文件編號	NCHU-ISMS-B-010	文件類別	資訊安全管理系統
權責單位	計算機及資訊網路中心	文件密等	一般
版　本	3.1	發行日期	111.07.01

國立中興大學
National Chung Hsing University

資訊應用系統安全管理辦法

機密等級:一般

文件編號:**NCHU- ISMS-B-010**

版　次:**3.1**

初版日期:**96.12.13**

文件制修訂紀錄			
訂日期	訂人員	修訂內容摘要	版次
96.12.13	陳建平	初版	1.0
98.8.18	陳建平	文件版型調整	2.0

文件編號	NCHU-ISMS-B-010	文件類別	資訊安全管理系統
權責單位	計算機及資訊網路中心	文件密等	一般
版　本	3.1	發行日期	111.07.01

文件制修訂紀錄			
訂日期	訂人員	修訂內容摘要	版次
105.11.08	葉宏	修訂文件編號 文件名稱刪除「計算機及資訊網路中心」 修訂1.目的 改為本校 修訂2. 適用範圍 改為全校 修訂4. 權責 整合 NCHU-I-ISMS-02-009資訊安全存取管理辦法2.0/ NCHU-I-ISMS-02-009資訊安全存取管理辦法2.0 修訂5.1. 資訊安全要求事項分析及規格5.2. 公共網路應用服務系統與服務交易安全5.3. 變更控制程序5.4. 作業系統變更後的應用系統技術審查5.5. 軟體套件變更的限制5.6. 安全應用系統工程原則5.7. 程式原始的存取控制5.8. 委外的軟體開發5.9. 系統測試資料的保護5.10. 應用系統測試/正式環境、資料庫之安全維護5.11. 技術脆弱性控制 修訂6.參考文件	3.0
111.07.01	賴怡君	等級改為一般	3.1

1. 目的 1
2. 適用範圍 1

3. 名詞定義 1
4. 權責 1
5. 要求事項 2
6. 參考文件 10

文件編號	NCHU-ISMS-B-010	文件類別	資訊安全管理系統
權責單位	計算機及資訊網路中心	文件密等	一般
版　本	3.1	發行日期	111.07.01

1. 目的

確保國立中興大學(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

所有本校與委外廠商執行應用系統開發及管理時均適用之。

3. 名詞定義

無。

4. 權責

4.1. 應用系統管理員

4.1.1. 應用系統規劃、上線與管理

4.1.2. 應用系統主機管理與保管

4.2. 委外廠商

4.2.1. 應用系統規劃、分析及設計。

4.2.2. 應用系統程式設計與測試。

4.2.3. 備份開發、測試所有應用系統之程式碼及設定檔。

4.2.4. 應用系統說明書、資料庫架構說明書、程式明細表、程式說明書、操作手冊製作撰寫。

5. 要求事項

5.1. 資訊安全要求事項分析及規格

系統負責人與委外廠商於系統正式開發前應建立下列系統文件:

5.1.1. 針對欲開發的系統執行機密性、完整性、可用性之「營運衝擊分析」, 以瞭解該系統對本校的影響。

5.1.2. 應用系統需求規格文件

5.1.2.1. 由應用系統負責人或需求部門撰寫(可彙整於系統招標需求規格書), 系統需求規格文件格式不拘, 惟內容應闡明系統應達成之功能、預期效益、使用者介面要求等。

5.1.2.2. 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。

5.1.3. 應用系統設計文件

5.1.3.1. 系統設計文件由應用系統負責人或委外廠商撰寫;

5.1.3.2. 系統設計文件格式不拘, 可兼採書面暨電子形式製作。

5.1.3.3. 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、稽核存錄安全性功能等,

5.1.4. 應用系統測試文件

5.1.4.1. 系統測試文件應包含測試計畫、測試報告, 並由系統負責人或得標廠商執行撰寫。

5.1.4.2. 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與勘誤。

5.1.4.3. 系統測試文件格式不拘, 惟應闡明以下各項測試項目:功能測試方式、輸出入介面測試方式、壓力(飽和)測試方式等。

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(如:加密或存取限制)。

5.2.3. 應保護對外服務應用系統之資訊交易(transaction)中涉及之資訊, 以防止不完整的傳輸、誤選路(mis-routing), 未經授權之訊息修改、未經授權之揭露、未經授權之訊息複製或重演。

5.2.4. 對外提供敏感性資料的傳輸(如線上交易、線上金流等)應採取加密傳輸, 以確保資料在網路傳輸過程中的安全性。

5.3. 變更控制程序

5.3.1. 新系統上線或系統重大改版前, 應進行系統功能與安全性測試, 測試功能無誤並評估上線之影響後, 由該系統負責人確認測試結果, 並經系統負責人組長覆核後始得上線提供服務。

5.3.2. 系統上線前, 系統負責人應對該系統上線可能影響之資料進行完整備份, 並評估系統上線衝擊。若未成功上線, 對既有系統使用者所會造成的衝擊, 同時與需求單位於上線計劃內事先擬定因應措施及具體處置步驟。

