雲林縣西螺鎮公所

資訊系統開發與維護管理程序

文件編號： XLTG-02-012

版　　次： V1.0

文件日期： 110 年 11 月 24 日

機密等級： 普通

文件制/修訂履歷

制/修訂 版次	制/修訂 日期	制/修訂 說明	作 者	備 註
V1.0	110.11.24	初版發行	ISMS 執行小組	

目　　錄

壹、 目的

雲林縣西螺鎮公所(以下簡稱本所)為確保資訊系統營運安全，就資訊系統軟硬體設備獲取、開發、安裝上線及維運時，有關資訊安全事項予以規範,特訂定本「資訊系統開發與維護管理程序」(以下簡稱本程序)。

貳、 適用範圍

本程序適用於本所資訊系統軟硬體設備獲取、開發、安裝上線及維運之相關作業。

參、 權責

一、 資安長或其授權人核定、發布本程序。

二、 ISMS 執行小組組長審查本程序，並督導本程序之執行。

三、 ISMS 執行小組研擬、評估及檢討本程序。

四、 ISMS 承辦人協調及彙總本程序之執行。

五、 主機房管理相關人員：

(一)審查「資訊服務申請表」及「資訊系統上線作業紀錄表」。

(二)建立資訊系統測試及安裝環境。

(三)確認資訊系統修補或測試的結果。

(四)資訊系統變更或維護時之公告。

(五)通知資訊系統所發現之弱點、漏洞或威脅予相關人員。

(六)對於資訊系統所發現之弱點、漏洞或威脅進行影響評估，並決定是否修補。

六、 應用系統管理人員：

(一)安裝應用程式和資料庫。

(二)於相關文件中規定資訊安全控制措施。

(三)對於資訊系統所發現之弱點、漏洞或威脅進行影響評估，並決定是否修補。

(四)評估資訊系統安全控制措施和系統的完整性。

(五)維護處理之過程紀錄。

七、 需求單位：

(一)進行資訊系統安全需求分析，並將安全需求納入需求規格相關文件中。

(二)申請系統測試作業。

(三)確認「資訊系統上線作業紀錄表」之要求項目，並執行掃瞄確定無任何已知病毒及漏洞存在。

(四)資訊系統建置、變更或測試需安裝上線時，填寫「資訊服務申請表」及「資訊系統上線作業紀錄表」。

八、 申請單位：

(一)執行資訊安全檢測。

(二)檢附需交付文件。

九、 開發單位：協助進行資訊系統安全性檢測。

肆、 定義

一、 資訊系統：提供網路資訊作業有關的軟硬體設備，包括網路基礎設備(網路連線設備、安全防護工具、網管軟體及伺服器)、作業系統、應用系統、資料檔案或資料庫等皆屬之。

二、 資訊系統變更:指改變資訊系統軟硬體環境之行為,如作業系統、應用系統、套裝軟體、資料檔案或資料庫、系統組態設定、系統主機與其週邊設備等的更換或更新。

三、 資訊系統修補：指修正資訊系統之弱點或漏洞。

四、 重大更新程式：指作業系統或應用系統大幅度更新版本，如 Windows XP 作業系統由 SP1 更新到 SP2 等。

五、 系統更新及維護：指系統程式增修或改版，以及維持系統正常運作之必要調校。

六、 資訊系統測試：指利用本所網路環境進行資訊系統軟硬體設備之安裝、運轉及安全性等檢測作業。

七、 資訊系統上線：指資訊系統安裝於本所網路環境的相關作業。

伍、 管理項目

在獲取新伺服器及資訊系統，或現有資訊系統之修補程式、更新程式須安裝上線及維運時，透過文件審查及安全檢測，以確保資訊系統之營運安全，有關資訊系統之安裝上線及維運作業程序如下圖 5-1 所示：

