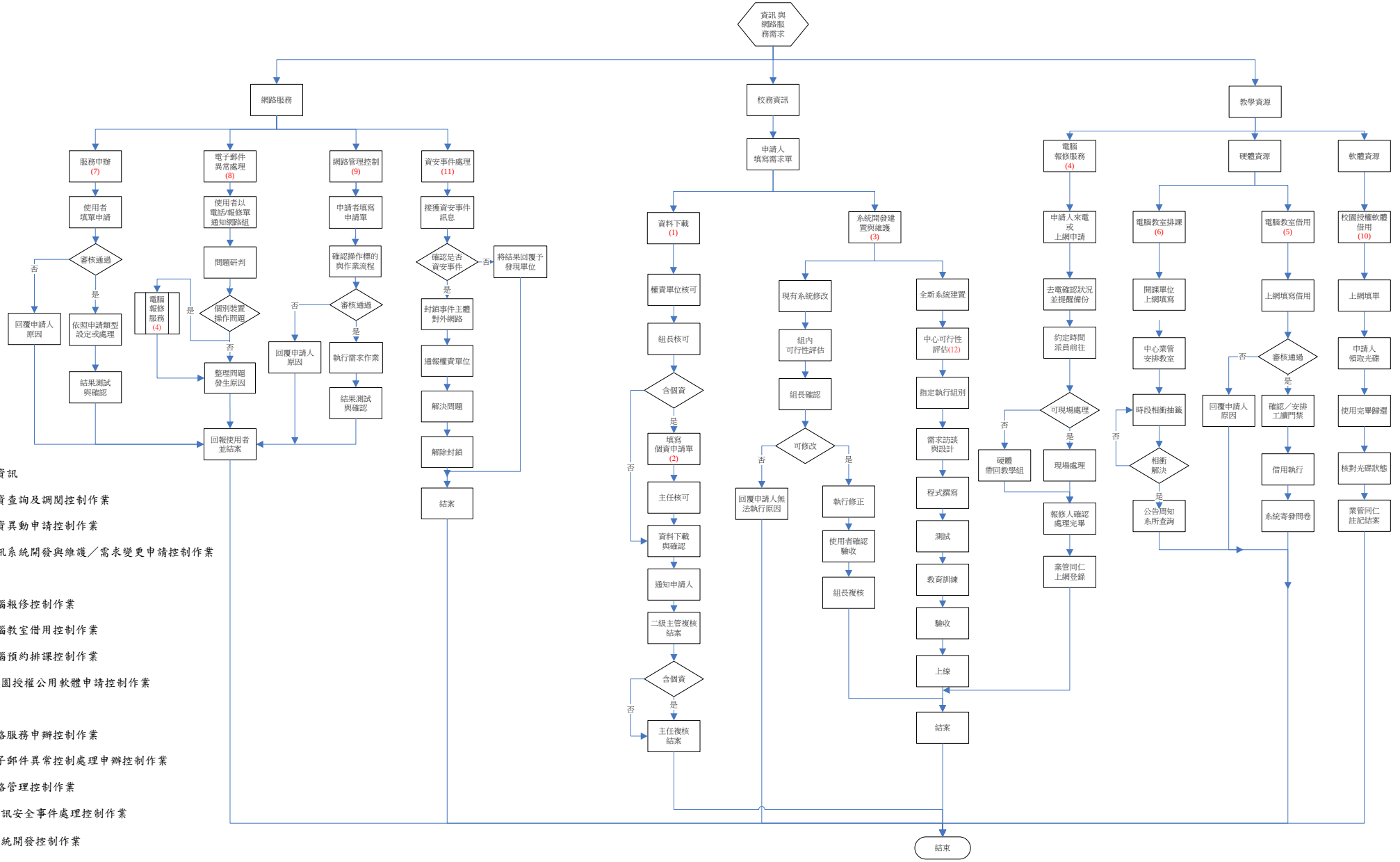

校務資訊

1. 個資查詢及調閱控制作業
2. 個資異動申請控制作業
3. 資訊系統開發與維護／需求變更申請控制作業

教學

4. 電腦報修控制作業
5. 電腦教室借用控制作業
6. 電腦預約排課控制作業
10. 校園授權公用軟體申請控制作業

網路

7. 網路服務申辦控制作業
8. 電子郵件異常控制處理申辦控制作業
9. 網路管理控制作業
11. 資訊安全事件處理控制作業
12. 系統開發控制作業

十、資訊管理循環內部控制點

資訊管理循環(如資訊取得、資料輸入、資料存取、檔案管理、個人資料保護、資通安全、資安檢查等之政策及程序)

