雲林縣西螺鎮公所

資訊安全手冊

文件編號： XLTG-01-002

版　　次： V1.0

文件日期： 110 年 10 月 08 日

機密等級： 普通

文件制/修訂紀錄

制(修)訂版次	制(修)訂日期	制(修)訂說明	作者	備註
V1.0	110.10.08	初版發行	ISMS 執行小組	

目　　錄

壹、 ISMS 方針與目標

雲林縣西螺鎮公所(以下簡稱本所)為強化資訊安全管理、確保資訊的機密性、完整性與可用性、資訊設備（包括電腦硬體、軟體、週邊等）與網路系統之可靠性，以及同仁對資訊安全之認知，並確保上述資源免受任何因素之干擾、破壞、入侵、或任何不利之行為與企圖，依據本所「資訊安全政策」及相關規範(詳見「法規遵循性管理程序」)，制定本「資訊安全手冊」，定義本所資訊安全管理系統（Information Security Management System，以下簡稱 ISMS）政策與目標。

一、 ISMS 方針

確保本所資訊業務之永續經營，建立資料處理、傳送及儲存之安全環境，以避免當發生人為疏失、蓄意破壞或自然災害時，遭致資訊資產不當使用、洩漏、篡改、毀損、遺失等情事，影響本所勤、業務運作或損及民眾權益。

二、 ISMS 目標

(一)導入並維持 CNS27001/ISO27001 標準並符合國家法規法令要求。

(二)確保本所提供之網路服務，於正常上班時間內因意外或操作錯誤造成無法使用持續達 4 小時以上之次數，每年不得高於 3 次。

(三)確保本所因資訊安全事件造成「限閱」等級以上資料外洩，每年不得有 1 件。

三、 適用範圍

(一)適用於本所相關資訊服務，以及提供服務所需之相關基礎設施(如機房空間、各式應用系統軟硬體設施、網路設備、環境控制設備等)之操作、維護及管理等。

(二)執行 ISMS 有關之人員(包含外部服務廠商)。

(三)本所所管理之主機房，係指位於本所 3 樓之主機房。

貳、 名詞定義

一、 資產（asset)：對組織有價值的任何事物。

二、 可用性(availability)：經授權個體因應需求之可存取及可使用的性質。

三、 機密性（confidentiality)：使資訊不可用或不揭露給未經授權之個人、個體或過程的性質。

四、 資訊安全（information security)：保存資訊的機密性、完整性及可用性；此外，亦能涉及如鑑別性、可歸責性、不可否認性及可靠度等性質。

五、 資訊安全事件（information security event)：系統、服務或網路發生一個已識別的狀態，其指示可能的資訊安全政策違例或保護措施失效，或是可能與安全相關而先前未知的狀況等。

六、 資訊安全事故（information security incident)：單一或一連串有顯著機率可能危害營運作業與威脅資訊安全之非所欲或非預期的資通安全事件。

七、 資訊安全管理系統（Information Security Management System,

ISMS)：整體管理系統的一部份，以營運風險導向(作法)為基礎，用以建立、實作、運作、監視、審查、維持及改進資訊安全。

八、 完整性（integrity)：保護資產的準確度(accuracy)和完全性(completeness)的性質。

九、 剩餘風險（residual risk)：風險處理後所剩餘的風險。

十、 風險接受（risk acceptance)：決定接受某風險。

十一、風險分析（risk analysis)：系統性的使用資訊，以識別緣由與估計風險。

十二、風險評鑑(risk assessment)：風險分析與風險評估的整個過程。

十三、風險評估（risk evaluation)：把預估的風險和已知的風險準則進行比較的過程，以決定風險的顯著性。

十四、風險管理（risk management)：藉由協調各項活動以指導與控管組織之有關風險。

十五、風險處理(risk treatment)：選擇與實作措施的過程藉以修正風險。

十六、適用性聲明(statement of applicability)：描述與組織之 ISMS 相關且對其適用之各項控制目標與控制措施的已文件化聲明。

參、 資訊安全管理系統(ISMS)

本資訊安全手冊之制定，係依據 ISO27001/CNS27001 標準要求事項第 4 節至第 10 節之各項要求，來進行管理系統之建立、實作、運作、監視、審查、維持與改進，詳述於後。

一、 一般要求

本所依據整體營運活動與所面臨的風險，建立、實作、運作、監視、審查、維持與改進 ISMS。ISMS 採用之過程如下頁圖 2-1 所示之 PDCA(Plan, Do, Check, Act)模型為基礎。

