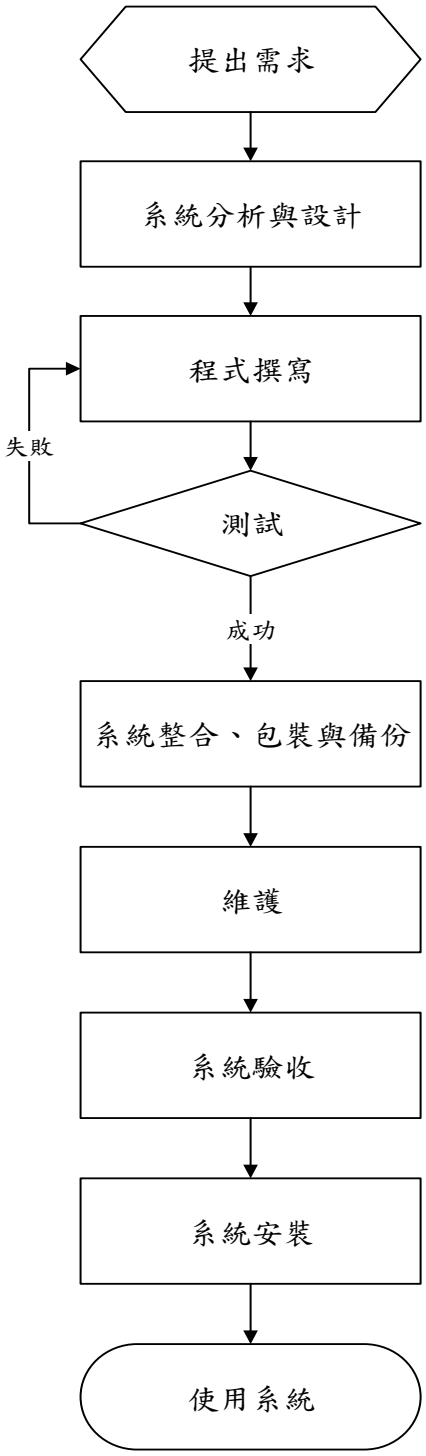
(八)資訊事項：

◎ 應用系統安全管理作業

1.流程圖：



2.作業程序與控制重點：

2.1 應用系統開發安全管理

2.1.1 需求評估

2.1.1.1 應用系統開發與異動時，業務需求單位應填寫「資中工作單」提出申請，經權責主管核可後始可實施，相關紀錄應留存備查。

2.1.1.2 應用系統新增或變更需求分析，除應考量可行性及成本效益外，亦應評估對現有環境之影響。

2.1.1.3 應用系統規劃時，專案承辦人員應考量系統需求做適當規劃，以確保足夠的電腦處理效能、儲存容量、電腦機房空間、電力及空調等。

2.1.1.4 委外應用系統發展需求作業程序，應依據「系統開發管理作業說明書」辦理。

2.1.1.5 安全需求

當開發新資訊系統或強化現有系統功能時，於系統規劃需求分析階段，應將以下安全需求要項納入系統功能：

2.1.1.5.1 使用者身分認證。

2.1.1.5.2 系統角色分工與存取權限控制。

2.1.1.5.3 系統輸入、輸出檢核處理。

2.1.1.5.4 機密與敏感資料保護。

2.1.1.5.5 系統作業紀錄與保存。

2.1.1.5.6 採用適當之加密保護機制。

2.1.1.5.7 其他需求考量之安全管控措施。

2.1.1.6 若使用雲端服務，宜考量使用雲端服務之資訊安全，例如：

2.1.1.6.1 使用雲端服務的範圍。

2.1.1.6.2 使用雲端服務的法令法規限制。

2.1.1.6.3 雲端服務的供應商和合約內容。

2.1.1.6.4 雲端服務的安全控制和監控方式。

2.1.1.6.5 雲端服務的資料保護和隱私資訊保護。

2.1.1.6.6 評估不再使用或移轉雲端服務時，退出雲端服務的執行方式。

2.1.2 分析與設計

2.1.2.1 系統分析設計文件應述明資料結構、應用系統架構、程式規格說明等，文件可以書面或電子檔案留存。

2.1.2.2 系統開發人員應視需要繪製系統流程圖或使用系統分析工具進行系統分析。如涉及重要資料之傳輸，應考量使用 SSL 加密金鑰，並依下列規定管理金鑰：

2.1.2.2.1 金鑰應有明確的啟動與止動日期，並於可用期間，保護其不被修改、遺失和破壞。

2.1.2.2.2 金鑰之使用與存取，應限於使用金鑰之系統管理者，不可由其他非系統管理者任意存取。

2.1.2.2.3 對於金鑰之使用、啟動、止動，皆應留存相關之紀錄。

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

2.1.2.3 委外需求應進行確認及分析，評估各項可行性方案，並依據「系統開發管理作業說明書」辦理。

2.1.3 程式原始碼編譯與審查

2.1.3.1 專案開發時宜制訂統一編譯之選項。

2.1.3.2 程式編譯過程中，視需要啟用編譯器檢查項目。

2.1.3.3 程式原始碼宜透過檢閱及審查方式進行安全檢查。

2.1.4 程式原始碼測試與維護

程式原始碼異動需經過單元測試及整體系統測試，避免錯誤發生，並將測試結果填寫測試報告。

2.1.5 應用系統測試

2.1.5.1 系統測試文件應包含測試計畫、測試報告，並由系統管理人員或委外廠商執行撰寫。

2.1.5.2 系統管理人員應監督系統功能錯誤之修正;業務需求單位協助對系統功能及資料之測試與勘誤。

2.1.5.3 系統測試計畫應包含功能測試及輸出入介面測試,視需要進行壓力或飽和測試等。

2.1.6 應用系統開發的程序，請參考「系統建置流程說明」。

2.2 維護安全管理

2.2.1 系統防駭測試

透過網路存取之應用系統應執行適當之防駭測試，考量測試下列項目以確認所開發之系統架構是否存在安全弱點。

2.2.1.1 資料庫伺服器檢測

測試內容應考量：Patch 更新、不必要之通訊協定、服務及通訊埠關閉、預設使用者資料庫移除、使用者與系統管理員帳號密碼安全強度、安全稽核功能設定及日誌檔(Log)備份等。

2.2.1.2 網站及應用伺服器檢測

測試內容應考量：跨網站指令碼(Cross Site Scripting，XSS)、Patch 更新考量、不必要之通訊協定、服務及通訊埠關閉、預設使用者資料庫移除、使用

者與系統管理員帳號密碼安全強度、安全稽核功能設定及日誌檔(Log)備份、每個網頁之安全控管等。

2.2.1.3 輸入欄位檢測

測試內容含：緩衝區溢位(Buffer Overflows)、輸入資料型態控管、資料隱碼(SQL Injection)等功能測試。

2.2.1.4 遠端存取功能檢測

測試內容含：遠端存取功能控管等。

2.2.2 系統輸入檢查與錯誤處理

2.2.2.1 系統應具備輸入、輸出錯誤檢查機制。

2.2.2.2 應考量使用者輸入資料之檢查方式，以降低程式或軟體面臨的威脅。

2.2.2.3 應考量應用程式於發生錯誤時提供相關錯誤資訊之方式。

2.2.2.4 例外狀況管理應考量擷取和回傳訊息、設計及傳送例外狀況資訊。

2.2.2.5 所有應用程式都應考量實作例外狀況處理機制，以擷取錯誤資訊。

2.2.3 系統身份驗證

2.2.3.1 應考量規範檢驗系統登入身份識別與密碼功能機制，以識別使用者身份，並提供授權、稽核等功能。

2.2.3.2 若無法使用作業平台提供的驗證機制，應考量在應用程式中使用自訂驗證機制。

2.2.3.3 應用系統密碼傳送應考量加密措施，以避免遭竊取。

2.2.4 系統權限管理

2.2.4.1 應考量規範滿足使用者業務需求之權限授予方式及最小權限。

2.2.4.2 系統應依據作業需求顯示適當資訊予以使用者。

2.2.4.3 未經授權者不得任意修改程式原始碼。

2.2.5 系統資料傳輸與流量管理

2.2.5.1 限制內部使用之應用系統，應考量避免對外提供資料傳輸。

2.2.5.2 依性質及需求，如線上交易、線上金流等，應考量採取加密傳輸，以確保資料在網路傳輸過程中的安全性。

2.2.5.3 對於網頁服務流量負載過重之系統，應考量採取負載平衡機制或限制頻寬。

2.2.6 系統資料庫存取

2.2.6.1 應用系統應考量有專屬資料庫，並規範防止使用者直接存取資料庫之設計。

2.2.6.2 應用程式連接後端資料庫，應考量經由可限制存取之網路設備連接統一控管，避免資料庫遭受入侵。

2.2.7 應用系統維護

2.2.7.1 本處自行維護之應用系統，應由業務需求單位提出維護申請，經權責單位主管核可後，由系統管理人員評估並處理，系統管理人員除需填寫處理結果外，並應妥為保存申請單以留下維護記錄。

2.2.7.2 委外廠商維護管理應依據「系統開發管理作業說明書」辦理。

2.2.7.3 應用系統主機維護

應用系統伺服器維護管理，應依據「主機與伺服器安全管理作業說明書」之維護辦理。

2.2.7.4 應用系統測試維護

2.2.7.4.1 測試環境所使用之設備環境應予獨立，不應與提供服務之設備環境共用。

2.2.7.4.2 提供委外廠商測試之資料，應將機敏性之資料內容轉換為虛擬資料；具機敏性之測試資料，應僅由系統管理人員進行存取。

2.2.7.4.3 當資料庫管理系統建置後，應立即更改所有管理權限之使用者密碼，防止非法連接資料庫內之資料；另資料庫管理系統應評估啟動稽核功能、保存資料庫管理系統特殊權限之異動記錄、使用者帳號新增、刪除等異動記錄、物件之建立、修改、刪除等紀錄至少保留 3 個月。

2.3 資料安全管理

2.3.1 新系統於規劃建置之初，即應評估所處理資料之重要性，並依據評估結果採購適當之系統軟、硬體或利用適當的資料儲存技術，如磁碟陣列、網路儲存設備(NAS)等進行資料之存放，以滿足資訊安全需求；儲存空間規劃應考量未來三年內資料量之成長率，避免發生儲存空間不足之狀況。

