敏惠醫護管理專科學校

「資訊安全管理系統」
風險評鑑與管理程序書

機密等級：一般

編號：IS-MHCHCM-02-004

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	修正頁首、頁尾、權責、名詞定義、作業說明	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 為建立敏惠醫護管理專科學校（以下簡稱本校）資訊安全管理制度（以下簡稱 ISMS）風險評鑑與管理規範，提供本校資訊流程之權責單位、保管單位，以及使用單位，共同遵行之風險評鑑標準，有效執行風險控管，預防資訊安全事件之威脅。

2 適用範圍

2.1 本校資訊業務流程之風險與機會管理。

3 權責

3.1 資訊安全委員會：負責核定可接受風險值、風險評鑑結果、風險改善計畫、控制措施、機會評鑑結果、機會實作計畫，並確認資產風險承受者。

3.2 資訊安全執行小組：負責複核相關資訊流程風險評鑑結果，並針對風險值超過可接受風險值之資訊流程，採取適當之控管措施，及產出「風險改善與機會實作計畫表」。

3.3 風險擁有者：

負責相關資訊資產風險評鑑結果與「風險改善計畫表」之核准，並確認可接受風險與改善後之殘餘風險。

3.4 權責單位主管：負責所屬單位業務範圍之風險評鑑結果審核作業。

3.5 資訊流程權責單位：負責執行資訊流程之威脅與弱點評估、風險值

計算等程序項目。

4 名詞定義

4.1 機密性(Confidentiality)

4.1.1 確保僅授權人員可存取資訊。

4.2 完整性(Integrity)

4.2.1 確保資訊與處理方法的正確性與完整性。

4.3 可用性(Availability)

4.3.1 確保經授權的使用者在需要時可以取得資訊及相關資產。

4.4 可接受風險值

4.4.1 各類資訊流程之最低風險容忍度。

4.5 殘餘風險(Residual Risk)

4.5.1 在採用相關控制措施之後剩餘的風險。

4.6 威脅(Threat)

4.6.1 可能對系統或本校造成傷害之意外事件。

4.7 弱點(Vulnerability)

4.7.1 因資訊資產本身狀況或所處環境之下，可能受到威脅利用而造成資產受到損害之因子。

4.8 風險(Risk)

4.8.1 可能對本校的資訊流程或資產發生損失或傷害的潛在威脅，通

常利用弱點所產生之影響及發生可能性來衡量。

4.9 機會(Opportunities)

4.9.1 除了因應風險改善之計畫外，其他可增進本校資訊安全的任何作為。

4.10 風險擁有者(Risk Owner)

