德明財經科技大學

資訊應用系統安全管理規定

機密等級：一般

文件編號：Takming - ISMS-B-010

版　次：V 1.2

初版日期：107.12.25

修 訂 紀 錄

版次	修訂日期	修訂頁次	修訂者	修訂內容摘要
1.0	107.12.25	N/A	執行小組	初版
1.1	115.06.09	3,4	推動小組	新增「資料遮蔽」項目
1.2	115.06.11	2,3	推動小組	新增「安全程式設計」項目

1. 目的

確保德明財經科技大學(以下簡稱本校)資訊應用系統之開發與管理安全。

2. 適用範圍

所有本校自行開發或委外之應用系統開發及管理，均適用之。

3. 名詞定義

無。

4. 權責

本校資訊系統的開發、維護人員及委外廠商相關人員皆應遵行本管理規定，以確保本校資訊系統與資料的資訊資產安全。

5. 要求事項

5.1. 資訊安全要求事項分析及規格

5.1.1. 應用系統需求申請

5.1.1.1. 本校各單位依業務實際需求，填寫「電子計算機中心軟硬體需求服務申請表」，陳單位主管核准後，向電子計算機中心提出應用系統需求之申請。

5.1.1.1.1. 系統自行開發

由承辦人員負責規劃與設計需求單位之應用系統。

5.1.1.1.2. 系統委外開發

請參考「資訊作業委外安全管理規定」辦理。

5.1.1.2. 系統開發或變更規劃內容應涵蓋系統安全品質、運作環境及內外部資源使用之安全性。

5.1.2. 應用系統設計文件

5.1.2.1. 系統設計文件由應用系統負責人或委外廠商撰寫；

5.1.2.2. 系統設計文件格式不拘，可兼採書面暨電子形式製作。

5.1.2.3. 系統設計文件內容應闡明應用系統之架構、輸出入資料規格、資料庫架構 (Schema)、介面設計構想、使用者操作說明，以及權限控管等。

5.1.3. 應用系統測試與驗收

5.1.3.1. 系統負責人應擔任系統功能錯誤之監督任務；需求部門應對系統進行功能及資料之測試。

5.1.3.2. 需求單位承辦人驗收後於「電子計算機中心軟硬體需求服務申請表」完成驗收簽核，並陳單位主管簽核後，由電子計算機中心完成結案簽核作業。

5.2. 公共網路應用服務系統與服務交易安全

5.2.1. 應用服務系統如公共網路提供服務(如全球資訊網或其他對外網站等)，應設計透過適當安全通訊管道進行傳輸，以防範於公共網路上傳送的應用服務中涉及之資訊，免於詐欺活動、契約爭議及未經授權揭露與修改。

5.2.2. 儘可能使用伺服器端程式，避免將程式置於客戶端(Client)執行，以免遭受破解，並且不要在伺服器端(Server)上留有暫存檔，若必須使用設定檔，應避免使用容易猜測之檔名或採取適當檔案保護措施。

5.3. 變更控制程序

5.3.1. 資訊系統如有變更需求，申請單位應填寫「電子計算機中心軟硬體需求服務申請表」，陳單位主管核准後，向電子計算機中心提出應用系統變更之申請。

5.3.2. 系統完成變更後，通知申請單位完成測試驗收作業，申請單位承辦人驗收後於「電子計算機中心軟硬體需求服務申請表」完成驗收簽核，並陳單位主管簽核後，由電子計算機中心完成結案簽核作業。