2.3.2 上線之應用系統除按時進行備份外，另應依其特性與需求不定時進行適當之備份；備份規劃由各應用系統管理人員依據「備份管理作業說明書」之備份作業程序辦理。

2.3.3 系統委外廠商依據系統可忍受中斷時間，訂定維護服務水準(SLA)。

2.3.4 備份資料至少每年執行資料回復測試，以確認備份資料之可用性，備份資料應依各系統資料安全要求異地存放，以強化資料安全性。

2.4 應用系統上線及異動管理

2.4.1 新系統上線或系統重大改版前，系統管理人員應進行系統功能測試、評估上線之影響，確認測試結果無誤，經權責主管複核後始得上線提供服務。

2.4.2 系統上線前，系統管理人員應對既有資料進行完整備份，同時應事先擬定因應措施及具體處置步驟。

2.4.3 上線過程遇問題，若無法排除，應立即進行回復作業，並進行原因分析與重新評估上線程序，於修正後應重新提出上線申請。

2.4.4 系統管理人員應於預定進行系統上線日前 3 個工作天，填妥系統上線流程表，

若為緊急上線可於事後 3 個工作天內補填申請單。

2.4.5 應用系統如需執行上線作業，系統管理人員應公告週知，以便相關人員配合。

2.4.6 系統完成上線作業後，應更新系統文件；舊版之系統文件、相關申請及異動紀錄應歸檔予以妥善保管，維護廠商須提供維護紀錄以作為佐證資料。

2.4.7 程式原始碼存取控管應依據「存取控制程序書」程式原始碼之存取控制辦理。

2.4.8 委外廠商執行系統上線及異動應依據「系統開發管理作業說明書」之上線階段辦理。

2.5 應用系統帳號管理

2.5.1 各應用系統管理員帳號應由系統管理人員持有，當委外廠商有使用應用系統管理員帳號之需求時，應由各系統管理人員協同該委外廠商進行登入。

2.5.2 應用系統帳號異動，應經由申請核准後，交付權責單位進行帳號異動處理。

3. 使用表單：

3.1 工作單系統。

3.2 系統功能表。

3.3 資料庫定義表。

3.4 單元測試表。

3.5 系統整合與測試紀錄表。

4. 依據及相關文件：

4.1 系統開發管理作業說明書。

4.2 存取控制程序書。

4.3 主機與伺服器安全管理作業說明書。

4.4 備份管理作業說明書。

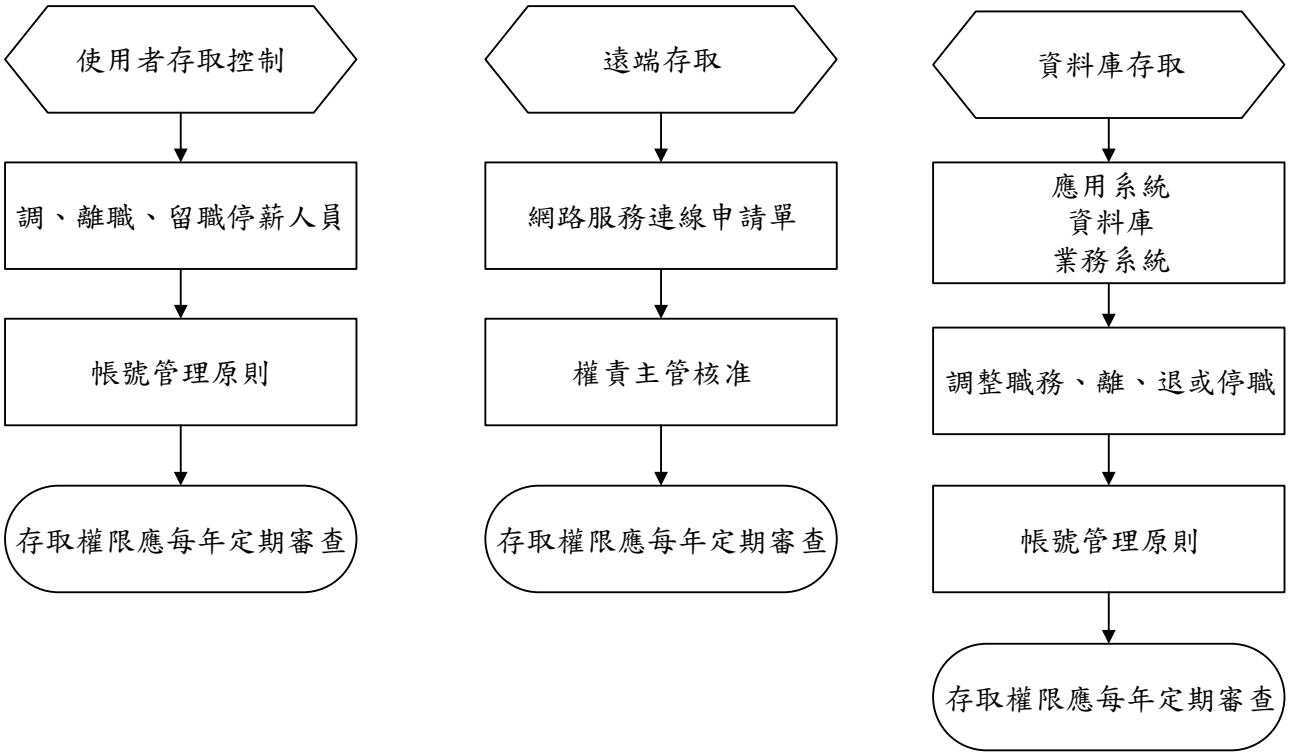
4.5 工作單系統。

4.6 系統建置文件。

4.7 系統建置流程說明。

◎ 存取控制作業

1. 流程圖：


使用者存取控制
調、離職、留職停薪人員
帳號管理原則
存取權限應每年定期審查
遠端存取
網路服務連線申請單
權責主管核准
存取權限應每年定期審查
資料庫存取
應用系統
資料庫
業務系統
調整職務、離、退或停職
帳號管理原則
存取權限應每年定期審查

2.作業程序與控制重點：

2.1 職務權責區分(Segregation of duties)與存取權限控管

2.1.1 人員的職務須考量適當的權責區隔，基於業務上之需要，各項工作應訂定工作職務代理人，盡可能符合權責區隔之原則。

2.1.2 各作業系統、應用系統、資料庫及網路設備之管理人員應對其所管理之標的制定存取角色。

2.1.3 使用者權限之申請宜以加入各種角色為原則，避免對個別使用者或帳號進行授權，若系統無法以角色給予權限時，則應另列清單執行帳號、權限控管。

2.2 存取控制政策

2.2.1 資訊資產之存取應與本身業務相關之範圍為主，任何人未經授權不得存取業務範圍外之資訊資產。

2.2.2 若因業務需要開放帳號予他人，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敏性，授與適當之存取權限及有效日期。

2.2.3 權責主管應審慎評估系統管理最高權限及作業控制特定人員之授權。

2.2.4 因需處理系統當機或異常狀況時，應視需求授予適當存取權限，並避免共用帳號。

2.2.5 可攜式電腦設備及儲存媒體，如筆記型電腦、隨身碟、外接式硬碟、光碟、磁帶等，應採取適當之控管措施，以防止未經授權資料、系統、網路之存取或病毒傳播。

2.2.6 資料、資訊之存取，必須符合「個人資料保護法」及「著作權法」等相關法令、法規之規定，或契約對資料保護及資料存取使用控管之規定。

2.2.7 公用程式路徑或公(共)用目錄之存取權限應適當控管，防止非授權使用者存取。

2.2.8 針對無人看管之資訊資產設備，應有適當控管程序，以防未經授權之存取或濫用。公共使用之影印機、印表機、傳真機或多功能事務機應定期由單位派人檢視有無機敏資料。

2.2.9 伺服器、個人電腦及可攜式電腦應設定螢幕保護程式，並設定密碼保護或採取 Ctrl+Alt+Del 登出方式進行鎖定；自行啟動螢幕保護程式之時間設定應不超過 10 分鐘。

2.2.10 應確保個人可識別資訊在傳輸、處理、儲存時能夠依風險程度被適當地遮蔽（可使用方式如：資料遮罩、匿名化、假名化、加密、變更數字或日期、置換，或雜湊等），以確保資訊不會被未經授權的人員所取得。

2.3 帳號與密碼管理

2.3.1 使用者帳號申請

2.3.1.1 本校根據使用者身份的不同，提供一組不同功能的帳號密碼，帳號申請依據資訊處首頁，資訊服務中之一般服務的個人帳號說明辦理。

2.3.1.2 應用系統使用者帳號依人事現職辦理，如有特殊需求，由使用者透過資中工作單系統進行申請。

2.3.2 管理者帳號管理

2.3.2.1 作業系統或網路設備管理人員應避免共用管理者帳號，重要系統管理者帳號與密碼之文件，應存放並上鎖於安全處所。

2.3.2.2 特殊權限之使用者必須與一般權限之使用者區分管理；針對特殊權限帳號，應妥善管理。

2.3.2.3 特殊權限之授權管理，必須依執行業務系統別之需求，如作業系統、資料庫管理系統、網路服務系統、監控管理系統等賦予系統存取特殊權限之授權，且以執行業務及職務所必要的最低資源存取權限為原則。

2.3.2.4 新購置之資訊設備或系統，安裝完成後應刪除或關閉不必要之帳號。

2.3.4 密碼管理

2.3.4.1 首次登入資訊設備或系統時，應立即變更密碼設定，並妥善保管帳號與維持密碼之機密性，保存帳號密碼之檔案應以加密方式處理。

2.3.4.2 應避免將帳號密碼張貼或放置於主機伺服器、個人電腦旁、螢幕或其他場所。

2.3.4.3 除特殊需求外，應避免使用者共用帳號密碼。

2.3.4.4 使用者懷疑密碼可能遭盜用或破解時，應立即變更密碼。

2.3.4.5 使用者存取系統時應避免使用記錄密碼之功能，導致開機時自動登入系統。

2.3.4.6 使用者密碼需英數字混合且不得與帳號名稱相同，使用者密碼長度至少 6 碼，重要系統主機管理者密碼長度至少 8 碼，密碼不得與前次設定相同，且應符合密碼設置原則。

2.3.4.7 帳號密碼至少 180 天更換密碼一次，並避免重複使用相同的密碼。

2.3.4.8 密碼設置原則

應儘量避免使用易猜測或公開資訊為設定，例如：

2.3.4.8.1 個人姓名、出生年月日、身分證字號

2.3.4.8.2 機關、單位名稱或其他相關事項

2.3.4.8.3 電腦主機名稱、作業系統名稱

2.3.4.8.4 電話號碼

2.3.4.8.5 空白

密碼設定必須符合複雜性需求：

2.3.4.8.6 不包含使用者的帳戶名稱全名中，超過兩個以上的連續字元

2.3.4.8.7 包含下列四種字元中的三種:

英文大寫字元 (A 到 Z)

英文小寫字元 (a 到 z)

10 進位數字 (0 到 9)

非英文字母字元 (例如:!、$、#、%)

