管理系統文件

文件類別	第二階文件	
文件編號	ISMS-P-010	
文件名稱	人力資源安全管理程序書	
發行單位	文件管制小組	
發行日期	106年09月08日	
版　　次	B	
訂修廢單位	審　　查	核　　准
資通安全處理小組	資訊網路中心 中心主任 華國棟	行政 副校長 翁順祥

（原版簽名頁保存於文件管制小組）

訂　　修　　廢　　記　　錄		
版次	發行日期	訂 修 廢 內 容 摘 要
A	104/07/06	初版發行
B	106/09/08	1.新增「ISMS-P-010-04 工作職掌表」

1. 目的

為促使本校資訊安全相關工作人員於任用、任職期間及離（調）職作業有一明確之安全規範，以減少人為過失、偷竊、詐欺、濫用及誤用資訊設施所造成之風險，特制定本程序書。

2. 適用範圍

凡本校正職、約聘(雇)、委外及臨時人員之安全管理，皆適用本程序書。

3. 參考文件

3.1. ISMS-W-002 一般資訊設備安全管理作業標準書。

3.2. ISMS-P-018 委外作業管理程序書。

3.3. ISMS-P-009 資訊安全事件管理程序書。

3.4. ISMS-P-013 帳號密碼及存取控制管理程序書。

4. 名詞定義

4.1. 員工

泛指本校編制內人員、聘用人員及約僱人員。

5. 作業內容

5.1. 人力資源安全管理流程圖

作業流程	權責單位	相關表單
任用前安全管理	資通安全處理小組	工作職掌表
任職期間安全管理	資通安全處理小組 資訊安全長	員工保密切結書
人員教育訓練管理	資通安全處理小組	教育訓練計畫表 教育訓練上課紀錄表
人員異動安全管理	資通安全處理小組	員工保密切結書
職務終止安全管理	資通安全處理小組	員工保密切結書
紀錄保存	相關業務承辦人員	

5.2. 任用前之安全要求

5.2.1. 員工應詳讀及遵守本校「資訊安全政策」及資訊安全相關之管理規範，並了解與本身所執行業務相關之工作責任與安全要求。

5.2.2. 各管理人員之專業能力應由直屬主管依其職務及功能劃分，將職務工作項目載明於「ISMS-P-010-04 工作執掌表」中，以明確定義職位角色與職務責任。

5.2.3. 為持續維持重要（核心）資訊系統之營運、管理、操作及維護作業，不致因員工休假而耽誤本校業務之正常運作，應建立職務代理人制度及人力備援機制，並將員工之資安責任、業務職掌及代理人載明於「ISMS-P-010-04 工作執掌表」，並適時更新。

5.2.4. 各項業務必須由主管指定專責之負責人及代理人，於業務負責期間擔負或代理業務之管理工作，並配合資訊安全政策之要求，進行安全管理。

5.3. 任職期間之安全管理

5.3.1. 人員安全管理

5.3.1.1. 主管應要求員工確實依本校資訊安全政策及各項安全管理作業規範與程序執行相關業務。

5.3.1.2. 本校員工於服務期間皆應遵守本校「ISMS-W-002 一般資訊設備安全管理作業標準書」之安全守則，於業務上所獲知之機密資訊，非經主管授權不得對外透露。

5.3.1.3. 機密等級屬「機敏」以上的重要資訊或足以影響本校業務永續運作管理的資訊，不可只由單獨一人知悉。如由單獨一人運作管理時，應有主管進行必要之監督與審查。