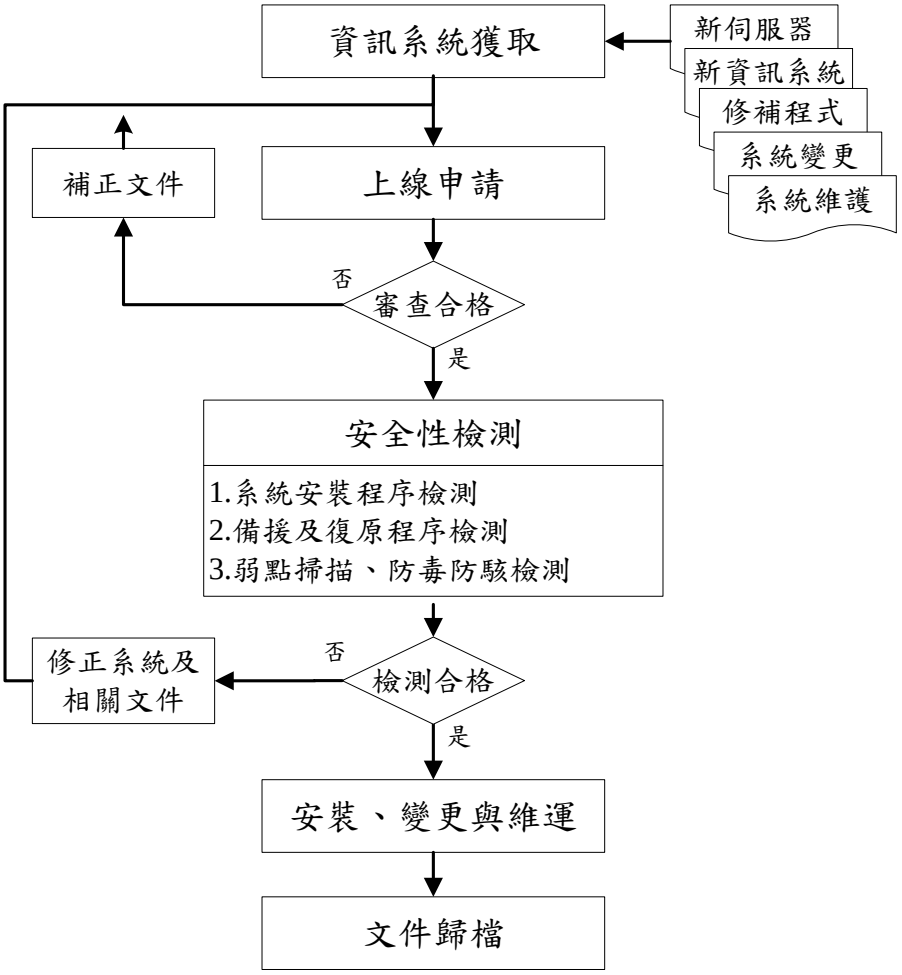

圖 5-1：資訊系統上線管理程序

一、 資訊系統獲取

規劃建置資訊系統及申請上線前，應注意下列事項：

（一）需求單位應在資訊系統規劃、新系統開發、現有系統功能強化之需求分析階段或套裝軟體採購前，進行資訊系統安全需求分析，並將安全需求納入需求規格相關文件中。

（二）資訊系統安全需求分析應考量事項如下：

1. 應遵守法規或合約上對資訊安全控制的要求。

2. 評估保護資訊機密性、完整性及可用性的需求：

(1)對具關鍵或敏感的資訊，應在傳輸或儲存過程中予以加密保護，以確保其機密性。

(2)對關鍵或敏感的資訊若有需要，應在傳輸或儲存過程中使用數位簽章或訊息鑑別碼，以偵測訊息內容是否遭受未經授權的更改或破壞，確保訊息的完整性與可鑑別性。

(3)應遵循本所訂定的資料保密規範，以及本所認可的加密模組，以確保加密技術產品的安全功能。

3. 對資訊及系統存取的控制：

(1)使用者權限控管措施，避免未經授權的使用或修改。

(2)重要業務應建立例行性的稽核制度，並為特定查核之事項建立稽核軌跡。

4. 對資訊及系統檔案的保護：

(1)系統檔案之權限應限制僅有系統管理者可以存取，以確保其安全性。

(2)應保護機密性或敏感性資料，防止洩露或被竄改，必要時應使用資料加密等技術保護。

(3)重要的系統檔案及業務資料，應有備份與復原機制。

（三）系統安全原則：

(1)輸入及輸出資料應有確認機制，以確保所處理及儲存資料的正確性。

(2)重要的資料，應在資料處理過程的每一階段，或是特別選定的某一階段，檢查及保護資料的真確性。

(3)應記錄適當之稽核軌跡，以協助資通安全事件之調查與存取控制監視。

2. 找出及決定各種不同的安全控制措施，訂定系統回復作業程序，以防範、偵測電腦當機或發生安全事件時,能立即執行回復作業。

3. 系統的安全需求及控制程度，應與資訊資產價值相稱，並考量安全措施不足對機關可能帶來的傷害程度。

4. 應於相關文件規定資訊安全控制措施，以利使用者及應用系統管理人員明瞭資訊系統內建之安控系統功能。

（四）機房管理相關人員或應用系統管理人員於取得資訊系統重大更新程式後,應於測試環境進行測試,確認不影響資訊系統運作再申請上線。

（五）資訊系統軟硬體設備需使用網路進行系統測試時，需求單位得申請系統測試作業，以建立系統測試環境。系統測試環境之安全性檢測，由需求單位會同機房管理相關人員辦理。