2.3.4.9 使用者遺忘密碼時：

本校個人密碼一經設定後，即無法查詢，僅可重新設定密碼，因本組帳號密碼提供重要校務服務，若因遺忘須變更時，應依據本處之個人帳號說明辦理。

2.3.5 密碼封存原則

2.3.5.1 重要系統及設備帳號管理人員應建立彌封之密碼函，並賦予流水編號管控，作為當發生緊急事故時啟用之備份密碼。

2.3.5.2 單位權責主管應負責彙整收集並進行封存作業，再交付資訊安全官。

2.3.5.3 資訊安全官檢查封存後放置於安全地點。

2.3.5.4 資訊安全官與業務負責人雙方確認彌封之密碼函數目正確後，雙方簽收「密碼函簽收清單」，業務負責人並將前次彌封之密碼函簽收並銷毀。

2.4 使用者存取管理

2.4.1 對於職務異動如調、離職、留職停薪人員等，依本處帳號管理原則辦理，據以註銷或停用存取權限。

2.4.2 使用者申請及註銷應保留核准紀錄，存取權限應每年定期審查。

2.4.3 本處同仁需經由外部連線至本處使用資訊設備時，須填寫「網路服務連線申請單」，經本處核准後始得使用。

2.4.4 系統相關作業人員需經正式授權存取業務相關之資訊資產，其識別資料與帳號必須為唯一之識別碼，禁止借用他人之帳號或共用帳號。

2.4.5 應每年定期將主機伺服器及網路管理設備之帳號進行帳號權限清查，同時將查核結果陳權責主管審查。

2.4.6 主機伺服器及網路管理設備之帳號如有異動，請填寫「變更需求申請單」。

2.5 作業系統存取控制

2.5.1 重要系統有提供紀錄功能應予以啟動。

2.5.2 系統紀錄存取，應限定僅由系統管理人員或具讀取權限者存取。

2.5.3 應避免於終端機登入程序中以明碼方式顯示密碼相關資訊。

2.5.4 使用者帳號應避免顯示任何足以辨識使用者特別權限之訊息，如顯示其為管理者或監督者。

2.5.5 系統應有設定連續密碼登入錯誤次數限制，要有錯誤紀錄，必要時得停止該帳號之登入或鎖定該帳號或 IP。

2.6 應用系統之存取控制

2.6.1 資訊存取之限制

2.6.1.1 應用系統資訊之使用，僅限業務相關之授權使用者，並應適當控制，如新增、刪除、修改或執行等。

2.6.1.2 應用系統之機敏資訊，應加強權限控管措施。

2.6.1.3 使用者登入具機敏性之應用系統後，若超過 1 小時無任何動作時，系統須設定將其帳號鎖定或登出。

2.6.1.4 系統若需使用憑證控管機制，應透過資中工作單提出申請，並留存紀錄備查。

2.6.2 程式原始碼之存取控制

2.6.2.1 應用程式原始碼，應依單位之特性集中存放，並依不同系統指定專人管理程式之增修作業。

2.6.2.2 開發中之程式原始碼，應與線上程式碼分開放置與控管。

2.6.2.3 程式原始碼應以版本控管之方式妥善保管，以備新版失敗之回復使用。

2.6.2.4 應用程式之異動需經適當控管，相關管理規範應依據「應用系統安全管理程序書」辦理。

2.7 網路存取控制

2.7.1 網路系統應依其性質之不同，分開成不同的領域，各領域應以特定安全設施，如防火牆及網路閘門等應加以保護，以降低可能之安全風險。

2.7.2 網路管理人員應定期檢視網路存取之紀錄，並留存查核紀錄。

2.7.3 對於開放提供外部客戶或廠商存取之服務，必須限制使用者之網路功能以確保網路安全。

2.7.4 網路路由之規劃必須確保任何網路連線或資訊傳輸符合網路存取之安全需求。

2.7.5 申請使用網路時，應依據「網路管理作業說明書」提出申請，由網路管理人員配予適當之 IP 位址。

2.8 遠端存取之限制

2.8.1 非經授權或允許，禁止執行遠端存取作業。

2.8.2 資訊設備連線之需求如為外部連線申請使用，須依據「網路管理作業說明書」填寫「網路服務連線申請單」，經權責主管核准後，始得開放。

2.8.3 非在申請連線之有效期間內，應確實關閉連線功能。

2.8.4 連線存取機敏資料時應限定連線來源及使用範圍。

2.8.5 未簽訂契約之廠商不得開放連線申請，除有特殊需求，應提出申請。

2.8.6 僅提供申請核可之網路服務項目、通訊協定與連線時間，所有行為不得與原有之網路安全相關限制、規定相抵觸。

2.9 資料庫存取控制

2.9.1 資料庫帳號管理

2.9.1.1 資料庫存取須由作業系統或資料庫執行身分識別機制。

2.9.1.2 資料庫系統存取帳號除特殊需求外，應依功能區分為應用系統、資料庫管理及業務系統執行之帳號，並需能鑑別個別存取者為原則。

2.9.1.3 資料庫系統存取權限之配賦，應以執行業務及職務所必需者為限，當使用者調整職務、離、退或停職時，依據本處帳號控管原則實施。

2.9.1.4 資料庫系統帳號密碼須英數字混合且不得與帳號名稱相同,密碼長度至少為 6 碼,管理者密碼長度至少為 8 碼。使用者密碼應嚴禁轉知他人，若已為他人知悉者，應報告權責主管，並立即更新密碼。

2.9.1.5 資料庫最高權限帳號之存取授權應僅限於資料庫管理人員或職務代理人。

2.9.1.6 資料庫預設帳號應變更密碼或是關閉使用。

2.9.2 資料庫異動與測試

2.9.2.1 應用系統之測試及正式作業所需資料庫管理系統，應分別在不同主機下執行，並避免資料遭意外竄改或不當使用。

2.9.2.2 提供委外廠商測試之資料，應將機敏性之資料內容轉換為虛擬資料；具機敏性之測試資料，應僅由系統管理人員進行存取。

2.9.2.3 正式資料庫系統變更作業前，如資料庫系統更新、安裝修補程式等，必須先經過測試，並評估對現行系統之影響後始得變更。

2.9.2.4 資料庫異動應填寫資中工作單，經權責主管審核後交資料庫管理人員執行，作業完成後之申請單應歸檔存查，若為維護廠商須附維護紀錄。

2.9.3 資料庫公用程式路徑之存取權限應適當控管，禁止一般使用者存取。

2.9.4 在不影響資料庫系統效能原則下,資料庫之存取紀錄應留存查核,且至少保存 3 個月。

3.使用表單：

3.1 變更需求申請單。

3.2 網路服務連線申請單。

3.3 工作單系統。

3.4 密碼函簽收清單。

3.5 主機暨設備帳號清單。

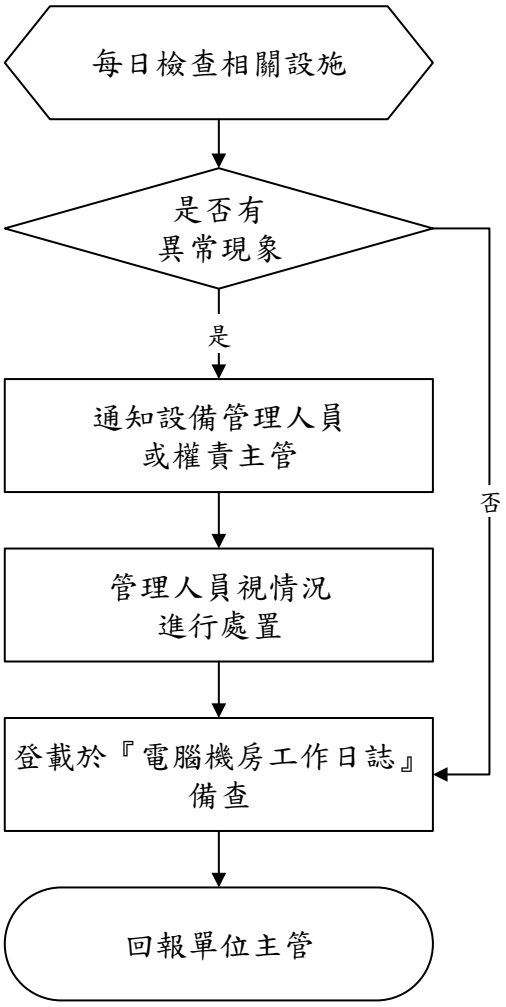
4.依據及相關文件：

4.1 網路管理作業說明書。

4.2 存取控制程序書。

◎ 電腦機房管理作業

1.流程圖：



2.作業程序與控制重點：

2.1 電腦機房門禁管制

2.1.1 為確保設備及資料之安全，應採有身分識別功能之安全門，做為必要之安全控管；門禁卡之使用須依據本處申請程序辦理，經權責主管核准後，由門禁系統管理人員設定門禁權限，權責主管需每半年審核門禁之權限。

2.1.2 除本處授權之人員外，其他因業務需要進入電腦機房，如廠商、訪客等，應由本處業務負責人、電腦機房維運人員或代理人陪同進入，並記錄於「電腦機房進出登記簿」，電腦機房維運人員應每月陳送權責主管核閱。

2.1.3 電腦機房出入口及機房內應設 24 小時動(靜)態監控,錄影紀錄應至少保留三個月。

2.1.4 門禁系統之進出紀錄日誌檔應定期備份;紀錄存放於安全區域並保存一年備查。

2.1.5 人員離職或異動後，應於離職或異動當日更新權限或繳回門禁卡。

2.2 資訊設備/物品進出與使用管理

2.2.1 需攜入電腦機房內執行測試、安裝、修理或更換等之資訊設備（含可攜式資訊設備／媒體）皆應遵守下列規定：

2.2.1.1 若攜入電腦主機房之設備需與本處網路或資訊設備界接時,須由廠商、業務負責人或電腦機房維運人員負責掃毒，確認安全並填寫於「電腦機房進出登記簿」之媒體使用說明原因後方得進入；若資訊設備需攜出機房維護時須填寫「設備進出紀錄表」，經權責主管或代理人核可後，始可攜出。

2.2.1.2 廠商借測設備進入電腦機房，非經授權不得與本處網路連線，若需使用本處網路，應依據「網路管理作業說明書」辦理。

2.3 機房環境安全管理

2.3.1 電腦機房內應保持整齊清潔，並嚴禁吸菸、飲食及堆置易燃物品，如紙箱、保麗龍及未經核准之電器用品等。

2.3.2 電腦機房溫濕度採固定區間控制，溫度應維持在 17℃至 30℃，相對溼度維持在 30%至 70%。

2.3.3 電腦機房應設置專用空調設備以維持資訊設備之正常運作。

2.3.4 空調設備應 24 小時運轉並設置備援設備，同時注意電力、供水、排水及保養問題。

2.3.5 電腦機房應設置安全出入口及停電緊急照明設備，並有明顯逃生路線標示。

2.3.6 電腦機房應設置專用之消防器材或系統，如熱感應、煙霧偵測、火災警報、滅火設備及火災逃生設備等，同時應符合消防法規並定期檢測與紀錄。

2.3.7 應具備保護線路及相關設備之機制。電力、網路及通信設備應予以保護，以防止遭有心人士截取或破壞。

2.3.8 電腦機房應定期做好電源線路及插座之安全檢查，以確保電力安全。

2.3.9 電腦機房應設置不斷電系統（UPS）或發電機，以保障正常維運，並定期檢測與紀錄。

2.3.10 電腦機房高架地板應考量重量承載能力、耐震功能，並部署地網。

2.3.11 電腦機房內實體環境應考量耐震、防火、防水、防盜及可監控之設計。

2.3.12 電腦機房入口應設置物品卸載區，於電腦機房大型設備報廢或新購時，搬運卸載相關物品使用。

2.3.13 電腦機房設備、主機伺服器、線路等應有適當標示，且排列放置定位，便於日常管理與突發狀況時能迅速處理。

2.3.14 電腦機房維運人員應施予適當之安全設備，如消防器材、火災逃生設備等使用訓練。

2.4 機房維護管理

2.4.1 電腦機房維運人員應每日檢查相關設施是否有異常現象，如發生異常，應即時處理並通知設備管理人員或權責主管、相關單位或廠商；人員執行檢查時，需將檢查結果記載於「電腦機房工作日誌」備查。

