



| | | | | | |
|------|-----------|------|--------------|----|--------|
| 文件編號 | IMS-P-014 | 文件名稱 | 系統發展與維護管理程序書 | | |
| 機密等級 | 內部使用 | 版次 | 3.3 | 頁次 | 1 / 16 |

管理系統文件

| | | |
|---------|--------------|----|
| 文件類別 | 第二階文件 | |
| 文件編號 | IMS-P-014 | |
| 文件名稱 | 系統發展與維護管理程序書 | |
| 發行單位 | 國立虎尾科技大學 | |
| 發行日期 | 111年07月02日 | |
| 版次 | 3.3 | |
| 適用單位/範圍 | 全校 | |
| 訂修廢單位 | 審查 | 核准 |
| | | |

(原版簽名頁保存於IMS推動小組)



| | | | | | |
|------|-----------|------|--------------|----|--------|
| 文件編號 | IMS-P-014 | 文件名稱 | 系統發展與維護管理程序書 | | |
| 機密等級 | 內部使用 | 版次 | 3.3 | 頁次 | 2 / 16 |

| 訂 修 廢 記 錄 | | |
|-----------|-----------|---|
| 版次 | 發行日期 | 訂修廢內容摘要 |
| 1.0 | 106/01/11 | 初版發行 |
| 2.0 | 106/10/03 | 新增條文 5.3.2、5.8.3、修正條文 5.8.1、5.8.2 |
| 3.0 | 108/08/21 | 因應資通安全管理法施行修訂相關用詞及規範。(4.1) (「應用系統」修訂為「資通系統」) |
| 3.1 | 109/07/06 | 新增條文 5.3.2.1.3 與 5.6.1.8 |
| 3.2 | 110/03/29 | <ol style="list-style-type: none"> (1) 修訂「3.1 附錄 A 資通安全管理規範」為：「3.3 國際標準資訊安全管理系統 (ISO27001：2013)」。 (2) 修訂名詞 4.1 「核心資通系統」定義。 (3) 流程圖角色，根據實務流程調整。 (4) 「資通系統及資料異動申請單/(5.2.1、5.9.6.1、5.9.6.2、5.9.7.1、6.1)」、「資通系統開發及維護測試驗收紀錄單/(5.8.1、6.2)」表單名稱一致化。 (5) 根據「資通安全責任等級分級辦法」規範，增訂相對應之條文，以利遵循法規(5.2.3、5.5.3、5.9.8.8、5.9.8.9)。 (6) 部分文字調整，使其閱讀通暢(5.2.1.1.2、5.2.1.2.3、5.3.1.3、5.3.2.1、5.3.2.1.1、5.9.6.3)。 (7) 刪除 5.3.2.1.3。 (8) 增訂「IMS-P-014-03 資通系統安全等級評估表」、「IMS-P-014-04 資通系統清冊」。 |
| 3.3 | 111/07/02 | 修訂條文 5.9.8.8、5.9.8.9 |



| | | | | | |
|------|-----------|------|--------------|----|--------|
| 文件編號 | IMS-P-014 | 文件名稱 | 系統發展與維護管理程序書 | | |
| 機密等級 | 內部使用 | 版次 | 3.3 | 頁次 | 3 / 16 |

1. 目的

為促使本校委外或自行開發之資通系統在取得、發展與維護有一明確之規範，以確保資通系統之安全性。

2. 適用範圍

本校委外或自行開發資通系統之取得、發展與維護之管理。

3. 參考文件

- 3.1 國際標準資訊安全管理系統(ISO27001：2013)。
- 3.2 資通安全責任等級分級辦法
- 3.3 教育體系資通安全暨個人資料管理規範
- 3.4 國立虎尾科技大學資通安全維護計畫
- 3.5 IMS-P-018 資通業務委外作業管理程序書。
- 3.6 IMS-P-013 帳號密碼及存取控制管理程序書。
- 3.7 IMS-P-009 資通安全事件管理程序書。
- 3.8 IMS-P-015 資訊備份管理程序書。
- 3.9 IMS-P-008 矯正預防及持續改善管理程序書。