NO	項目	內部控制點
10-1	資訊與網路服務需	
10-2	服務申辦	1.服務申請的目的是否正當 2.服務申請的資源是否合理
10-3	電子郵件管理與異常處理	**管理方面** 1.新建帳號於首次登入是否有要求變更密碼措施。 2.是否有提供帳號登入成功與失敗的紀錄。 3.離職人員之帳號信箱是否有依循規定處理。 **異常處理方式** 1.確認申請的單一帳號，用以確認其帳號相關資訊。 2.確認使用者使用電子郵件系統的方式(從網頁登入或是使用收信軟體)。 3.報修受理時，立即區分為系統問題(所有使用者或大部分使用者有問題)，或是個別帳號問題。 4.電話報修案件皆有登錄於報修系統中。
		1.防火牆規則是否定期檢視其適用性，且申請是否有確實申請並經權責主管同意；防火牆之管理連線是否有做安全性之控管。 2.路由交換器等重要設備之SNMP Community String值是否有確實修改，而非預設值;在連線至路由交換器等重要設備時，是否僅限定SSH協定或有控管之連線。 3.路由交換器等重要設備是否有限制人員管理權限並定期備份相關設定檔。 4.是否有記錄網路流量使用現況，以瞭解網路頻寬使用情形。 5.外部人員進行資訊系統、網路維護時，是否有依相關規定辦理。 6.發生網路安全事件是否確實依規定處理，及向權責主管反應。 7.上線伺服主機進行漏洞更新時，是否有事先對更新套件測試，確保無誤後才予以更新。 8.系統提供服務時是否有設定時間，以避免使用者長時間未登出。 9.伺服主機管理人員是否確實進行系統運作等狀況檢核，並記錄之。 10.伺服主機是否有確實檢核非合法授權安裝狀況。 11.伺服主機是否有確實更新Service Pack及病毒碼至最新。

十、資訊管理循環內部控制點

資訊管理循環(如資訊取得、資料輸入、資料存取、檔案管理、個人資料保護、資通安全、資安檢查等之政策及程序)

NO	項目	內部控制點
10-4	網路管理控制	1.人員進出時，是否提高警覺注意周遭不明人士。 2.門禁控管是否有確實核實機房授權權限。 3.委外人員是否有陪同人員進出機房，及攜帶資訊設備進入機房時，是否有確實登記。 4.門禁出入記錄是否保留。 5.機房電源是否有緊急電力配置，作為外部電力失效時的備援。 6.機房內溫濕度是否符合規定。 7.機房內電力、空調及消防設施是否定期保養，並保留記錄。 8.負責同仁是否確實檢測機房內各項措施，是否無安全疑慮。 9.針對網路及校務行政系統（包括行政用個人電腦）建立實體資安防護設施（例如：防火牆、防毒、IDS、郵件過濾等系統），防火牆應建立安全策略，阻絕外部對內網路連線通訊埠，依網路服務申辦作業開放連線。
		1.各資訊設備、系統是否確實建置身份鑑別機制。 2.權限設定是否依使用者身份給予最少的權限使用權利。 3.相關密碼原則是否確實依規定設定。 4.權限帳號清單是否確實定期進行清查與核對。 5.人員異動是否確實異動系統之帳號權限。 6.系統是否有設閒置時間，超過規定後是否有自動登出機制。

十、資訊管理循環內部控制點

資訊管理循環(如資訊取得、資料輸入、資料存取、檔案管理、個人資料保護、資通安全、資安檢查等之政策及程序)

