中央研究院

資訊科學研究所

應用系統發展及維護安全管理作業說明書

機密等級：□公開 ■內部 □敏感

編　　號：B330-I311

版　　本：1.3

核准日期：115 年 4 月 24 日

文件制／修訂紀錄表

版次	修訂日期	修訂單位	修訂者	核准者	修訂內容
1.0					新擬訂文件
1.1	112/04/10	資訊室			依總統府稽核發現修訂
1.2	114/11/18	資訊室			依據 ISO27001 改版進行文件調整
1.3	115/03/31	資訊室			新增九、應用系統下線作業程序

目　錄

壹、目的

中央研究院資訊科學研究所（以下簡稱本所）為提供系統與軟體開發、變更維護之管理程序，並提供自行維護系統之資通系統管理者或委外維護的承包廠商進行資通系統軟體變更維護，訂定應用系統發展及維護安全管理作業說明書（以下簡稱本作業說明書）。

貳、依據

一、 中央研究院資通安全暨個人資料保護政策及規範

二、 中央研究院資通安全管理規範實施要點

三、 資通系統籌獲各階段資安強化措施(行政院 1110526 版)

參、適用範圍

資通系統開發、變更管理維護作業，涉及程式原始碼、執行碼或設定檔變更者，適用本程序。

肆、權責

資通系統管理者應依據本作業說明進行變更管理或監督系統開發維護廠商依據本作業說明進行軟體變更管理。

伍、作業說明

本所同仁受理獲取、開發或維護各項應用系統時，可參照安全系統開發生命週期(Secure Software Development Life Cycle, SSDLC)管理，要求與下列作業程序及應用系統開發及維護之資訊安全注意事項，以落實應用系統發展生命週期之需求、設計、開發、測試及部署等各階段資訊安全。

一、 需求階段

(一) 本所各單位如有應用系統獲取、開發或變更需求，應依業務實際需要，填寫線上「行政作業系統-新功能申請回報」申請單後向資訊單位提出，並可視開發專案之規模大小，自行調適內容大綱。

(二) 資訊單位進行需求訪談，評估資料量、使用量、成長幅度、設施需求與資通安全需求，完成訪談後，於申請單回覆可行性評估結果。

(三) 經可行性評估後，若為可自行開發之系統，由資訊單位先與需求單位確認其需求，規劃人力與進度，系統之資通安全需求應符合「資通安全責

任等級分級辦法」附表九所定資通系統防護需求與附表十相應之控制措施，撰寫時將其納入「需求分析書」。

(四) 需委外之系統專案，依據本院適用之採購法規，進行委外採購流程，相關作業規範，依「B330-I314_委外安全管理作業說明書」辦理。

(五) 應納入各種容量之規格需求，包括中央處理器、系統記憶體、儲存媒體、網路頻寬等，避免系統上線後因容量不足而產生資料遺失、錯置或延遲等狀況。

(六) 需求分析書權限控管應依最小授權原則，詳列需求；對於個資項目之存取權限，參照「中央研究院資通安全管理規範實施要點」辦理。

(七) 電子形式軌跡資料(Log)

1. 紀錄應保存 6 個月以上，並定期檢視其紀錄異常狀態。
2. 登入作業完成後，宜顯示前一次登入成功或失敗之時間或相關訊息
3. 紀錄訊息應包含以下情況：

A. 系統管理人員及具備特殊權限帳號者之登入成功及失敗事件。

B. 使用者帳號異動及對通行碼之讀取與變更。

C. 程式原始碼及執行碼之變更。

D. 直接進入資料庫管理系統變更資料。

E. 系統設定檔之存取及變更。

(八) 本院對外服務網站之資安防護須遵守下列規定

1. 應提供符合至少 TLS 1.2 安全規定之加密連線方式。
2. 應用系統設定檔、記錄檔及備份檔禁止存放於公開網頁目錄中。
3. 敏感性資料應以加密傳輸，進行加密連線、數位簽章時不得使用已遭破解或具有高度風險之演算法。

(九) 其他

1. 應限制連續登入失敗次數之上限，登入失敗次數達上限者，應暫停該帳號一定時間之登入，或鎖定該帳號直到系統管理人員重新啟動。
2. 必要時應限定使用者之 IP 位址。
3. 宜設定可開放連線之時間或連線逾時自動登出之機制。

