資訊中心分層負責明細表

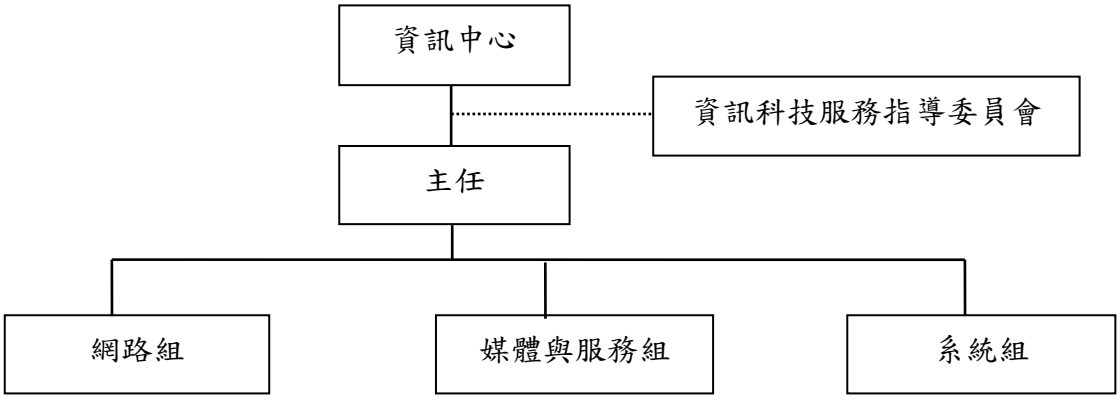
承辦單位	工作項目與內容		分層負責劃分				備註
	項目	內容	校長	一級主管	二級主管	承辦人	
網路組	校園網路維運與資訊安全管理	1.校園網路系統之設置、管理、維護與更新。		核定	審核	擬辦	
		2.共通性資訊安全規範之制訂。	核定	審核	審核	擬辦	
		3.資訊安全稽核作業。		核定	審核	擬辦	
		4.資訊安全事件通報應變處理作業。	核定	審核	審核	擬辦	資通安全長核定
系統組	校務行政管理資訊系統	1.校務行政管理資訊系統之規劃、開發、建立、管理、維護與更新。			核定	擬辦	
		2.辦理校務行政管理資訊系統之使用與諮詢。			核定	擬辦	
媒體與服務組	一般行政管理、訓練	1.資訊科技服務指導委員會要點訂定、召開。	核定	審核	審核	擬辦	
		2.辦理資訊教育訓練。		核定	審核	擬辦	
		3.公文系統維護。		核定	審核	擬辦	
		4.資訊中心電腦教室使用與管理。		核定	審核	擬辦	
		5.電腦採購之諮詢服務。		核定	審核	擬辦	
		6.AI 運算學生學習平台使用申請。			核定	擬辦	由老師提出申請
	多媒體作業	1.本校全球資訊網(3W)之規劃、建置與管理。	核定	審核	審核	擬辦	
		2.全校性數位影片、照片典藏系統管理。		核定	審核	擬辦	
		3.全校性公告訊息管理。		核定	審核	擬辦	
		4.全校性影片拍攝與後期製作。		核定	審核	擬辦	

國立雲林科技大學資訊中心內部控制制度

一、作業層級目標

(一) 建立本校資訊安全管理規範，符合相關法令規章。
(二) 提升學校同仁資訊安全意識，強化學校資訊安全環境。
(三) 確保本校資訊安全管理制度之推動，有效分配資訊安全責任。
(四) 遵守個人資料保護法，避免人格權受侵害，促進個人資料之合理使用。

二、作業層級組織圖



三、風險評估

為提升學校同仁資訊安全意識，強化學校資訊安全環境、分配資訊安全責任，本校建立資訊安全管理制度規範，作為校內各單位資訊安全運作之準則，使每位教職員工生認知資訊安全之重要性，確實落實執行資訊安全控制措施，期能維持並持續運作本校資訊安全機制，避免資訊安全事件之發生，使災害損失降至最低，並保護資訊資產的機密性、可用性與完整性。

參考「風險管理及危機處理作業手冊」中所列之風險來源，進行風險辨識。主要風險來源有科技之應用，其風險情境及影響為「發生重大資訊安全事故時，若未能在有限時間內，採取緊急應變行動，甚而影響核心業務運作」。因此辨識出落實「資訊安全管理」規範為可能降低發生資訊安全事件風險之項目。

四、控制作業

各項資訊安全控制項目，係為建立安全及可信賴的資訊環境，以確保資訊資產的機密性、可用性與完整性，採取適當的控制措施與透過稽核作業，實地檢視控制規範落實情形，確保資訊的適當安置及資訊安全實務作業的可行性與有效性。依據教育部資訊安全基礎引申訂定下列資訊安全管理規範項目

(一)個人電腦使用安全
(二)伺服器安全管理
(三)資產(個資)盤點
(四)個人資料保護管理
(五)文件管理
(六)通訊與作業管理
(七)實體與環境安全控管
(八)委外廠商管理
(九)資訊安全事件處理

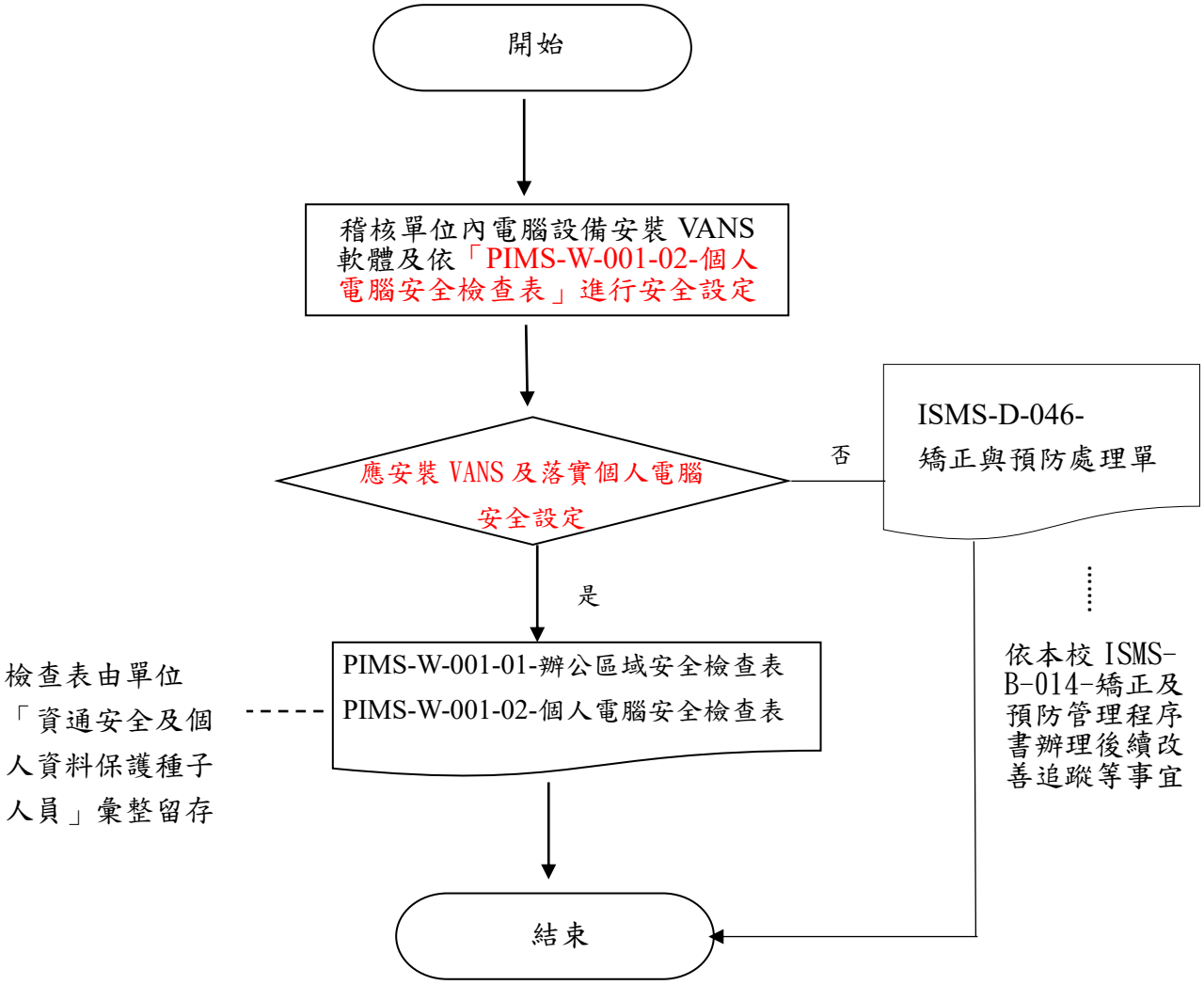
五、監督

為落實資訊安全管理規範，校內各單位指派之「資通安全及個人資料保護種子人員」，瞭解資訊安全管理制度概念及實作方法，協助組織內部人員實施資安規範與紀錄，配合實地查訪稽核作業，協助將資訊風險降低至可接受之程度內，而單位內其他人員須接受資訊安全教育訓練與執行資訊安全防護措施、定期執行資安自我檢查；資訊中心資安稽核小組每學年排定稽核計畫，實地查訪檢核各單位資訊安全執行情況與監督改善缺失，期能建立一個較安全、可靠的資訊安全環境。

