OOOO 公司

資訊系統獲取、開發及維護管理作業程序

ISMS-B-008

版本 1.0

中華民國 105 年 MM 月 DD 日

1. 目的

為使 OO 公司（以下簡稱本公司）為建立資訊應用系統之獲取、開發及維護管理，依循相關資訊安全管理規定，以確保資訊系統開發與敏感資訊處理之安全性，保障開發流程之品質，並維持系統的安全與正常運作。

2. 範圍

適用於資訊安全管理制度範圍內相關部門之資訊系統開發、維護或獲取及操作人員、委外承包商與服務提供廠商，執行應用系統開發維護作業均適用之。

3. 權責

3.1 資訊單位主管

3.1.1 指派應用系統委外開發及維護之承辦人員。

3.1.2 協助採購單位審查系統開發或變更之招商與驗收。

3.1.3 指派各應用系統發展及維護之承辦負責人。

3.1.4 監督應用系統發展工作。

3.1.5 審查應用系統發展、上線或系統變更申請。

3.2 應用系統負責人

3.2.1 負責或協助應用系統發展工作。

3.2.2 執行管理應用系統發展及變更作業。

3.2.3 確認與管理應用系統維護、備份規劃與回復測試等作業。

3.3 業務需求單位

提出應用系統使用或發展之需求申請。

4. 定義

4.1 委外廠商

承攬本公司應用系統開發與維護作業之第三方機構。

4.2 系統發展生命週期 (System Development Life Cycle; SDLC)：以有組織的方式用來開發一個企業的資訊系統。

4.3 非涉及應用系統程式邏輯異動之系統變更

變更作業不影響程式原始設計之修改，例如使用者介面調整，系統參數調整。

4.4 應用系統程式邏輯異動之系統變更

變更作業影響程式原始設計之修改，例如系統錯誤修改，系統功能擴充。

4.5 應用系統程式緊急變更

因作業時效急迫，而無法遵循標準變更審核程序，需要立即進行變更之程式修改作業。

5. **作業內容**

5.1 系統開發一般安全要求

5.1.1 於資訊系統開發或獲取前，須將資訊安全需求納入考量並獲得核可，並於專案管理作業中實施。

5.1.2 資訊系統開發維護作業應區分正式服務環境、開發測試環境，以確保資訊系統、程式與資料之機密性、完整性、可用性與個人資料之要求。

5.1.3 防止資訊系統中的輸入資訊錯誤、遺失與未經授權的修改或使用。

5.1.4 必要時採用加解密機制以保護資訊的機密性、完整性、可用性與個人資料之安全。

5.1.5 系統檔案及資料庫之存取權限，應限制僅被授權者可以存取，以確保其安全性。

5.2 系統開發之專案管理安全要求

5.2.1 應將資訊安全要求整合納入專案需求與其管理作業，以確保將識別並處理資訊安全風險作為專案之一部份。例如：核心業務流程、資訊系統、設施管理與其他支援流程之系統開發或獲取。

