敏惠醫護管理專科學校

「資訊安全管理系統」
資訊安全組織程序書

機密等級：一般

編號：IS-MHCHCM-02-001

版本編號：1.1

制訂日期：112.10.30

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	110.12.30	資訊安全執行小組	初版發行	執行秘書
1.1	112.10.30	資訊安全執行小組	修訂頁首、頁尾、作業說明及相關文件	執行秘書

本程序書由資訊安全執行小組負責維護。

目錄：

1 目的

1.1 促進敏惠醫護管理專科學校（以下簡稱本校）資訊安全管理制度執行之有效性，期使本制度達成既定之目標，以增進業務運作之安全。

2 適用範圍

2.1 本校承辦之資訊安全相關業務作業流程。

3 權責

3.1 詳見本程序書作業說明。

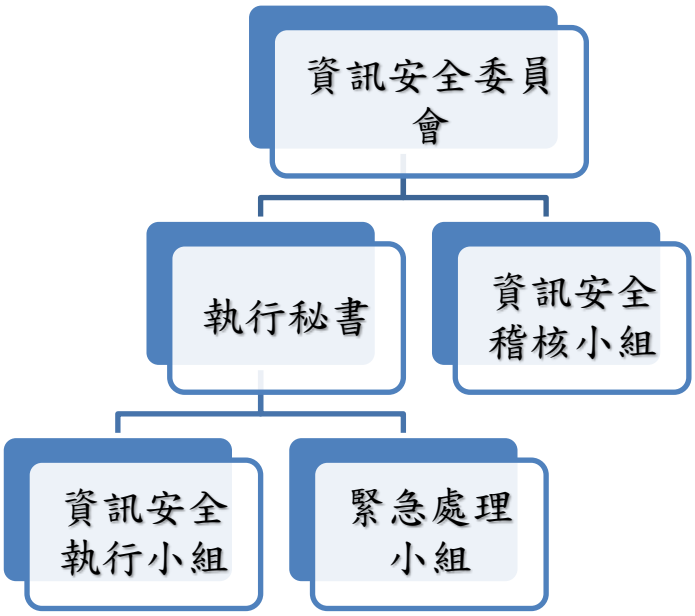
4 名詞定義

4.1 無。

5 作業說明

5.1 資訊安全委員會架構與工作執掌

5.1.1 資訊安全委員會架構如下圖所示：



5.1.2 資訊安全委員會：由本校校長擔任資通安全長及召集人，委員由行政及學術單位一級主管擔任，如因職務調動，應由召集人指派遞補人員與其辦理交接。

5.1.2.1 每年定期或視需要召開會議，審查資訊安全管理相關事宜。

5.1.2.2 視需要召開跨部門之資源協調會議，負責協調資訊安全管理制度執行所需之相關資源分配。

5.1.2.3 資訊安全委員會召集人（以下簡稱召集人）：

5.1.2.3.1 確保資訊安全政策與目標一致性，且切合本校策略方向；

5.1.2.3.2 確保整合 ISMS 要求於本校流程中；

5.1.2.3.3 滿足資訊安全相關要求的承諾；

5.1.2.3.4 溝通有效的 ISMS 與遵循 ISMS 要求的重要性；

5.1.2.3.5 確保 ISMS 達成預定成效；

5.1.2.3.6 指揮與支援人員貢獻於 ISMS 有效性；

5.1.2.3.7 推動持續改善資訊安全管理系統的承諾；

5.1.2.3.8 支援其他管理角色來展現用於負責領域的領導性。

5.1.3 執行秘書：由召集人指派主任秘書擔任。

5.1.3.1 協調資訊安全執行小組與緊急處理小組執行資訊安全相關作業。

5.1.3.2 負責對資訊安全狀況進行預警、監控，並對資訊安全狀況與事件進行處置。

5.1.3.3 對於資訊安全管理之改善提出建議，以及協助執行資訊安全之自我檢核。

5.1.3.4 對於存取控制管理定期進行事件紀錄檢核，以及管理程序檢核。

5.1.4 資訊安全執行小組：由資訊安全委員會指派人員組成，並依『教育部與所屬機關(構)及學校資通安全責任等級分級作業規

定』規定配置一名兼任資通安全專職人員，負責規劃及執行各項資訊安全作業。

5.1.4.1 制定資訊安全管理相關規範。

5.1.4.2 推動資訊安全相關活動。

5.1.4.3 辦理資訊安全相關教育訓練。

5.1.4.4 建立風險管理制度，執行風險管理。

5.1.4.5 建立安全事件緊急應變暨復原措施。

5.1.4.6 執行稽核改善建議事項。

5.1.4.7 規劃並執行矯正措施。

5.1.4.8 研討新資訊安全產品或技術。

5.1.4.9 執行資訊安全委員會決議事項。

5.1.4.10 鑑別資訊安全相關之法規與契約：

資訊安全執行小組應每年於召開管理審查會議前，針對本校提供之資訊服務來識別資訊安全的相關法令、法規與契約之要求，明確定義至「外來文件一覽表」中，且定期更新該列表，並經執行秘書審核。