2.4.2 系統管理人員於電腦機房內完成維運作業後，應依據其需求將處理紀錄記載於「維護紀錄表」，外部廠商則應填寫「維護紀錄表」或自行提供維護紀錄，以備查核。

2.4.3 電腦機房維運設備，如消防、電力、空調設備等或重要資訊設備，如主機伺服器及網路設備等應與合格專業廠商簽訂維護合約，定期實施保養與妥善維護，以確保設備之完整與安全。

2.4.4 資訊設備專用電源插座，不得使用於資訊設備以外之裝置，以免耗用電源，發生跳電當機情形，影響正常作業。

2.4.5 UPS 應定期檢視蓄電及負載能力，並有相關維護紀錄。

2.4.6 電腦機房主控台（Console）管理

本處人員使用主控台（Console）進行操作時需使用帳號及密碼。委外人員若需使用主控台（Console）時應由本處人員協助登入，並應避免委外人員獲知使用帳號及密碼。

2.5 災害防制與應變處理

各式人為或天然災害如設備電源中斷、設備故障、水電空調故障、火災、水災、地震、颱風等緊急狀況，依據「營運持續管理程序書」辦理。

3.使用表單：

3.1 電腦機房進出登記簿。

3.2 設備進出紀錄表。

3.3 電腦機房工作日誌。

3.4 維護紀錄表。

4.依據及相關文件：

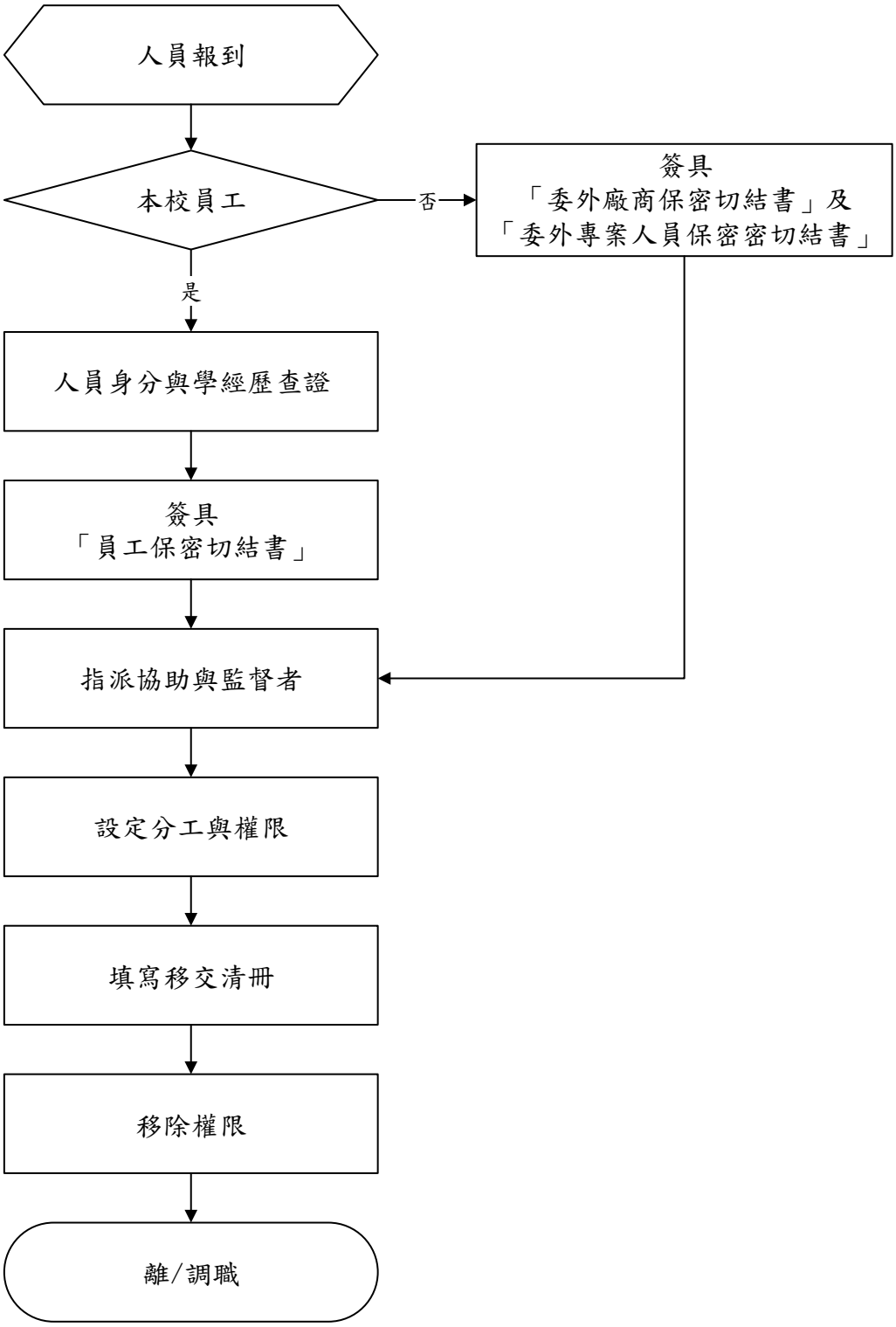
4.1 資訊安全事件管理程序書。

4.2 網路管理作業說明書。

4.3 營運持續管理程序書。

◎ 人力資源安全管理作業

1.流程圖：



2.作業程序與控制重點：

2.1 人員安全管理

2.1.1 員工報到時，除依據中國文化大學人事相關規章制度辦理外，並應簽具本處「員工保密切結書」，使其充分瞭解資訊安全相關作業規範及其重要性。

2.1.2 晉用人員時，人事室應針對學歷、經歷、身分證明文件等進行查證。

2.1.3 本處員工與委外服務廠商人員皆應遵守本處資訊安全政策及資訊安全管理規定。人員於在職及離、退職後，均不得洩漏所知悉之機敏業務資訊，或為不當之使用，否則得視其情節輕重予以處分或追究其民、刑事責任。

2.1.4 資訊業務之管理、維護、設計及操作人員權責分工應明確，應建立人力備援機制，並得視需要實施人員輪調。

2.1.5 重要資訊、限閱等級以上資訊或足以影響本處業務永續運作管理的資訊，應避免僅由一人知悉。若由單獨一人運作管理時，應有確實的主管監督審查機制。

2.1.6 本處新進用或經驗不足的人員，於授權存取資訊資產時，須提供協助與監督。

2.1.7 本處員工離職時，應依據本校離職流程辦理，並辦妥移交手續，將名下保管財產清單中所列資訊資產完成移交，並依相關管理作業規範辦理，移除相關資源之存取權限。

2.1.8 本處員工、接觸本處業務資料之外部人員、委外服務廠商、教師、學生等使用違反智慧財產權相關的軟體、資訊或文件，應負相關的法律責任。

2.1.9 委外服務廠商之管理規範，請參考「資訊作業委外管理程序書」之相關規定。

2.2 教育訓練

2.2.1 為提升本處人員之資訊安全意識與專業知識，權責單位每年應舉辦相關資安教育訓練課程，或派員接受外單位辦理之專業資安課程或研討活動，以提升人員資訊安全知識及警覺意識，降低人為錯誤或故意誤用資訊之風險。