4. 名詞定義

4.1 核心資通系統

依據行政院所頒佈「資通安全管理法施行細則」第七條第一項所定義核心資通系統，指支持核心業務持續運作必要之系統，或依資通安全責任等級分級辦法附表九資通系統防護需求分級原則之規定，判定其防護需求等級為高者。



| | | | | | |
|------|-----------|------|--------------|----|--------|
| 文件編號 | IMS-P-014 | 文件名稱 | 系統發展與維護管理程序書 | | |
| 機密等級 | 內部使用 | 版次 | 3.3 | 頁次 | 4 / 16 |

5. 作業內容

5.1 系統發展與維護管理流程圖

| 作業流程 | 權責單位 | 相關表單 |
|--|--|---|
| <pre> graph TD A([確立系統開發需求]) --> B{評估及審查} B -- No --> A B -- Yes --> C[系統分析] C --> D{規格確認} D -- No --> C D -- Yes --> E[系統開發建置] E --> F{系統測試} F -- No --> E F -- Yes --> G[輔導系統上線] G --> H[技術轉移或編寫技術文件] H --> I{驗收} I -- No --> E I -- Yes --> J[系統維護與管理] J --> K([紀錄保存]) </pre> | 需求單位/業務承辦人員 業務承辦單位 業務承辦人員/委外廠商 業務承辦人員/需求單位 業務承辦人員/委外廠商 業務承辦人員/需求單位 業務承辦人員/ 需求單位/委外廠商 業務承辦人員/委外廠商 業務承辦單位/需求單位 業務承辦單位/委外廠商 業務承辦單位 | 資通系統及資料異動申請單 資通系統開發及維護測試驗收紀錄單 資通系統及資料異動申請單 系統說明文件/系統操作手冊 資通系統開發及維護測試驗收紀錄單 資通系統及資料異動申請單 資通系統及資料異動申請單 |



| | | | | | |
|------|-----------|------|--------------|----|--------|
| 文件編號 | IMS-P-014 | 文件名稱 | 系統發展與維護管理程序書 | | |
| 機密等級 | 內部使用 | 版次 | 3.3 | 頁次 | 5 / 16 |

5.2 確立系統開發需求與評估審核

5.2.1 資通系統需求申請

本校各單位依業務實際需求，填寫「IMS-P-014-01 資通系統及資料異動申請單」，陳單位主管核准後，向業務承辦人員提出資通系統需求之申請。

5.2.1.1 系統自行開發

5.2.1.1.1 本校需求單位之系統需求，須經討論及評估系統開發可行性。

5.2.1.1.2 由業務承辦人員負責規劃與設計需求單位所申請之資通系統。

5.2.1.2 系統委外開發

5.2.1.2.1 本校所需之資通系統經評估其可行性後，提請相關需求單位辦理系統委外開發提案與編列預算。

5.2.1.2.2 審核通過列入年度預算之資通系統委外開發案，得依本校採購程序及本程序書之資通系統安全要求，進行委外採購。

5.2.1.2.3 由業務承辦人員協助審查資通系統之資訊技術與提供支援。

5.2.2 系統委外發展專案規劃

委外專案應協助需求單位，由需求單位依據本校相關採購流程，進行委外採購程序，並注意以下事項：

5.2.2.1 任何性質之專案需求，必須在「需求規格書」中清楚明確的定義與表達。

5.2.2.2 專案委外採購時，簽約的委外廠商應進行專案細部規劃，並提出「專案執行計畫書」，內容必須包含發展時程、效益與人力需求分析與資通系統所應達成的功能。

5.2.2.3 本校委外作業，應依據「IMS-P-018 資通業務委外作業管理程序書」之規定辦理。



| | | | | | |
|------|-----------|------|--------------|----|--------|
| 文件編號 | IMS-P-014 | 文件名稱 | 系統發展與維護管理程序書 | | |
| 機密等級 | 內部使用 | 版次 | 3.3 | 頁次 | 6 / 16 |

