敏惠醫護管理專科學校

「資訊安全管理系統」
系統開發與維護程序書

機密等級：一般

編號：IS-MHCHCM-02-009

版本編號：1.2

制訂日期：113.10.17

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	執行秘書
1.2	113.10.17	資訊安全執行小組	內外部元件清冊更改為資訊資產清單	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 本程序書制訂之目的在於確保敏惠醫護管理專科學校（以下簡稱本校）資訊系統開發、測試與維護作業之安全管理。

2 適用範圍

2.1 本校應用系統程式開發相關活動，如系統安全需求分析、系統測試、修改、維護、上線變更、原始碼之管控與儲存等作業。

3 權責

3.1 本校相關資訊系統開發、維護人員與委外人員：遵守本程序書之相關規定，以確保本校相關軟體與資料等資訊資產之安全。

4 名詞定義

4.1 SSDLC (Secure Software Development Life Cycle)

4.1.1 安全的系統發展生命週期，除考量系統功能性的同時，導入安全性的思維，於系統整個開發過程，進行各項必要的安全防護措施，以降低系統後續維護的成本，以及遭受到攻擊行為時的損失。

5 作業說明

5.1 保全系統開發政策及安全系統工程原則

5.1.1 採行安全的系統發展生命週期(SSDLC)，作為本校各項軟體系統開發作業的策略，以下說明各階段之安全處理作業。

5.1.1.1 分析設計階段

有關分析設計階段應評估、考量是否有資訊安全需求。

5.1.1.2 架構設計階段(規劃及程式開發前)

5.1.1.2.1 檢查系統各項防護措施是否符合系統的需求，以及是否留存相關紀錄，並選用最適當的實作技術。

5.1.1.2.1.1 防止資料隱碼（SQL Injection）攻擊機制設計。

5.1.1.2.1.2 分析新技術之安全風險及潛在威脅，以避免遭受已知的攻擊。

5.1.1.2.2 依據系統開發所使用的程式語言，訂定安全的編碼準則。

5.1.1.2.3 評估系統之資產價值與資安威脅發生頻率。

5.1.1.2.4 建立及保存各帳號之使用紀錄。

5.1.1.2.5 評估各使用者身分及權責的適當性。

5.1.1.2.6 評估各使用者使用之資料與服務的適當性。

5.1.1.2.7 開發期程內設置之安全查核點。

5.1.1.2.8 應建立系統軟體更新的版本控制機制。

5.1.1.2.9 本校自行及委外開發之安全程式設計應遵守已訂定之需求為原則。

5.1.1.2.10 本校宜避免已知有缺陷之開發方法。

5.1.1.2.11 本校宜建置訂定開發工具，如 IDE。

5.1.1.2.12 遵守開發工具和環境公司所訂的使用注意事項。

5.1.1.2.13 使用最新版的開發工具或持續取得更新。

5.1.1.2.14 程式撰寫與開發人員需要具備必要足夠資格或能力，例如避開、找出及修補程式脆弱性。

5.1.1.2.15 使用安全設計與安全架構的概念，如先進行威脅模型分析。

5.1.1.2.16 應使用安全程式開發標準或指引。

5.1.1.2.17 應在可以控制的環境中執行開發。

5.1.1.3 程式開發階段

5.1.1.3.1 驗證使用者輸入的資料，確認其完整性與合法性，判別其中可能的攻擊語法。

5.1.1.3.2 確認使用者身分以及擁有的權限，並建立有效的通行密碼審核、檢查機制，避免可能的身分假冒或非授權存取。

5.1.1.3.3 建立不同階層的使用者權限，控制其對於系統資源和功能操作的存取，避免權限集中的問題。

5.1.1.3.4 避免在系統操作的過程中，洩漏系統環境、預設參數及作業程序的設定資訊。

5.1.1.3.5 必須有適當的保護措施，以防止洩漏系統內的機敏性資料。(例如，使用安全性較高的工具進行加密)