2.2.2 應針對組織內不同人員角色及職能，規劃不同的訓練重點課程。

2.2.3 為確保教育訓練執行之成效，可採行隨堂抽問、案例討論、習題演練或隨堂測驗等方式進行成效評估。

2.2.4 本處新進人員正式執行業務前，應辦理職前教育訓練，並留存相關紀錄備查。

2.3 本處員工接受外部資訊安全訓練結束後，可提供結業證明或心得報告或教育訓練等相關資料，作為教育訓練紀錄備查。

2.3.1 本處員工受訓完成後，應視業務需要，於本處辦理相關課程，以充實其他人員資訊安全知識，促其遵守資訊安全規定。

2.3.2 對本處員工進行之資訊安全教育訓練，亦適用於委外服務廠商人員。

2.3.3 承辦本處之資訊安全教育訓練之權責單位，應備妥教育訓練簽到紀錄留存備查。

3.使用表單：

3.1 教育訓練需求表。

3.2 受訓結果報告表。

3.3 人員能力認知與訓練總表。

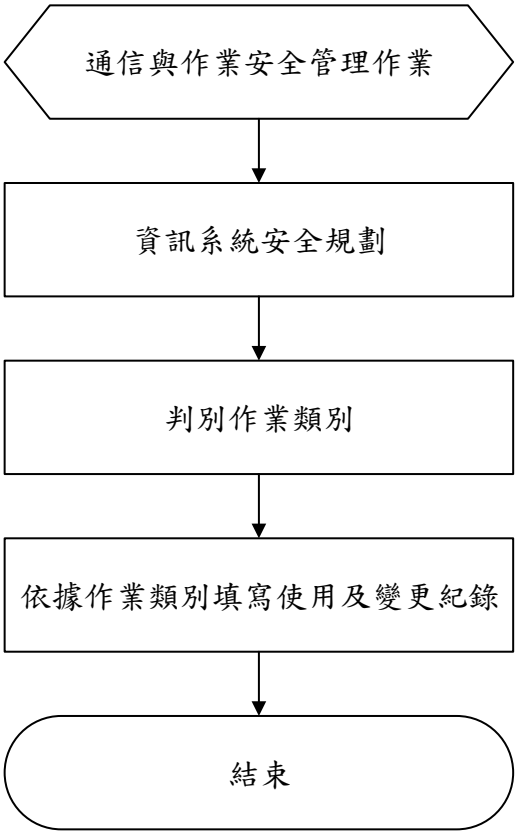
4.依據及相關文件：

4.1 資訊作業委外管理程序書。

4.2 員工保密切結書。

◎ 通信與作業安全管理作業

1. 流程圖：



2.作業程序與控制重點：

2.1 資訊系統安全規劃作業

2.1.1 應建立資訊系統之安全控管機制，以確保資料安全，保護系統及網路作業，防止未經授權之存取。

2.1.2 資訊系統管理職務與責任應加以區隔；足以影響業務永續運作的資訊或服務，應避免只由一人知悉。若因人力資源限制，無法加以區隔，應有確實的監督審查機制。

2.1.3 主機、伺服器及網路設備應指定管理人員，並負責該項資訊設備安全管理與正常運作。

2.1.4 應分隔開發、測試及運作之環境,以降低對運作之系統未經授權存取或變更的風險。

2.1.5 系統及設備建置前，業務單位應對系統需求做適當規劃，以確保系統效能及儲存容量。

2.1.6 系統設備與軟體之建置應依照「資訊作業委外管理程序書」、「應用系統安全管理程序書」及「系統開發管理作業說明書」辦理。

2.1.7 系統及設備建置前，宜規劃資料洩露預防的實作。

2.1.9.1 偵測和防止個人或系統未經授權的揭露和存取。

2.1.9.2 識別和分級資訊。

2.1.9.3 遵守資訊安全政策、要求事項和控制措施。

2.1.9.4 技術漏洞管理。

2.1.9.5 監控網路活動。

2.1.9.6 網頁過濾。

2.1.9.7 安全編碼。

2.2 變更管理

2.2.1 系統管理人員應評估變更影響與處理時間，如有必要，應邀請相關人員召開會議討論，使變更影響降至最低。

2.2.2 變更之影響範圍，若包含其他單位，應同時公告相關單位，並於變更執行前，協調實施時間，以利變更程序之執行。

2.2.3 變更執行過程若有相關紀錄，如網路、作業系統設定或參數調整，應確實遵循備份原則保存，以供後續管理之參考。

2.2.4 各項資訊系統或設備之變更等作業，應依照「應用系統安全管理程序書」、「主機與伺服器安全管理作業說明書」、「網路管理作業說明書」及「防火牆管理作業說明書」等辦理。

2.2.5 新增設備及網路變動，應即時修改網路拓樸圖及設備資料。

2.2.6 宜透過自動化、或人工定期抽查等方式監控當前組態是否有未經授權的異動，例如：

2.2.6.1 安全組態（如：特權帳號、禁用不安全的身份、變更預設密碼等與安全有關預設參數等）。

2.2.6.2 監控組態（如：定期審查存取活動、手動/自動矯正誤差等）。

2.2.6.3 管理組態（如：上次組態變更日期、版本等）。

2.3 惡意軟體之防範

2.3.1 禁止使用、下載及安裝未經授權之軟體，必要時應以使用者角色職責進行適當權限控管。

2.3.1.1 本處各組可依據業務執行需求，列舉適當軟體供同仁參考使用，如:軟體類型(網路管理軟體、計算軟體、其他工具軟體)、軟體屬性(授權軟體、共享軟體、免費軟體)等。

2.3.2 Windows 平台伺服器與個人電腦皆須安裝防毒軟體，並定期更新病毒 資訊，以防止病毒攻擊及擴散，相關管理作業依據「電腦病毒管理作業說明書」辦理。

2.4 網路安全管理

2.4.1 網路使用者安全管理

2.4.1.1 需經授權並賦予相關存取權限後，始得使用網路資源。

2.4.1.2 已授權的使用者，僅能在授權範圍內存取網路資源。

2.4.1.3 應遵守網路安全規定，並確實瞭解其應負的責任，如有違反網路安全情節，依相關法規處理。

2.4.1.4 不得將自己的登入帳號與密碼交付他人使用。

2.4.1.5 禁止以任何方法竊取他人的登入帳號與密碼。

2.4.1.6 禁止以任何儀器設備或軟體工具竊聽網路上的通訊。

2.4.1.7 不得以任何手段蓄意干擾或妨害網路系統的正常運作。

2.4.1.8 網路使用權限申請應依據「網路管理作業說明書」辦理。

2.4.1.9 為防止濫用網路系統，禁止使用者下列行為：

2.4.1.9.1 散佈電腦病毒、干擾或破壞系統機能之程式。

2.4.1.9.2 擅自截取網路傳輸訊息。

2.4.1.9.3 將個人帳號借予他人使用。

2.4.1.9.4 窺視他人之資料文件或檔案。

2.4.1.9.5 以任何方式濫用網路資源，包括以電子郵件大量傳送廣告信、連鎖信或無用之信息，或以灌爆信箱、掠奪資源等方式，影響系統之正常運作。

2.4.1.9.6 利用無線網路資源從事非工作相關之活動或違法行為。

2.4.1.9.7 私自於辦公室架設無線網路基地台存取網路資源。

2.4.1.9.8 對於違反本規範或影響網路正常運作者，得暫停其使用權利，使用者若發現網路有安全之虞或任何疑問，應儘速通報網路管理人員進行處理。

2.4.2 網路服務安全管理

2.4.2.1 本處只開放必須的網路服務功能與通訊協定。如需異動，由相關人員進行安全評估，確定可行且無安全之顧慮，經由權責主管核可後方得開放。

2.4.2.2 應對所有必須開放的網路服務功能與通訊協定列表管制。

2.4.2.3 應依據「資訊安全事件管理程序書」通報網路安全事件。

2.4.2.4 為確保網路的服務持續暢通，本處與外界網路的連接，應有一個以上的替代路徑，並確保替代路徑受到安全管控。

2.4.2.5 網路連線時間限制

本處提供之 VPN 連線時間限制以不超過連續 5 小時為原則。

2.4.2.6 本處內電腦設備應透過本處提供之網路服務，連線至本處伺服器。

2.4.2.7 網路服務之運行，宜評估與考量可用性之需求，建置具高可用性之資訊設備架構(如：雲端架構、備援、HA、虛擬化、簽訂維護合約或 SLA、透過 BCP 演練等機制)，避免單點失效之風險，以確保網路服務之可用性。

2.4.2.8 網路管理人員應定期利用網路管理工具，偵測及分析網路流量，監視網路、應用系統之異常行為（如異常之服務輸入/輸出和存取、組態檔案更動、事件日誌之趨勢分析），並採取適切措施，以評估潛在資訊安全事件。

2.5 網路頻寬管理

2.5.1 應進行網路流量之監控，保障網路頻寬之正常使用。

2.5.2 禁止網路使用者將網路資源用於非法之私人用途。

2.5.3 網路系統管理人員如發現流量異常，應立即採取適當措施，並分析網路異常原因。若為使用者非法使用或是中毒，應依據「資訊安全事件管理程序書」之通報流程進行通報。

2.6 網路通訊設備管理

2.6.1 網路通訊設備之安裝、上線、測試或維護改善，其工作內容應有相關紀錄。

2.6.2 網路通訊設備安裝、維護前應進行安全與作業影響評估，與廠商或相關人員進行安裝前協調，以充分了解該項維護之影響層面與作業風險，必要時需請廠商到場協助，提供技術支援。

2.6.3 廠商進行網路設備安裝、維護工作時，人員必須全程陪同或以監視器與操作紀錄機制輔助監控。

2.6.4 廠商對本處之維護方式以到場服務為原則。但若有實際需要需做遠端連線測試時，必須經權責主管核准後方可實施。

2.6.5 網路通訊設備安裝應考慮裝置場地之安全性，儘可能設置於有門禁管制之地點，並考慮通風散熱問題。

2.6.6 為維持本處網路的持續正常運作，重要之網路通訊設備應有備援設計或備品。

2.6.7 重要之網路通訊設備應加裝不斷電系統(UPS)，以防止不正常的斷電狀況。

2.6.8 網路通訊設備應由專人負責定期維護檢查相關軟硬體，並紀錄維護狀況。

2.6.9 詳細網路通訊設備管理作業，依據「網路管理作業說明書」辦理。

2.7 佈線安全管理

2.7.1 網路線路佈設時，應注意電腦機房之電力線路架構，以避免產生線路間之干擾問題。

2.7.2 光纖或易遭受破壞之線路設施應妥善保護，以免因其他工程裝設而影響網路之運作。

2.7.3 線路得佈建於天花板高架或高架地板，以防止線路遭破壞或損毀。

2.7.4 線路配置需注意維護安全與方便，應避免糾結與裸露。

2.8 網路防毒安全管理

2.8.1 網路防毒安全管理，依據「電腦病毒管理作業說明書」辦理。

2.8.2 使用者如偵測到電腦病毒入侵或其他惡意軟體，應依據「資訊安全事件管理程序書」辦理。

2.9 防火牆安全管理

防火牆安全管理，依據「防火牆管理作業說明書」辦理。

2.10 網路入侵偵測/防禦安全管理

2.10.1 應於網路重要區段或是節點，佈署網路入侵偵測及防禦系統，進行入侵偵測與防禦。

2.10.2 網路管理人員應配合資訊安全政策及規定，隨時檢討及調整網路入侵偵測系統的設定，以反應最新的狀況。

2.10.3 如發現或疑似有被入侵網路系統情形，應依據「資訊安全事件管理程序書」辦理。

2.11 弱點掃描安全管理

弱點掃描安全管理，依據「弱點管理作業說明書」辦理。

2.12 紀錄與蒐證安全管理

2.12.1 內、外部人員進行網路維護作業，均應建立紀錄。

2.12.2 對入侵者的追查與防範，應使用紀錄或日誌執行反向追蹤，並進行防堵措施。

2.12.3 紀錄、日誌與蒐證安全管理作業，應依據「網路管理作業說明書」辦理。

2.12.4 應尊重網路隱私權，不得任意窺視使用者之個人資料或有其他侵犯隱私權之行為。但有下列情形之一者，不在此限：

2.12.4.1 為維護或檢查系統安全。

2.12.4.2 依合理之根據，懷疑有違反本處規定（利益）之情事，應通報單位主管後，陳報上層審議或處置。

2.12.4.3 配合司法單位合法之調查。

2.12.4.4 配合相關職權機關依職務需要之調查或使用。

2.12.4.5 配合本校之法令或法規。

2.13 無線網路使用之管理

2.13.1 無線網路基地台之使用應經適當控管。

2.13.2 無線網路設備之安裝設定應經核准。

2.13.3 無線網路設備之使用應取得授權，禁止於內部網路私自使用任何無線網路產品。

2.13.4 無線網路設備之使用應有適當管理機制，如授權使用之 IP 數量、連接埠、紀錄網卡位址（Mac address）等。

2.13.5 無線網路之資料傳輸應就安全與資訊風險之考量，增加適當之防護機制以避免資料外洩。

2.14 電子傳訊安全管理

2.14.1 機敏資料應避免以電子郵件、即時通訊、傳真機等方式傳送。

2.14.2 不得傳遞大量且非必要的資訊，避免網路壅塞及資源浪費。

2.14.3 電子郵件之傳送與接收，應審慎檢視郵件主旨、內容、附加檔案及地址後，方可傳送或開啟。

2.14.4 對來路不明之電子郵件，不宜隨意開啟，以免感染病毒或遭植入惡意程式，確保資訊資產之安全。

2.14.5 應建立電子郵件之安全管理機制，以降低電子郵件可能帶來之風險，相關管理作業應依據「電子郵件管理作業說明書」辦理。

2.15 對公眾服務之網站

2.15.1 對 HTTP 伺服器開放可存取的範圍，應限制僅能存取資訊系統之某一特定區域之功能與權限。

2.15.2 權責單位主管應審核公告資訊之完整性，並確認未含機敏或違反智慧財產權及法令所明定禁止公開之資訊。

2.15.3 開放對外查詢之應用系統，應防止非授權使用者進入系統或存取資料庫資料。

2.15.4 對外服務之伺服器，若需下載檔案，應掃描是否隱藏電腦病毒或惡意程式。

2.15.5 對外服務之應用系統應有防範機制，防止不法者以指令破壞系統或獲取系統內重要資訊。

2.16 電腦管理及安全防護

2.16.1 系統管理人員應定時檢查作業系統及硬體設備之效能，並注意作業系統版本更新及問題資訊，做適當之建議及設定。

2.16.2 主機、伺服器管理人員應進行運行監控，檢查系統、安全及應用程式日誌紀錄或其它有關之系統狀況。一旦發現任何問題得請相關人員協同處理，必要時並通知廠商處理，相關管理作業應依據「主機與伺服器安全管理作業說明書」辦理。