（六）需求單位於申請資訊系統上線前，應就「資訊系統上線作業紀錄表」內所要求項目進行確認，並執行掃瞄確定無任何已知病毒及安全性高之漏洞存在。

二、 系統變更流程

（一）提出申請

資訊系統建置、變更或測試需安裝上線時,需求單位應填寫「資訊服務申請表」及「資訊系統上線作業紀錄表」,於作業說明欄載明申請原由或依據、作業方法、影響範圍，經核可後始得辦理。

（二）審查作業

1. 機房管理相關人員於接獲需求單位提出申請時，應審查「資訊服務申請表」及「資訊系統上線作業紀錄表」內容與檢附文件是否齊備，並填具審查意見。

2. 「資訊服務申請表」審查時，應注意以下事項：
   (1)作業說明與作業項目是否一致。
   (2)攜帶設備或媒體之用途是否適宜，並考量風險程度，決定是否允許攜入。
   (3)有關申請作業時間，應考量安全性檢測相關設備準備及執行測試所需時間。
   (4)作業地點應考量實際需要，可於機房外之辦公場所或操作室以遠端登入連線方式進行，如非必要儘量避免進入機房。
   (5)防火牆設定申請之連線，應考量實際系統之作業需要。
   (6)實體 IP 申請，應考量網路作業需求及安全防護措施。

3. 「資訊系統上線作業紀錄表」審查時，應注意以下事項：
   (1)本所現有設備環境或軟硬體設備計畫所提供之設備環境，是否能滿足資訊系統運作環境需求。
   (2)於現有設備安裝(含更新或修補)資訊系統時，是否有檢附對現有設備內其他系統之影響(或相容性)評估或測試報告。
   (3)資訊安全檢測結果日期是否為最近一個月內所完成，且檢測結果處理是否可於上線前完成。
   (4)病毒及木馬程式偵測須敘明使用工具及版本，且無已知病毒或木馬程式。
   (5)應有取急復原制與相關文件(如:安裝手冊、網路/資料庫架構示意圖)

三、 安全性檢測

「資訊服務申請表」審查通過後，機房管理相關人員依據「資訊系統上線作業紀錄表」所記載之資訊系統環境需求說明，準備系統測試所需相關設備，將作業系統及修補程式更新到申請單位資訊安全檢測之最後更新日期(尚未更新部分由應用系統管理人員依系統變更方式處理)後，進行下列安全性檢測，並保全測試資料，必要時得要求需求單位或開發單位人員協助辦理。

（一）系統安裝程序檢測

1. 按系統安裝文件所記載之操作說明及步驟，進行系統安裝，以驗證系統安裝文件之正確性。
2. 安裝測試資料，按系統操作手冊之說明，挑選適當功能進行基本之操作，以確認系統可正常運行。
3. 檢測結果如發現安裝文件或操作手冊與實際結果不符或有所疑義，應予記錄，提供申請單位查明並修正系統及相關文件。