5.3.3. 系統完成變更作業後，應更新系統文件。

5.4. 安全程式設計

5.4.1. 開發前階段：規劃與準備

5.4.1.1. 制定程式碼撰寫原則

5.4.1.1.1. 撰寫 系統安全開發之程式碼撰寫原則，內容涵蓋：

5.4.1.1.1.1. 組織允許的例外規範：如使用特定編程語言特性的例外情形。

5.4.1.1.1.2. 常見資訊安全漏洞：列出 OWASP Top 10 等常見威脅及其應對措施。

5.4.1.1.1.3. 開發工具配置及維護：如 IDE 配置、版本控制工具及其更新策略。

5.4.1.1.1.4. 開發人員資格要求：參與安全程式設計培訓並具備相應證明。

5.4.1.1.1.5. 安全設計與架構：包括分層設計原則、最小權限模型等。

5.4.1.1.2. 開源及第三方組件管理

5.4.1.1.2.1. 建立組件清單，明確核可的程式庫及框架，並確保版本為最新。

5.4.1.1.2.2. 配置自動化工具掃描依賴項，檢查是否存在已知漏洞。

5.4.1.1.3. 開發環境配置與保護

5.4.1.1.3.1. 設置隔離的開發及測試環境，防止未經授權存取。

5.4.1.1.3.2. 定期更新和備份環境配置，避免

因系統變更引入漏洞。

5.4.2. 開發期間：實作與測試

5.4.2.1. 安全程式碼撰寫技術

5.4.2.1.1. 使用結構化編程技術，避免無法追蹤的執行流程。

5.4.2.1.2. 遵守輸入驗證與輸出編碼原則，防範 SQL Injection、XSS 等攻擊。

5.4.2.1.3. 避免硬編碼密碼或憑證，使用加密工具妥善管理敏感資訊。

5.4.2.2. 自動化與靜態程式碼分析

5.4.2.2.1. 使用靜態程式碼分析工具（如 SonarQube、Bandit）檢測潛在漏洞。

5.4.2.2.2. 定期執行單元測試，驗證程式碼在各種輸入情境下的安全性。

5.4.3. 檢視與維護

5.4.3.1. 程式碼保護與存取控制

5.4.3.1.1. 將程式碼儲存於版本控制系統中，設置角色基於權限的存取策略。

5.4.3.1.2. 定期審查存取記錄，檢測潛在的未授權存取行為。

5.4.3.2. 程式碼安全掃描與漏洞管理

5.4.3.2.1. 使用程式碼掃描工具檢查程式庫、組件及軟體是否安全且更新至最新版本。

5.4.3.2.2. 若發現漏洞，應即時修復並更新記錄，包括修補原因與實施細節。

5.4.3.3. 版本發布與維護策略

5.4.3.3.1. 軟體包裝與部署時應進行簽名，確保完整性與真實性。

5.4.3.3.2. 維護正式版本的更新日誌，便於追溯變更歷史。

5.4.4. 教育訓練與持續改進

5.4.4.1. 開發人員安全教育

5.4.4.1.1. 定期提供 OWASP Top 10、Secure SDLC 等相關培訓。

5.4.4.1.2. 鼓勵開發團隊參加業界安全技術交流會議。

5.4.4.2. 威脅情資與設計改進

5.4.4.2.1. 追蹤產業最新威脅情資，結合案例不斷優化設計準則。

5.4.4.2.2. 建立反饋機制，將漏洞經驗轉化為改進方

案。

5.4.5. 文件與記錄

5.4.5.1. 系統安全開發之程式碼撰寫原則。

5.4.5.2. 開發工具及第三方元件清單。

5.4.5.3. 程式碼審查報告與掃描結果。

5.4.5.4. 漏洞修補記錄與版本更新日誌。

5.4.6. 定期審查與改進

5.4.6.1. 每半年稽核一次安全程式設計實踐，檢查原則落實情況與工具使用狀況。

5.4.6.2. 當威脅情資或開發工具更新時，資訊安全團隊需檢視原則文件並進行必要修訂。

5.5. 安全應用系統工程原則

5.5.1. 輸入資料確認

5.5.1.1. 輸入欄位檢測：緩衝區溢位、輸入資料型態控管(SQL Injection/XSS)測試。

5.5.1.2. 遠端存取功能檢測：遠端存取功能控管等。

5.5.2. 內部處理的控制措施

5.5.2.1. 資料庫伺服器檢測：Patch 更新考量、不必要之服務及通訊埠關閉、通訊協定、帳號、管理員帳號密碼安全程度、安全稽核功能設定及紀錄檔(Log)存放等。

5.5.2.2. 網頁伺服器檢試測試內容含：Patch 更新考量、不必要之服務及通訊埠關閉、通訊協定、帳號、管理員帳號密碼安全程度、安全稽核功能設定及紀錄檔(Log)存放、URL 直接跳頁瀏覽站內網頁結構之限制、網頁功能、上架資料庫之連結等。

5.5.3. 輸出資料確認

5.5.3.1. 系統應依據作業需求顯示適當資訊予以使用者。

5.5.3.2. 使用者存取行為，系統應保存適當紀錄，以便後續追蹤與蒐證。

5.5.3.3. 系統應具備輸入輸出錯誤檢查機制，並提示使用者輔助資訊。

5.5.3.4. 使用者處理系統所產生之相關資訊，依據「資訊資產管理規定」辦理。

5.5.4. 訊息完整性

5.5.4.1. 如設計以應用程式傳輸敏感性資料時，需於系統中記錄傳輸的相關資訊，包含傳輸來源、接收目的位址、傳送時間與傳輸成功或失敗資訊。

5.5.4.2. 傳遞資訊至外部單位，應設計透過適當安全通訊管道進行傳輸。

5.5.4.3. 儘可能使用伺服器端程式，避免將程式置於客戶端(Client)執行，以免遭受破解，並且不要在伺服器端(Server)上留有暫存檔，若必須使用設定檔，應避免使用容易猜測之檔名或採取適當檔案保護措施（如：加密或存取限制）。