4. 除帳號、通行碼外，應依業務需求考量是否採用其他適切之身分鑑別技術。

(十) 應限制內含個人可識別資訊(PII)之敏感資料暴露，並遵循法律、法令、法規及契約的要求。

(十一) 除業務需求外，個人可識別資訊(PII)之敏感資料除必要顯示資訊外，宜採用資料遮蔽技術予以保護之。

二、 設計階段

(一) 依需求分析書展開設計，並撰寫系統設計書，內容得包含功能、模組、使用介面、作業流程、權限控管、資料綱要、共用模組或元件之設計與設施規格等，完成後於「redmine 系統」紀錄資通服務工作，得製作雛形畫面供需求單位確認。

(二) 應用系統之使用者登入驗證宜參照本院之使用者驗證機制，如：單一簽入機制（SSO），如有特殊情形須經作業單位主管同意。

(三) 系統設計書由作業單位主管查核功能設計是否符合涵蓋需求分析書之全部需求。

(四) 對於複雜程度較小之應用系統，其需求分析書與系統設計書可以合併。

三、 開發階段

(一) 於開發區編寫程式並對程式原始碼版本進行管理，如；「Git 系統」。

(二) 程式撰寫應注意事項，但不僅限於如下：

1. 可使用同一資料夾來存取應用系統自身的資源，確保應用系統容易移轉。
2. 適時加上註釋，幫助解讀。
3. 以參數化方式設計，可能變動的資料。
4. 資料源存取控制，採循最小授權原則。
5. 程式所用通行碼應經過加密。
6. 驗證使用者輸入的資料。