NO	項目	內部控制點
10-5	資安事件處理	1.檢視每次資安事件是否確實記錄。 2.資訊安全工作小組是否針對資訊安全事件有確實判斷事件等級。 3.資訊安全事件是否有保全證據，供後續查核。 4.權責單位是否確實通報資訊安全事件。 5.教育訓練應定期進行 6.資安防禦設備應定期維護更新 7.檢測作業應定期執行 8.學校應成立資安推動組織、訂定資訊安全策略，導入資訊安全管理制度，對二項核心系統通過第三方稽核認證。 9.建立配合「國家資通安全緊急應變中心」建立緊急通報應變組織，處理資安問題，資安事件於二十四小時內進行通報，並於三十六小時內處理完成。 10.針對主管、資訊人員、資安人員、一般教職員（分別各需至少三、六、十六、三小時）規劃基本時數以上之資訊安全教育訓練。 11.遵循教育體系資通安全暨個人資料管理規範，建立網路、主機、資料庫、網站等核心系統對外服務申辦作業，建立安全稽核機制，以保護存取、處理或儲存於核心系統之資訊，並通過第三方驗證機構稽核認證。
		1.個人資料蒐集、處理或利用 (1)個資申請的目的是否正當。 (2)個資申請的資料來源是否存在。 (3)取得個人資料時是否依法規定進行告知並徵求同意。 (4)在處理或利用機敏文件時，是否取得主管同意。 (5)對於機敏個人資料之調閱是否經申請並核准，並加以記錄調閱者身分及行為。 (6)基於學術研究需求，提出使用本校所保管之個人資料，是否經單位主管核准。 (7)個人資料保管期限已到期，是否有依法銷燬。 (8)單位個人資料保護聯絡人是有公佈在網站，供使用者查詢。 (9)是否提供當事人依法行使權利時的管道及作法。 (10)當當事人行使個人資料更正時，是否依規定回覆。

十、資訊管理循環內部控制點

資訊管理循環(如資訊取得、資料輸入、資料存取、檔案管理、個人資料保護、資通安全、資安檢查等之政策及程序)

NO	項目	內部控制點
		2.事故預防、通報及應變 (1)當個人資料外洩時，是否依規定通報主管。 (2)當已確認個人資料外洩時，是否依規定通報並確實紀錄。 (3)當事故發生時，是否有保存證據措施作為未來的證據。 (4)當外洩事故處理完後，是否進行檢討與改善計畫。 **3.認知宣導及教育訓練** (1)處理個人資料檔案之人員是否參與資訊安全與個人資料保護之教育訓練。 (2)是否定期於單位內宣導個人資料保護之重要性。 (3)是否有將個人資料保護教育訓練納入職員教育訓練核心課程。(個資上路後之前幾年有推動?) **4.人員安全管理** 處理個人資料檔案之人員離職時，是否將所保管之個人資料列冊移交，並依規定辦理離校手續。 **5.檔案資料安全管理** (1)是否針對保有之個人資料檔案採取適當之防護措施，以防外洩或不當竄改。 (2)是否針對所保管之個人資料進行備份，並確保備份之有效性。 (3)公務電腦送修時，是否有將個人資料之儲存媒體抹除或拔除。 (4)當個人資料保管之文件或儲存媒體不用時，是否有妥善保管。 (5)機敏性個人資料存取，是否採取帳密通行碼機制更為嚴格之控管措施。
10-6	資料下載	

十、資訊管理循環內部控制點

資訊管理循環(如資訊取得、資料輸入、資料存取、檔案管理、個人資料保護、資通安全、資安檢查等之政策及程序)

NO	項目	內部控制點
		6.資料安全管理 (1)是否指定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。 (2)公務電腦是否安裝防毒軟體，並定期更新病毒碼。 (3)公務電腦是否定期檢視、更新作業系統、應用程式漏洞。 (4)是否禁止使用點對點(P2P)軟體及Tunnel相關工具下載或提供分享檔案。 (5)是否禁止在社群網站、部落格、公開論壇或其他利用網際網路形式公開業務所知悉之個人資料。 (6)同仁的帳號密碼是否依規定設定密碼長度及複雜性。 (7)在辦公室區域是否張貼含有認證、IP、密碼等資訊。 (8)公務電腦是否有設定螢幕保護功能。 (9)伺服器是否有依身份與用途分別設定對應之使用權限。 (10)系統是否保有適當的日誌或稽核紀錄，供備查。主機系統是否有安裝防火牆，開放適當的規則。 (11)伺服器是否安裝未經授權之軟體。 (12)伺服器管理者應定期進行備份及弱點掃描之作業。 (13)伺服器管理者應設定可管理連線之區域或IP。 **7.實體及環境安全管理** (1)所擁有個資蒐集之書面或電子資料，是否妥善保管並存放至有門禁管理或上鎖之鐵櫃內。 (2)當外來廠商維修資訊設備時，是否有專人全程陪同。