5.2.2 應將資訊安全政策要求或資訊安全目標，依專案特性適度的納入專案管理目標內。

5.2.3 應於專案作業中，實施資訊安全之風險評鑑，以識別出必要的控制措施。

5.2.4 應對專案作業人員，界定其角色與配置其相關之資訊安全責任。

5.2.5 應定期處理與審查，專案作業是否符合資訊安全相關政策要求。

5.3 系統開發及支援過程的安全

5.3.1 應考量下列安全開發作業之原則

5.3.1.1. 開發環境之安全設計。

5.3.1.2. 軟體開發生命週期之安全指引：

5.3.1.2.1. 軟體開發各流程之安全要求。

5.3.1.2.2. 所用每一程式語言之安全編碼指導綱要。

5.3.1.3. 系統設計階段之安全要求。

5.3.1.4. 軟體開發生命週期之各階段安全查核點。

5.3.1.5. 儲存庫、版本控制安全設計。

5.3.1.6. 開發作業之應用系統安全知識及監測、避開、發現或修補脆弱性之能力。

5.3.1.7. 應權衡資訊安全之需求與可行性之需求，將安全性設計納入所有架構內(營運流程、資料流程、應用系統流程及技術應用）。

5.3.1.8. 確認軟體、硬體之供應者，其組織管理、技術能力與人員等安全控制的嚴謹性，應與公司本身相當。

5.3.1.9. 應評鑑個別系統開發工作有關之風險，建立安全發展環境，並考量下列項目：

5.3.1.9.1. 系統處理、儲存及傳輸之資料的敏感性。

5.3.1.9.2. 適用之外部及內部要求事項， 如法規或政策要求。

5.3.1.9.3. 支援系統發展已被要求，並建立安全控制措施。

5.3.1.9.4. 對發展環境存取之控制措施。

5.3.1.9.5. 對環境及存於其中程式碼變更之監視。

5.3.1.9.6. 異地備份儲存之位置與安全設計。

5.3.1.10. 針對新的及更新之系統(包括自行開發或採購獲得)需在開發過程中經過測試及查證，包括測試活動詳細時程、測試輸入及在條件範圍內預期輸出等。若為內部開發，開發人員宜最先執行上述測試，然後再進行獨立的驗收測試（內部及委外皆然）以確保系統如預期且僅如預期運作。

5.3.2 資訊系統需執行修補程式或關閉不使用之服務，以降低因使用已公布的資訊系統技術弱點而導致的風險。

5.3.3 除了資訊系統自動的安全控制外，亦可加入手動執行安全控制措施。

5.3.4 資訊系統相關文件(如該系統之操作手冊/維護手冊)應明確標示資訊安全控制措施（如：備份與回復方式），以利使用者及技術支援人員瞭解系統之安全控制措施。

5.3.5 應將資訊系統及資料庫之處理過程記錄於作業或稽核日誌（Log）。

5.4 資訊系統檔案的保護

5.4.1 對具關鍵或敏感的資訊，應在傳輸或儲存過程中利用加密或其他合宜之措施保護(如數位簽章或訊息鑑別碼)，以確保資訊的機密性、完整性、可用性與個人資料之安全。

5.4.2 應遵循本公司訂定的資料保密規範，及本公司認可的加密或其他合宜之措施，以確保加密技術產品的安全功能。

5.5 應用系統發展需求分析

5.5.1 業務需求單位向本公司資訊單位提出應用系統發展需求，或

於系統維護過程產生之系統功能增修需求，應填寫資訊系統需求申請單，請業務需求單位確認後，進行系統開發與變更事宜。

5.5.2 年度編列執行工作應用系統發展項目，得經由權責主管核可後，進行辦理。

5.5.3 未列入年度編列執行工作應用系統發展項目，須由業務需求單位自行尋求預算來源與評估系統開發的效益及成本，並簽請總公司長核准後，一併向本公司資訊單位提出開發需求申請，且視其需要得報請本公司資訊安全管理委員會覆核。

5.5.4 系統取得、開發或變更需求確認，應參考現有的系統或作業文件，了解現行的作業流程，利用分析所收集到的資料，進行可行性暨技術、作業執行及應用效益之評估，亦應考量對現有環境之影響。

5.5.5 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。

5.5.6 系統取得、開發或變更需求經評估可行後，由本公司資訊單位承辦人員展開系統開發規劃工作，若不同意則須分析原因，並以資訊系統需求申請單或公文回覆業務需求單位。如需進行委外，則依據本程序之委外應用系統開發安全管理規劃辦理。

5.5.7 執行應用系統發展與維護之各階段活動時應參考「應用系統相關文件內容檢核表」產生相關文件。

5.5.8 承辦人員或委外廠商應對應用系統提出未來資料量的成長趨勢，並依實際資料量及成長量大小申請空間，以避免發生資料儲存空間不足的情況；評估應用系統使用量，以維持應用系統上線效能。若服務負載過重的應用系統採取垂直與水平延展擴充，避免效能問題發生。

5.5.9 承辦人員依據應用系統特性規劃應用系統程式備份，應用系統備份作業依據【通訊與作業管理作業程序】規範辦理。

5.5.10 目前系統欠缺之必要文件，應排定計畫補齊。

5.6 應用系統安全功能

5.6.1 程式開發需使用帳號驗證機制時，應考慮使用其他安全驗證機制整合，以確保安全性，如公開金鑰基礎架構（PKI）、授權認證（CA）機制、輕量級目錄存取協定（LDAP）與自訂使用者資料庫(帳號、密碼編碼原則)。