5.1.1.3.6 須保護使用者在操作系統功能時之存取、資料傳輸、紀錄等互動內容。

5.1.1.3.7 必須控管與防護系統中各項使用參數之輸入。

5.1.1.3.8 系統運作過程中發生之未預期錯誤或異常狀況，須有安全的處理程序，避免透露重要資訊。

5.1.1.3.9 針對系統稽核與登入紀錄的管理，除保護並定期紀錄備份外，亦應分析其內容，找出可能的弱點與攻擊行為。

5.1.1.3.10 對正在使用的程式語言和開發技術落實安全開發原則。

5.1.1.3.11 落實安全設計方法，如結對程式設計(pair programming)、程式法重構(code refactoring)、同行審查(peer code review)、安全迭代(security iterations)、測試驅動開發 TDD (Test-Drive Development)。

5.1.1.3.12 宜使用結構化程式設計技術。

5.1.1.3.13 宜保留程式碼註解並盡可能排除程式設計瑕疵。

5.1.1.3.14 避免使用不安全的設計技術，如將密碼寫死在程式碼

(hard-coded passwords)、未經核准認證或可能危害本機關資通安全的範例程式碼、以及未驗證的網頁服務。

5.1.1.4 系統測試階段

5.1.1.4.1 應依據系統各項控管機制與防護措施，進行攻擊模擬或安全測試，並留存相關紀錄。

5.1.1.4.2 若與其他既有系統進行界接或資料交換，應檢測既有系統保護措施執行成效及受影響的範圍，並留存相關紀錄。

5.1.1.4.3 應針對需求單位核准之作業軟體，進行系統相容與安全性測試。

5.1.1.4.4 系統開發人員進行測試時，除了功能面測試外，亦應包含系統安全功能測試。

5.1.1.4.5 應製作系統測試報告，向需求單位提報，並控管相關文件紀錄。

5.1.1.4.6 應落實最小權限原則與減少受攻擊面。

5.1.1.4.7 以常見的程式開發錯誤(error)態樣進行分析，並將這些錯誤態樣進行修復並紀錄之。

5.1.1.5 上線部署階段

5.1.1.5.1 有關上線部署階段之安全處理作業，應遵循本校「系

統開發與維護作業說明書」。

5.1.1.6 運作與維護階段

5.1.1.6.1 應依據系統運作與維護之需求評估，建立適當的系統安全檢測機制。

5.1.1.6.2 應依據系統各項目標與需求，建立適當的防護措施檢核表。

5.1.1.6.3 應要求系統委外供應商，配合本校提出系統安全之風險與機會評鑑資料。

5.1.1.6.4 得依據應用系統重要程度，進行技術檢測作業，如原始碼檢測、弱點掃描或滲透測試。以確保重要應用系統無高風險漏洞存在。

5.2 建立安全的開發環境

5.2.1 有關系統發展過程之系統檔案安全管理作業，請參閱本程序 5.6 規範。

5.2.2 有關系統發展過程之人員安全管理作業，請參閱本系統「人員安全與教育訓練程序書」。

5.2.3 有關系統發展過程中網路、作業系統、應用系統之存取及權限管理作業，請參閱本系統「存取控制管理程序書」。

5.2.4 有關系統發展過程之實體環境、設備安全管理作業，請參閱本系

統「實體安全管理程序書」。

5.2.5 有關系統發展過程之網路安全管理作業，請參閱本系統「通訊與作業管理程序書」。

5.2.6 有關系統發展過程中，適用的法規及智慧財產權的管理作業，請參閱本系統「資訊資產管理程序書」、「人員安全與教育訓練程序書」。

5.3 資訊系統之安全需求

5.3.1 新開發之資訊系統，或是現有系統功能之強化，應在系統規劃階段，即將安全需求納入系統功能。

5.3.2 除由系統自動執行之安控措施之外，亦可考量由人工執行安控措施；在採購套裝軟體時，亦應進行相同之安全需求分析。

5.3.3 在取得或採購軟體（含套裝軟體）時，依照其安全需求，準用本程序書之規定。除事前經權責單位主管核准外，應避免修改套裝軟體，如需修改應依本程序書之變更作業控制措施加以控管。