（二）備援及復原程序檢測

1. 按備援及復原計畫所記載之操作說明及步驟，進行資料備援，並確認是否與計畫之預期結果相符。
2. 按備援及復原計畫所記載之操作說明及步驟，進行資料復原，完成復原後，應比對復原結果與原資料是否一致。
3. 如發現備援及復原計畫與執行結果不符或有所疑義，應予記錄，提供申請單位查明並修正系統及相關文件。

（三）弱點掃描、防毒防駭檢測

1. 應用檢測工具確保程式碼無病毒或後門程式或執行弱點掃描處

理高風險項目。

（四） 系統測試資料之保護

1. 應保護及控制測試資料，避免以含有個人資料或敏感資訊的資料進行測試；如需應用，應於完成測試作業後立即移除，或將可辨識之個人資料或敏感訊息修改為無法辨識。

2. 在使用真實的資料進行測試時，應採行下列的保護措施：

(1)適用在實際作業系統的存取控制措施，亦應適用在測試用的系統。

(2)真實資料被複製到測試系統時，應依複製作業的性質及內容，在取得授權後始能進行。

(3)測試完畢後，真實資料應立即從測試系統中刪除。

(4)真實資料的複製情形應予以記錄，以備日後稽核之用。

四、 資訊系統安裝及維運

資訊系統於安裝、變更或維運時，可於機房外之辦公場所或操作室以遠端登入連線方式進行，如非必要儘量避免進入機房。如需進入機房作業，應先載明於「資訊服務申請表」內，經核可後始得進入。

（一） 資訊系統安裝

通過申請審查及檢測之資訊系統，始得安裝上線使用。為降低可能損及作業系統的風險，安裝資訊系統時，應依下列規定辦理：

1. 應用程式和程式庫的安裝或更新活動，應由機房管理相關人員或經授權之人員執行。

2. 將核准的執行碼放在作業環境內(原始碼及編譯程式禁止放在作業環境內)。

3. 應建立作業程式庫的更新活動稽核日誌。

4. 應保留資訊系統舊版軟體，以作為緊急應變措施之用。

5. 只有在必要時且經申請核准後，才能允許本所以外單位進行實體或邏輯存取。

6. 不得修改或破解商用套裝軟體(如:office/Windows)。

（二）資訊系統維運

1. 資訊系統需進行維護時，應評估其對重要的營運應用系統是否有負面的衝擊，或者產生安全問題。

2. 為避免遭到暗藏後門程式而對資訊系統進行未授權存取，造成資訊洩漏的風險，應執行下列事項：

(1)定期掃描對外通信埠，找出隱藏資訊。

(2)使用通過安全認證的系統和軟體。

3. 應用系統管理人員，應將維護之處理過程予以記錄並留存備查。

4. 應建立與相關資訊安全組織或廠商之聯絡管道，隨時獲取最新的技術性弱點即時資訊，評估本所所使用的資訊系統是否存在該弱點，並採取適切的安全措施或進行修補，以控管可能面臨的風險。

5. 在作業環境上執行應用軟體，應嚴格執行下列控制程序，減少可能危害作業系統的風險：

(1)應用系統資料之異動作業(如新增、修改、刪除等)，應於應用系統上為之，非經核可，不得逕自資料庫中修改。

(2)輸入應用系統的資料應予核對，以避免疏漏或誤植。

(3)經資訊系統處裡後的輸出資料應予以確認，以確保處理結果的正確性及完整性。

(4)作業用的應用程式館更新作業，應限定只能由授權的人員才

可執行。

（三）安全開發環境

(1)應保留舊版的軟體，以作為緊急應變措施之用。

(2)至少保留前一版穩定之程式碼，且進行版本控制。

(3)開發環境之重要資料或程式碼應有權限控管。

（四）委外開發

(1)應對委外系統開發商進行監督，確保交付程式之安全無病毒或惡意程式。

(2)委外開發合約應闡述資訊安全要求。

(3)委外開發程式碼資料應確保僅有相關專案成員可存取。

陸、 參考文件

一、 備份與回復管理程序。

柒、 使用表單

一、 資訊服務申請表。

二、 資訊系統上線作業紀錄表。

三、 重大安全更新確認表。