國立高雄餐旅大學

NATIONAL KAOHSIUNG UNIVERSITY
OF HOSPITALITY AND TOURISM

「資訊安全管理系統」
人員安全與教育訓練程序書

機密等級：一般

編號：IS-02-005

版本編號：2.2

修定日期：105.12.15

使用本文件前,如對版本有疑問,請與修訂者確認最新版次。

本文件歷次變更紀錄：

版次	修訂日	修訂者	說明	核准者
1.0	100.04.01	資訊安全執行小組	初稿修訂	圖資館 副館長
1.0	100.07.26	資訊安全執行小組	首次發行	圖資館 副館長
1.1	100.10.17	資訊安全執行小組	修訂 5.2.8	圖資館 副館長
1.2	101.08.27	資訊安全執行小組	修訂 5.1.7、5.2.1 及新增 6.6	圖資館 副館長
2.0	104.08.17	資訊安全執行小組	新增 5.4 及 5.5	圖資館 副館長
2.1	105.07.19	資訊安全執行小組	修訂 5.1.7 及 6.4	圖資館 副館長
2.2	105.12.15	資訊安全執行小組	修訂 5.1.3	圖資館 館長

本程序書由 ISMS 執行小組負責維護。

目錄：

1 目的

1.1 規範國立高雄餐旅大學（以下簡稱本校）辦理全體同仁之安全管理及教育訓練，減少人員因資訊安全認知不足所引發之資訊安全事件。

2 適用範圍

2.1 本校正職人員、約聘（僱）人員與委外人員。

3 權責

3.1 資訊安全執行小組負責擬定相關服務規範，以及於契約中提出適當之資訊安全需求。

3.2 資訊安全執行小組負責辦理資訊安全教育訓練相關事宜。

3.3 資訊安全管理代表負責審查服務規範內容，確認是否符合本校相關法規之規定。

4 名詞定義

4.1 無。

5 作業說明

5.1 人員安全管理

5.1.1 本校正職人員、約聘（僱）人員與委外人員皆應遵守資訊安全政策及相關程序書之規範。

5.1.2 本校人員與約聘（僱）人員於服務期間皆應遵守「人員資訊安全守則」，於業務上所獲知之機密資訊，非經主管授權不得對

外透露。

5.1.3 人員若有下列角色或需求時，應填寫「保密切結書」:

5.1.3.1 本校新到職之資訊人員。

5.1.3.2 因執行業務需進入本校網路機房。

5.1.3.3 需遠端連線本校核心系統。

5.1.3.4 廠商駐點人員。

5.1.3.5 需接觸本校「密」等級（含）以上資料之人員。

5.1.3.6 若有下列狀況，經確認後得可不簽署保密切結：

5.1.3.6.1 進入本校網路機房，但未接觸任何設備、資訊，如清潔人員、實體環境施工人員。

5.1.3.6.2 已簽署過保密切結書，且該切結資料尚在保存期限(3年)內。

5.1.4 資訊系統之管理、維護、設計及操作人員之權責分工應明確，得視人員安全與教育訓練程序書需要實施人員輪調，建立人力備援制度，並填寫「人員職掌清冊」。

5.1.5 重要資訊、【密】以上資訊或足以影響本校營運持續運作管理的資訊，不可只由單獨一人知悉。如由單獨一人運作管理時，應有確實的主管監督審查機制。

5.1.6 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。

5.1.7 本校人員離職時，應辦妥移交手續，將「離職人員帳號停用查核表」中所列出的資訊資產移交給下一個負責人，並依相關管理作業規範辦理，於移交日期一週後移除相關資源之存取權限。

5.1.8 本校人員於開發、設計或維護系統時，禁止使用違反智慧財產權相關的軟體、資訊或文件。

5.1.9 本校人員於未經授權核准而使用違反智慧財產權相關的軟體、資訊或文件，應負相關的法令責任。

5.1.10 委外人員之管理規範，請參考「委外管理程序書」之相關規定。

5.2 教育訓練

5.2.1 為提升本校人員之資訊安全意識與專業知識，規劃相關資安教育訓練課程，於年終前提出下年度之教育訓練計畫或派員接受外部單位辦理之專業資安課程，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。

5.2.2 資訊安全教育及訓練的內容宜包括：本校資訊安全政策、資訊安全法令規範、資訊安全作業管理程序、安全責任、各資訊系統之安全防範或資料交換、機密性或敏感性資料之妥善收藏、

如何正確使用資訊設備與資訊管理系統，以及作業相關處理程序之訓練等。

5.2.3 本校新進人員正式執行操作前，應先安排作業及相關處理程序之教育訓練。

5.2.4 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、隨堂測驗之方式進行成效評估。

5.2.5 本校人員接受外部資訊安全訓練結束後，應繳交教育訓練相關資料（例如：結業/上課證明、心得報告或課程講義等），呈直屬主管核閱後交專責人員列冊建檔。

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

5.2.7 對本校人員進行資訊安全教育及訓練之政策，亦適用於約聘（僱）人員及委外駐點人員。

5.2.8 本校得要求委外廠商提供服務人員之資訊安全相關受訓證明，若無相關訓練證明，則應參與本校資訊安全相關教育訓練。

5.2.9 承辦本校之資訊安全教育訓練之負責人，應備妥「教育訓練簽到表」，並於課程結束後將教育訓練紀錄歸檔留存。

5.3 資訊安全事件通報責任

5.3.1 本校人員、約聘（僱）人員與委外人員於任何資訊安全事件發

生時，應依照正式通報程序通知相關負責人員。

5.3.2 資訊系統使用者，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，應隨時向相關單位報告。

5.3.3 其他有關資安事故通報之管理規範，請參考「安全事故管理程序書」之相關規定。

5.3.4 當資訊安全事件發生且涉及法律時，資訊安全管理小組須配合警調單位進行蒐證。

5.4 能力分析與評估

5.4.1 職能分析：

為確保本校執行資訊安全各項作業的人員，皆能有充足之能力來確保資訊安全的運作績效，故資訊安全執行小組應分析各項職務所需之職能，並將分析結果填入「人員職掌清冊」。

5.4.2 職能評估：

資訊安全執行小組應於年度管理審查會議時，提報現有人員職能評估成果，並針對職能落差部份，擬定改善計畫，並取得管理階層之核准。

5.5 溝通與傳達

為確保與內、外部關注者具備有效的溝通與傳達管道，應於年度管理審查時，決定溝通與傳達之事項，包括：

5.5.1 溝通或傳達事項。

5.5.2 溝通或傳達時間。

5.5.3 溝通或傳達對象。

5.5.4 溝通或傳達人員。

5.5.5 進行有效溝通或傳達所採用過程。

6 相關文件

6.1 人員資訊安全守則

6.2 保密切結書

6.3 人員職掌清冊

6.4 離職人員帳號停用查核表

6.5 教育訓練簽到表

6.6 教育訓練計畫