5.2.3 需求單位於新系統需求申請時，應依據「資通安全責任等級分級辦法」之「附表九-資通系統防護需求分級原則」，填具「IMS-P-014-03 資通系統安全等級評估表」鑑別該資通系統安全等級。

5.3 系統分析

5.3.1 一般要求

5.3.1.1 進行系統需求單位之資訊收集，包含下列資料：

5.3.1.1.1 需求單位現行各項作業表單（含報表）。

5.3.1.1.2 需求單位內部之相關管理文件。

5.3.1.2 系統採委外開發時，系統開發委外廠商需要會同承辦人員，對於需求單位進行需求訪談。

5.3.1.3 自行發展之資通系統，由業務承辦人員與需求單位使用者進行需求訪談，並留存訪談紀錄文件。

5.3.1.4 系統開發委外廠商依據資料收集及訪談結果，撰寫系統開發相關文件。

5.3.2 資通安全要求項目

5.3.2.1 在進行系統分析時，可考量下列安全項目：

5.3.2.1.1 資通系統應視使用者業務需求，具備檢驗登入身分識別與密碼功能。

5.3.2.1.2 資通系統權限應視使用者業務需求，給予不同角色並對應適當權限。

5.4 規格確認

5.4.1 系統開發應依據系統開發相關文件與需求單位進行規格確認，包含下列事項：

5.4.1.1 確認資通系統作業流程。

5.4.1.2 確認使用者操作畫面。



| | | | | | |
|------|-----------|------|--------------|----|--------|
| 文件編號 | IMS-P-014 | 文件名稱 | 系統發展與維護管理程序書 | | |
| 機密等級 | 內部使用 | 版次 | 3.3 | 頁次 | 7 / 16 |

5.4.1.3 確認系統可產出的管理報表格式。

5.4.1.4 確認資料庫資料格式與欄位。

5.5 系統開發建置

5.5.1 依據系統分析及規格確認結果進行系統程式開發。

5.5.2 資通系統安全規範

資通系統進行開發時須包含以下安全要求：

5.5.2.1 身分驗證

5.5.2.1.1 資通系統應具備檢驗登入身分識別與密碼功能。

5.5.2.1.2 無法使用作業系統提供的驗證機制，則需在資通系統中使用自訂驗證機制。

5.5.2.1.3 使用者登入核心資通系統後，若超過 24 分鐘閒置時間而無任何動作時，系統須設定將其帳號登出（若屬功能限制或系統老舊無法提供此功能，待版本升級或更新系統時改善）。

5.5.2.2 權限管理

5.5.2.2.1 資通系統權限應視使用者業務需求，給予不同角色並對應適當權限。

5.5.2.2.2 資通系統應紀錄使用者處理敏感性資訊交易之相關資訊。

5.5.2.3 系統錯誤處理

5.5.2.3.1 資通系統應該實作且具有例外狀況處理機制，以擷取錯誤資訊。

5.5.2.3.2 例外狀況管理包含擷取和回傳例外狀況、設計例外狀況、傳送例外狀況資訊，並避免直接顯示原始完整錯誤資訊給予使用者。

5.5.2.4 資料庫存取安全



| | | | | | |
|------|-----------|------|--------------|----|--------|
| 文件編號 | IMS-P-014 | 文件名稱 | 系統發展與維護管理程序書 | | |
| 機密等級 | 內部使用 | 版次 | 3.3 | 頁次 | 8 / 16 |