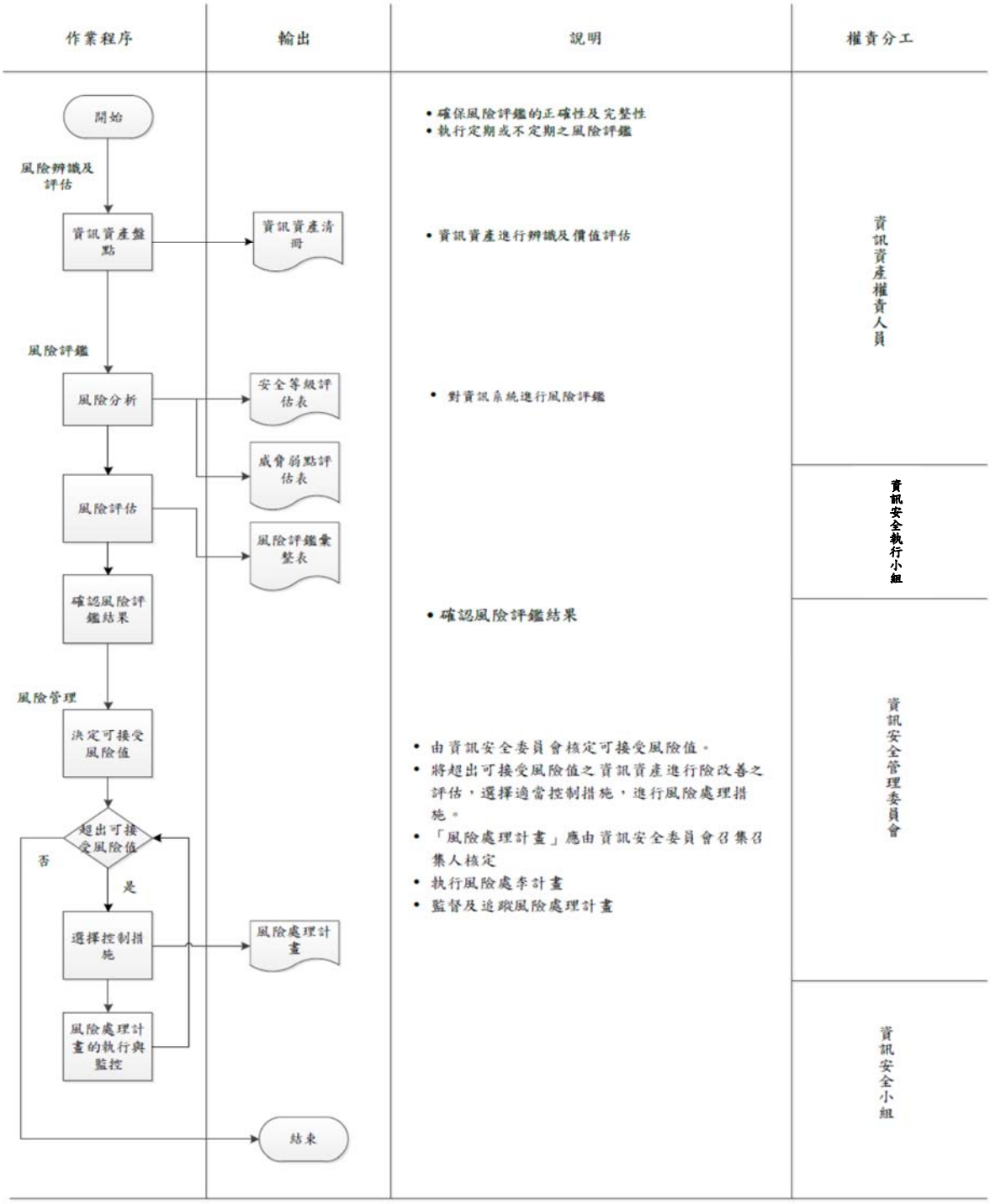
4.10.1 本校內針對各項資訊流程風險管理具備核准與確認者。

4.10.2 本校風險擁有者為單位主管。

5 作業說明

5.1 資訊資產之鑑別應依據本校「資訊資產管理程序書」進行鑑別及分類。

5.2 流程圖



5.3 流程說明

5.3.1 組織全景

界定內部與外部環節之參數

5.3.1.1 外部前後環節

與外部利害相關者關係及其感知與價值認定，組織面臨外部之區域、文化、相關法令法規之規範以及天然環境因素，影響組織目標衝擊的人員與趨勢。

5.3.1.2 內部前後環節

組織目標、組織文化、制定之政策、相關人員委任角色與責任、內部資源、與內部利害相關者關係及其感知與價值認定、合約關係的形式與規範等。

5.3.2 溝通與協商

組織依據溝通管理程序書中之規範，與利害相關者進行風險管理之對話與處理。

5.3.3 執行高階風險評鑑

5.3.3.1 本校自行或委外開發之資通系統，應依據『資通安全責任等級分級辦法』之規定，分別就機密性、完整性、可用性、法律遵循性等構面評估資通系統防護需求分級。

5.3.3.2 高階風險評鑑應每年至少執行一次，當資訊系統新增或異動時，承辦人員應填寫「防護需求等級評估表」，並由資訊安全執行小組彙整「資訊系統清冊」，以鑑別資訊系統防護需