資訊中心作業程序說明表

項目編號	TCX001
項目名稱	個人電腦使用安全
承辦單位	資訊中心網路組
作業程序說明	一、依「資通安全責任等級分級辦法」要求，導入資通安全弱點通報機制(Vulnerability Analysis and Notice System,以下簡稱 VANS)，電腦設備應安裝 VANS 軟體。 二、單位內電腦設備請依「PIMS-W-001-02-個人電腦安全檢查表」要求，落實安全設定。 三、稽核時，實地查檢電腦設備應安裝 VANS 軟體及個人電腦安全設定；發現不符合事項時，依本校「ISMS-B-014-矯正及預防管理程序書」填寫「ISMS-D-046-矯正與預防處理單」辦理後續改善追蹤等事宜。 四、每年定期執行個人電腦安全檢查後，請填寫「PIMS-W-001-01-辦公區域安全檢查表」與「PIMS-W-001-02-個人電腦安全檢查表」，檢查結果為”否”之項目，請依規定落實安全設定。使用者設定完成於檢查表簽章後，逕送單位「資通安全及個人資料保護種子人員」彙整留存。
控制重點	一、單位內電腦設備應安裝 VANS 軟體及依「PIMS-W-001-02-個人電腦安全檢查表」進行安全設定，稽核作業時實地觀察與抽樣檢視。 二、稽核時發現之缺失，受稽單位應針對稽核缺失擬定矯正預防處理計畫與執行改善措施。
法令依據	一、資通安全管理法與施行細則。 二、資通安全責任等級分級辦法 三、國際標準 ISO 27001:2013 資訊安全管理制度 四、本校資訊安全管理制度(ISMS) 五、本校個人資料保護管理制度(PIMS)
使用表單	一、PIMS-W-001-01-辦公區域安全檢查表 二、PIMS-W-001-02-個人電腦安全檢查表 三、ISMS-D-046-矯正與預防處理單

資訊中心 個人電腦使用安全設定 作業流程圖



資訊中心內部控制制度控制作業自行評估表

_____年度

評估單位：資訊中心

作業類別(項目)：個人電腦使用安全設定

評估期間：○○年○○月○○日至○○年○○月○○日

評估日期：○○年○○月○○日

滾動式修正風險評量表：

	發生可能性(L)	影響程度(I)	風險值(R)=(L)×(I)
前期風險評量			
本期風險評量			

控制重點	評估情形					改善措施
	落實	部分落實	未落實	不適用	其他	
一、單位內電腦設備應安裝VANS 軟體及依「PIMS-W-001-02-個人電腦安全檢查表」進行安全設定，稽核作業時實地觀察與抽樣檢視。						
二、稽核時發現之缺失，受稽單位應針對稽核缺失擬定矯正預防處理計畫與執行改善措施。						
填表人：　　複核：						

註：

1.單位得就 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，將作業流程之控制重點納入評估。

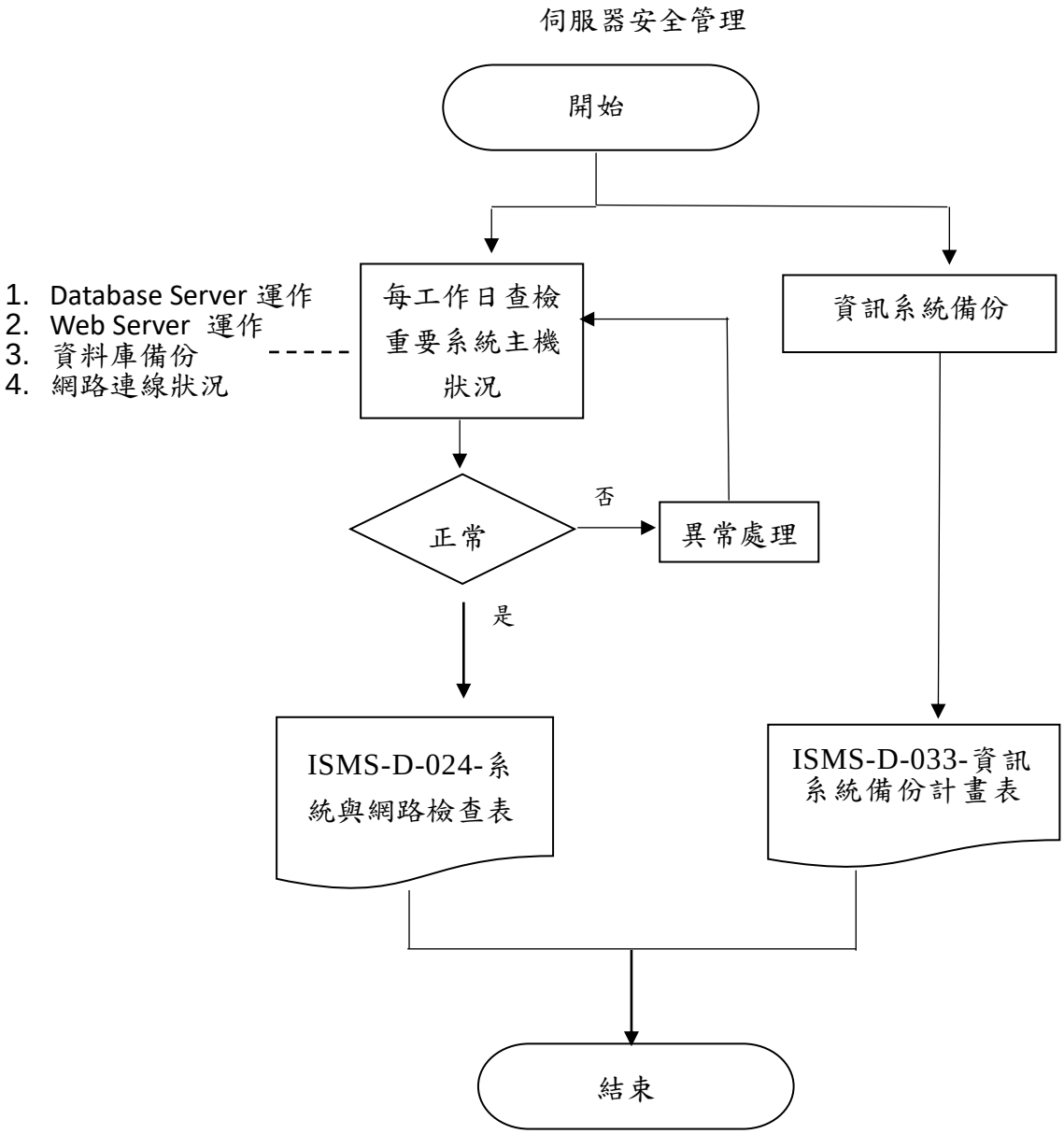
2.各單位依評估結果於評估情形欄勾選「落實」、「部分落實」、「未落實」、「不適用」或「其他」；其中「不適用」係指評估期間法令規定或作法已修正，但控制重點未及配合修正者；「其他」係指評估期間未發生控制重點所規範情形等，致無法評估者；遇有「部分落實」、「未落實」或「不適用」情形，於改善措施欄敘明需採行之改善措施。

資訊中心作業程序說明表

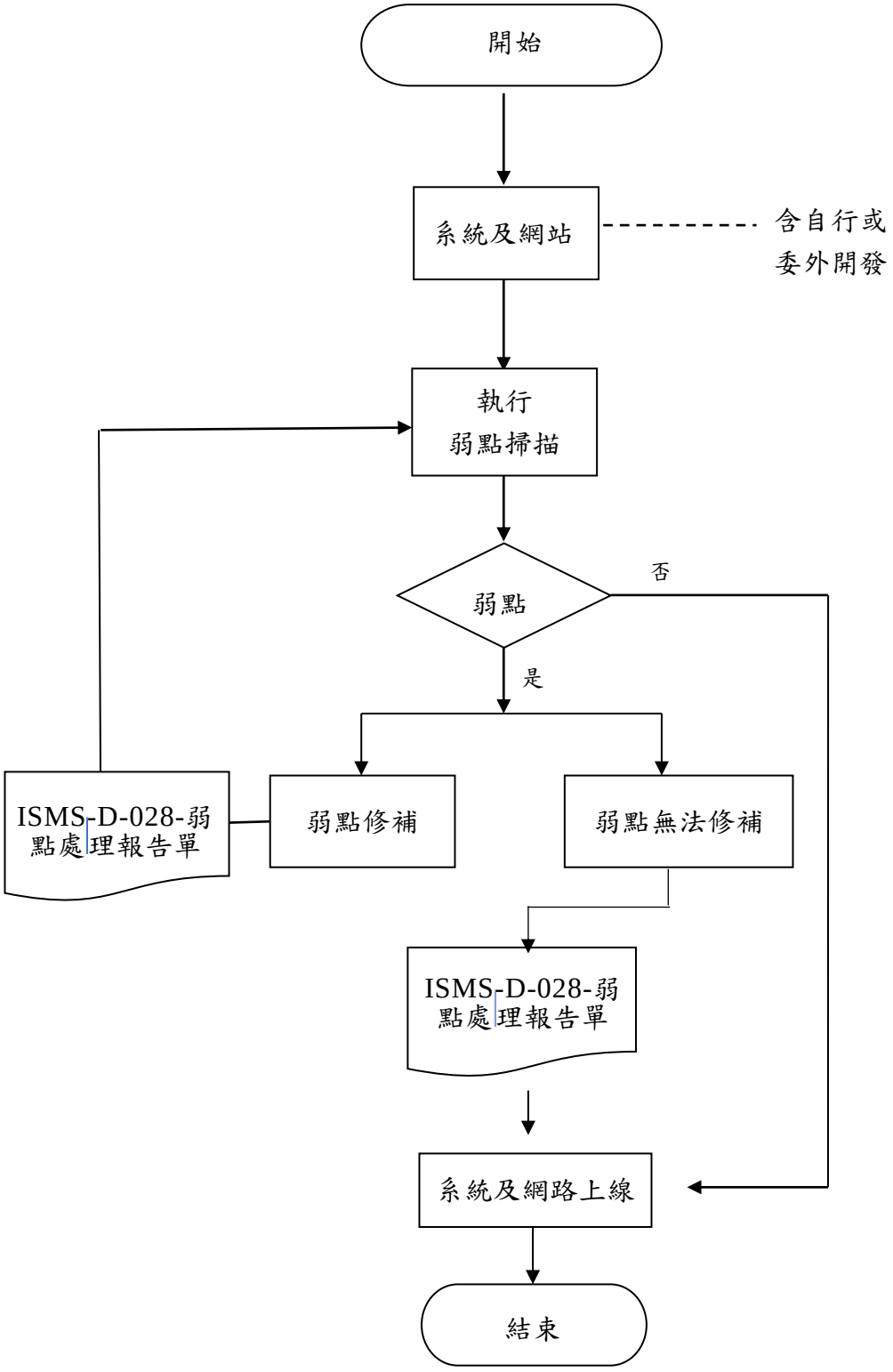
項目編號	TCX002
項目名稱	伺服器安全管理
承辦單位	資訊中心網路組
作業程序說明	一、行政及教學單位對外開放網際網路服務之伺服器，應符合「國立雲林科技大學伺服器管理辦法」之規定。 二、設定防火牆以控管外界與單位內網路間之資料傳輸與資源存取，應符合「國立雲林科技大學防火牆系統管理規範」，並關閉不使用的通訊埠，以避免病毒感染及駭客攻擊。 三、單位開發之系統及網站(含委外開發)，應於完成後，先執行弱點掃描與完成修補風險弱點始可上線；運作中網站亦請定期進行必要的系統及網站弱點掃描。 四、每次掃描完成後應產出弱點掃描報告與進行相關漏洞修補，確保弱點均已處理無遺漏。弱點若因故無法修補，應於「ISMS-D-028-弱點處理報告單」說明無法修補之原因與防禦因應方法。 五、伺服器管理者應於每工作日時依「ISMS-D-024-系統與網路檢查紀錄表」所列項目檢查重要系統主機狀況，以確保系統正常運作。 六、重要系統設定檔、網頁資料、伺服器檔案、資料庫及機敏性檔案資料均應訂定備份週期，並依據週期執行系統排程或手動備份。備份檔宜以加密方式保護，備份狀況記錄於「ISMS-D-033-資訊系統備份計畫表」。
控制重點	一、 伺服器主機資訊安全及防護措施應落實執行。 二、 弱點掃描漏洞~~是否~~已修補，無法修補時應說明原因與防禦因應方法並紀錄於「ISMS-D-028-弱點處理報告單」。 三、 伺服器管理者每個工作日應依「ISMS-D-024-系統與網路檢查紀錄表」所列項目檢查重要系統主機狀況。 四、 重要系統設定檔、網頁資料、伺服器檔案、資料庫及機敏性檔案資料均應定期備份。
法令依據	一、 資通安全管理法與施行細則。 二、 資通安全責任等級分級辦法。 三、「國立雲林科技大學伺服器管理辦法」 四、「國立雲林科技大學防火牆系統管理規範」 五、 教育部「校園通用資安管理原則」 六、 國際標準 ISO 27001:2013 資訊安全管理制度。 七、 本校資訊安全管理制度(ISMS)。
使用表單	一、 ISMS-D-028-弱點處理報告單 二、 ISMS-D-024-系統與網路檢查紀錄表