5.5.2.4.1 資料庫連接字串之產生，應對於字串的輸入加以過濾，並限制長度。

5.5.2.4.2 加強資料庫帳號與權限管理，應用程式連結帳號權限應考量賦予最小之必要權限，系統管理者的帳號應視需要予以管制使用。

5.5.2.5 系統輸入檢查

5.5.2.5.1 針對資料欄位的輸入，如為已知之資料範圍，應提供選單或選項之方式進行輸入。

5.5.2.5.2 資通系統應具備資料輸入及輸出錯誤之檢查機制，並提示使用者輔助資訊，確保資訊輸入輸出的正確與完整。

5.5.2.5.3 進行資料強制輸入檢查，並且限制前端資通系統資料輸入的長度與型別，並於輸入敏感資訊時使用適當之顯示遮罩功能。

5.5.3 於新系統開發時，應針對需求單位所定義之資通系統分級結果，依據「資通安全責任等級分級辦法」之「附表十-資通系統防護基準」進行相對應之控制措施。

5.6 系統測試與輔導系統上線

5.6.1 系統測試

為確保資通系統符合本校需求單位之需求，須依以下之規範進行相關系統測試。

5.6.1.1 進行測試前，應建構測試環境及測試案例，同時分析並調整測試案例，以提高測試效率。

5.6.1.2 系統如透過網路存取，應執行適當之防駭測試。

5.6.1.3 測試系統與正式系統所使用之環境、資料應獨立分開。

5.6.1.4 系統測試需經開發者與使用者至少各一人以上進行測試。

5.6.1.5 測試資料除了進行正常資料測試外，並需測試不正常之資料輸入，如過長或過短的輸入資料、輸入格式錯誤的資料、可能造成緩衝區溢載之大量輸入資料等，以及早發現系統問



| | | | | | |
|------|-----------|------|--------------|----|--------|
| 文件編號 | IMS-P-014 | 文件名稱 | 系統發展與維護管理程序書 | | |
| 機密等級 | 內部使用 | 版次 | 3.3 | 頁次 | 9 / 16 |

題。

5.6.1.6 系統開發人員與系統測試人員若是校內人員得以正式資料測試，否則測試資料需去除足以辨識個人之資料。

5.6.1.7 測試完成後需填寫「IMS-P-014-02 資通系統開發及維護測試驗收紀錄單」呈送權責主管審核。

5.6.1.8 系統測試或驗收，即應針對需求單位所定義之資通系統分級結果，確認是否依照「資通安全責任等級分級辦法」之「附表十-資通系統防護基準」實作相對應的防護要求。

5.6.2 輔導系統上線

5.6.2.1 上線前應進行系統備份，並通告相關人員系統上線期間之影響。

5.6.2.2 上線過程若遇問題無法排除，應立即進行回復作業，並進行原因分析與重新評估上線程序。

5.7 技術轉移或編寫技術文件

5.7.1 技術轉移

適用於資通系統委外發展之專案。

5.7.1.1 由委外廠商到本校舉辦系統軟體技術轉移說明會，技術轉移內容必須包含下列事項：

5.7.1.1.1 作業系統、資料庫及系統程式安裝。

5.7.1.1.2 系統及網路相關參數設定。

5.7.1.1.3 開發工具安裝。

5.7.1.1.4 系統安全設定。

5.7.1.1.5 網路環境設定。

5.7.1.1.6 辦理系統操作及使用訓練。

5.7.1.2 委外廠商應提交下列相關資料：

5.7.1.2.1 系統操作及使用手冊文件。



| | | | | | |
|------|-----------|------|--------------|----|---------|
| 文件編號 | IMS-P-014 | 文件名稱 | 系統發展與維護管理程序書 | | |
| 機密等級 | 內部使用 | 版次 | 3.3 | 頁次 | 10 / 16 |

5.7.1.2.2 資料庫檔案結構說明。

5.7.1.2.3 原廠的系統使用授權書。

5.7.2 編寫技術文件

適用於資通系統自行發展之專案。

5.7.2.1 由系統開發人員編寫「系統說明文件」做為日後維護與管理使用。

5.7.2.2 由本校編寫「系統操作手冊」提供使用者參考使用。

5.8 驗收

5.8.1 自行開發之資通系統，依本校驗收流程由需求單位進行驗收作業，並將驗收結果記錄於「IMS-P-014-02 資通系統開發及維護測試紀錄單」，呈送權責主管審核備查。