求等級，並交文件管理人員彙整。

5.3.4 執行詳細風險評鑑

本校之資訊系統或「資訊系統清冊暨安全等級評估表」中所定義資訊系統安全等級為高者，應進行詳細風險評鑑，步驟如下：

5.3.4.1 資產識別

藉由資訊系統所提供的業務流程活動，識別該資訊系統之資訊資產。

5.3.4.2 資訊資產價值評量：

5.3.4.2.1 CIA 評分：在資訊資產發生事件時，以破壞「機密性」、「完整性」及「可用性」造成的後果，以「風險評鑑彙整表」之定性量化的數值鑑別資訊資產的價值。

5.3.4.3 威脅暨弱點評估

5.3.4.3.1 將應進行威脅弱點評估之資訊系統、服務，可能面臨之事件(威脅-弱點)分為六類，並建立各類別「威脅弱點評估表」包括：

5.3.4.3.1.1 人為：包含因人員有意或無意行為、人力資源管理不當所產生之風險。

5.3.4.3.1.2 文件/資料：包含資料、文件之建立、維護、控管、傳遞之不當所產生之風險。

5.3.4.3.1.3 軟體：包含系統設計、維護、操作之不當所產生之

風險。

5.3.4.3.1.4 硬體：包含所有硬體設施之失效、損毀等可能風險。

5.3.4.3.1.5 通訊：包含資料、影像、聲音傳輸媒介失效等所可能產生之風險。

5.3.4.3.1.6 環境：包含天災、供水、用電、空調等，整體資訊環境，可能發生之風險。

5.3.4.3.2 評估各類事件，並將各資產面臨之主要事件登載於「威脅弱點評估表」。

5.3.4.3.3 資訊資產價值之數值若為 7（含 7）以上，必須進行威脅弱點評估。

5.3.4.3.4 資訊資產之機密性、可用性及完整性之數值，若其中一項數值為 4 者，必須進行威脅弱點評估。

5.3.4.4 資訊資產群組化

5.3.4.4.1 針對有相同功能、機制、處於相同環境或面臨相同之威脅弱點之資訊資產進行群組化動作，並針對群組化之類別進行風險評鑑作業。

5.3.4.5 群組化之類別需由資訊安全小組開會決議後，於每年定期風險評鑑前公告，以供各資訊資產權責單位參考。

5.3.4.6 事件發生機率及衝擊的評估

5.3.4.6.1 事件發生機率及衝擊的評估可依以下步驟進行：

5.3.4.6.1.1 依各資訊資產之分類，查照「資訊資產評估項目對應表(附件)」進行選擇所需評估的事件(威脅-弱點)類別。

5.3.4.6.1.2 依以下之標準評估各事件發生機率及衝擊程度：

5.3.4.6.1.2.1 事件發生機率的評估：事件(威脅-弱點)發生機率值可參考下表得出。

事件發生機率/等級對應表

可能性	評估標準	數值
無或微	■無發生可能或不適用之情形。 ■對於可預期之資訊安全威脅缺乏動機或能力不足以利用脆弱點造成資安事件。 ■資訊安全事件因控制措施執行得當，有效降低脆弱點被利用，幾乎不可能發生。 ■三年發生之次數約 1 次或不發生，或屬於天災無法預估其發生可能性。	1
低	■很少發生。 ■對於可預期之資訊安全威脅具有動機但能力不足以利用脆弱點造成資安事件。 ■資訊安全事件因控制措施執行得當，有效降低脆弱點被利用，致使威脅發生之可能性極低。 ■一年發生之次數約 1 次，或三年 1 次以上 3 次以下。	2
中	■偶爾發生。 ■對於可預期之資訊安全威脅具有動機且有能力利用脆弱點造成資安事件。 ■已採行部份資訊安全措施，脆弱點仍未被有效降低或減少，致使威脅發生之機率略高。 ■一季發生之次數約 1 次，或一年 1 次以上 4 次以下。	3
高	■經常發生。 ■對於可預期之資訊安全威脅具有動機且有能力利用脆弱點造成資安事件。 ■未實行資訊安全措施或安全措施無效，脆弱點仍未被有效降低或減少，致使威脅發生機率偏高。 ■一個月發生次數 1 次以上，或一季發生 2 次。	4

5.3.4.6.1.2.2 事件衝擊程度的評估：主要針對各項威脅利用弱點而產生事件，判斷該事件發生對於資訊資產價值的衝擊程度，可由機密性、完整性與可用性三方面綜合考量。

5.3.4.6.1.2.3 衝擊評估標準/等級對應表

衝擊性	衝擊評估標準	數值
無或微	■資訊安全事件發生時，對資產並不會造成損失或僅造成極小的損失。 ■對於業務執行沒有影響。 ■可以立即完成復原。 ■若持續發生且次數頻繁，對業務執行可能帶來潛在風險。	1
低	■資訊安全事件發生時，對資產會造成輕微的損失。 ■對於整體營運或業務執行影響不大。 ■造成的損害可能僅影響單一業務或系統。 ■損失僅影響個人或少數幾人。 ■可以由內部人員進行復原。 ■修復或進行復原的措施可以在很短時間(一天)內完成。	2
中	■資產機密等級誤判或機密性維護機制失能時，對資產本身或相關資產造成間接或輕微的影響。 ■資訊安全事件發生時，對資產會造成較大的損失。 ■對於本校數項業務營運或執行造成停頓。 ■造成的損害可能影響多種業務、數個系統、多個部門或合作夥伴。 ■復原的措施必須由專業人員才能進行。 ■復原可能要一天到三天才能完成。 ■可能造成人員遭遇危險或受到傷害。	3
高	■資產機密等級誤判或機密性維護機制失能時，對資產本身或相關資產造成直接且嚴重的影響。 ■資訊安全事件發生時，對資產會造成嚴重的損失。 ■對於本校多項業務營運或執行造成停頓。 ■造成的損害可能影響本校或利益相關者。 ■復原的措施僅能由外部特定專業人員才能進行或修復人員不易取得。 ■復原無法於三天到一週內完成。 ■可能造成人員傷亡。	4