	三、 ISMS-D-033-資訊系統備份計畫表

資訊中心 伺服器安全管理 作業流程圖



系統及網站弱點掃描


開始
系統及網站
含自行或委外開發
執行弱點掃描
弱點
否
是
ISMS-D-028-弱點處理報告單
弱點修補
弱點無法修補
ISMS-D-028-弱點處理報告單
系統及網路上線
結束

資訊中心內部控制制度控制作業自行評估表

_____年度

評估單位：資訊中心

作業類別(項目)：伺服器安全管理

評估期間：○○年○○月○○日至○○年○○月○○日

評估日期：○○年○○月○○日

滾動式修正風險評量表：

	發生可能性(L)	影響程度(I)	風險值(R)=(L)×(I)
前期風險評量			
本期風險評量			

控制重點	評估情形					改善措施
	落實	部分落實	未落實	不適用	其他	
一、伺服器主機資訊安全及防護措施應落實執行。						
二、弱點掃描漏洞應修補，無法修補時應說明原因與防禦因應方法並紀錄於「ISMS-D-028-弱點處理報告單」。						
三、伺服器管理者每個工作日應依「ISMS-D-024-系統與網路檢查紀錄表」所列項目檢查重要系統主機狀況。						
四、重要系統設定檔、網頁資料、伺服器檔案、資料庫及機敏性檔案資料均應定期備份。						
填表人：			複核：			

註：

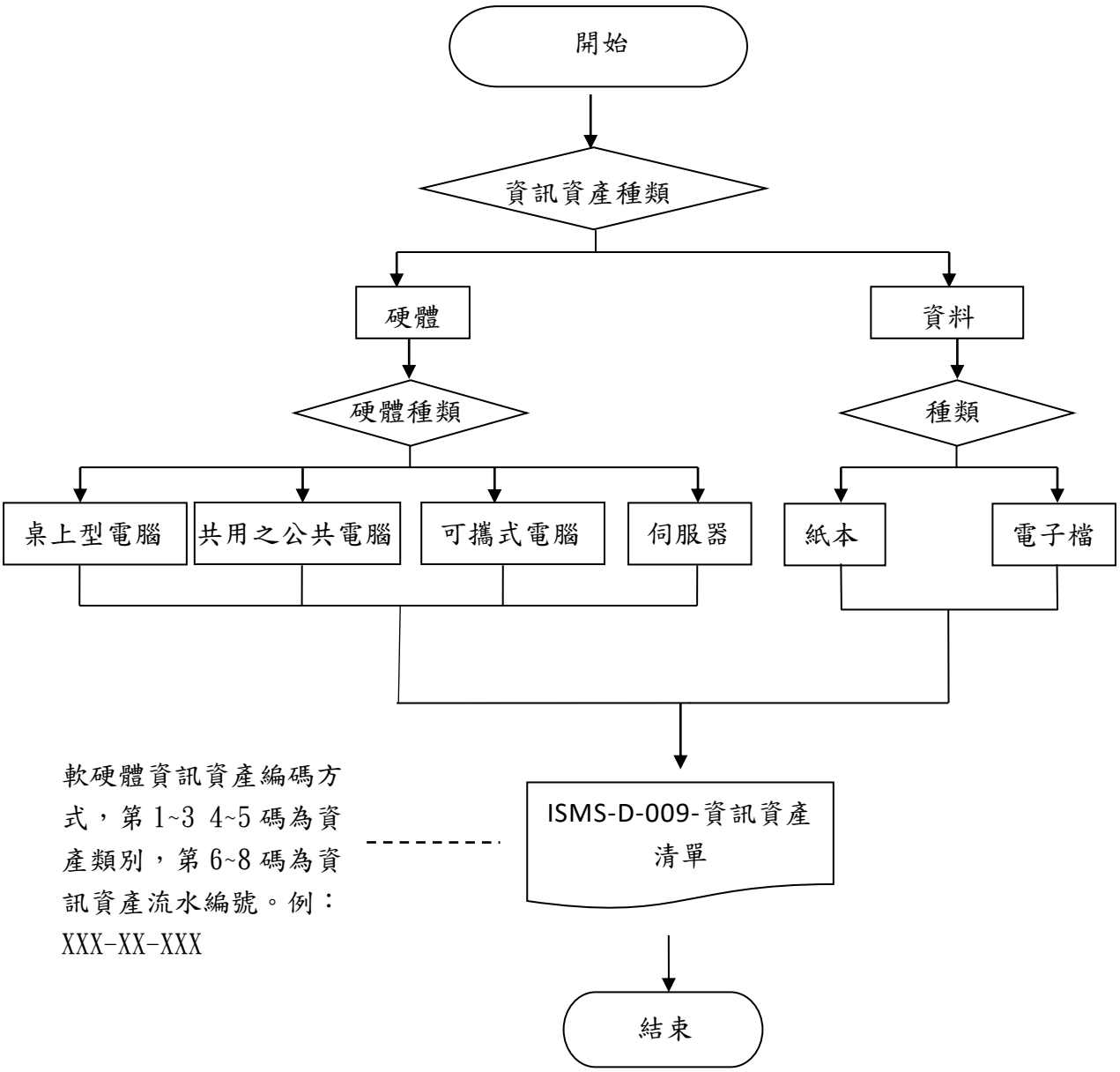
1.單位得就 1 項作業流程製作 1 份自行評估表，亦得將各項作業流程依性質分類，同 1 類之作業流程合併 1 份自行評估表，將作業流程之控制重點納入評估。

