敏惠醫護管理專科學校

「資訊安全管理系統」
安全事件管理程序書

機密等級：一般

編　　號：IS-MHCHCM-02-011

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。

安全事件管理程序書					
文件編號	IS-MHCHCM-02-011	機密等級	一般	版次	1.1

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、附件流程說明	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 確保敏惠醫護管理專科學校（以下簡稱本校）於資訊安全事件發生時，能迅速依程序進行通報，並採取必要之應變措施與建立事件學習機制，以降低事件所造成之損害。

2 適用範圍

2.1 本校資訊業務之資訊安全事件管理。

3 權責

3.1 資訊安全委員會：審核本校「資訊安全事件通報與應變作業流程」，並督導資訊安全事件之管理作業。

3.2 資訊安全執行小組：研擬資訊安全事件通報流程。

3.3 發現人員：所有人員（含：本校人員、約聘僱人員與委外人員），發現疑似資訊安全事件時，皆負有即時通報之責任。

3.4 權責單位：資訊安全事件處理之權責單位，須執行資訊安全事件之分析及處理。

3.5 執行秘書：督導資訊安全事件通報、處理及分析作業。

3.6 緊急處理小組：

3.6.1 確定事件影響範圍，並評估損失。

3.6.2 協助資訊安全事件之通報、處理及分析作業。

3.7 支援單位：

3.7.1 內部單位：協助處理相關法律、人事懲處及採購等問題。

3.7.2 委外廠商：協助處理資訊安全事件。

4 名詞定義

4.1 資訊安全事件：凡於作業環境中，導致資訊資產之機密性、完整性、可用性遭受影響之事或弱點，依照損害及影響程度可分為重大事故、一般事故以及一般事件。

4.2 內部危安事件：發現（或疑似）遭人為惡意破壞毀損、作業不慎等事件，但不影響業務進行，即一般事件。

4.3 外力入侵事件：發現（或疑似）電腦病毒感染事件、駭客攻擊（或非法入侵）等事件。

4.4 天然災害：颱風、水災、地震等。

4.5 突發事件：火災、爆炸、重大建築災害及資訊網路系統骨幹（主幹寬頻）中斷事件等。

4.6 資訊安全事件等級區分為：

4.6.1 一級事件：

4.6.1.1 非核心業務資訊遭輕微洩漏。

4.6.1.2 非核心業務資訊或非核心資通系統遭輕微竄改。

4.6.1.3 非核心業務之運作受影響或停頓，於可容忍中斷時間內回復

正常運作，造成本校日常作業影響。

4.6.2　二級事件：

4.6.2.1　非核心業務資訊遭嚴重洩漏，或未涉及關鍵基礎設施維運之核心業務資訊遭輕微洩漏。

4.6.2.2　非核心業務資訊或非核心資通系統遭嚴重竄改，或未涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭輕微竄改。

4.6.2.3　非核心業務之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作，或未涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，於可容忍中斷時間內回復正常運作。

4.6.3　三級事件：

4.6.3.1　未涉及關鍵基礎設施維運之核心業務資訊遭嚴重洩漏，或一般公務機密、敏感資訊或涉及關鍵基礎設施維運之核心業務資訊遭輕微洩漏。

4.6.3.2　未涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭嚴重竄改，或一般公務機密、敏感資訊、涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭輕微竄改。

4.6.3.3　未涉及關鍵基礎設施維運之核心業務或核心資通系統之運作

受影響或停頓，無法於可容忍中斷時間內回復正常運作，或涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，於可容忍中斷時間內回復正常運作。

4.6.4 四級事件：

4.6.4.1 一般公務機密、敏感資訊或涉及關鍵基礎設施維運之核心業務資訊遭嚴重洩漏，或國家機密遭洩漏。

4.6.4.2 一般公務機密、敏感資訊、涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭嚴重竄改，或國家機密遭竄改。

