳程序是否完整。

制定單位：秘書室				公布日期：104/12/24	
文件編號	SC 電教 002	版本	01	頁次	5/5
作業名稱	資訊應用能力檢定作業				
主要負責單位	圖書與資訊處				
相關法令	教育體系資通安全管理規範				

(三)、獎勵金申請作業：

1. 確認是否在大一或大二完成檢定且於成績公告後一個月內上網申請獎勵金。
2. 申請學生的轉帳帳號是否正確。

(四)、免檢核作業：

1. 申請學生填寫的資料與文件格式是否完整且符合免檢核資格。
2. 確認登錄作業是否無誤。

(五)、通過檢定登錄作業：

1. 確認學生填寫”資訊應用能力檢定登錄及免檢核申請表”和CSF組織送來通過資訊應用能力檢定名單是否正確且符合”中華大學學生資訊應用能力檢定實施辦法”。
2. 確認登錄作業是否無誤。

四、使用表單：

- (一)、資訊應用能力檢定登錄及免檢核申請表

五、依據及相關文件：

- (一)、中華大學學生資訊應用能力檢定實施辦法
- (二)、中華大學學生資訊應用能力檢定TQC證照獎勵作業要點