5.3.1.4. 本校新進用或經驗不足的人員，於授權的敏感性資訊系統執行管理作業之存取時，必須由管理者協助與監督。

5.3.1.5. 在丟棄任何曾經儲存本校機密資訊之電子媒介前，應將電子媒介中的資訊刪除，並徹底消磁或銷毀至無法解讀之程度。

5.3.1.6. 含有「密」等級（含）以上資訊之紙本文件不再使用時，應

以碎紙機銷毀該份紙本文件，並刪除電子檔。

5.3.1.7. 重要機密文件或合約，應妥善保存。若為電子檔案應考慮設定保護密碼。

5.3.1.8. 所有人員應留意各相關資訊資產對應之機密等級，防止資訊不當外洩。

5.3.1.9. 本校員工應恪遵「個人資料保護法」之規範，保護本校個人資料使用之合法性、機密性與完整性。

5.3.1.10. 本校業務承辦人員應以適當方式（如：網站）隨時向員工公告最新的資訊安全相關訊息，以提升本校員工資訊安全認知。

5.3.1.11. 委外人員之管理規範，請依據「ISMS-P-018 委外作業管理程序書」之規定辦理。

5.3.2. 違反資通安全規定

5.3.2.1. 員工執行業務時，若違反本校資訊安全政策、資訊安全管理規範及相關法令法規，或發生其他任何危及本校資訊安全之行為（如電腦洩密、盜取個人資料…等），都將依正式懲戒程序處置相關違紀人員或訴諸法律行動。

5.3.2.2. 內部員工違反內部規定或怠忽職守，單位主管視其情節輕重，予以口頭懲戒或再教育。如情節較重者將報請資訊安全長處理。

5.3.2.3. 內部員工應瞭解於工作期間所有取得之資訊皆為本校之資產，未經允許禁止做任何其他未授權之使用。

5.3.3. 員工保密協定

5.3.3.1. 本校人事業務承辦人員應要求新進人員及所屬員工簽署「ISMS-P-010-01 員工保密切結書」，使員工充分了解所執行業務之工作責任與安全要求，以克盡保密之責。

5.3.3.2. 所屬員工皆須簽署「ISMS-P-010-01 員工保密切結書」，承諾任職期間，因職務上所獲悉或持有之任何營運上的機密，非經主管授權不得對外透露或加以濫用。

5.3.4. 資訊安全事件通報責任

5.3.4.1. 本校所有員工與委外廠商人員於資訊安全事件發生時，應依據「ISMS-P-009 資訊安全事件管理程序書」之通報程序，通知相關負責人員。

5.3.4.2. 本校員工若發現資訊系統可疑的弱點或可能對資訊系統造成傷害的威脅時，應向「資通安全處理小組」通報。

5.3.4.3. 其他有關資訊安全事件通報之管理規範，請參考「ISMS-P-009 資訊安全事件管理程序書」之相關規定。

5.3.4.4. 當資訊安全事件發生且涉及法律時，須由「資通安全處理小組」配合警調單位進行蒐證。

5.4. 人員教育訓練之管理

5.4.1. 訓練需求提出

5.4.1.1. 為提升本校員工安全意識與專業知識，主管單位每年應編列資訊安全教育訓練經費，規劃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。

5.4.1.2. 主管可配合人事單位鑑別本校各單位員工各項業務之專業訓練需求，並實施必要之資安教育訓練，以確保適任各項資安工作。

5.4.1.3. 訓練目的為促使所有員工瞭解資訊安全之重要性及各種可能的安全風險，並說明違反資訊安全規定時可能招致處罰及法律責任，以提高本校員工資訊安全意識，降低人為錯誤或故意誤用資訊之風險。

5.4.2. 擬定訓練計畫

本校應對資訊安全訓練需求擬定訓練計畫，訓練內容應包括：本校「資訊安全政策」、資訊安全管理規範及資訊安全相關法令法規等。一般資安訓練計畫有如下之類別。

5.4.2.1. 定期訓練

訓練業務承辦人應擬定年度之「ISMS-P-010-02 教育訓練計畫表」，經權責主管核准後安排教育訓練。訓練內容主要以

增進本職學能為主。

5.4.2.1.1. 需依其角色與職務，接受相關資訊安全教育訓練：

A. 本校主管級以上人員，每年應至少參加 3 小時以上（含）之資訊安全相關訓練。

B. 本校資安（訊）人員，每年應至少參加 12 小時以上（含）之資訊安全相關訓練。

C. 本校一般員工，每年應至少參加 3 小時以上（含）之資訊安全相關訓練。

5.4.2.2. 臨時訓練

訓練業務承辦人除每年度擬訂「ISMS-P-010-02 教育訓練計畫表」之外，若發生臨時訓練需求，仍須擬訂「ISMS-P-010-02 教育訓練計畫表」，經主管核准後使得安排訓練。