5.8.2 自行開發之資通系統，經驗收不合格的項目，系統開發人員進行改善並另擇日驗收以符合系統開發需求。

5.8.3 系統委外採購時，經驗收不合格的項目，委外廠商須限期改正，並另擇日驗收以符合採購契約之驗收規定。

5.9 系統維護與安全管理

5.9.1 系統帳號及權限管理

5.9.1.1 資通系統之管理帳號與使用者帳號、密碼與權限管理原則，須依據「IMS-P-013 帳號密碼及存取控制管理程序書」之規定，妥善保存及管理系統帳號及密碼。

5.9.1.2 系統使用權限指派考量，應僅賦予資通系統使用者適當的權限，以降低誤用系統的風險。

5.9.1.3 因個人基本資料保密考量，應用程式應對資料匯出做適當管控。

5.9.1.4 人員停職、離職或調職時，應依據本校離調職作業流程通知帳號管理者，進行人員帳號停用、刪除或變更。

5.9.1.5 資通系統使用者存取行為，系統應保存適當紀錄，以便後續



| | | | | | |
|------|-----------|------|--------------|----|---------|
| 文件編號 | IMS-P-014 | 文件名稱 | 系統發展與維護管理程序書 | | |
| 機密等級 | 內部使用 | 版次 | 3.3 | 頁次 | 11 / 16 |

追蹤與蒐證，提供相關單位進行查核。

5.9.2 系統使用需求

- 5.9.2.1 若需資通系統之使用權限，使用者應須依據「IMS-P-013 帳號密碼及存取控制管理程序書」規定填寫系統使用權限申請單，說明欲申請之系統名稱、帳號種類及相關細節，經權責主管核准後，向資通系統管理者提出申請。
- 5.9.2.2 委外廠商或外單位人員如需使用管理者帳號進行資通系統之維護與管理時，應經單位主管核准後始可進行，並且系統管理者於委外廠商或外單位人員作業完成後立即停用該帳號。
- 5.9.2.3 使用單位因業務需求，需新增或修改資通系統時，應經單位權責主管核准後，向系統管理者提出申請。

5.9.3 系統帳號設置

- 5.9.3.1 資通系統之帳號、密碼及使用權限之建立與管理，應依據「IMS-P-013 帳號密碼及存取控制管理程序書」之相關規定，進行系統使用帳號之設置。
- 5.9.3.2 資通系統帳號建立、授權及相關設定作業完成後，使用者於初次使用時應立即變更預設密碼（若屬功能限制或系統老舊無法提供此功能，待版本升級或更新系統時改善）。

5.9.4 系統使用測試

- 5.9.4.1 使用者經單位主管核准後，取得系統使用授權，由資通系統管理者協助進行系統之使用。
- 5.9.4.2 系統安裝完成後，系統管理者應協助使用者依所申請之帳號及密碼，進行首次系統登錄與系統測試，以確認系統正常運作，並由系統管理者詳細告知使用者系統使用之安全規範。

5.9.5 系統使用

- 5.9.5.1 使用者於使用資通系統時，若發生系統使用之問題，應立即通知系統管理者進行問題處理，若屬資安事件時，應依據「IMS-P-009 資通安全事件管理程序書」之規定進行處理。



| | | | | | |
|------|-----------|------|--------------|----|---------|
| 文件編號 | IMS-P-014 | 文件名稱 | 系統發展與維護管理程序書 | | |
| 機密等級 | 內部使用 | 版次 | 3.3 | 頁次 | 12 / 16 |

5.9.5.2 資通系統在用戶端、伺服器與網路應用程式方面，如有授權限制，應符合授權契約條款使用軟體。

5.9.6 資通系統變更

5.9.6.1 資通系統若需進行變更時（如：新增功能或改善需求...等），須填寫「IMS-P-014-01 資通系統及資料異動申請單」經主管核准後通知系統開發人員或委外廠商進行處理，並告知需求單位處理結果。

5.9.6.2 變更之設定項目需記錄於「IMS-P-014-01 資通系統及資料異動申請單」，以供後續管理上參考。

5.9.6.3 委外廠商進行資通系統變更如以遠端連線方式進行，則須依「IMS-P-018 資通業務委外作業管理程序書」之規範開啟網路存取權限，在系統管理者之監控下進行系統變更。