5.6.2 自訂使用者資料庫存放使用者密碼時應避免存放明碼，在密碼寫入資料庫時考慮利用加解密元件或是用雜湊，以保護密碼不被外洩。

5.6.3 應用程式申請使用資料庫系統的 Table，若確定這些 Table 並不需要使用到時，應提出申請予以刪除，以免惡意使用者利用這些 Table 獲取過多資訊。

5.6.4 程式設計應對字串的輸入加以過濾，並限制長度，例如單、雙引號都應過濾。

5.6.5 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。

5.6.6 進行資料強制輸入檢查，並限制前端應用程式資料輸入的長度與型別，另於輸入敏感資訊時使用適當之顯示隱碼功能。

5.6.7 應用程式應設計各種例外狀況管理（擷取和回傳例外狀況、設計例外狀況案例、傳送例外狀況資訊）與處理機制，以擷取與存錄錯誤資訊，並防止直接顯示原始完整錯誤資訊給予使用者。

5.6.8 應用程式應具備檢驗登入身分識別、認證與密碼保護功能（例如密碼長度限制、密碼組合限制、密碼錯誤次數限制與變更密碼歷史管理等）。

5.6.9 應用程式應具備依據【資訊資產管理作業程序】之資訊控管程序，以確保資訊受到適當等級之保護。

5.6.10 自行開發或委外專案開發之程式，應進行惡意程式碼之檢查並予以紀錄留存備查。

5.7 系統檔案安全

5.7.1 作業系統控制

5.7.1.1. 作業系統安全管理，應依據【通訊與作業管理作業程序】與【存取控制管理作業程序】規範辦理。

5.7.1.2. 各作業系統與應用系統應均規劃適當之閒置時間，並於使用者登入超過該時間且無任何動作時，自動將其帳號登出。

5.7.1.3. 程式執行檔與暫存檔應採取適當檔案保護措施（例如：加密或存取限制）。

5.7.1.4. 現有系統無法達到上述要求，且維護不符合效益，應於獲取、開發時納入考量。

5.8 應用系統資料管理

5.8.1.1. 為保護資料的安全，應依據【資訊資產管理作業程序】與【通訊與作業管理作業程序】規範辦理。

5.8.1.2. 測試系統與正式系統所使用之環境、資料應適當區隔，使用者測試前之測試資料若為真實資料，應應保護測試資料，並將敏感性之資料內容轉換為相同格式之虛擬資料內容或是採取與真實環境相同程度之安全管控。

5.8.2 應用系統開發程式原始碼管控

5.8.2.1. 若程式原始碼為本公司所有，進行應用程式變更前，應確認現行使用程式版本，並取出現行使用程式版本之原始碼，進行變更之程式開發作業。

5.8.2.2. 應用程式變更完成後，應請承辦人或委外廠商提供變更後之程式版本，存放於不可抹寫之儲存媒體或存入程式庫納管。

5.8.2.3. 測試產品之前，應對程式原始碼進行抽查及評審，必要時執行程式原始碼審查(Code Review)。

5.9 應用系統開發與維護安全

5.9.1 應用系統上線管理

5.9.1.1. 應依據執行應用系統發展與維護之各階段活動時參考「應用系統相關文件內容檢核表」所產出相關文件進行上線管理作業。

5.9.1.2. 依據需求規格書之規範，決定是否進行壓力測試並提出報告，若測試無法通過，由承辦人員或委外廠商進行環境設定或其他調整，再次進行測試。

5.9.1.3. 承辦人員或委外廠商之程式設計須事先研擬測試計畫並制定測試計畫書，測試過程須有各階段之測試紀錄，測試計畫書應經應用系統承辦人或請業務申請單位協助審核通過後才作為測試之依據。

5.9.1.4. 承辦人員或委外廠商應依據測試計畫書備妥測試環境後，由應用系統承辦人及業務需求單位等使用者進行系統測試。

5.9.1.5. 承辦人員或委外廠商程式測試完成後，須製作測試報告書，經由應用系統承辦人或請業務需求單位協助審核後，始得進行系統驗收與上線。

5.9.1.6. 業務需求單位依承辦人員或委外廠商之測試報告書進行再確認及測試，如測試中發現系統錯誤，應請承辦人員或委外廠商完成錯誤修正。非系統錯誤之建議修改需求，承辦人員或委外廠商應盡力完成，若無法達成，則由承辦人員或委外廠商與業務需求單位進行協調。