2.各單位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。

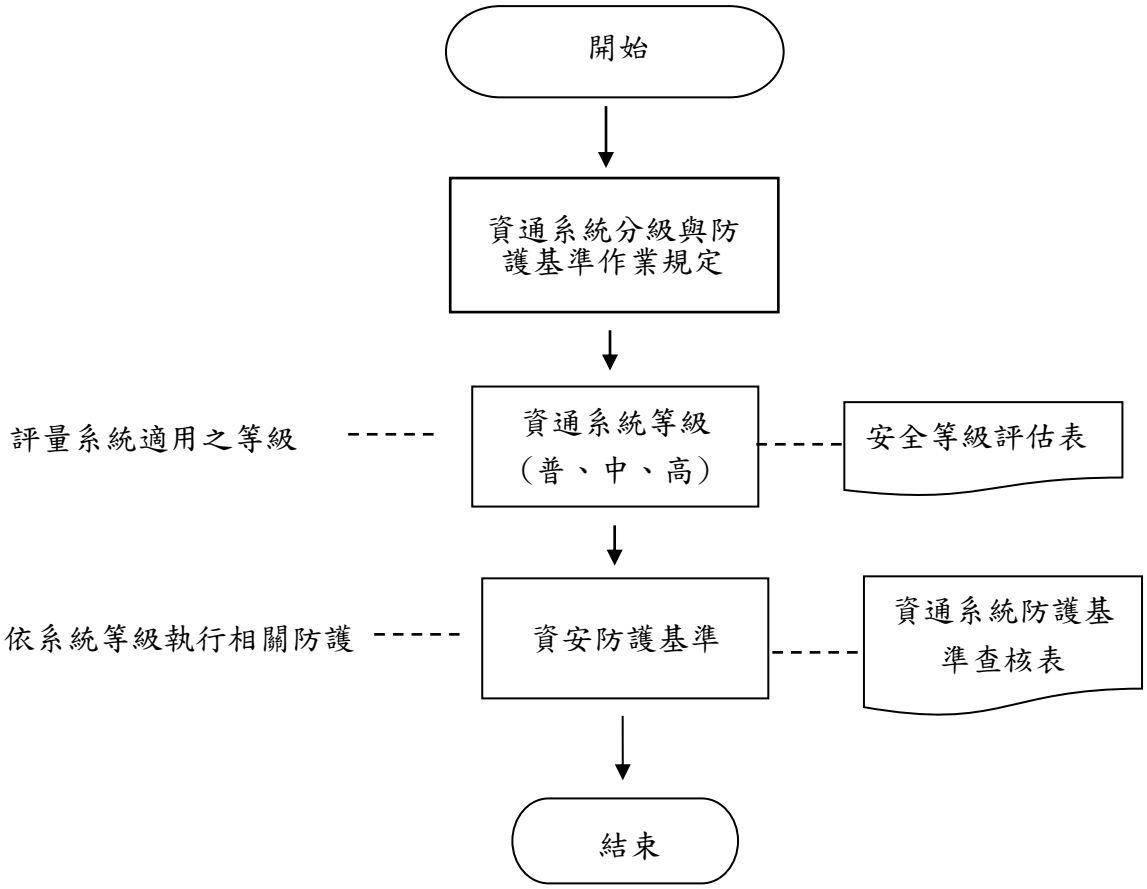
資訊中心作業程序說明表

項目編號	TCX003
項目名稱	資訊資產盤點
承辦單位	資訊中心網路組
作業程序說明	一、 各單位應鑑別所管轄資訊相關設備建立「ISMS-D-009-資訊資產清單」。 二、 每年至少進行乙次資產盤點與資訊資產清單覆核，以更新及確保資訊資產清單的正確性及完整性。 三、 針對自行或委外開發之資通系統，依資通安全責任等級分級辦法附表九完成資通系統分級；每年至少檢視一次資通系統分級妥適性，並完成資通安全責任等級分級辦法附表十資通系統防護基準查核表。
控制重點	一、單位內軟、硬體之資訊資產應詳實盤點並填列於「ISMS-D-009-資訊資產清單」。 二、每年執行資通系統安全等級評估及資通系統防護基準查核表。
法令依據	一、 資通安全管理法與施行細則。 二、 資通安全責任等級分級辦法。 三、 國際標準 ISO 27001:2013 資訊安全管理制度。 四、 本校資訊安全管理制度(ISMS)。 五、 教育部「校園通用資安管理原則」。
使用表單	一、 ISMS-D-009-資訊資產清單 二、 安全等級評估表 三、 資通系統防護基準查核表

資訊中心 資產(個資)盤點 作業流程圖



資訊中心 資通系統分級暨防護基準 作業流程圖



資訊中心內部控制制度控制作業自行評估表

_____年度

評估單位：資訊中心

作業類別(項目)：資訊資產盤點

評估期間：○○年○○月○○日至○○年○○月○○日

評估日期：○○年○○月○○日

滾動式修正風險評量表：

	發生可能性(L)	影響程度(I)	風險值(R)=(L)×(I)
前期風險評量			
本期風險評量			

控制重點	評估情形					改善措施
	落實	部分落實	未落實	不適用	其他	
單位內軟、硬體之資訊資產應詳實盤點並填列於「ISMS-D-009-資訊資產清單」。						
每年執行資通系統安全等級評估及資通系統防護基準查核表。						
填表人：　　複核：						

註：

1.單位得就 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，將作業流程之控制重點納入評估。

2.各單位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。

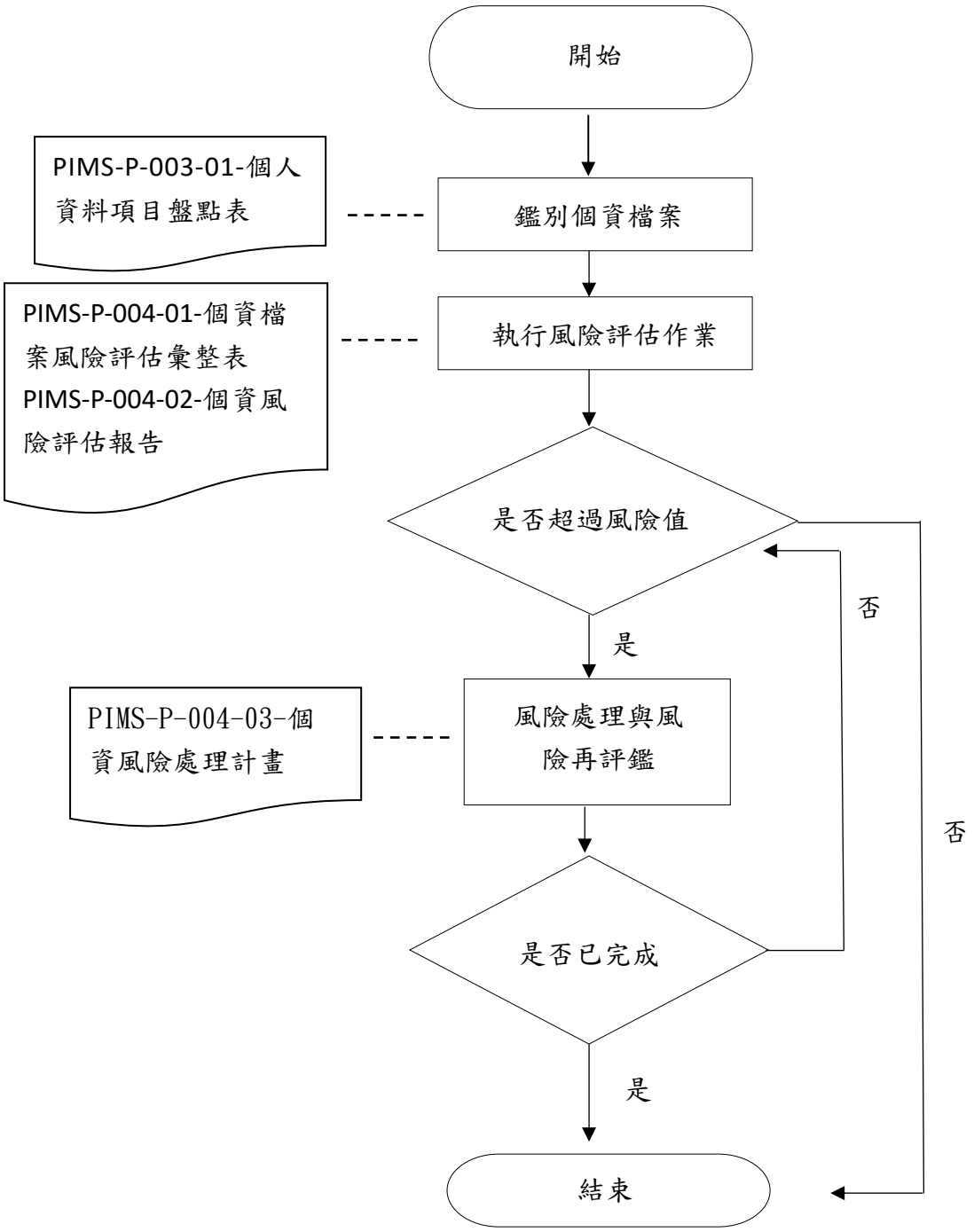
資訊中心作業程序說明表

項目編號	TCX004
項目名稱	個人資料保護管理
承辦單位	資訊中心網路組
作業程序說明	一、向當事人蒐集個人資料時，除法律明文規定外，需經當事人同意並明確告知蒐集目的、個人資料之類別、利用期間、地區、對象及方式。 二、蒐集個人資料時，需經適當之授權與監督並僅就所需之必要欄位進行蒐集。 三、應就業務之流程，屬於個人資料作業、流程及範圍內進行個人資料識別、清查與盤點。 四、應明確鑑別高風險、敏感及特種個人資料。 五、各單位組織變更、業務新增變動或業務流程改變時，應重新進行各單位個人資料盤點作業。 六、各單位每年定期進行個人資料盤點作業。應依據各單位處理個人資料之業務流程及內容，進行個人資料鑑別與盤點作業，並將所鑑別之個人資料，填具於「PIMS-P-003-01-個人資料項目盤點表」中列管。 七、各單位應每年辦理個人資料風險評鑑作業，請依據「PIMS-P-004-個人資料風險評鑑與處理管理程序」執行風險評估與分析，並將評估結果記錄於「PIMS-P-004-01-個資檔案風險評估彙整表」。 八、完成「PIMS-P-004-01-個資檔案風險評估彙整表」後，由各單位承辦人員負責撰寫各單位之「PIMS-P-004-02-個資風險評估報告」。 九、「資通安全暨個人資料保護推動委員會」每年召開會議檢討本校可接受之風險值，針對高於可接受風險值之檔案，應由各單位業務承辦人員對需降低風險值之個人資料檔案，擬訂「PIMS-P-004-03-個資風險處理計畫」，確認風險處理計畫執行達到風險減緩預期目標。 十、 根據中華民國個人資料保護法與施行細則與個人資料當事人請求，並且尊重當事人對個人資料相關權利之行使，確保當事人權利有效處理。個人資料權利行使之申請人應填寫「PIMS-P-010-01-當事人權利行使第一類申請表) 」或「PIMS-P-010-02-當事人權利行使第二類申請表」，處理期限與過程應依個人資料保護法與施行細則執行。
控制重點	一、單位個人資料蒐集、保存期限、使用之合理性。 二、各單位定期執行個人資料鑑別與盤點、風險評鑑等相關作業。 三、個人資料相關權利行使應確保當事人請求有效處理，處理期限與過程應依個人資料保護法與施行細則要求執行。
法令依據	一、個人資料保護法與施行細則。 二、教育體系資通安全暨個人資料管理規範。 三、本校個人資料保護管理制度(PIMS)。