5.3.4 系統之安全需求及控制程度，應與資訊資產價值相稱，並考量安全措施不足，可能帶來之傷害程度。

5.3.5 資訊系統安全需求分析應考量事項如下：

5.3.5.1 評估保護資訊機密性、完整性及可用性的需求。

5.3.5.2 利用各種不同的安全控制措施，以防範、偵測電腦當機或發

生安全事件時，能立即執行回復作業。

5.3.5.3 對資訊及系統之存取控制。

5.3.5.4 重要業務，應建立例行性的稽核制度，並為特定查核之事項建立紀錄。

5.3.5.5 重要資料，應在資料處理過程中，檢查及保護資料之完整性。

5.3.5.6 應遵守法規或契約上對資訊安全控制的要求。

5.3.5.7 重要的程式、資料，應複製備份。

5.3.5.8 應訂定電腦當機之立即回復作業程序，尤其是對高使用率的系統應有妥適的回復措施。

5.3.5.9 應保護系統避免未經授權之異動。

5.3.5.10 應儘可能促使系統滿足稽核人員的安全控制需求。

5.3.5.11 應於相關文件規定資訊安全控制措施，以利使用者及資訊人員明瞭電腦系統內建之安控系統功能。

5.4 應用系統之正確處理

5.4.1 輸入應用系統之資料，應於輸入前查驗，以確保資料的完整性。

5.4.2 資料輸入應考量的安控措施如下：

5.4.2.1 是否有超出設定範圍的數值。

5.4.2.2 資料檔案是否有錯誤的文、數字。

5.4.2.3 資料是否有毀損或是不正確。

5.4.2.4 是否有未經授權或是前後不一致之資料。

5.4.2.5 超過資料量的上下限。

5.4.3 應適當建立輸入的資料是否有被竄改情形之安控措施。

5.4.4 應適當建立資料錯誤更正或手動更改資料庫的作業程序。

5.4.5 應依據各系統之重要性，適當建立驗證程序。

5.4.6 為確保應用系統內訊息之鑑別性與安全性，應適當建立安控措施。

5.4.7 應用系統資料輸出應經確認，以確保所儲存資料處理之正確性。

5.5 密碼控制措施與金鑰管理

5.5.1 使用加密技術時，如資訊專業人力及經驗不足，可請外界的學者專家提供技術諮詢服務。

5.5.2 應遵守權責主管機關訂定的資料保密規範，及使用權責主管機關檢驗合格或認可的加密模組，以確保加密技術產品的安全功能。

5.5.3 藉由使用密碼控制措施，保護資訊的機密性、鑑別性或完整性，並應備妥適當的密碼管理，以使用密碼技術。

5.5.4 重要應用系統為強化安全防護採行加密控制措施，可應用於資料庫加密、資料傳遞過程加密及存取控制身份識別等。

5.5.5 採行任何加密控制措施時，金鑰或憑證應有妥善管理機制。

5.6 應用系統檔案之安全

5.6.1 應備妥各項應用系統之作業程序，以控制作業系統上軟體之安裝。

5.6.2 應保護及控制測試資料，盡量避免以真實資料庫進行測試。

5.6.3 應用系統程式尚未測試成功，且未被使用者接受前，不應在正式環境執行。

5.6.4 應用系統程式更新上線作業，應取得主管核准，限定只能由授權的管理人員才可執行，並應限制原始碼的存取。

5.6.5 應建立應用系統程式的更新紀錄。

5.6.6 應適當保留舊版的軟體，以作為緊急應變措施之用，回復作業限定只能由授權的管理人員才可執行。

5.7 使用外部元件與函式庫

5.7.1 管理外部函式庫及定期更新，並紀錄於「資訊資產清單」。

5.7.2 選擇、授權和重複使用經過嚴格驗證的元件，特別是身份驗證 (authentication) 和加密元件 (cryptographic components)，並紀錄於「外部元件清冊」。