5.9.6.4 資通系統變更前，應評估對各使用單位之影響，若影響業務單位之正常運作時，需通告各相關單位並協調系統變更時間，以降低對業務運作之影響。

5.9.6.5 資通系統完成變更作業後，應更新相關系統文件。

5.9.7 資通系統維護

5.9.7.1 資通系統有資料庫異動需求時，申請單位須填寫「IMS-P-014-01 資通系統及資料異動申請單」提出申請，經權責主管核准後方可對資料庫進行異動作業。

5.9.7.2 每年由資通系統管理者，針對資通系統維運與軟硬體進行檢查；若系統為委外處理，則須要求委外廠商定期實施系統檢查，並將檢查結果回覆給系統管理者，以確保系統之維運與安全。若發生異常事件，則由系統管理者進行異常處理。

5.9.7.3 檢查紀錄時需檢視是否符合資通系統服務品質目標之設定，以供單位主管不定期檢視系統運作狀況，作為維護、擴充系統及日後改善之參考。

5.9.7.4 資通系統使用者發現系統有異常情形，應立即通知報修。



| | | | | | |
|------|-----------|------|--------------|----|---------|
| 文件編號 | IMS-P-014 | 文件名稱 | 系統發展與維護管理程序書 | | |
| 機密等級 | 內部使用 | 版次 | 3.3 | 頁次 | 13 / 16 |

5.9.7.5 本校與委外廠商所簽訂之相關維護契約內容，依據契約內規範通知委外廠商處理。

5.9.8 資通系統之安全管理

5.9.8.1 資通系統於規劃建置初期，即應評估所處理資料之重要性，並依據評估結果，採購適當之系統軟、硬體或利用適當的資料儲存技術（如：磁碟陣列、儲存區域網路(storage area network, SAN)）進行資料的存放，以滿足資通安全之需求。

5.9.8.2 儲存空間之規劃並應考慮未來資料量的成長趨勢，避免發生資料儲存空間不足的情況。

5.9.8.3 對於上線之各資通系統，除主要資料儲存空間之規劃考量外，平時亦須進行適當之資料備份，備份作業應依據「IMS-P-015 資訊備份管理程序書」之規定辦理。

5.9.8.4 資通系統管理者或使用者，對於使用或控管流程須負有保密之責。

5.9.8.5 處理機密資料之資通系統，若採取委外開發，應謹慎考慮業務機密洩漏之風險，並遵守「IMS-P-018 資通業務委外作業管理程序書」之規範。

5.9.8.6 資通系統如有程式安裝光碟或是程式原始碼光碟，應由資通系統保管人負責保管。

5.9.8.7 資通系統開發過程中，如有使用商業軟體元件（如：COM、API 等），應取得合法使用授權後始得使用，並注意該商業軟體元件授權相關規定。

5.9.8.8 依據「資通安全責任等級分級辦法」要求，資通系統安全等級，應每年至少檢視一次資通系統分級妥適性，相關檢視期程由 IMS 推動小組公告週知。各業務承辦單位於公告期程內填具「IMS-P-014-04 資通系統清冊」及初估或異動之「IMS-P-014-03 資通系統安全等級評估表」，經單位主管核可後送 IMS 推動小組審查確認。

5.9.8.9 各單位依 5.9.8.8 程序要求完成單位內資通系統分級檢視



| | | | | | |
|------|-----------|------|--------------|----|---------|
| 文件編號 | IMS-P-014 | 文件名稱 | 系統發展與維護管理程序書 | | |
| 機密等級 | 內部使用 | 版次 | 3.3 | 頁次 | 14 / 16 |