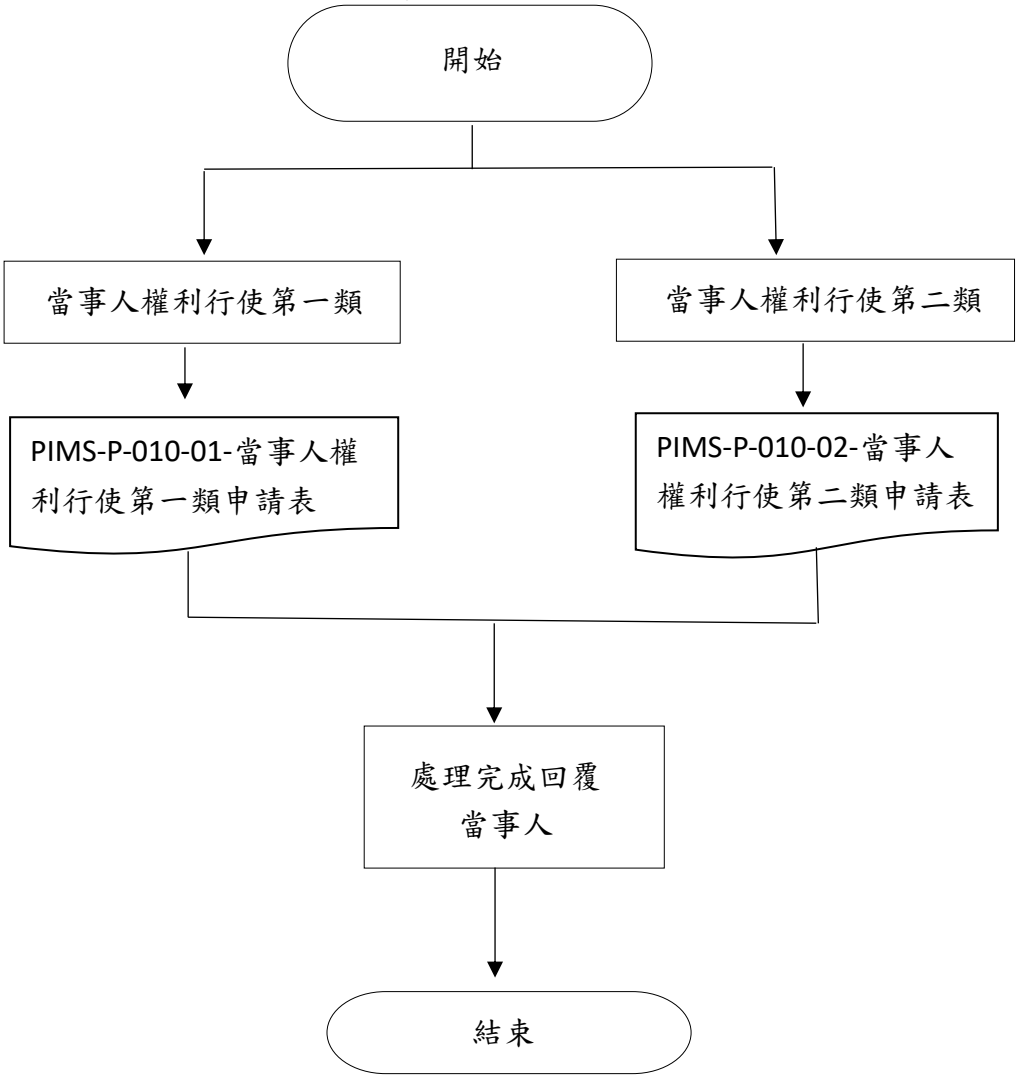
使用表單	一、 PIMS-P-003-01-個人資料項目盤點表 二、 PIMS-P-004-01-個資檔案風險評估彙整表 三、 PIMS-P-004-02-個資風險評估報告 四、 PIMS-P-004-03-個資風險處理計畫 五、 PIMS-P-010-01-當事人權利行使第一類申請表 六、 PIMS-P-010-02-當事人權利行使第二類申請表

資訊中心 個人資料保護管理 作業流程圖

個人資料保護管理



當事人權利行使


開始
當事人權利行使第一類
當事人權利行使第二類
PIMS-P-010-01-當事人權利行使第一類申請表
PIMS-P-010-02-當事人權利行使第二類申請表
處理完成回覆當事人
結束

資訊中心內部控制制度控制作業自行評估表

_____年度

評估單位：資訊中心

作業類別(項目)：個人資料保護管理

評估期間：○○年○○月○○日至○○年○○月○○日

評估日期：○○年○○月○○日

滾動式修正風險評量表：

	發生可能性(L)	影響程度(I)	風險值(R)=(L)×(I)
前期風險評量			
本期風險評量			

控制重點	評估情形					改善措施
	落實	部分落實	未落實	不適用	其他	
一、單位個人資料蒐集、保存期限、使用之合理性。						
二、各單位定期執行個人資料鑑別與盤點、風險評鑑等相關作業。						
三、個人資料相關權利行使應確保當事人請求有效處理，處理期限與過程應依個人資料保護法與施行細則要求執行。						
填表人：　　複核：						

註：

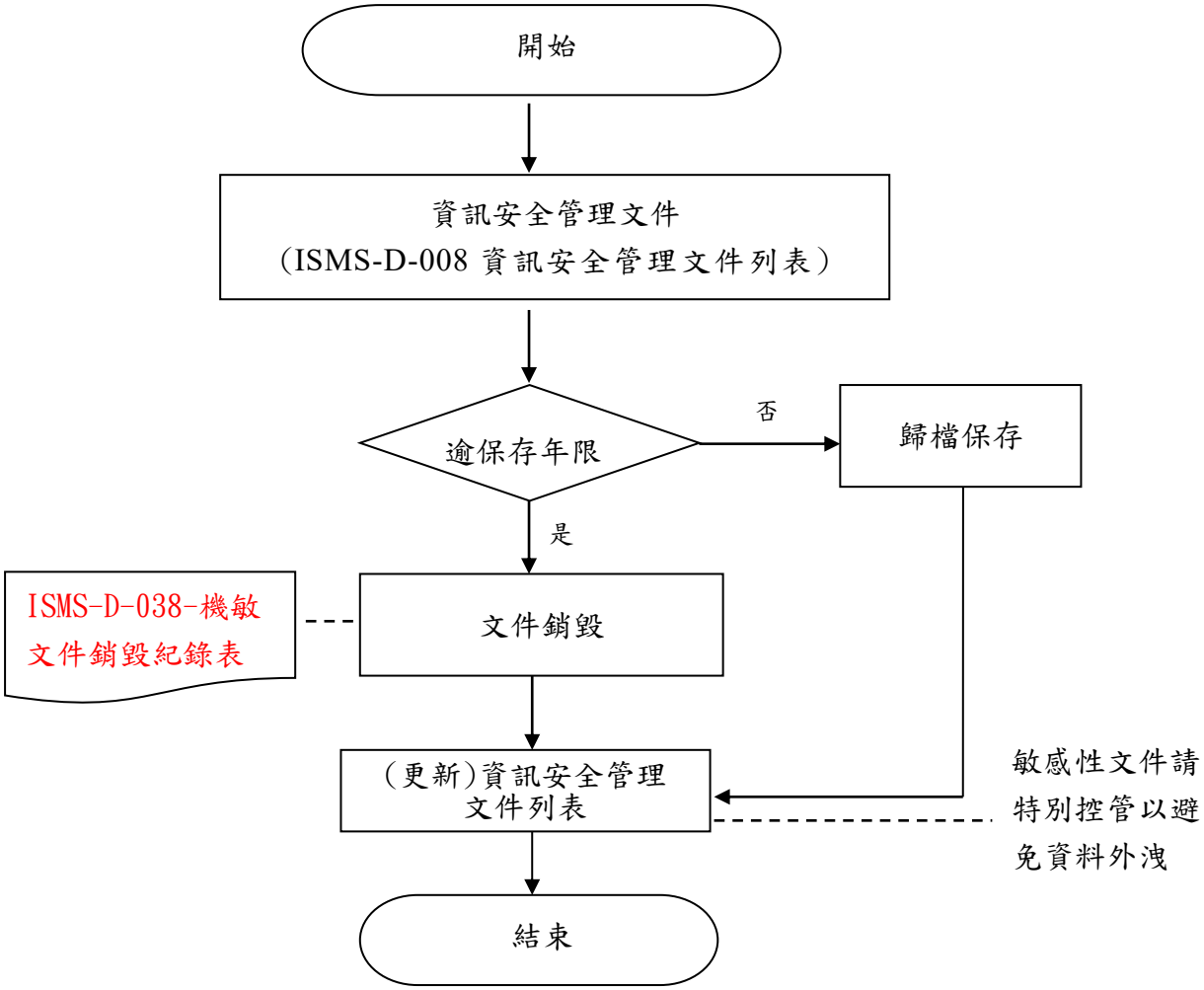
1.單位得就 1 項作業流程製作 1 份自行評估表，亦得將各項作業流程依性質分類，同 1 類之作業流程合併 1 份自行評估表，將作業流程之控制重點納入評估。