5.7.3 外部元件應註明授權來源、安全性（是否存在已知弱點）、版次與發行時間，並記於「外部元件清冊」。

5.7.4 外部軟體宜確保尚在維護 (maintainable)且可追蹤的 (tracked)，

並源自經過驗證且信譽良好的來源，並紀錄於「外部元件清冊」。

5.7.5 上述資源與產品應具備較長的可用時效，如避免使用試用版，並將授權到期日記於「資訊資產清單」。

5.8 套裝軟體元件的變更

5.8.1 應建立必要的控制措施與破壞完整性的風險。

5.8.2 是否取得套裝軟體元件廠商的同意。

5.8.3 若軟體更新係從廠商獲取之，則應納入程式更新標準程序。

5.8.4 應考量若修改軟體元件，將使本機關需要負擔該元件維護之衝擊與影響。

5.8.5 宜考量與其他使用中的軟體元件之相容性。

5.9 開發與維護過程之安全

5.9.1 應建立正式的變更程序並嚴格執行，以降低可能的安全風險。

5.9.2 應找出系統變更作業所需修正的電腦軟體、資料檔案、資料庫及硬體項目。

5.9.3 在執行變更作業前，應確保系統變更作業能為使用者接受。

5.9.4 系統文件在每次完成變更作業後，應定期更新，舊版的系統文件亦應妥善保管及處理。

5.9.5 應建立系統軟體更新的版本控制機制。

5.9.6 在實際執行變更作業前，變更作業的細項建議，應取得權責主管人員之核准。

5.9.7 授權之管理人員若透過遠端方式進行系統程式更新，應依照遠端連線步驟進行，相關流程請參考附件一。

5.9.8 系統程式更新上線及緊急復原作業步驟，請參考附件二。

5.9.9 所有的系統變更作業請求，皆應建立紀錄。

5.9.10 新系統上線作業前，應執行適當的測試。

5.9.11 新系統納入正式作業前，應注意下列事項：

5.9.11.1 評估系統作業效能及電腦容量是否滿足系統使用者的需求。

5.9.11.2 檢查發生錯誤後之回復作業、系統重新啟動的準備作業以及資安事件之緊急應變措施完備與否。