5.3.3. 系統如於完成上線後需執行變更或維護作業, 系統負責人應事先公告週知變更項目及時程, 以便相關人員配合。

5.3.4. 系統完成變更作業後, 應更新系統文件, 舊版之系統文件及相關申請及變更紀錄應歸檔予以妥善保管。

5.4. 作業系統變更後的應用系統技術審查

5.4.1. 若作業系統須變更(含設定變更、作業系統版本變更、修正程式更新等)時, 應通知相關應用系統管理人員, 並評估其變更之影響在決定是否執行變更。

5.4.2. 作業系統變更後, 應對現有應用系統之影響進行相關測試。

5.4.3. 作業系統完成變更作業後, 應更新相關系統文件, 提供相關單位審查。

5.5. 軟體套件變更的限制

5.5.1. 應盡量避免修改軟體套件, 且僅限於必要變更, 並應嚴格控制所有變更。

5.5.2. 軟體套件軟體之修改, 應委由原廠進行或取得原廠軟體授權同意後, 於不影響軟體功能及系統安全下, 依據應用系統變更與維護相關管理程序進行修改。

5.6. 安全應用系統工程原則

5.6.1. 輸入資料確認

5.6.1.1. 輸入欄位檢測:緩衝區溢位、輸入資料型態控管(SQL Injection)、防呆功能測試。

5.6.1.2. 遠端存取功能檢測:遠端存取功能控管等。

5.6.2. 內部處理的控制措施

5.6.2.1.　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。

5.6.2.2.　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。

5.6.3. 輸出資料確認

5.6.3.1.　系統應依據作業需求顯示適當資訊予以使用者。

5.6.3.2.　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。

5.6.3.3.　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。

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

5.6.4. 訊息完整性

5.6.4.1.　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。

5.6.4.2.　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。

5.6.4.3.　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)。

5.6.4.4.　對外提供敏感性資料的傳輸(如線上交易、線上金流等)應採取加密傳輸，以確保資料在網路傳輸過程中的安全性。

5.6.5. 應用系統帳號身分驗證與使用管制

5.6.5.1.　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。

5.6.5.2.　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。

5.6.5.3.　程式設計需使用帳號驗證機制時，應優先考慮與其他安全驗證機制整合，並以較嚴謹之機制為優先，參考順序為授

權認證(CA)機制、輕量級目錄存取協定(LDAP)、作業系統帳號整合。

5.6.5.4.　無法使用作業系統提供的驗證機制，則需在應用程式中使用自訂驗證機制，並加密處理後寫入資料庫。

5.6.6. 系統錯誤處理

5.6.6.1.　應用程式應設計各種例外狀況處理機制，以擷取錯誤資訊，並防止直接顯示原始完整錯誤資訊給予使用者。

5.6.6.2.　程式設計應避免造成緩衝區(Buffer)溢位，或將函式失敗時可能產生的錯誤碼交由例外程式處理(Exception handling)情形。

5.7. 程式原始碼的存取控制

5.7.1. 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。

5.8. 委外的軟體開發

系統開發或變更委外作業時，由系統承辦人依據政府採購法相關規定，進行委外採購流程，並注意以下事項：

5.8.1. 由應用系統承辦人規劃資訊服務，並依採購評選方式，撰寫徵求建議書說明文件或徵求企劃書說明文件、外包說明書(以下簡稱RFP)，其內容應清楚明確表達出所需服務，以供廠商瞭解專案範圍，並據以提出合理價格。

5.8.2. 專案執行過程發現專案執行效益不彰、政令變更或是委外廠商無法履行合約等不利專案繼續執行之因素時，如專案需暫停或取消，系統承辦人須以行政程序辦理專案暫停或取消，並以公文會辦相關單位辦理。

5.8.3. 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，其相關資訊安全規範請參考「資訊作業委外安全管理辦法」辦理。

5.8.4. 委外開發或維護之應用系統，應於合約中明訂下列事項：

(1) 作業時如發生錯誤或資料漏失，經確認屬得標廠商責任者，應由得標廠商負責更正；另損及他人權利義務，得標廠商亦須負責。

(2) 得標廠商對業務上所接觸之資料，應視同機密文件採必要之保密措施，得標廠商及人員均應依本校規定填具資訊安全保密契約書、切結書，任何因得標廠商人員洩密所致之賠

償及刑事責任，概由得標廠商負責，並列入本校拒絕往來戶。

5.9. 系統測試資料的保護

5.9.1. 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。

5.9.2. 測試資料存取應僅限制為系統負責人及委外廠商。

5.10. 應用系統測試/正式環境、資料庫之安全維護

5.10.1. 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。

5.10.2. 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。

5.10.3. 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。

5.10.4. 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。

5.10.5. 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。

5.11. 技術脆弱性控制

5.11.1. 應向系統開發單位或委外廠商確認相關系統修正或安全問題更新程式之影響與處理方式，以建立應用系統技術脆弱性資訊之取得管道，評估可能帶來之風險。

5.11.2. 應用系統應定期維護，維護內容應包含應用系統容量、應用系統日誌與資訊安全弱點檢視等等，維護紀錄應進行歸檔保存。

5.11.3. 透過網路存取之系統應執行適當之弱點掃描，弱點掃描應依據系統架構，以確認所開發的系統架構是否存在安全弱點。

6. 參考文件

6.1. 資訊資產管理辦法。

6.2. 資訊作業委外安全管理辦法。

6.3. 應用系統權限申請表。

6.4. 國立中興大學校務行政電腦系統工作申請單。