2.各單位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。

資訊中心作業程序說明表

項目編號	TCX005
項目名稱	文件管理
承辦單位	資訊中心網路組
作業程序說明	一、「資通安全及個人資料保護種子人員」協助管制、保管、維護、建檔資訊安全管理相關文件，將其鎖在安全的儲櫃或其他安全場所，並建立「ISMS-D-008-資訊安全管理文件列表」列管。 二、文件須分類歸檔，並依使用者職權賦予適當之文件存取權限，對於具機密性資料及文件，於文件、表單上載明為「限閱文件」，應特別控管以避免資料外洩。 三、單位承辦人保有之敏感文件，不需使用時應置放於上鎖之安全儲櫃或其他安全場所內。 四、使用影印機、印表機、傳真機、掃描機或多功能事務機後，應立即將紙本資料取走。 五、敏感紙本文件不再使用時，嚴禁挪為廢紙回收再使用，應以碎裂。 六、敏感（含）以上文件應以碎紙機銷毀或焚毀之方式銷毀，文件銷毀前應取得「權責主管」同意，並將銷毀結果記錄於「ISMS-D-038 機敏文件銷毀紀錄表」。 七、含個人資料之紀錄紙本文件請依相關法令規定或契約保存年限保管，不再使用時請銷毀或依相關法令規定妥善處理，個資文件保留以最小化為原則。
控制重點	一、資訊安全管理相關文件應管制、保管、維護，將其鎖在安全的儲櫃或其他安全場所。 二、敏感文件廢止時，應依相關法令規定妥善處理。敏感文件之廢止填寫「ISMS-D-038 機敏文件銷毀紀錄表」。
法令依據	一、 資通安全管理法與施行細則。 二、 資通安全責任等級分級辦法。 三、 個人資料保護法與施行細則。 四、 教育部「校園通用資安管理原則」。 五、 國際標準 ISO 27001:2013 資訊安全管理制度。 六、 本校資訊安全管理制度(ISMS)。 七、 教育體系資通安全暨個人資料管理規範。 八、 本校個人資料保護管理制度(PIMS)
使用表單	ISMS-D-008-資訊安全管理文件列表 ISMS-D-038 機敏文件銷毀紀錄表

資訊中心 文件管理 作業流程圖



資訊中心內部控制制度控制作業自行評估表

_____年度

評估單位：資訊中心

作業類別(項目)：文件管理

評估期間：○○年○○月○○日至○○年○○月○○日

評估日期：○○年○○月○○日

滾動式修正風險評量表：

	發生可能性(L)	影響程度(I)	風險值(R)=(L)×(I)
前期風險評量			
本期風險評量			

控制重點	評估情形					改善措施
	落實	部分落實	未落實	不適用	其他	
資訊安全管理相關文件應管制、保管、維護，將其鎖在安全的儲櫃或其他安全場所。						
敏感文件廢止時，應依相關法令規定妥善處理。敏感文件之廢止填寫「ISMS-D-038 機敏文件銷毀紀錄表」。						
填表人： 複核：						

註：

1.單位得就 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，將作業流程之控制重點納入評估。

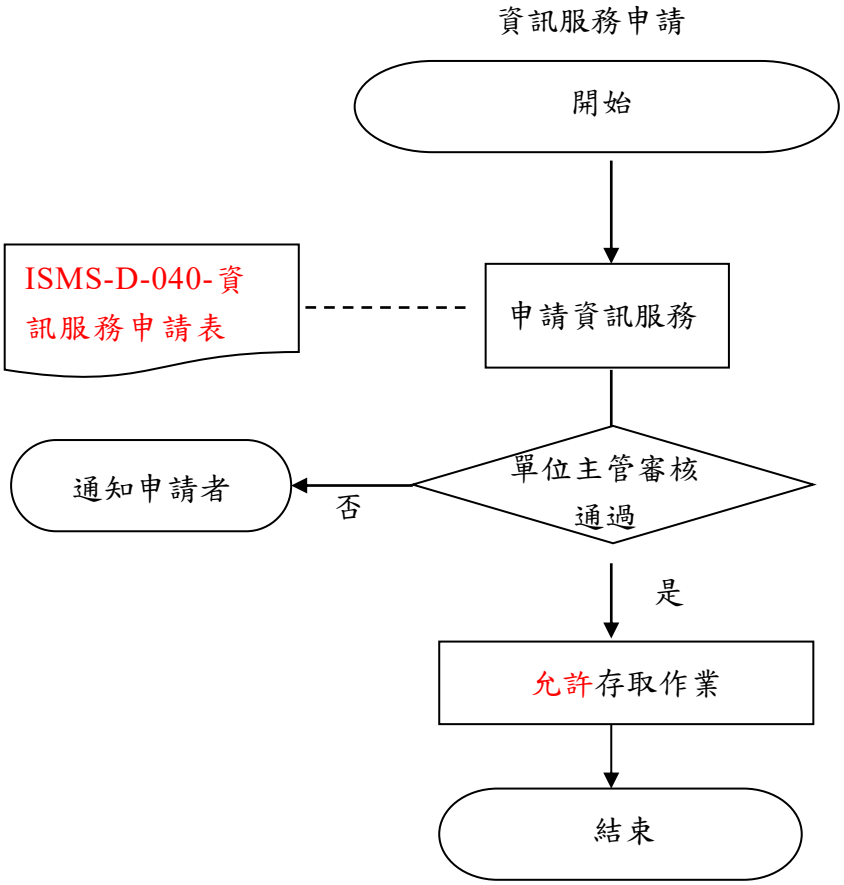
2.各單位依評估結果於評估情形欄勾選「落實」、「部分落實」、「未落實」、「不適用」或「其他」；其中「不適用」係指評估期間法令規定或作法已修正，但控制重點未及配合修正者；「其他」係指評估期間未發生控制重點所規範情形等，致無法評估者；遇有「部分落實」、「未落實」或「不適用」情形，於改善措施欄敘明需採行之改善措施。

資訊中心作業程序說明表

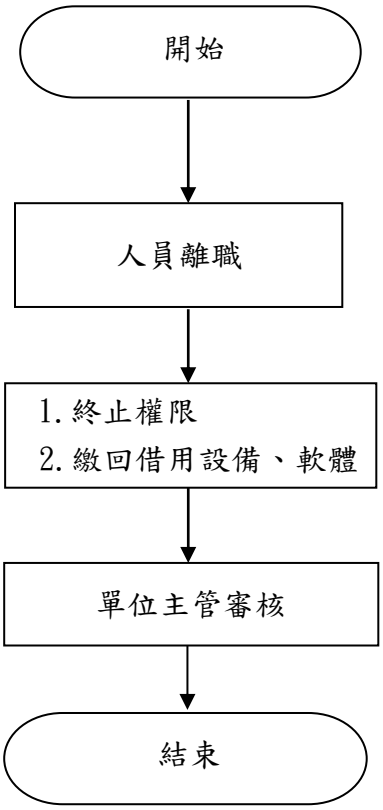
項目編號	TCX006
項目名稱	通訊與作業管理
承辦單位	資訊中心網路組
作業程序說明	儲存管理 一、 電腦儲存設備、可攜式資訊媒體若需連接資訊媒體設備或網路時，應先進行電腦病毒掃描，確認無問題後始可使用。 二、 機敏性資料若儲存於電腦儲存設備、可攜式資訊媒體，應考量使用加密技術或其他技術加強安全控管。 三、 重要之儲存媒體(含機敏性資料之電腦儲存設備)、可攜式資訊媒體，不使用時應置放於實體安全區域及環境（如：門禁控管辦公區域內之上鎖之防潮箱、書櫃）或由專人管理，僅經授權或簽署保密協議後方可使用。 存取管理 一、 使用者職務異動或離職時，應即時通知相關單位調整或終止使用者之存取權限。 二、 使用者經正式授權存取業務相關之系統資料時，其識別資料與帳號必須為唯一，禁止借用他人之帳號或共用帳號。 三、 重要資訊系統及特殊權限之存取帳號之密碼變更期間應較一般權限之帳號頻繁。 四、 使用者或委外廠商之人員如因作業需求，需對系統進行存取，請填寫「ISMS-D-040-資訊服務申請表」提出申請，經主管授權或允許執行存取作業。「ISMS-D-040-資訊服務申請表」中應載明作業需求內容、所需權限、帳號有效時間，由系統管理者依照所需權限及帳號有效時間，建立必要之帳號供使用。
控制重點	一、機敏性資料若儲存於電腦儲存設備、可攜式資訊媒體，應使用加密技術或其他技術加強安全控管。 二、使用者職務異動或離職時，應即時通知相關單位調整或終止使用者之存取權限。 三、使用者或委外廠商之人員如因作業需求，需對系統進行存取，應填寫「ISMS-D-040-資訊服務申請表」提出申請。
法令依據	一、 資通安全管理法與施行細則。 二、 資通安全責任等級分級辦法。 三、 個人資料保護法與施行細則。 四、 國際標準 ISO 27001:2013 資訊安全管理制度。 五、 本校資訊安全管理制度(ISMS)。 六、 本校個人資料保護管理制度(PIMS)。

	七、 教育部「校園通用資安管理原則」。
使用表單	ISMS-D-040-資訊服務申請表

資訊中心 通訊與作業管理 作業流程圖



人員離職



資訊中心內部控制制度控制作業自行評估表

_____年度

評估單位：資訊中心

作業類別(項目)：通訊與作業管理

評估期間：○○年○○月○○日至○○年○○月○○日

評估日期：○○年○○月○○日

滾動式修正風險評量表：

	發生可能性(L)	影響程度(I)	風險值(R)=(L)×(I)
前期風險評量			
本期風險評量			

控制重點	評估情形					改善措施
	落實	部分落實	未落實	不適用	其他	
一、機敏性資料若儲存於電腦儲存設備、可攜式資訊媒體，應使用加密技術或其他技術加強安全控管。						
二、使用者職務異動或離職時，應即時通知相關單位調整或終止使用者之存取權限。						
三、使用者或委外廠商之人員如因作業需求，需對系統進行存取，應填寫「ISMS-D-040-資訊服務申請表」提出申請。						
填表人： 複核：						