5.9.11.3 進行新系統正式納入例行作業程序之準備及測試。

5.9.11.4 新系統的建置是否影響現有系統的作業，尤其是對系統尖峰作業時段之影響。

5.9.11.5 得適當辦理新系統作業及使用者教育訓練。

5.9.12 執行變更作業後應檢視系統安全控制，以確保系統變更作業不致影響或破壞系統原有的安全控制措施。

5.9.13 套裝軟體的修改，應嚴格控管。

5.9.14 應控制並檢查軟體的採購、使用及修改，以防止可能的秘密通道

及特洛伊木馬程式。

5.9.15 應防範資訊洩漏的機會。

5.9.16 針對往來廠商服務之提供、監控及變更管理，應建立相關之控管機制。

5.9.17 對往來廠商之軟體系統建置及維護人員，應規範及限制其可接觸之系統與資料範圍，並嚴禁核發長期性之帳號及通行密碼。

5.9.18 建立往來廠商人員管理之相關程序，請參閱「人員安全與教育訓練程序書」。

5.10 技術脆弱性管理

5.10.1 作業系統應定期更新（例如安裝新的版本）；作業系統變更時，應評估其對應用系統是否造成負面的影響，或是產生安全問題。

5.10.2 作業系統變更之評估程序，應考量的事項如下：

5.10.2.1 評估應用系統的安全控制措施及查驗系統之完整性，以確保其未受作業系統變更之影響。

5.10.2.2 作業系統變更的評估及測試結果，如須進行必要的資源調整，應提出資源分配及調整計畫。

5.10.2.3 作業系統的變更應即時通知相關人員，以便在作業系統變更前，相關人員可以進行適當及充分的評估作業。

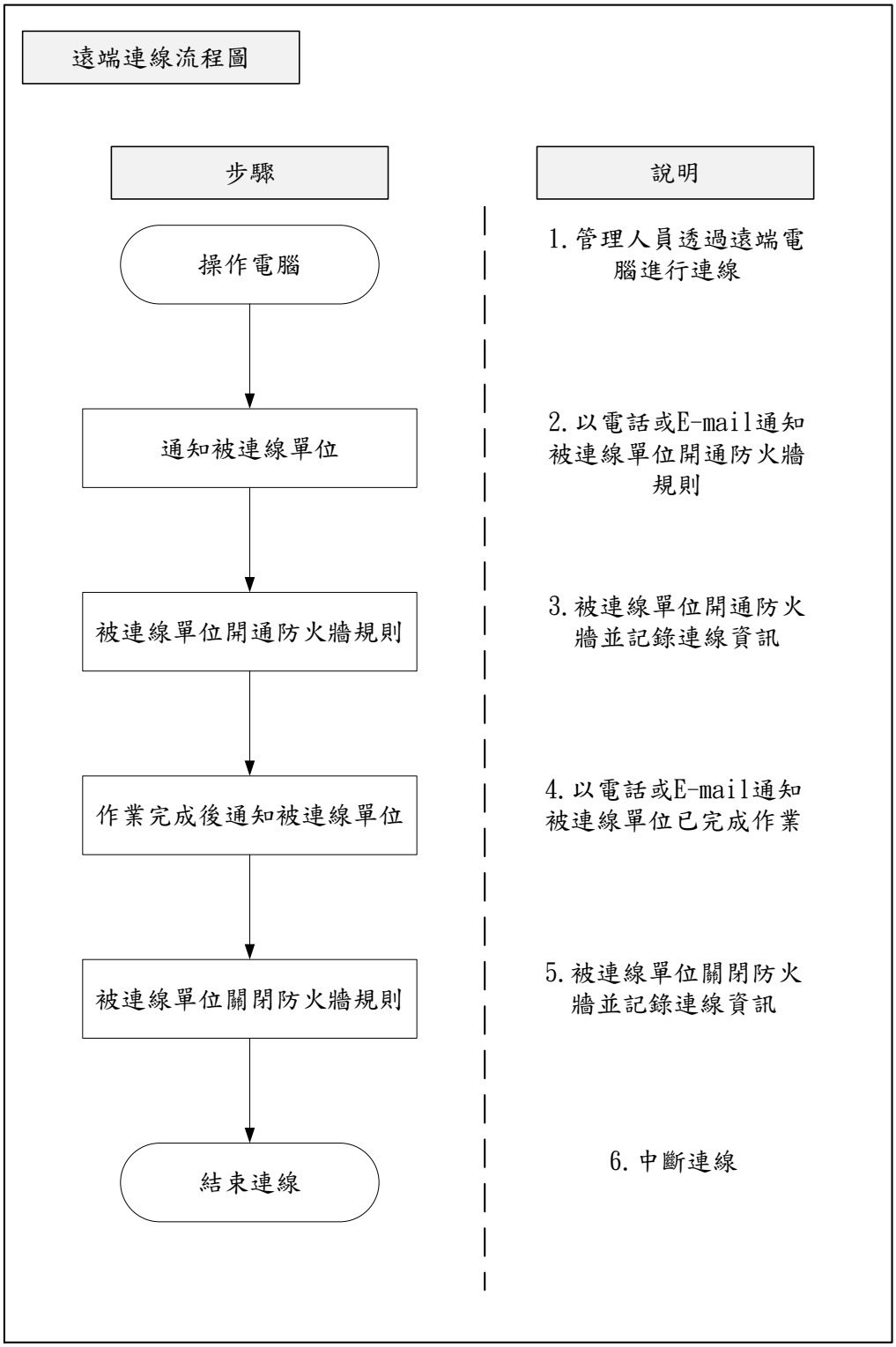
5.10.2.4 應取得關於使用中資訊系統之技術脆弱性資訊，並評估該脆

弱性對本校可能造成之威脅，以及採取適當措施以因應相關風險。

6 相關文件

6.1 資訊資產清單。

附件一：



附件二：