4.6.4.3 涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作。

5 作業說明

5.1 資訊安全事件之管理

5.1.1 應建立資訊安全事件之處理作業程序，並賦予相關人員必要責任，以便迅速有效處理資訊安全事件。

5.1.2 除正常應變計畫（如：系統及服務之回復作業），資訊安全事件之處理程序，應視需要納入下列事項：

5.1.2.1 導致資訊安全事件原因之分析。

5.1.2.2 防止類似事件再發生之補救措施。

5.1.2.3 電腦稽核軌跡及相關證據之蒐集。

5.1.2.4 與受影響之使用者進行溝通及說明。

5.1.3 電腦稽核軌跡及相關證據應以適當方法保護，以利下列管理作業：

5.1.3.1 作為研析問題之依據。

5.1.3.2 作為研析是否違反契約或資訊安全規定之證據。

5.1.3.3 作為與委外廠商協商如何補償之依據。

5.1.4 應依據「資訊安全事件通報與應變作業流程」處理資訊安全事件。相關作業程序應注意下列事項：

5.1.4.1 考量單位資源，於最短的時間內，確認回復後之系統及相關安全控制是否完整及正確。

5.1.4.2 向管理階層報告處理情形，並檢討、分析資訊安全事件。

5.1.4.3 限定僅授權之人員可使用回復後正常作業之系統及資料。

5.1.4.4 緊急處理步驟應詳實記載，以備日後查考。

5.2 內部通報程序

5.2.1 疑似資訊安全事件發生時，發現人員應依事件歸屬通報權責單位，並告知直屬主管。

5.2.2 權責單位於收到通知後，研判為資訊安全事件或內部危安事件。若：

5.2.2.1 判定為內部危安事件時，則將結果回覆予發現人員。

5.2.2.2 判定為資訊安全事件時，初估事件處理時間，並通知執行秘書。

5.2.3 權責單位於發生資訊安全事件時，應立即填具「資訊安全事件通報單」。

5.3 外部通報作業：

5.3.1 發生資訊安全事件時，應遵循『資通安全事件通報及應變辦法』進行外部通報作業。

5.3.2 權責單位確認發生資訊安全事件時，應於 1 小時內於「教育機構資安通報平台」完成通報作業。

5.3.3 一般事故：屬於「資通安全事件通報及應變辦法」區分一級或二級事件，權責單位應於知悉事件後 72 小時內完成損害控制或復原作業之辦理，並應留存紀錄；重大事故：屬於「資通安全事件通報及應變辦法」區分三級或四級事件，權責單位應於知悉事件後 36 小時內完成損害控制或復原作業之辦理，並應留存紀錄。

5.3.4 一般事件：非屬以上四級，事件發生不影響業務進行，可立即修復。

5.3.5 有關是否啟動營運持續運作計畫，依「營運持續運作管理程序書」辦理。

5.4 危機處理程序

5.4.1 本校資訊安全危機處理包括事前建置安全防護機制、事中主動預警與緊急應變，以及事後復原、追蹤、鑑識與偵查等步驟。說明如下：

5.4.1.1 事前建置安全防護機制：

5.4.1.1.1 建置資訊安全管理系統及整體防護架構。

5.4.1.1.2 彙整及備妥資訊安全相關文件。

5.4.1.2 事中主動預警與緊急應變：

5.4.1.2.1 事件辨識：辨識事件之歸屬及採取之對策，如內部資安事件、外力入侵事件、天然災害或重大突發事件等，並決定處理的方法與程序。

5.4.1.2.2 事件控制：依據各類事件危機處理之程序，進行事件傷害控制，降低影響的程度及範圍。

5.4.1.2.3 問題解決：事件處理權責單位或負責人須將問題解決。必要時，應向資訊安全委員會提出建議方案。

5.4.1.2.4 恢復作業：問題解決後，系統需恢復至事件發生前之正常運作狀態。

5.4.1.3 事後復原追蹤鑑識偵查：

5.4.1.3.1 後續追蹤之精神乃係檢討相關資訊安全事件是否會重複發生，並審視現有環境漏洞，透過研析相關資料，

以釐清事件發生之原因與責任。

5.4.1.3.2 受損單位依復原程序實施災後復原重建。

5.4.1.3.3 三級或四級資訊安全事件應保留事件發生之線索，如有需要得向國家資通安全會報技術服務單位或檢警單位申請數位鑑識（電腦、網路鑑識）。

6 相關文件

6.1 資訊安全事件通報與應變作業流程(附件)