2.17 可攜式設備及儲存媒體管理

2.17.1 可攜式設備管理

2.17.1.1 本處可攜式設備僅限於公務使用。

2.17.1.2 未經許可禁止於本處使用可攜式設備進行拍攝或是螢幕畫面捕捉之行為及存取本處資料。

2.17.1.3 可攜式設備於本處使用時，應視需要安裝防毒軟體，以避免電腦、系統與網路受到病毒威脅。

2.17.2 可攜式儲存媒體管理

2.17.2.1 機敏資料若需以可攜式媒體保存時，該媒體應存放於安全設備或處所。

2.17.2.2 儲存媒體所使用之密碼或編碼技術不應透露予遞送人員或與業務無關之人員。

2.17.2.3 儲存媒體遞送前應加以妥善包裝保護，避免發生實體損壞。

2.17.2.4 儲存媒體若委由外部單位遞送,如郵局或快遞公司,應選擇具有信譽之廠商,並考量採取以下控制措施：

2.17.2.4.1 放置於上鎖之容器或以彌封方式處理。

2.17.2.4.2 當面送達並簽收。

2.17.2.4.3 資料內容應使用密碼保護。

2.17.2.5 儲存媒體之報廢依據「資訊資產管理程序書」辦理。

2.18 資料交換安全管理

2.18.1 提供或交換資料之安全

2.18.1.1 視業務需要如須對外提供資料時，不論以任何型式，均應審視是否符合「個人資料保護法」或其他相關法令之規定。

2.18.1.2 資料需求申請人需配合本處、主管機關或相關法令需求辦理。若有資料提供或交換之需求時，應填寫資中工作單透過正式流程提出申請，經資料權責單位之主管核准後，始能提供。

2.18.1.3 禁止利用公共網路傳送未經加密的敏感性資訊，以避免資料在公共網路傳輸過程中遭竊取或篡改。

2.18.1.4 對於跨組織之電腦網路系統，應特別加強網路安全管理，防止資訊外洩。

2.18.1.5 本處同仁由外部對本處存取內部網路資源，應依據「網路管理作業說明書」辦理。

2.19 資料備份

2.19.1 各項系統設定檔、網頁資料、主機、伺服器檔案及資料庫資料均應由各系統管理人員訂定備份週期，並依據週期執行系統排程。

2.19.2 應定期於測試主機上測試備份復原是否正確。

2.19.3 重要系統資料應考量建立異地備份機制。

2.19.4 相關備份管理作業原則應依據「備份管理作業說明書」辦理。

2.20 安全稽核事項

2.20.1 對各項系統視需要留存系統最新參數設定檔。

2.20.2 系統維護、技術諮詢服務與電腦機房管理人員之工作，應依職務與相關規定確實記錄於電腦機房工作日誌或維護紀錄中，以備查核。

2.20.3 每月應檢視一次各資訊設備中系統時間是否一致，並進行時鐘同步校正。

2.20.4 系統稽核資料應依系統重要性進行備份保護作業，並由專人定期審核，系統管理人員不得新增、刪除或修改稽核資料，審查週期不得超過 6 個月。

2.21 行動裝置管理

2.21.1 本處禁止使用行動裝置進行非經授權之機敏資訊之存取，若因業務或特殊使用之需求，應進行申請及授權方可進行使用存取。

2.21.2 行動裝置應妥善設定通行碼，以避免未經授權之存取。

2.21.3 行動裝置閒置時應設定螢幕保護鎖定功能，最長不得超過 10 分鐘。

2.21.4 行動裝置上所執行的作業系統、軟體及 APP，必須安裝具合法使用版權之軟體，且應保持在該設備或軟體所提供之最新版本。

2.21.5 APP 安裝前應考量其要求開放之讀取權限是否合理，如：讀取設備通訊錄、讀取 GPS 訊息等相關權限與資訊，再評估是否進行安裝。

2.21.6 使用者應依設備特性，進行適當之防護設定。

2.21.7 禁止行動裝置儲存敏感等級以上資料，以避免檔案或資料遭洩露。

2.21.8 於本處網路使用筆記型電腦時，應遵守相關網路安全管理規範，未經申請授權，嚴禁執行封包收集與分析之軟體以及任何網路偵測之行為。

2.21.9 使用行動裝置時，應做好安全管理工作，避免裝置遺失或資料遭竊取等情事發生。

2.21.10 行動裝置內之重要資料應定期備份，確保重要機敏資料之完整性。若需於第三方提供之雲端空間進行資料備份，應謹評估其備份項目、資料屬性是否適宜放置於雲端空間，避免機敏資料暴露在公用網路，亦應透過加密軟體進行加密保護。

2.21.11 為避免行動裝置遺失或失竊造成資料外洩之風險，可於行動裝置安裝遠端資料抹除軟體，以達到資料安全防護。

2.21.12 應避免使用公開之無線 Wi-Fi 網路進行資料存取與傳遞。

2.21.13 若無傳輸連線之需求，裝置應關閉短距連線傳輸功能，如：Bluetooth、NFC 等。

2.21.14 若無定位之需求，建議裝置應關閉 GPS 定位功能。

2.21.15 如遭嚴重惡意程式感染且影響其他資訊設備安全，應立即與網路離線，直到確認惡意程式消除後，才可重新連線。

2.21.16 私人的行動裝置應做好安全管理工作，並依上述規範進行安全防護。

2.22 金鑰管理

2.22.1 於公眾網路提供服務之系統，凡資訊內容包含敏感資訊者（包含帳號、密碼或個人資料等），通訊傳輸應使用加密技術，例如：HTTPS。

2.22.2 應用系統獨立設計密碼系統者，密碼的保管儲存應採取適當的保護措施，以避免洩密或盜用之情事發生。

2.22.3 應用系統如採用憑證金鑰之加密技術者，應對金鑰採取適當的保護措施。

2.22.4 伺服器上之金鑰如為檔案形式存在，則應對伺服器之金鑰檔案存取權限作適當保護，並作適當的備份保管。如係以韌體形式存在於資訊設備時，則僅需保護其實體存取之安全。

2.23 網頁過濾管理

2.23.1 網路管理人員宜採用適當的技術手段，來限制或阻止組織內部使用者訪問不安全或不適當的外部網站。例如：考慮使用威脅情報來識別和封鎖惡意網站、制定網頁過濾的規則和設定等。