註：

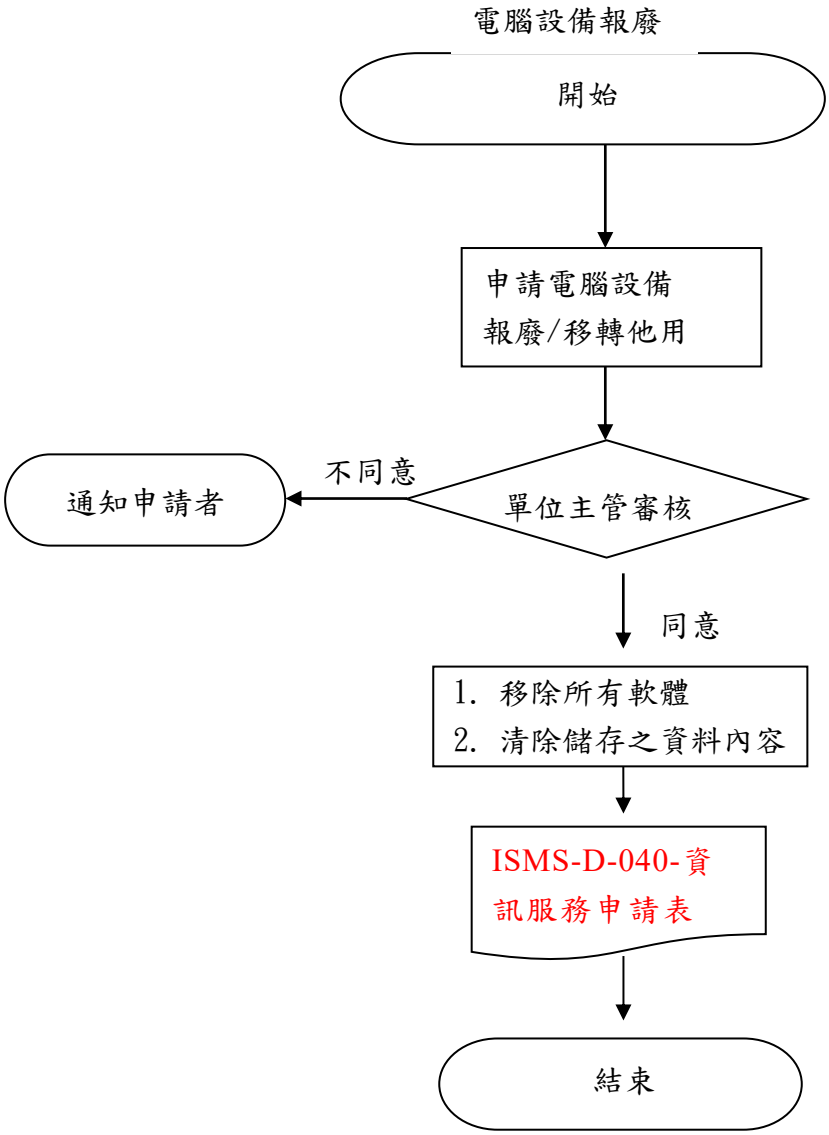
1.單位得就 1 項作業流程製作 1 份自行評估表，亦得將各項作業流程依性質分類，同 1 類之作業流程合併 1 份自行評估表，將作業流程之控制重點納入評估。

2.各單位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。

資訊中心作業程序說明表

項目編號	TCX007
項目名稱	實體與環境安全控管
承辦單位	資訊中心網路組
作業程序說明	一、 無人時或下班最後一人離開時，需將辦公室關門上鎖。 二、 於單位安全區域與辦公室內需隨時注意身分不明或可疑的人員。發現不明身分之人員時，需主動詢問並儘速通知相關單位進行處理。 三、 若外部人員或單位內部未具機房或管制場所進出權限之人員，因執行業務需求進入該場所時，應指派人員隨行並填寫「ISMS-D-019-人員進出機房登記表」後方可進出。 四、 報廢後移作他用之電腦設備，請移除所有軟體(含作業系統與應用軟體等)並清除儲存之資料內容。 五、 儲存機敏性資料檔案之電腦或相關設備，於報廢或移轉他用時，應利用資料清除軟體工具，清除儲存之內容，確認所儲存之資料已清除且無法還原閱讀其內容。 六、 軟、硬體資訊資產報廢時，應更新修改「ISMS-D-009 資訊資產清單」，經單位主管審核並確認資料、軟體清除後，方可進行資訊資產報廢程序。
控制重點	一、外部人員或單位內部未具機房或管制場所進出權限之人員進出該場所時，應指派人員隨行並填寫「ISMS-D-019-人員進出機房登記表」。 二、報廢後移作他用之電腦設備，應移除所有軟體(含作業系統與應用軟體等)並清除儲存之資料內容。 三、軟、硬體資訊資產報廢時，應更新修改「ISMS-D-009-資訊資產清單」。
法令依據	一、 資通安全管理法與施行細則。 二、 資通安全責任等級分級辦法。 三、 個人資料保護法與施行細則。 四、 國際標準 ISO 27001:2013 資訊安全管理制度。 五、 教育部「校園通用資安管理原則」。 六、 本校資訊安全管理制度(ISMS)。 七、 本校個人資料保護管理制度(PIMS)。
使用表單	一、 ISMS-D-019-人員進出機房登記表 二、 ISMS-D-009-資訊資產清單

資訊中心 實體與環境安全控管 作業流程圖



資訊中心內部控制制度控制作業自行評估表

_____年度

評估單位：資訊中心

作業類別(項目)：實體與環境安全控管

評估期間：○○年○○月○○日至○○年○○月○○日

評估日期：○○年○○月○○日

滾動式修正風險評量表：

	發生可能性(L)	影響程度(I)	風險值(R)=(L)×(I)
前期風險評量			
本期風險評量			

控制重點	評估情形					改善措施
	落實	部分落實	未落實	不適用	其他	
一、外部人員或單位內部未具機房或管制場所進出權限之人員進出該場所時，應指派人員隨行並填寫「ISMS-D-019-人員進出機房登記表」。						
二、報廢後移作他用之電腦設備，應移除所有軟體(含作業系統與應用軟體等)並清除儲存之資料內容。						
三、軟、硬體資訊資產報廢時，應更新修改「ISMS-D-009-資訊資產清單」。						
填表人：　　複核：						

註：

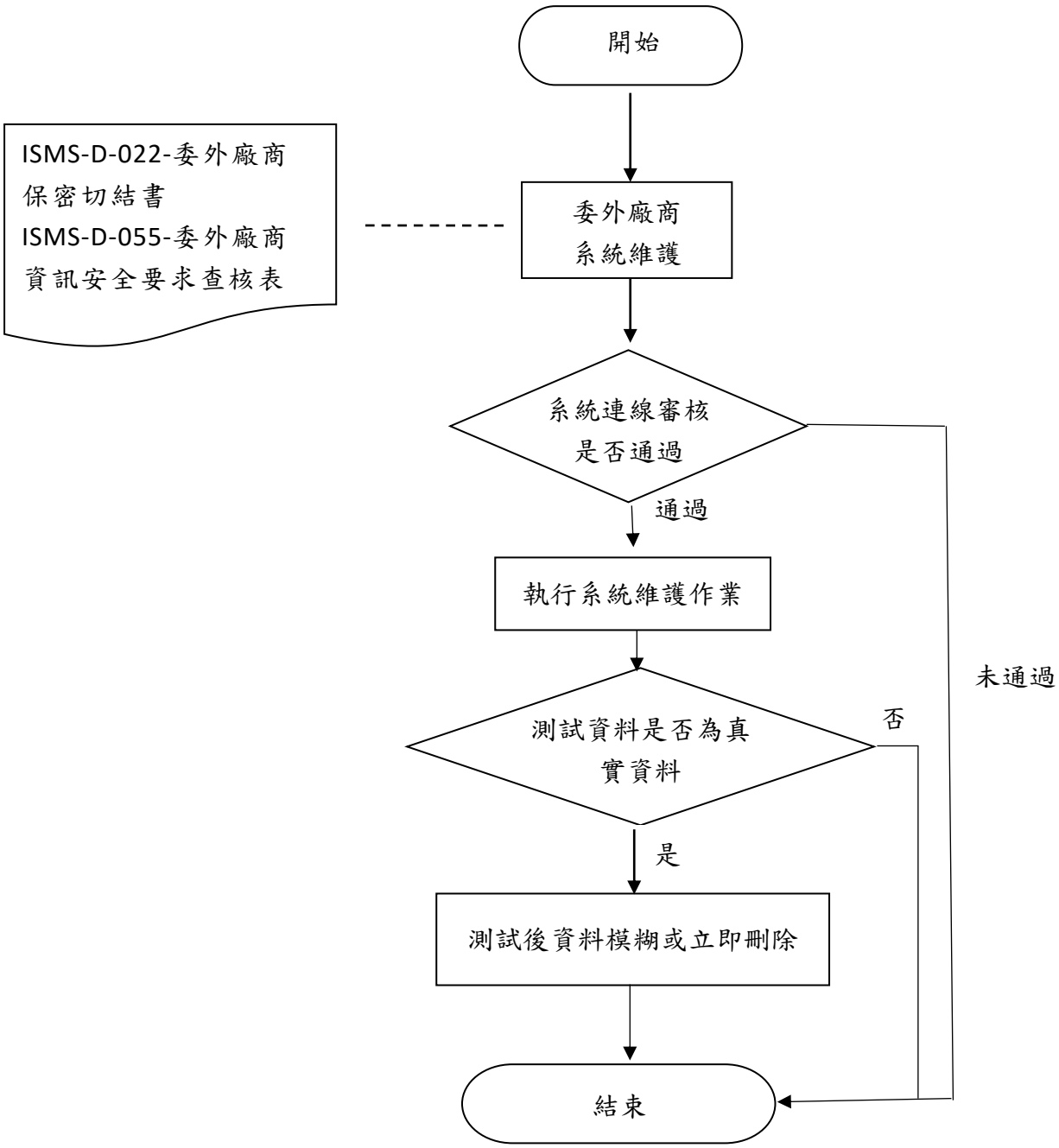
1.單位得就 1 項作業流程製作 1 份自行評估表，亦得將各項作業流程依性質分類，同 1 類之作業流程合併 1 份自行評估表，將作業流程之控制重點納入評估。