5.4.2.3. 新進人員訓練

本校新進人員於正式執行操作之前，應先由訓練業務承辦人擬定「ISMS-P-010-02 教育訓練計畫表」，經主管核准後安排訓練，內容以瞭解本校資安規範及其所擔任職務應具備之專業知識為主。

5.4.2.4. 外部訓練

本校同仁有外部訓練需求時，須擬定「ISMS-P-010-02 教育訓練計畫表」，經資安長核准後，始得報名參加訓練。

5.4.3. 訓練執行

5.4.3.1. 內部訓練

辦理各類內部訓練時，應於上課前通知講師及受訓人員，並請受訓人員於上課時，在「ISMS-P-010-03 教育訓練上課紀錄表」上簽到，並於課後與其他訓練紀錄存檔備查，以作為日後稽查之佐證。

5.4.3.2. 外部訓練

5.4.3.2.1. 員工至外部機構參加資訊安全各類訓練後，應取得上課（結業）證明文件或教育訓練等相關紀錄文件，呈權責

主管核閱後交專責人員保管。

5.4.3.2.2. 員工完成外部訓練後，可視業務需要於本校辦理相關課程，以充實其他人員資訊安全知識，促其遵守資訊安全相關規定，促進學習移轉的成效。

5.4.4. 成效評估

5.4.4.1. 完成辦理各類訓練後，應由授課講師進行必要之訓練成效評估，以確認教育訓練之有效性。可採用如下方式進行：

5.4.4.1.1. 課堂隨機抽問。

5.4.4.1.2. 案例討論。

5.4.4.1.3. 隨堂測驗。

5.4.4.1.4. 分組討論。

5.4.4.1.5. 實地操作及演練。

5.5. 人員異動及職務終止之安全要求

5.5.1. 員工離（停）職

5.5.1.1. 內部人員離（調）職時，由各系統管理者依本校「教職員工離職手續表」之生效日一個月內，將離（調）職人員所有使用之系統帳號及存取權限停用或移除。

5.5.1.2. 員工離（停）職時，應辦妥移交手續，並將於執行業務時所擁有及使用之資訊資產移交給下一個負責人或歸還原單位，並依相關作業規範辦理調整或終止相關資源之存取權限。

5.5.1.3. 員工於離（停）職後，應根據「ISMS-P-010-01 員工保密切結書」之要求，持續負有資訊保密之責任。

5.5.2. 員工調職

5.5.2.1. 本校員工調職時，由各系統管理者依本校人事單位所通知之調職日期，將調職員工所有原使用之系統帳號及存取權限停用或移除。

5.5.2.2. 員工調派至新部門時，若需賦予新職務所需之系統帳號及存取權限時，則依據「ISMS-P-013 帳號密碼及存取控制管理程序書」之相關規定重新提出申請。

5.6. 紀錄保存

相關業務承辦人員應參照如下規範，妥善保存各項紀錄。

編號	表單名稱	保存地點	保存期限
1	員工保密切結書	資網中心	永久保存
2	教育訓練計畫表	資網中心	至少 1 年
3	教育訓練上課紀錄表	資網中心	至少 1 年
4	工作執掌表	資網中心	至少 1 年

6. 附件

6.1. ISMS-P-010-01 員工保密切結書。

6.2. ISMS-P-010-02 教育訓練計畫表。

6.3. ISMS-P-010-03 教育訓練上課紀錄表。

6.4. ISMS-P-010-04 工作執掌表。