5.9.1.7. 系統如透過網路存取，承辦人員或委外廠商應執行適當之安全測（試例如：是否有不必要的帳號、管理員帳號密碼安全程度、是否有設定安全稽核功能及是否存在緩衝區溢位問題等）。

5.9.1.8. 應用系統上線前，承辦人員或委外廠商應產出系統文件，以輔助業務需求單位系統之使用與管理，系統文件

管理依據【通訊與作業管理作業程序】規範辦理。

5.9.1.9. 承辦人員與業務需求單位應對委外廠商進行驗收作業規劃，並依驗收作業規劃辦理驗收。

5.9.2 應用系統變更與維護管理

5.9.2.1. 全公司應用系統應進行變更與維護管理，其餘系統應保留適切程式異動相關紀錄。

5.9.2.2. 執行應用系統維護與作業（如直接異動資料檔、變更系統設定、更新 Patch 等），應填寫「應用系統維護紀錄表」，交承辦人員覆核。

5.9.2.3. 涉及資料庫變更，填寫「應用系統維護紀錄表」陳核後，送本公司承辦人員進行變更作業。

5.9.2.4. 變更之影響範圍，若包含其他單位，應同時通知相關處單位，並於變更執行前，與各單位協調實施時間，以利變更程序之執行。

5.9.2.5. 非涉及應用系統程式邏輯異動變更

5.9.2.5.1. 經本公司判斷，若為不影響應用系統程式邏輯之單純應用系統之變更或設定，則承辦人員或委外廠商將欲更動之變更或設定項目填寫於「應用系統維護紀錄表」，變更作業完成後由承辦人員進行覆核。

5.9.2.5.2. 更動之設定項目需詳加記錄（如應用系統設定或參數調整），以供後續管理或系統文件修訂參考。

5.9.2.5.3. 變更項目如已有系統管理或是相關紀錄控管，且經承辦人員簽核，可將該紀錄作為應用系統變更紀錄保存並備查。

5.9.2.6. 應用系統程式邏輯異動變更

5.9.2.6.1. 承辦人員或委外廠商確實測試變更程式之正確性與其他未修改程式之影響，不因執行程式變更導致系統其他問題。

5.9.2.6.2. 應用程式修改完成後，承辦人員或委外廠商填寫「應用系統維護紀錄表」，經承辦人員核准，始得進行變更作業，且申請表中應特別註明變更項目及變更原因，並由承辦人判斷檢附下列資料之必要性：

5.9.2.6.2.1. 新版本程式或設定之測試執行結果。

5.9.2.6.2.2. 新舊版本程式或設定之差異分析比較。

5.9.2.6.2.3. 依據備份現況，並制訂還原步驟。

5.9.2.7. 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。

5.9.2.8. 作業系統變更應依據【通訊與作業管理作業程序】規範辦理，並對現有應用系統之影響，進行相關測試。

5.9.2.9. 商業套裝軟體之修改，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管理程序進行修改，如因特殊需求需要變更，應考量下列事項：

5.9.2.9.1. 是否會破壞系統內建的安全控制以及系統的完整性。

5.9.2.9.2. 應得到套裝軟體供應商的允許。

5.9.2.9.3. 應考量標準化的系統更新方式，並請供應商進行必要的變更，同時執行變更或修改之相關作業應符合資訊安全相關要求。

5.9.2.9.4. 應考量如自行變更套裝軟體，日後對軟體維護作業的影響。

5.9.2.9.5. 套裝軟體如需變更，應保留原始軟體，所有變更應有完整的測試並記錄，俾利日後軟體升級之用。

5.9.3 應用系統程式緊急變更

5.9.3.1. 承辦人若判斷為緊急狀況時，報請承辦人員同意後進行變更。

5.9.3.2. 變更完成後，應補填「應用系統維護紀錄表」，並備妥相關附件備查。

5.9.4 應用系統變更紀錄保管

5.9.4.1. 「應用系統維護紀錄表」變更紀錄由承辦人或委外廠商填寫，待變更作業與表單覆核完成後，由資訊安全文件管理中心進行歸檔。

5.9.4.2. 執行變更申請程序中所附之相關附件由應用系統承辦人員自行歸檔保管。

5.9.5 委外應用系統開發安全管理規劃

5.9.5.1. 系統開發或變更委外作業時，由承辦單位依據採購相關規定，進行委外採購流程。

5.9.5.2. 由承辦單位規劃資訊服務依採購評選方式，撰寫需求規格書，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。