5.5.4.4. 對外提供敏感性資料的傳輸應採取加密傳輸，以確保資料在網路傳輸過程中的安全性。

5.5.5. 應用系統帳號身分驗證與使用管制

5.5.5.1. 對於限制存取的應用系統，應採取身分認證(如帳號、密碼)或其他身分鑑別的機制。

5.5.5.2. 程式設計應具備檢驗登入身分識別與密碼功能，並可將身分驗證之相關紀錄提供其他稽核工具使用。

5.6. 程式原始碼的存取控制

5.6.1. 系統於開發或測試階段時，委外廠商應備份所有應用系統之程式碼及設定檔，並於開發完成後提供完整的程式安裝檔，供系統負責人保存。

5.6.2. 系統開發如需使用正式線上之資料執行測試，在正式資料轉移至測試主機前應將敏感性之資料內容轉換為相同格式之虛擬資料，以消除資料之敏感性。

5.6.3. 測試資料存取應僅限制為系統負責人及委外廠商。

5.7. 應用系統測試/正式環境、資料庫之安全維護

5.7.1. 應將敏感性系統隔離，並明確識別應用系統的敏感性並加以文件化。

5.7.2. 在共用環境中執行敏感的應用程式時，宜識別各共用資源的應用系統與其對應的風險。

5.7.3. 測試環境所使用之設備環境應予獨立，不應與提供線上服務之設備環境共用。

5.7.4. 開發或測試階段時，委外廠商應備份所有應用系統之程式碼及設定檔。

5.7.5. 當資料庫管理系統建置後，應立即更改所有管理權限的 sys 和 system 使用者的密碼，防止非法使用者連接資料庫內之資料。

5.8. 資料遮蔽

5.8.1. 需求評估

5.8.1.1. 識別敏感資料：確定需要遮蔽的資料範圍。

5.8.1.2. 場景分析：明確遮蔽的應用場景，如測試環境、外部共享或內部特定使用需求。

5.8.2. 遮蔽技術選擇：根據具體業務需求，選擇適當的遮蔽技術。

5.8.2.1. 加密：對敏感資料加密並限制密鑰存取權限。

5.8.2.2. 字元清空或部分遮蔽：如顯示「1234****5678」。

5.8.2.3. 數字或日期替換：用隨機數字或日期代替原資料。

5.8.2.4. 替換：以模板或虛構值取代資料（如使用「測試用名稱」）。

5.8.2.5. 雜湊值替換：將敏感資料替換為不可逆的雜湊值（可選擇加鹽處理）。

5.8.3. 遮蔽實施與測試：部署遮蔽機制至系統。進行遮蔽效果測試，驗證是否正確隱藏敏感資訊。

5.8.4. 例外處理：所有要求存取未遮蔽資料的請求，需經資料擁有者審核並記錄在案。

5.8.5. 遮蔽記錄留存：對於遮蔽處理的過程，需完整記錄並保存至少一年，或遵循當地法律規範。

5.8.6. 最小權限存取：設置角色基礎的存取控制機制，確保使用者僅能存取必要資料。使用查詢與遮罩技術，僅顯示與用戶角色相關的最少資訊。

5.8.7. 資料儲存分離：假名化處理後，將敏感性資料與可識別資訊分開儲存並獨立保護。

5.8.8. 法規與合規要求：確保所有遮蔽行為遵循當地法律法規，如GDPR、個資法等。若涉及第三方供應商，確保在合約中加入相關遮蔽要求。

5.8.9. 定期測試與事件檢討：每季測試遮蔽技術的實施效果，特別是針對新的敏感性資料或業務場景。若發生資料洩露事件，需立即檢討遮蔽機制是否有效，並據此改進措施。

5.8.10. 定期審查與改進：根據最新的業務需求、技術進展和法規變更，定期更新遮蔽策略和技術。進行全員培訓，提升員工對資料遮蔽和敏感性資料保護的意識。

6. 參考文件

6.1. 資訊資產管理規定。

6.2. 資訊作業委外安全管理規定。

6.3. 電子計算機中心軟硬體需求服務申請表。(含系統權限申請)