後，將資料呈送 IMS 推動小組，並由本校資安專職人員負責彙整該年度全校資通系統清冊，送資通安全長核定。

5.9.9 資料庫之安全管理

5.9.9.1 資料庫安全存取控制

- 5.9.9.1.1 使用資料庫須經資料庫管理者進行身分認證與權限管理，且須使用獨立之帳號及密碼登入。
- 5.9.9.1.2 進行資料庫存取之身分驗證機制，須由系統內部安全機制提供。
- 5.9.9.1.3 系統管理者須建立專屬帳號，不得多人共用同一帳號。
- 5.9.9.1.4 資料庫使用者之帳號密碼設定必須依據「IMS-P-013 帳號密碼及存取控制管理程序書」之相關規定辦理。
- 5.9.9.1.5 資料庫最高權限帳號之存取授權應僅限於資料庫管理者。
- 5.9.9.1.6 資料庫預設帳號應變更密碼，或是關閉使用。
- 5.9.9.1.7 僅系統管理者擁有異動資料庫相關檔案的作業權限。
- 5.9.9.1.8 除系統管理者外，非經授權禁止直接連接資料庫進行新增、修改與刪除等作業。

5.9.9.2 資料庫管理系統安全性

- 5.9.9.2.1 針對資料庫系統已知漏洞，在不影響現行作業狀況下，應立即進行修補。
- 5.9.9.2.2 應用程式禁止使用資料庫管理者帳號連結資料庫進行存取。
- 5.9.9.2.3 為確保資料庫內資料之安全性，針對資料庫之權限控管制定原則，資料庫存取帳號、權限應視不同資通系統、人員存取之需求進行適當設定。

5.9.9.3 資料庫備份

- 5.9.9.3.1 重要資料庫應定期備份，並且抽檢備份資料是否可用。



| | | | | | |
|------|-----------|------|--------------|----|---------|
| 文件編號 | IMS-P-014 | 文件名稱 | 系統發展與維護管理程序書 | | |
| 機密等級 | 內部使用 | 版次 | 3.3 | 頁次 | 15 / 16 |

5.9.9.3.2 資料庫備份之存放點應進行控管，防止非相關人員存取。

5.9.9.3.3 資料庫備份請依據「IMS-P-015 資訊備份管理程序書」之規定辦理。

5.9.9.4 資料庫存取稽核紀錄

5.9.9.4.1 資料庫系統在不影響正常運作之效能，針對存放敏感性資料啟動相關安全稽核紀錄功能（包含異動）。

5.9.9.4.2 僅授權之人員可讀取資料庫稽核紀錄。

5.9.9.4.3 系統管理者應不定期檢視資料庫稽核紀錄，防止資料庫不當操作與存取。

5.10 異常處理

5.10.1 發生資安事件時，應立即依據「IMS-P-009 資通安全事件管理程序書」所訂定之通報管道，迅速通報單位主管及系統管理者進行問題處理。

5.10.2 異常狀況無法有效解決時，應依據「IMS-P-008 矯正預防及持續改善管理程序」之相關規定執行矯正與預防措施，進行問題矯正及風險預防的作業，確保問題不再發生。

5.11 紀錄保存

相關業務承辦人員應參照如下規範，妥善保存各項紀錄。

| 編號 | 表單名稱 | 保存地點 | 保存期限 |
|----|----------------|---------|------|
| 1 | 資通系統及資料異動申請單 | 電子計算機中心 | 至少3年 |
| 2 | 資通系統開發及維護測試紀錄單 | 電子計算機中心 | 至少3年 |
| 3 | 資通系統安全等級評估表 | 電子計算機中心 | 至少3年 |
| 4 | 資通系統清冊 | 電子計算機中心 | 至少3年 |

6. 附件

6.1 IMS-P-014-01 資通系統及資料異動申請單。

6.2 IMS-P-014-02 資通系統開發及維護測試紀錄單。

6.3 IMS-P-014-03 資通系統安全等級評估表。



| | | | | | |
|------|-----------|------|--------------|----|---------|
| 文件編號 | IMS-P-014 | 文件名稱 | 系統發展與維護管理程序書 | | |
| 機密等級 | 內部使用 | 版次 | 3.3 | 頁次 | 16 / 16 |

6.4 IMS-P-014-04 資通系統清冊。