5.9.5.3. 系統開發或變更專案，投標廠商應提出服務建議書或企劃書等文件，內容須包含開發時程、效益與人力需求分析，並須說明應用系統所應達成的功能；否則應於其他正式文件中規劃前述內容，供系統承辦人員審核。

5.9.5.4. 應用系統維護合約期間之變更需求(如小幅度之功能增

修)，由本公司資訊單位承辦人員依據維護合約內容，聯繫廠商進行系統開發或變更評估作業，並記錄於維護工作報告中，屬系統簡易修改，須於當年度維護合約期限內完成，否則列入下次採購案辦理；若評估須另起專案處理（大幅修改或變更）則依專案程序辦理。

5.9.5.5. 為確保安全性與可靠性，委外開發或維護之應用系統，應於合約中明訂下列事項：

5.9.5.5.1. 委外開發或維護之系統，應與委外廠商明訂服務水準協議（Service Level Agreement)，以規範支援及維護方式，確保系統或業務的正常進行。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，應依據服務水準協議對委外廠商進行罰責。若專案需暫停或取消，承辦單位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。

5.9.5.5.2. 作業時如發生錯誤或資料漏失，經確認屬委外廠商責任時，應由委外廠商負責更正；另損及他人權利義務，委外廠商亦須負責。

5.9.5.5.3. 委外廠商對業務上所接觸之資料，應視同密級文件採必要之保密措施，委外廠商及人員均應依本公司規定填具【人力資源安全管理作業程序】之委外廠商保密切結書，任何因程式開發洩密所致之賠償及刑事責任，概由委外廠商負責，並列入本公司拒絕往來戶。

5.9.5.5.4. 委外廠商於重大之資訊安全威脅發生時應主動提供之維護服務內容。

5.9.5.5.5. 依據業務流程分析結果，要求各委外廠商依據系統之重要性訂定維護服務內容，並執行必要的應用系統架構復原演練，維護服務內容至少應包含服務廠商人員資歷、服務時間、問題處理與回覆方式、問題處理時限、系統回復時限與系統備援程序等。

5.10 系統技術脆弱性管理

5.10.1 應向承辦人員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。

5.10.2 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。

5.10.3 系統弱點管理

5.10.3.1. 由資訊安全工作分組擬定弱點掃描計畫，並經資訊安全推動組召集人同意後進行。

5.10.3.2. 執行掃描作業前，應通知相關負責人，以預為應變。

5.10.3.3. 資訊安全推動組每半年執行一次掃描作業，必要時可委由廠商執行。

5.10.3.4. 弱點掃描後應產生弱點掃描報告。弱點掃描報告格式不拘，但應包含弱點掃描檢測時間、範圍、風險程度說明。

5.10.3.5. 掃描出之弱點應限期改善，並填寫「弱點處理報告單」，且於修補後進行再次檢測。

5.10.3.6. 弱點修補應先測試環境評估無礙後（必要時可委由廠商執行），方可執行修補作業，並將弱點修補結果彙整後交權責主管覆核。

5.10.3.7. 弱點若因故無法修補，相關管理人員於「弱點處理報告單」說明無法修補之原因與防禦因應方法。

5.11 現有系統無法達到上述要求，且維護不符合效益，應於重新獲取、開發改版時納入考量。

6. 相關資料

6.1【通訊與作業管理作業程序】

6.2【存取控制管理作業程序】

6.3【資訊資產管理作業程序】

6.4【資訊安全管理作業程序】

6.5【遵循性管理作業程序】

6.6【人力資源安全管理作業程序】

7. 附件

7.1 應用系統相關文件內容檢核表

7.2 應用系統維護紀錄表

7.3 弱點處理報告單