5.1.5 緊急處理小組：由本校各關鍵業務流程負責人員組成。成員相關權責及作業內容分述如下：

5.1.5.1 組長：

5.1.5.1.1 當重大資安事件發生時，負責聯絡召集緊急處理小組。

5.1.5.1.2 協調及督導各關鍵業務流程負責人執行作業，並協調資源之調派使用。

5.1.5.1.3 依據事件評估之結果，得依現況請召集人決議是否宣布災變及啟動營運持續計畫。

5.1.5.1.4 當災變發生時，配合救災單位負責搶救人員、物資與設備等及現場指揮工作。

5.1.5.1.5 負責災後協調指揮清理災害現場。

5.1.5.1.6 負責規劃原營運場所之現場復原工作。

5.1.5.2 各關鍵業務流程負責人：

5.1.5.2.1 負責召集相關人員，發展、維護、更新修訂及執行各災害復原程序。

5.1.5.2.2 每年負責召集相關人員進行計劃之測試演練。

5.1.5.2.3 負責災害現場證據收集，俾利未來訴訟與損害求償事宜。

5.1.5.2.4 災害現場評估損害狀況及執行原營運場所之現場復原工作。

5.1.6 資訊安全稽核小組：由資訊安全委員會指派，負責評估資訊安全管理制度之執行情形。

5.1.6.1 擬定資訊安全內部稽核計畫。

5.1.6.2 執行資訊安全內部稽核。

5.1.6.3 撰寫資訊安全內部稽核報告。

5.1.6.4 追蹤不符合事項之改善執行情形。

5.1.7 應每年檢視「資訊安全委員會」成員離退狀態，更新「資訊安全組織成員表」，並經召集人審核。

5.2 管理審查會議

5.2.1 資訊安全委員會每年應召開一次「管理審查會議」，必要時得召開臨時會議。

5.2.2 管理審查會議審查內容建議包含如下：

5.2.2.1 先前管理審查之議題的處理狀態。

5.2.2.2 與資訊安全管理系統有關之內部及外部議題之變更。

5.2.2.3 資訊安全管理系統的績效回饋，包含下列趨勢：

5.2.2.3.1 稽核結果；

5.2.2.3.2 不符合項目及矯正措施；

5.2.2.3.3 資訊安全目標執行狀況報告：

5.2.2.3.3.1 本校係以「資訊安全政策」設定之目標為資訊安全目標。

5.2.2.3.3.2 本校依「資訊安全政策」所列之範圍及目標制定「ISMS 有效性量測表」，並以該表之量測結果做為本項審查項目之主要討論內容。

5.2.2.3.3.3 資訊安全執行小組應藉由「ISMS 有效性量測表」之量測項目與目標水準建立 ISMS 績效指標，收集各項量測項目之相關資料，據以評估本校資訊安全目標之達成情形。

5.2.2.3.4 審查與量測結果。

5.2.2.4 利害相關者回饋。

5.2.2.5 風險評鑑結果及風險處理計畫~~之狀態~~。

5.2.2.6 持續改善之機會。

5.2.3 管理審查會議之結論建議應包括：

5.2.3.1 與持續改善機會有關之決策。

5.2.3.2 任何對資訊安全管理系統變更之需要。

5.2.3.3 資訊安全制度執行之各項改進措施。

5.2.3.4 更新風險評鑑與風險處理計畫。

5.2.3.5 針對可能影響資訊安全制度之內外部事件，修正資訊安全管理流程與控制措施。內外部事件包括：

5.2.3.5.1 營運需求的變更。

5.2.3.5.2 安全需求的變更。

5.2.3.5.3 影響現行營運需求的業務程序變更。

5.2.3.5.4 管理或法規需求的變更。

5.2.3.5.5 契約要求的變更。

5.2.3.5.6 可接受風險等級或標準的變更。

5.2.3.6 針對資訊安全制度之需要，協調所需之資源。

5.2.3.7 控制措施有效性評量方式的改善。

5.2.3.7.1 評量時應決定執行事項、所需資源、負責人員、完成時間、成果評估方式等項目，以確認資訊安全目標之達成。

5.2.3.7.2 資訊安全小組應每年檢視「ISMS 有效性量測表」之量測執行狀況。

5.2.3.8 資訊安全小組如經檢視後，發現「ISMS 有效性量測表」之量測項目與目標水準有進行調整之需要，將運用本項審查項目進行討論與改善決議。

5.2.4 管理審查紀錄

5.2.4.1 管理審查為資訊安全管理制度重要之活動，審查紀錄應依「文件管理程序書」辦理，並產出「會議紀錄」。

5.3 關注方的合作及協調

5.3.1 須建立與本資訊安全管理制度相關之「外部單位聯絡清單」。

5.3.2 「外部單位聯絡清單」由資訊安全執行小組負責維護更新，視組織或合約變動適時更新。

5.3.3 應參考「資通安全事件通報及應變辦法」與相關權責單位建立通報管道並執行通報作業，聯繫方式應詳列於「外部單位聯絡清單」。

5.3.4 本機關如因組織變革、組織章程變更或組織法修正等足以影響本單位資通安全政策與目標者，資訊安全處理小組因重新擬定資訊安全政策與目標，識別利害關係人與議題，進行業務衝擊分析，並報請資安長同意召開管理審查會議，審查前揭項目之妥適性。

5.4 專案管理

5.4.1 專案需求分析宜考量資訊安全相關事宜，並列入專案管理工作計畫或合約中。

5.4.2 專案啟始時應執行風險評鑑，以評估專案實施階段可能發生的資訊安全風險。

5.4.3 專案執行過程中，應對於資訊安全要求進行審查改善。

5.4.4 專案管理應對專案相關人員進行角色界定與責任配置。

5.5 行動裝置及遠距工作

為確保本校遠距工作與行動裝置使用之安全，應訂定作業管理規範，以降低遠距工作與行動裝置使用時的風險，相關程序與方法請參閱「通信與作業管理程序書」。

6 相關文件

6.1 資訊安全組織成員表。

6.2 外來文件一覽表。

6.3 會議紀錄。

6.4 外部單位聯絡清單。

6.5 ISMS 有效性量測表。