2.各單位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。

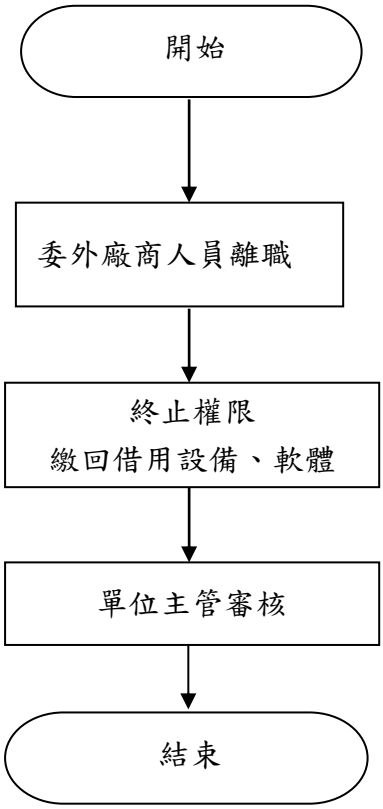
資訊中心作業程序說明表

項目編號	TCX008
項目名稱	委外廠商管理
承辦單位	資訊中心網路組
作業程序說明	一、委外、租賃或購買套裝應用資訊系統時，請依「ISMS-B-010-委外管理程序書」辦理。 二、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機敏性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），及權限控管及留存稽核紀錄。 三、委外廠商於支援執行業務時，處理之個人資料或獲知敏感等級(含)以上資訊，應遵守「個人資料保護法」及本校之相關規定，不得對外透露、任意複製或攜出機密性之業務資料，為確保前述事項之落實，要求廠商及其人員簽署「ISMS-D-022-委外廠商保密切結書」與「ISMS-D-055-委外廠商資訊安全要求查核表」，更換廠商或人員時亦同。 四、自行開發或委外處理個人資料檔案之資訊系統，避免以真實個人資料進行測試，如需使用，完成測試作業後立即移除，或將可辨識之個人資料修改為無法辨識之模糊資訊。 五、委外廠商相關系統之開發或負責人員離職時，應繳回其所借用之設備、軟體及終止作業權限。
控制重點	一、接觸、處理機敏性資訊之委外廠商人員應簽署「ISMS-D-022-委外廠商保密切結書」與「ISMS-D-055-委外廠商資訊安全要求查核表」。 二、委外廠商相關系統之開發或負責人員離職時，應繳回其所借用之設備、軟體及終止作業權限。
法令依據	一、資通安全管理法與施行細則。 二、資通安全責任等級分級辦法。 三、個人資料保護法與施行細則。 四、國際標準 ISO 27001:2013 資訊安全管理制度。 五、教育部「校園通用資安管理原則」。 六、本校資訊安全管理制度(ISMS)。 七、本校個人資料保護管理制度(PIMS)
使用表單	一、ISMS-D-022-委外廠商保密切結書 二、ISMS-D-055-委外廠商資訊安全要求查核表

資訊中心 委外廠商管理 作業流程圖



委外廠商人員離職



資訊中心內部控制制度控制作業自行評估表

_____年度

評估單位：資訊中心

作業類別(項目)：委外廠商管理

評估期間：○○年○○月○○日至○○年○○月○○日

評估日期：○○年○○月○○日

滾動式修正風險評量表：

	發生可能性(L)	影響程度(I)	風險值(R)=(L)×(I)
前期風險評量			
本期風險評量			

控制重點	評估情形					改善措施
	落實	部分落實	未落實	不適用	其他	
一、接觸、處理機敏性資訊之委外廠商人員應簽署「ISMS-D-022-委外廠商保密切結書」與「ISMS-D-055-委外廠商資訊安全要求查核表」。						
二、委外廠商相關系統之開發或負責人員離職時，應繳回其所借用之設備、軟體及終止作業權限。						
填表人：　　複核：						

註：

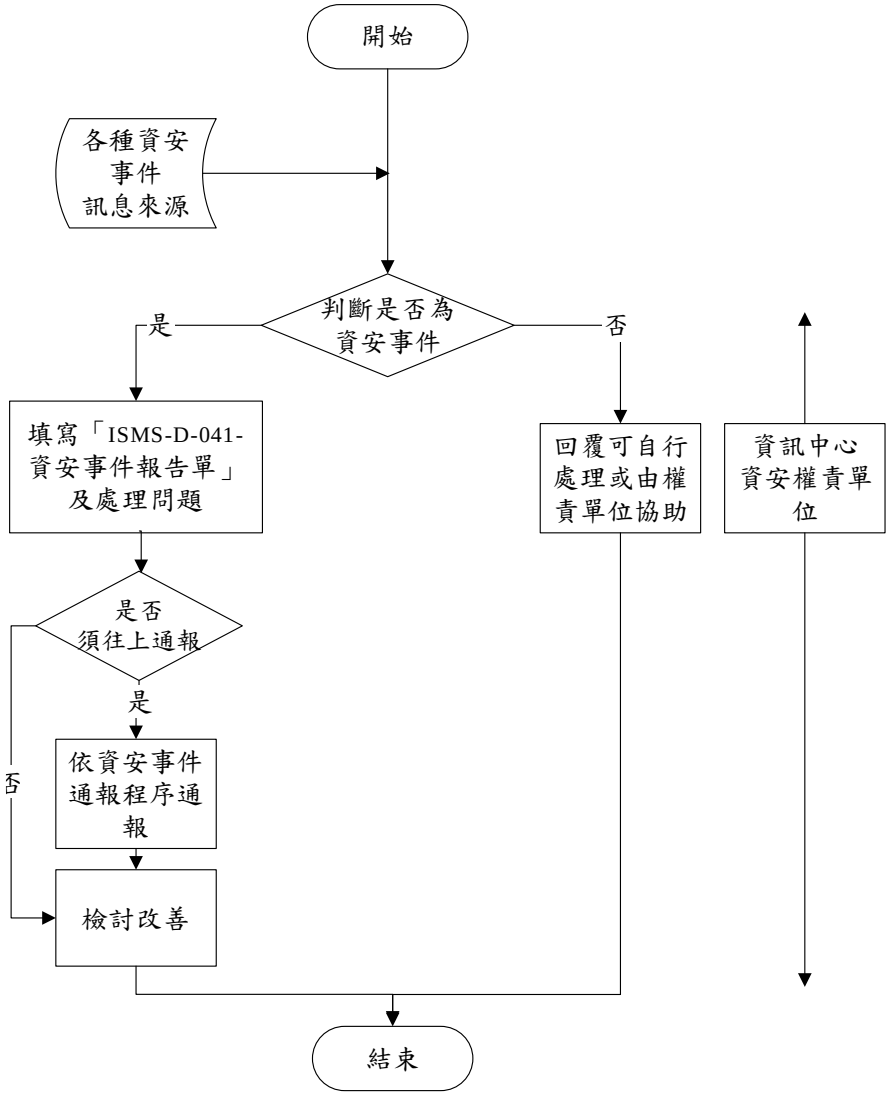
1.單位得就 1 項作業流程製作 1 份自行評估表，亦得將各項作業流程依性質分類，同 1 類之作業流程合併 1 份自行評估表，將作業流程之控制重點納入評估。

2.各單位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。

資訊中心作業程序說明表

項目編號	TCX009
項目名稱	資通安全事件處理
承辦單位	資訊中心網路組
作業程序說明	為即時掌控資通安全事件，並有效降低其所造成之損害，本校應訂定資通安全事件通報、應變及演練相關機制，詳如本校 ISMS 安全事件管理程序書 5 作業說明。 【文件編號:YUNTECH-ISMS-B-011 名稱：安全事件管理程序書】
控制重點	一、於發生資安事件時，應依通報作業程序，於規定的期限內，至「教育機構資安通報平台」通報登錄資安事件(https://info.cert.tanet.edu.tw/)。 二、應建立入侵偵測及防禦機制、執行安全掃描及弱點檢測等安全檢測工作。 三、本校應依訂定之應變程序處置，事後彙整事件之處置過程紀錄、解決方案及強化措施等資訊，並檢討應變作業。
法令依據	一、資通安全管理法與施行細則。 二、資通安全事件通報及應變辦法。 三、國際標準 ISO 27001:2013 資訊安全管理制度。 四、本校資訊安全管理制度(Information Security Management System, ISMS)。 五、臺灣學術網路各級學校資通安全通報應變作業程序。
使用表單	ISMS-D-041-資訊安全事件報告單。

資訊中心 資通安全事件處理 作業流程圖



資訊中心內部控制制度控制作業自行評估表

_____年度

評估單位：資訊中心

作業類別(項目)：資通安全事件處理

評估期間：○○年○○月○○日至○○年○○月○○日

評估日期：○○年○○月○○日

滾動式修正風險評量表：

	發生可能性(L)	影響程度(I)	風險值(R)=(L)×(I)
前期風險評量			
本期風險評量			

控制重點	評估情形					改善措施
	落實	部分落實	未落實	不適用	其他	
一、於發生資安事件時，應依通報作業程序，於規定的期限內，至「教育機構資安通報平台」通報登錄資安事件(https://info.cert.tanet.edu.tw/)						
二、應建立入侵偵測及防禦機制、執行安全掃描及弱點檢測等安全檢測工作。						
三、本校應依訂定之應變程序處置，事後彙整事件之處置過程紀錄、解決方案及強化措施等資訊，並檢討應變作業。						
填表人：			複核：			

註：

1.單位得就 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，將作業流程之控制重點納入評估。

2.各單位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。