(三) 若系統服務屬於 Web 型態，不得於 Web 目錄內放置非Web 服務相關檔案，並防止前端使用者線上瀏覽內容。

(四) 需求單位對資通系統開發/維護，應對進行開發/維護之資通系統軟體程式碼的版次及內容，進行妥善的管控紀錄於「Git 系統」，並視版本更新情形隨時調整。

(五) 若使用開源軟體進行資通系統開發作業，使用時應注意：

1、 宜為開放原始碼促進會（OSI）出版的文件，以確定軟體之許可證是獲得該會的開源軟體標記。

2、 開源軟體宜自開放原始碼促進會（OSI）會員取得，以確保其授權與安全性。

3、 宜取自各公開、具公信力之開發論壇；如：GitHub。

4、 宜經開放原始碼分析檢測後，無資安疑慮之軟體，且能提供修復服務。

5、 未經檢測或無檢測說明、報告之第三方元件，宜確認其安全性後方可利用。

四、 測試階段

(一) 進行測試前，應執行程式碼審查作業，建構獨立測試環境及測試案例，將結果填寫於「redmine 系統」。

(二) 系統應執行原始碼檢測及黑箱測試安全檢測，檢測後評估嚴重程度及必要性，至少修補或排除嚴重及高等級之軟體弱點。

(三) 測試資料由需求單位提供或以模擬資料進行，如需取自正式資料庫填寫**「redmine 系統」**申請，經核可後才能使用，測試完畢不再使用後應逕行銷毀。

(四) 測試區與正式區所使用之環境、資料應予以區隔。

(五) 逐項測試功能規格，除正常操作功能，亦應充分測試不當操作，檢測權限控管與防呆控制是否齊全。並記錄異常狀況程式，將結果填寫於「redmine 系統」。

(六) 開發者完成測試後，得開放使用者於測試區進行測試，如有效能遲緩或設施容量不足疑慮時，進行壓力測試。

(七) 測試結果如屬程式錯誤，由程式開發者改正；如屬系統平台問題，由該平台負責人員處理；如屬資料庫問題，由資料庫管理者處理。

(八) 參加測試的人員對資料負保護與保密之責，尤其是機敏資料。

(九) 應用系統建議使用之瀏覽器種類皆應進行測試，如有使用限制，應於應用系統上做適當公告或說明。

五、 部署階段

(一) 應用系統於開發完成後部署至測試區，通過測試後，部署至正式區，並將過程記載於「redmine 系統」。

(二) 視需要撰寫操作手冊，並舉辦推廣及教育訓練。

六、 變更管理

(一)應用系統設定變更之項目應詳加記錄，如作業系統設定或參數調整紀錄於「git 系統」，供管理上參考。

(二) 需求變更管理

1. 應用系統開發人員(委外系統則由專案承辦人)應說明變更緣由及範圍，填寫「行政作業系統-新功能申請回報」，經核准後執行。
2. 如欲於採遠端連線方式進行應用系統變更時，執行變更之單位應提出變更計畫；包含變更失敗時之回復作業，並依「B330-I310 網路安全管理作業說明書」之規範開啟網路通道，由管理者監控系統之變更。
3. 應用系統變更前，應評估對各使用單位之影響，並公告系統變更時間，並先確認該系統已完成備份，變更過程若遇問題無法排除，應即進行回復作業，分析原因並重新評估變更作業。
4. 應用系統完成變更作業後，應更新相關系統文件並將過程記載於「redmine 系統」。

七、 維運作業

(一) 因應法規變遷、業務部門需求新增或變更與使用者建議進行系統維護。

(二) 維護需求依影響範圍進行需求、設計、開發、測試與部署五階段。

(三) 進行測試時，應測試變動的程式碼及相關聯之功能。

(四) 若增補權限控管功能，應檢測資料是否異常並改正。

(五) 應用系統之權限異動作業依「B330-I309 存取控制作業說明書」辦理。

八、 資料庫安全管理與維護

(一) 資料庫使用者安全

1. 資料庫系統管理者帳號應為專屬，並限制資料庫系統管理者群組之成員，資料庫僅供成員使用。
2. 資料庫系統管理者應每年至少辦理帳號、權限清查一次，檢視權限與職務之適切性，以及是否留存閒置帳號等。

(二) 資料庫管理系統安全性

1. 資料庫存取帳號、權限應視不同資訊系統、人員存取之需求進行適當設定。
2. 資料庫系統管理者應定期檢查是否有異常狀況，並進行必要之分析與處理。

(三) 資料庫維護

測試區及正式區之資料庫維護作業，應填寫於**「redmine 系統」**，並經核准後始可由資料庫系統管理者辦理。

(四) 資料庫備份

1. 重要資料庫應定期備份，並定期抽檢備份資料是否可用，資料庫備份之存放點，僅供授權人員存取。
2. 資料庫備份請參考「B330-I308 備份與復原作業說明書」。

(五) 資料庫存取稽核紀錄，針對所存放敏感性資料啟動相關安全稽核紀錄功能（包含查詢與異動），於不影響正常運作效能之情況下，由經授權人員讀取資料庫稽核紀錄。

九、 應用系統下線作業程序

(一) 系統下線程序

1. 系統管理單位於執行系統下線前，應提出下線作業規劃，經權責主管核准後始得執行。
2. 系統下線前，應完成資料盤點、資料取回及後續資料處置之規劃。
3. 系統正式下線後，應停止所有對外服務及一般業務使用，並更新資訊資產清冊。

(二) 資料取回程序

1. 系統下線前，系統管理單位應盤點系統內所儲存之業務資料、個人資料及其他敏感性資訊。
2. 如系統資料未來仍具業務需求，應於系統下線前完成資料匯出或備份，並依資料分類原則安全保存於經核准之儲存環境。

(三) 系統重啟程序

1. 已下線之系統不得重啟使用，如因特殊或不可避免之業務需求有重啟必要時，應事前提出申請，經權責單位審核同意後，始得進行。
2. 系統重啟前，應確認系統已完成惡意程式掃描、弱點檢視及必要之安全設定，並於重啟期間限制系統對外連線及使用範圍。
3. 系統重啟完成後，應立即執行必要之資料取回作業，並於作業完成後再次關閉系統，不得長時間維持啟用狀態。

(四) 資料清除程序

1. 確認系統資料已完成取回或確認無須再保存後，應依資料敏感性及相關法令規定，執行資料清除或銷毀作業。
2. 資料清除方式應確保資料無法被復原或再次存取，以降低資訊外洩風險。

貳、參考文件

一、 B330-I310 網路安全管理作業說明書

二、 B330-I314_委外安全管理作業說明書

三、 B330-I309 存取控制作業說明書

四、 資通系統籌獲各階段資安強化措施(行政院 1110526 版)

參、使用表單