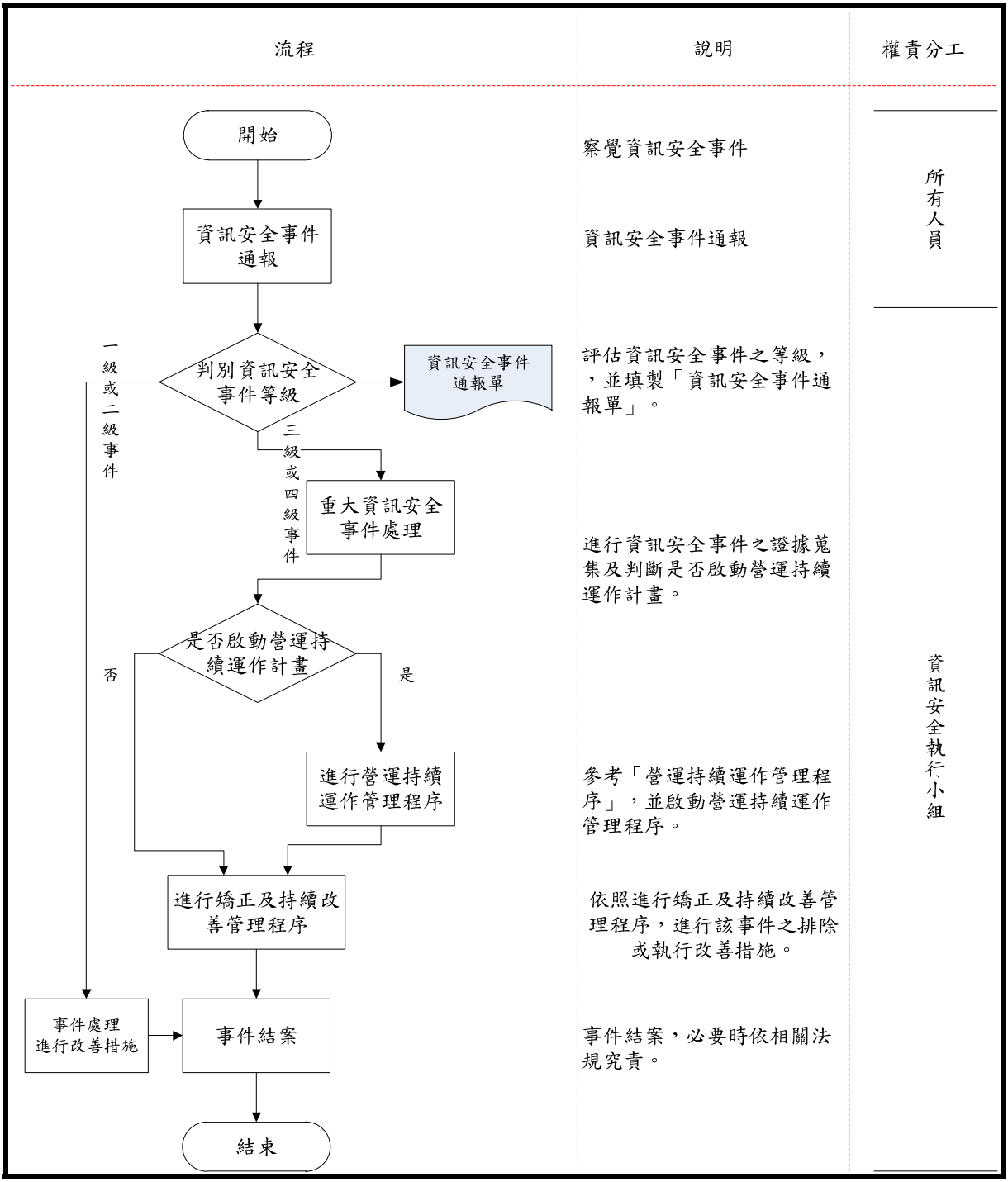
6.2 資訊安全事件通報單

6.3 『資通安全事件通報及應變辦法』

附件：

資訊安全事件通報與應變作業流程

1　流程圖：



2　流程說明：

2.1　資訊安全事件通報：

2.1.1　本校所有人員於業務處理過程中發生資訊安全事件，或發現與資訊安全有關之潛在風險時，應向資訊安全通報窗口通報。

2.2　判別資訊安全事件等級：

2.2.1　權責單位於收到通知後，研判是否為資訊安全事件。若：

2.2.1.1　判定為非資訊安全事件時，則將結果回覆予發現人員。

2.2.1.2　判定為資訊安全事件時，初估事件處理時間，釐清僅須紀錄或立即進行處理因應作業，並通知權責主管及執行秘書。

2.2.2　資訊安全通報窗口於收到通報後，應立即進行該事件等級評估，並填寫「資訊安全事件通報單」。

2.2.3　若為「一級或二級事件」，直接進行改善作業後記錄並歸檔；若為「三級或四級事件」，則依照下列資訊安全事件流程處理；若為「一般事件」，直接進行改善作業後記錄並歸檔。

2.3　資訊安全事件處理：

2.3.1　證據蒐集：

2.3.1.1　當三級或四級資訊安全事件發生時，若涉及行政或法律責任之追究，資訊安全執行小組應協助蒐集完整證據(如 Log、表單記錄、合約等)。

2.3.1.2 判斷是否啟動營運持續運作計畫：

2.3.1.2.1 依照「營運持續運作管理程序書」內有營運持續運作計畫啟動條件，判斷是否啟動營運持續運作管理程序。

2.3.2 進行營運持續運作管理程序

2.3.2.1 依照「營運持續運作管理程序書」之流程處理。

2.3.3 進行矯正及持續改善管理程序

2.3.3.1 若資訊安全事件有再發情形，則需進行矯正預防措施。

2.3.3.2 依照「矯正及持續改善管理程序書」之流程處理。

2.3.4 事件結案

2.3.4.1 資訊安全事件必須確實排除後始得結案。

3 相關文件：

3.1 資訊安全事件通報單