十、資訊管理循環內部控制點

資訊管理循環(如資訊取得、資料輸入、資料存取、檔案管理、個人資料保護、資通安全、資安檢查等之政策及程序)

NO	項目	內部控制點
		8.業務永續運作計畫管理 (1)是否建立與維護個人資料檔案清冊。 (2)是否依規定進行個人資料盤點作業。 (3)是否依規定進行風險評估作業。 (4)是否依規定進行個人資料稽核作業。 **9.使用紀錄、軌跡資料及證據保存** (1)是否確實保管各種使用紀錄、軌跡資料、證據。 (2)是否依規定將超過保管期限之使用紀錄、軌跡資料、證據等銷燬。 **10.委外作業安全管理** (1)委託他人執行前，是否對受託人依法進行適當的規範，保障自身權益。 (2)是否依規定請受委辦單位填寫委外廠商保密切結書。 (3)個資外洩時，委外廠商是否有善盡配合本校事件通報及應變流程之責任。 11.針對行政人員、教職員等人員網際資訊工具（個人電腦、3G手機、電子書等），建立使用安全規範；因應處理個人資料，建立個人資料保護與管理規範。

十、資訊管理循環內部控制點

資訊管理循環(如資訊取得、資料輸入、資料存取、檔案管理、個人資料保護、資通安全、資安檢查等之政策及程序)

NO	項目	內部控制點
10-7	系統開發建置與維護	1.新系統開發是否有需求系統申請資料。 2.系統於規劃建置時是否有評估所處理資料之機密性、可用性、完整性，確認後續資源的支援。 3.新系統開發設計是否有依據系統安全性設計規格表進行設計。 4.系統開發完成後在交付提出者時，是否有要求填寫需求測試紀錄。 5.系統變更時是否有針對法令規範、版本控制等，評估作業平台是否足以影響變更後的穩定。 6.對系統程式原始碼、文件是否有備份予以妥善保管。 7.系統上線時，系統負責人是否有執行環境安全測試、程式碼檢核，並填寫相關表單。 8.系統管理員之帳號是否有依密碼原則要求。 9.業務執行單位之承辦人是否有登記於權限帳號清單中。 10.資料庫管理系統是否針對機敏性資料之新增、異動等情況進行記錄。
10-8	電腦報修服務	1.是否於兩日內主動通知。 2.是否提醒重要資料備份、私密資料移除或加密保護。 3.到點維修時是否於檢測前簽認維修同意書。 4.維修完畢後是否確實結案存查。

十、資訊管理循環內部控制點

資訊管理循環(如資訊取得、資料輸入、資料存取、檔案管理、個人資料保護、資通安全、資安檢查等之政策及程序)

NO	項目	內部控制點
10-9	硬體資源	1.借用之目的是否符合以教學、研討目的之活動。 2.借用電腦教室所使用之軟體是否為合法授權軟體。 3.教師上課指定使用軟體是否為本校授權軟體；所提供之軟體是否有已有合法授權。 4.各系所單位開課負責人之權限是否已正常開通，並每學期清查、管制異動之帳號。 5.課程安排完畢後，是否確實通知系所單位開課負責同仁。
10-10	軟體資源	1.系統應於畫面顯眼處顯示「尊重著作權」說明。 2.軟體已確實依照授權範圍分類，提供下載。 3.系統已確實依照身份別，授權予使用者下載可下載之軟體。 4.授權到期軟體已確實從伺服器端移除，並公開提醒使用者勿再使用。 5.光碟借用是否歸還。