5.3.4.7 風險值的計算

5.3.4.7.1 群組化類別風險值=事件發生可能性(等級)X 事件衝擊(等級)。

5.3.4.7.2 資訊資產風險值=資訊資產價值 X 群組化類別風險值。

5.3.4.8 風險評鑑彙整表

5.3.4.8.1 依風險評鑑彙整逐項確認風險擁有者。

5.3.4.8.2 將上述評估資料彙整後產生「風險評鑑彙整表」。

5.3.4.8.3 將「風險評鑑彙整表」經資訊安全小組開會決議執行。

5.3.5 確認風險評估結果

5.3.5.1 運用「風險評鑑彙整表」彙整相關資訊流程綜合風險值，產出「風險與機會評鑑報告」，供資訊安全委員會作風險管理之依據。

5.3.6 風險管理

5.3.6.1 可接受風險值的決定

5.3.6.1.1 本校相關資訊資產之可接受風險值，需經資訊安全小組討論且由風險擁有者~~核准~~確認，並記載於會議紀錄中。

5.3.6.1.2 資訊安全小組每年召開會議檢討可接受風險值。可接受風險值得考量本校環境及作業之安全需求作適當調整。

5.3.6.2 選擇控制措施

5.3.6.2.1 評估資訊流程之最終風險值後，風險分析結果應陳報~~風~~資訊安全小組召集人。若風險值超出可接受風險值之資訊資產，應參考 ISO27001 標準選擇適當之控管措施。產出「風險改善與機會實作計畫表」，說明風險控管措

施之執行辦法。

5.3.6.2.2 「風險改善與機會實作計畫表」應陳報資訊安全小組開會審核，並由風險擁有者審核，並列入追蹤管理程序。

5.3.6.3 風險改善狀況的後續追蹤

5.3.6.3.1 對風險評鑑後所提出之風險改善計畫應彙整控管，持續追蹤至完成改善為止。

5.3.6.3.2 改善完成後，應將改善後的資產風險值登錄於「風險評鑑彙整表」中。

5.3.6.4 產出「適用性聲明」

5.3.6.4.1 依據 5.2.4.2.1 所選擇之控制措施，對照 ISO/IEC27001 最新版本附錄 A，產出「適用性聲明」。

5.3.6.4.2 若所選擇之控制措施不在 ISO/IEC27001 最新版本附錄 A 中，則仍須於「適用性聲明」中進行說明。

5.3.7 監督、量測、分析及評估

5.3.7.1 應針對所選擇之各項控制措施，挑選必要之項目進行監督與量測，詳細作業程序請參閱本校「監督與量測管理程序書」。

5.3.8 機會評鑑與實作

5.3.8.1 機會評鑑：應參照組織全景分析中內、外部議題以及關注者對

於本校資訊安全要求與期望，評估可增進本校資訊安全之各項機會。

5.3.8.2 資訊安全執行小組應針對所識別之各項機會進行可行性評估，並將評估結果寫入「風險與機會評鑑報告」中。

5.3.9 資訊安全執行小組應針對已識別之機會進行實作程序討論，並將實作內容填入「風險改善與機會實作計畫表」，陳報風險擁有者核准。

5.3.10 複核

5.3.10.1 監控

5.3.10.2 控制措施的實施必須建立相對應的指標或紀錄，以反應出控制措施實施的狀況及成效，以便於管理階層及相關人員做定期或不定期審視。

5.3.10.3 持續改善

5.3.10.3.1 為保持本風險評鑑方法之有效性與適用性，資訊安全小組得定期檢討可接受風險值與威脅及弱點評估表之項目，以期確保本校資訊資產均處於最佳保護之下，提供持續不中斷的營運。

5.3.10.4 風險與機會重新評估

5.3.10.4.1 每年應至少執行 1 次風險與機會評鑑。

5.3.10.4.2當範圍內有以下的狀況發生之時，則實施不定期的複核，以更新及確保資訊流程風險評估的正確性及完整性：

5.3.10.4.2.1　有新增、變更或移除資訊資產，且該資訊資產價值超過7(含7)以上。

5.3.10.4.2.2　作業環境改變。

6　相關文件

6.1『資通安全責任等級分級辦法』。

6.2 防護需求等級評估表。

6.3 資訊系統清冊。

6.4 威脅弱點評估表。

6.5 風險評鑑彙整表。

6.6 風險改善與機會實作計畫表。

6.7 風險與機會評鑑報告。

附件：資訊資產評估項目對應表

風險種類 / 資產類別	環境風險	資料、文件風險	軟體風險	硬體風險	通訊風險	人為風險
硬體	✓			✓		✓
軟體			✓	✓		✓
資料		✓	✓	✓		✓
文件		✓				✓
人員						✓
通訊				✓	✓	✓
環境	✓					✓