2.23.2 可使用的網頁過濾技術，如下：

2.23.2.1 網址過濾

利用網頁分類資料庫，比對使用者訪問的網址是否屬於允許或禁止的類別，例如色情、賭博、暴力等。

2.23.2.2 內容過濾

利用關鍵字、詞彙或語意分析，檢查網頁的內文是否含有不適當或危險的內容，例如敏感詞、惡意程式碼等。

2.23.2.3 網站過濾

利用威脅情報、黑名單或白名單，識別和封鎖惡意網站或不信任的來源，例如釣魚網站、惡意下載等。

2.23.2.4 應用程式過濾

利用協定分析、封包檢測或代理伺服器，控制或阻止使用者使用特定的網路應用程式，例如即時通訊、P2P 傳輸、串流媒體等。

3. 使用表單：

3.1 可攜式設備與媒體使用申請紀錄。

3.2 工作單系統。

4. 依據及相關文件：

4.1 資訊作業委外管理程序書。

4.2 應用系統安全管理程序書。

4.3 系統開發管理作業說明書。

4.4 主機與伺服器安全管理作業說明書。

4.5 網路管理作業說明書。

4.6 防火牆管理作業說明書。

4.7 電腦病毒管理作業說明書。

4.8 資訊存取控制作業程序。

4.9 資訊安全事件管理程序書。

4.10 弱點管理作業說明書。

4.11 電子郵件管理作業說明書。

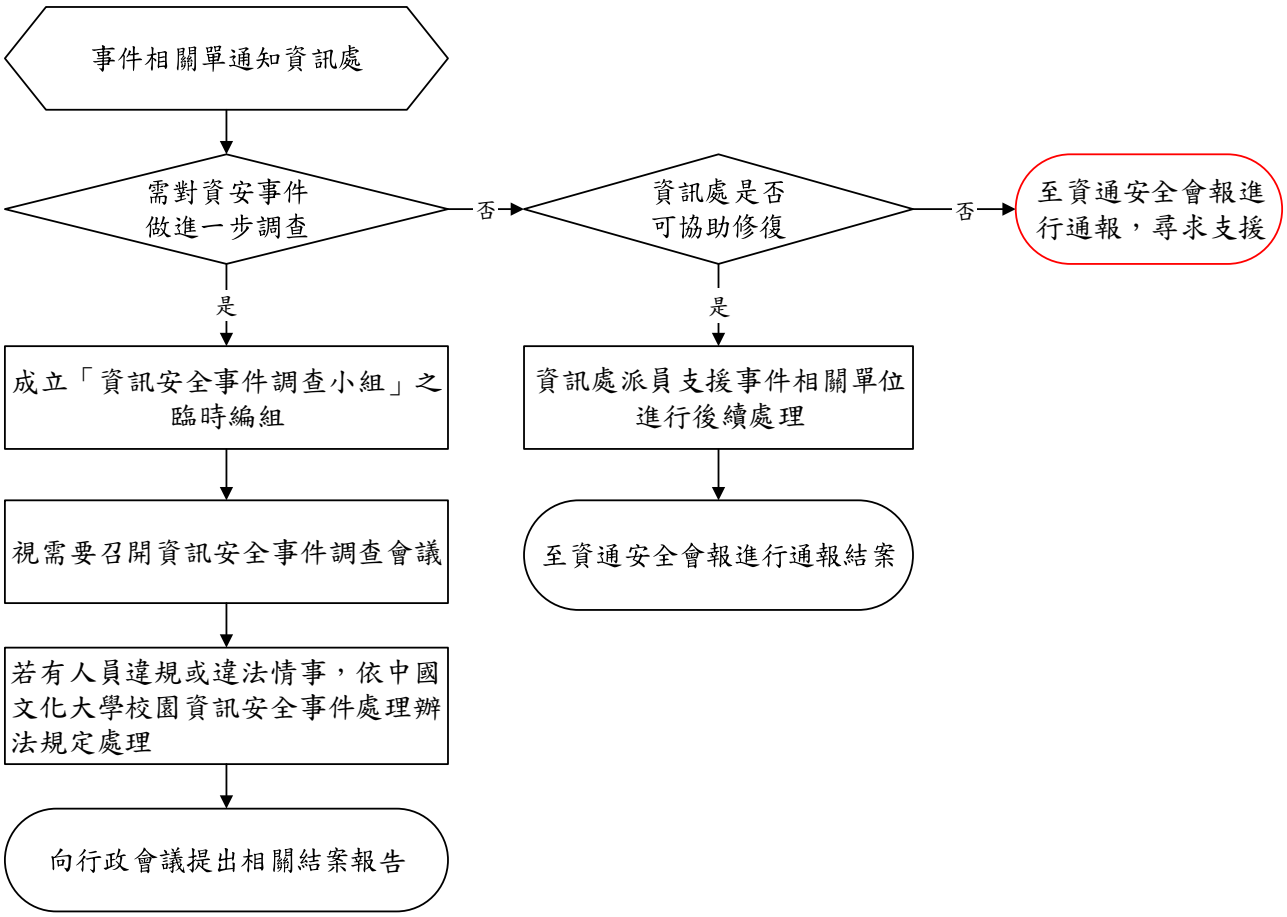
4.12 資訊資產管理程序書。

4.13 個人資料保護法。

4.14 備份管理作業說明書。

◎ 資訊安全事件管理作業

1. 流程圖：



2.作業程序與控制重點：

2.1 資訊安全事件之管理

2.1.1 應依內部指定之管道，定期收集、分析和評估威脅情資，以便及早發現和應對威脅，並採取適切的減緩措施來因應。例如：建立威脅情報收集和分析程序、確定威脅情報的重要性、確定威脅情報的影響範圍等。

2.1.2 應建立資訊安全事件之處理作業程序，並賦予相關人員必要責任，以便迅速有效處理資訊安全事件。

2.1.3 除正常應變措施（如：系統及服務之回復作業）外，資訊安全事件之處理程序，應視需要納入下列事項於營運持續計畫：

2.1.3.1 導致資訊安全事件原因之分析。

2.1.3.2 防止類似事件再發生之補救措施。

2.1.3.3 電腦稽核軌跡及相關證據之蒐集。

2.1.3.4 與受影響之使用者進行溝通及說明。

2.1.4 電腦稽核軌跡及相關證據應以適當方法保護，以利下列管理作業：

2.1.4.1 作為研析問題之依據。

2.1.4.2 作為研析是否違反契約或資訊安全規定之證據。

2.1.4.3 作為與委外廠商或保險公司協商如何補償之依據。

2.1.5 應依據「中國文化大學資訊安全事件處理流程」處理資訊安全事件。相關作業程序應注意下列事項：

2.1.5.1 考量單位資源，於最短的時間內，確認回復後之系統及相關安全控制是否完整及正確。

2.1.5.2 向管理階層報告處理情形，並檢討、分析資訊安全事件。

2.1.5.3 緊急處理步驟應詳實記載，以備日後查考。

2.2 通報程序

2.2.1 疑似資訊安全事件發生時，發現人員應依事件歸屬通報權責單位，並副知直屬主管，可參考「中國文化大學校園資訊安全事件處理辦法」辦理。

2.2.2 權責單位於收到通知後，研判是否為資訊安全事件。若：

2.2.2.1 判定為非資訊安全事件時，則將結果回覆予發現人員。

2.2.2.2 判定為資訊安全事件時，初估事件處理時間，並通知資訊安全官。

2.2.2.3 資訊安全事件等級區分為：

2.2.2.3.1 A 級：國家機密資料遭洩漏；或關鍵資訊基礎設施系統或資料遭嚴重竄改；或關鍵資訊基礎設施運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作。

2.2.2.3.2B 級：密級或敏感資料遭洩漏；或核心業務系統或資料遭嚴重竄改;抑或關鍵資訊基礎設施系統或資料遭輕微竄改；或核心業務運作遭影響或系統停頓，無法

於可容忍中斷時間內回復正常運作;抑或關鍵資訊基礎設施運作遭影響或系統停頓，於可容忍中斷時間內回復正常運作。

2.2.2.3.3C 級：核心業務(含關鍵資訊基礎設施)一般資料遭洩漏；或非核心業務系統或資料遭嚴重竄改;抑或核心業務系統或資料遭輕微竄改；或非核心業務運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作;抑或核心業務運作遭影響或系統停頓，於可容忍中斷時間內回復正常運作。

2.2.2.3.4D 級：非核心業務一般資料遭洩漏；或非核心業務系統或資料遭輕微竄改；或非核心業務運作遭影響或系統停頓，於可容忍中斷時間內回復正常運作。

2.2.3 權責單位於發生資訊安全事件時，應立即填具「資訊安全事件報告單」。

2.2.4 決策處理：

2.2.4.1 當事件影響較低、衝擊性較小，或僅涉及單位內部、受損程度輕微時（如：電腦病毒感染），由權責單位或委由廠商處理，並將處理後狀況通知單位主管及資訊安全官。

2.2.4.2 處理過程中如發現造成之影響大於原先判定事件，權責單位應立即向資訊安全官報告，重新執行事件分析辨識。

2.2.4.3 資訊安全官應參考『國家資通安全會報通報與應變作業流程』，並依據權責單位所提報之事件影響報告，決定是否向上級主管單位通報。若需要通報，應由資訊安全推動委員會確認後執行。

2.2.5 有關是否啟動營運持續計畫，依「營運持續管理程序書」辦理。

2.3 危機處理程序

2.3.1 本處資訊安全危機處理包括事前建置安全防護機制、事中主動預警與緊急應變，以及事後復原追蹤鑑識偵查等步驟。說明如下：

2.3.1.1 事前建置安全防護機制：

2.3.1.1.1 建置資訊安全管理系統及整體防護架構。

2.3.1.1.2 彙整及備妥資訊安全相關文件。

2.3.1.2 事中主動預警與緊急應變：

2.3.1.2.1 事件辨識：辨識事件之歸屬及採取之對策，如內部資安事件、外力入侵事件、天然災害或重大突發事件等，並決定處理的方法與程序。

2.3.1.2.2 事件控制：依據各類事件危機處理之程序，進行事件傷害控制，降低影響的程度及範圍。

2.3.1.2.3 問題解決：事件處理權責單位或負責人須將問題解決。必要時，應向資訊安全推動委員會提出建議方案。

2.3.1.2.4 恢復作業：問題解決後，系統需恢復至事件發生前之正常運作狀態。

2.3.1.3 事後復原追蹤鑑識偵查：

2.3.1.3.1 後續追蹤之精神乃係檢討相關資訊安全事件是否會重複發生，並審視現有

環境漏洞，透過研析相關資料，以釐清事件發生之原因與責任。

2.3.1.3.2 受損單位依復原程序實施災後復原重建。

2.3.1.3.3 重大資訊安全事件應保留事件發生之線索，如有需要得向國家資通安全會報技術服務中心或檢警單位申請數位鑑識（電腦、網路鑑識）。

3.使用表單：

3.1 資訊安全事件報告單。

4.依據及相關文件：

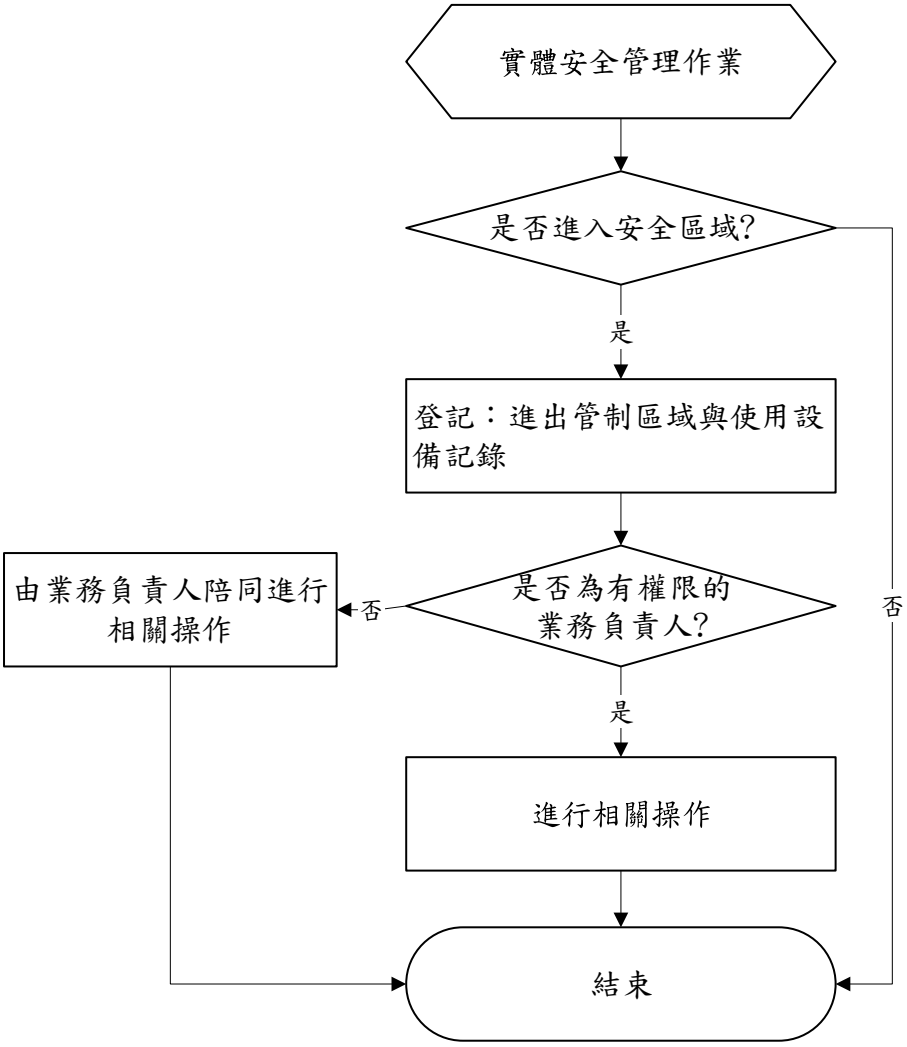
4.1 中國文化大學校園資訊安全事件處理辦法。

4.2 營運持續管理程序書。

4.3 中國文化大學資訊安全事件處理流程。

◎ 實體安全管理作業

1.流程圖：



2.作業程序與控制重點：

2.1 安全區域

2.1.1 為確保相關資訊資產之安全，非經權責單位同意之人員不得擅自進入安全區域使用相關資訊設備。

2.1.2 未具電腦機房進出權限之人員，因執行業務需求進入電腦機房時，必須由業務負責人、電腦機房維運人員及代理人陪同，並依據「電腦機房管理作業說明書」之管理規定辦理。

2.1.3 電腦機房之門禁紀錄應適當保存與定期審查。

2.1.4 安全區域應採取下列之方式進行持續監控，例如：感應器、入侵偵測警報、影像監視器（CCTV）等。

2.2 辦公區域安全管理

2.2.1 本處門禁管理人員須負責確認訪客來訪登記，通知拜訪人員，並執行訪客出入管理。

2.2.2 廠商或訪客進出本處時需於門禁管理人員處填寫「來賓登記表」，紀錄訪客進出時間。

2.2.3 本處重要之出入口均應設置門禁管理機制及錄影監視系統。

2.2.4 本處所有同仁應保持警覺，留意陌生人員進出，並予以詢問。

2.2.5 進入辦公室環境，未經許可禁止使用錄音、錄影、照相設備及可攜式設備。

2.2.6 人員異動或離職後，應於離職或異動當日更新或取消通行之權限。

2.2.7 委外廠商及訪客應於指定區域內執行作業。

2.2.8 未經授權或非業務權責需要，不得將設備、軟體、或文件攜出安全區域。若有需要，須經主管核准，始得進行。

2.3 電腦機房安全管理

有關電腦機房之安全管理，依據「電腦機房管理作業說明書」辦理。

2.4 辦公環境管理

2.4.1 下班時應關閉不需使用之資訊及電器設備。

2.4.2 辦公室最後一人下班離開時，需將辦公室門窗上鎖。

2.4.3 辦公區域環境內嚴禁抽煙。

2.4.4 辦公區域環境內應設置適當之消防設備，如手提式滅火器、煙霧偵測器等，設備存放環境應保持淨空，以確保其可用性，並定期檢測與紀錄。

2.4.5 重要資訊設備如主機、伺服器等，應置於電腦機房。

2.4.6 資訊資產之使用及管理，依據「資訊資產管理程序書」辦理。

2.4.7 可攜式設備及媒體的管理，應依據「通訊與作業安全管理程序書」之可攜式設備及儲存媒體管理辦理。

2.4.8 本處應由專人負責公文、郵件之收發。

2.4.9　使用影印機、印表機、傳真機或多功能事務機後，應立即將資料取走。

2.4.10 公用設備未經授權不得擅自使用或搬移。

2.4.11 為防止未經授權之存取，應遵守桌面淨空政策，將機敏性文件與可攜式資訊設備，放置於抽屜或儲櫃並上鎖，以避免資訊外洩。

2.4.12 本處同仁需隨時清理個人電腦之資源回收筒，以確保已經刪除的重要資料不會因為遺留在資源回收筒未清理，而遭未經授權之使用。

2.4.13 未經授權不得將公用設備、軟體、儲存資訊之媒體或文件攜出安全區域。如有需要，須經權責主管核准，始得進行。

2.4.14 受管制的資訊設備如需攜出辦公環境維護時須填寫「設備進出紀錄表」，經權責主管或代理人核可後，始可實施。

3.使用表單：

3.1 設備進出紀錄表。

3.2 資訊處來賓登記表。

4.依據及相關文件：

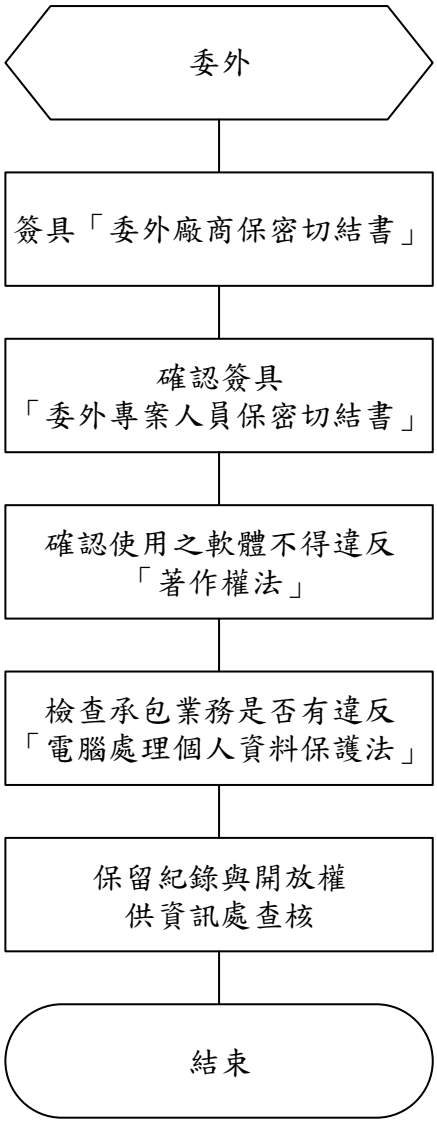
4.1 電腦機房管理作業說明書。

4.2 資訊資產管理程序書。

4.3 通訊與作業安全管理程序書。

◎ 資訊作業委外管理作業

1.流程圖：



2.作業程序與控制重點：

2.1 一般條款

2.1.1 委外廠商人員，因業務涉及本處機敏資料時，應遵守「個人資料保護法」及本處相關規定。

2.1.2 委外廠商人員，處理本處業務時所獲得之資訊，不得對外透露，廠商及專案人員並應分別簽署本校個人資料管理制度文件「委外廠商保密切結書」及「委外專案人員保密切結書」。

2.1.3 委外廠商履行合約所使用之軟體不得違反「著作權法」之規定，若因使用非法軟體造成本處資訊安全風險，委外廠商須承擔所有法律責任。

2.1.4 委外廠商使用之工具軟體及處理作業執行紀錄，本處有權進行稽核，廠商不得異議。

2.1.5 委外廠商應留存異常處理紀錄，本處得視需要進行查核。

2.1.6 委外廠商所交付之標的物內容，如有侵害第三人合法權益時，應由承包廠商負責處理並承擔一切法律責任。

2.1.7 委外廠商如因其員工業務過失，造成本處損害時，委外廠商需負賠償或復原責任。

2.1.8 委外廠商相關人員離調職或專案完成時，應繳回所借用之設備、移除軟體及刪除作業權限等。

2.1.9 資訊作業委外之分包與轉包，應依本校合約要求辦理。

2.1.9.1 應於合約內載明對協力廠商稽核的權力。

2.1.9.2 應於合約內載明協力廠商應對提供系統軟體的維護和責任。

2.1.9.3 應於合約內載明協力廠商能驗證遵循法規的能力。

2.1.9.4 應於合約內載明協力廠商應揭露使用開放程式碼(Open Source)的組件。

2.1.9.5 應於合約內載明協力廠商應(對自己及包括對下游的分包商)建立完善的安全控制措施，並能監控流程與驗證正確。

2.1.10 系統委外開發與硬體設備採購，應考量或評估供應鏈及來源國可能帶來之風險。

2.2 資訊系統委外服務需求

2.2.1 業務單位因業務需求提出資訊委外服務時，應適當評估資訊委外之必要性。

2.2.2 確認進行資訊委外時，應依本校採購辦法相關規定建立委外作業流程，訂定建議書徵求文件（Request For Proposal，RFP）大綱等，並依專案需求於 RFP 或合約中擬定資訊安全相關要求事項。

2.2.3 建議書徵求文件之擬訂，可參考行政院研考會「建議書徵求文件（RFP）作業參考手冊」辦理。

2.3 硬體採購與維護

2.3.1 廠商應提供設備主機之架構、操作、管理、維護等相關之操作手冊、文件及技術

支援，必要時應提供教育訓練課程。

2.3.2 若委外採購涉及資訊設備，業務單位應對系統需求做適當規劃，以確保足夠的電腦處理效能、儲存容量、電腦機房空間、電力及空調等。

2.3.3 硬體維護應視本處需求與廠商簽屬服務水準。

2.4 系統開發及維護

2.4.1 委外開發之系統，廠商應依 RFP 所載交付項目及時程，須經由本處業務單位人員審查及確認。

2.4.2 委外廠商應確實控管程式與文件版本之一致性。

2.4.3 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以上之業務資料。

2.4.4 宜規範委外廠商所交付之系統進行原始碼測試，確保系統資訊安全，並提供相關檢測報告。

2.4.5 委外開發之系統，應由需求單位或權責單位進行系統測試，確定符合需求後，始得依「應用系統安全管理程序書」之程序進行上線。

2.4.6 程式修改與開發需遵守本處「應用系統安全管理程序書」之規定，若有例外，須經權責主管同意以後，方可實施。

2.4.7 系統維護應依據本處要求建立服務水準。

2.5 系統帳號管理

2.5.1 委外開發之系統、作業系統及資料庫等最高權限帳號，應由本處承辦人員保管，不得直接授予委外廠商使用。

2.5.2 委外廠商人員如因作業需求，需對本處系統進行存取，應參考「存取控制程序書」5.2 之存取控制政策辦理。

2.5.3 委外廠商人員對於系統帳號應善盡保管之責，系統帳號不得任意交由非業務相關人員使用。

2.5.4 委外廠商人員對於系統之操作，本處各系統管理人員應盡監督之責，委外廠商人員不得從事非工作範圍內之操作。各系統管理人員並視需要於委外廠商人員完成工作後檢視系統紀錄。

2.6 委外廠商可攜式電腦及儲存媒體管理

委外廠商人員如需攜帶可攜式電腦或儲存媒體如磁片、光碟、隨身碟、外接式硬碟等進入本處電腦機房使用時，需經陪同之單位承辦人員同意，並依「電腦機房管理作業說明書」及「通信與作業安全管理程序書」辦理。

2.7 委外廠商網路使用規範

委外廠商若有遠端維護或使用內網需求時，需依據「網路管理作業說明書」辦理，並填寫「網路服務連線申請單」提出申請。

2.8 例外作業

資訊委外服務之業務單位應遵循本程序書之規範，提出適當安全需求項目。但若因成本、時效、委外服務之特性、委外廠商之局限性等相關因素之考量，而致本程序書所規範之安全需求無法完全適用時，業務單位應提出適切之安全需求與規劃，經資訊長簽核同意。

2.9 服務變更管理

委外廠商所提供之相關服務內容如有變更，需正式發文本處，經資訊長簽核同意，方能進行變更。

2.10 新增委外安全需求

業務單位每年進行風險管理作業所新增之 ISO27001/CNS27001 控管措施，可視需要決定是否明訂於合約之中。

3.使用表單：

3.1 委外廠商保密切結書。

3.2 委外專案人員保密切結書。

3.3 網路服務連線申請單。

4.依據及相關文件：

4.1 應用系統安全管理程序書。

4.2 存取控制程序書。

4.3 電腦機房管理作業說明書。

4.4 通信與作業安全管理程序書。

4.5 網路管理作業說明書。

4.6 建議書徵求文件（RFP）作業參考手冊。