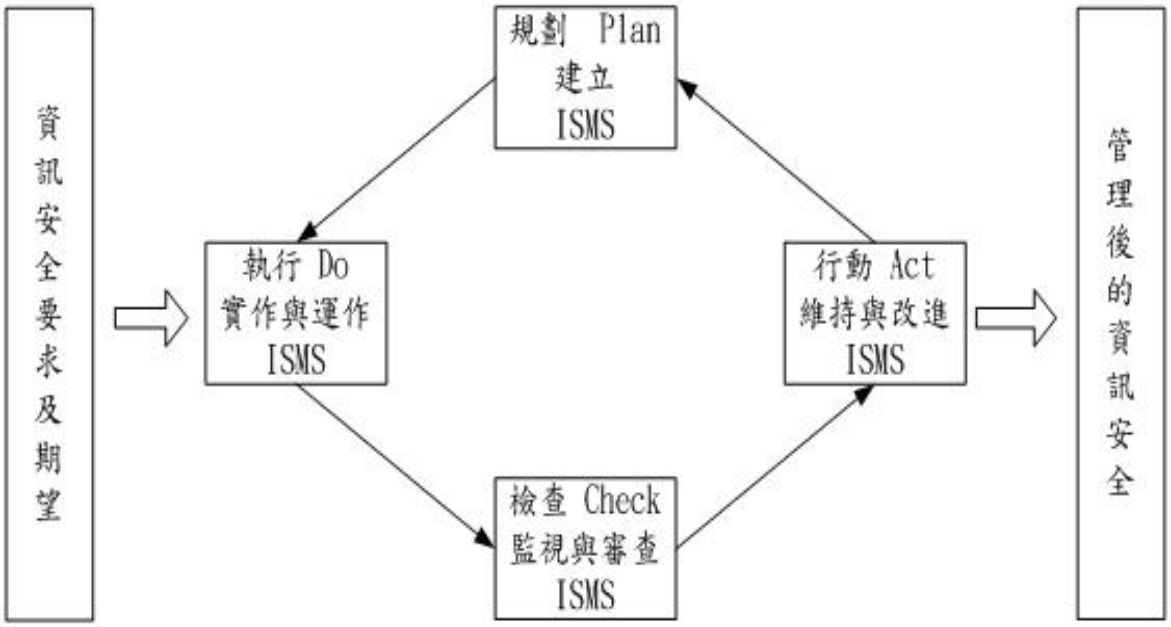

圖 2-1：ISMS 持續改善之 PDCA 模型

二、 ISMS之建立與管理

（一） 為統籌本所資訊安全相關業務之整體規劃、評估、督導、協調、推動及資通安全事件處理等事項，特設置跨單位之「資訊安全管理委員會」，並於「資訊安全管理委員會」下設立「資訊安全管理系統執行小組」(以下簡稱ISMS執行小組，其餘文件同)及「資訊安全管理系統稽核小組」(以下簡稱ISMS稽核小組，其餘文件同)。

（二） 採用會議形式考慮內、外部議題、利害相關者期望(關注方)進行風險識別與機關全景分析以及ISMS適用範圍的決定。

（三） 建立本所 ISMS，含風險評鑑、風險識別、風險分析與評估、風險處理、剩餘風險的核准、管理階層之授權、適用性聲明等。

（四） 監視與審查本所ISMS資安目標量測控制措施的有效性、審查風險評鑑及剩餘風險的等級與已識別的可接受風險、維持與改進ISMS。

（五） ISMS 於執行上之問題，其所對應之各項矯正措施處理。詳見「資訊安全稽核程序」之矯正措施處理。

（六） 確保與資訊業務相關的資訊安全事件與弱點，能夠及時通報與處理，以期快速回復至正常狀態，詳見「資訊安全事故管理程序」。

（七） 在本所所界定的安全區域範圍內，必須防範核心業務資訊，不遭受未授權的存取、破壞及干擾，人員帳號、密碼不得揭露於辦公室明顯處，電腦也應啟動螢幕保護程式以密碼保護，詳見「實體與環境安全管理程序」。

（八） 為確保網路服務及正確與安全地操作資訊處理設施，應建立安全

防護措施及管理機制，詳見「網路安全管理程序」以及「通訊與操作管理程序」。

（九） 資訊系統應訂定定期備份原則，並做復原測試。詳見「備份與回復管理程序」。

（十）為避免資訊系統因未授權之存取而使機密性或敏感性資料遭不當使用，應考量人員職務授予適切權限，詳見「存取控制管理程序」。

（十一）有關資訊系統安全規劃、設計、資訊系統異動上線管理等，詳見「資訊系統開發與維護管理程序」。

（十二）營運持續的需求須做完整規劃，以支援相關資訊系統。詳見「營運持續管理程序」。

三、 ISMS 文件管理

本所 ISMS 文件，係為管制資訊安全各項管理性及支援性作業而建立之必要程序，文件架構如下圖 2-2 所示，各階文件應加以文件化，並注意適時更新，讓有需要的使用者均可隨時取得。有關建立符合 ISMS 有效運作之文件與紀錄，詳見「文件與紀錄管理程序」。

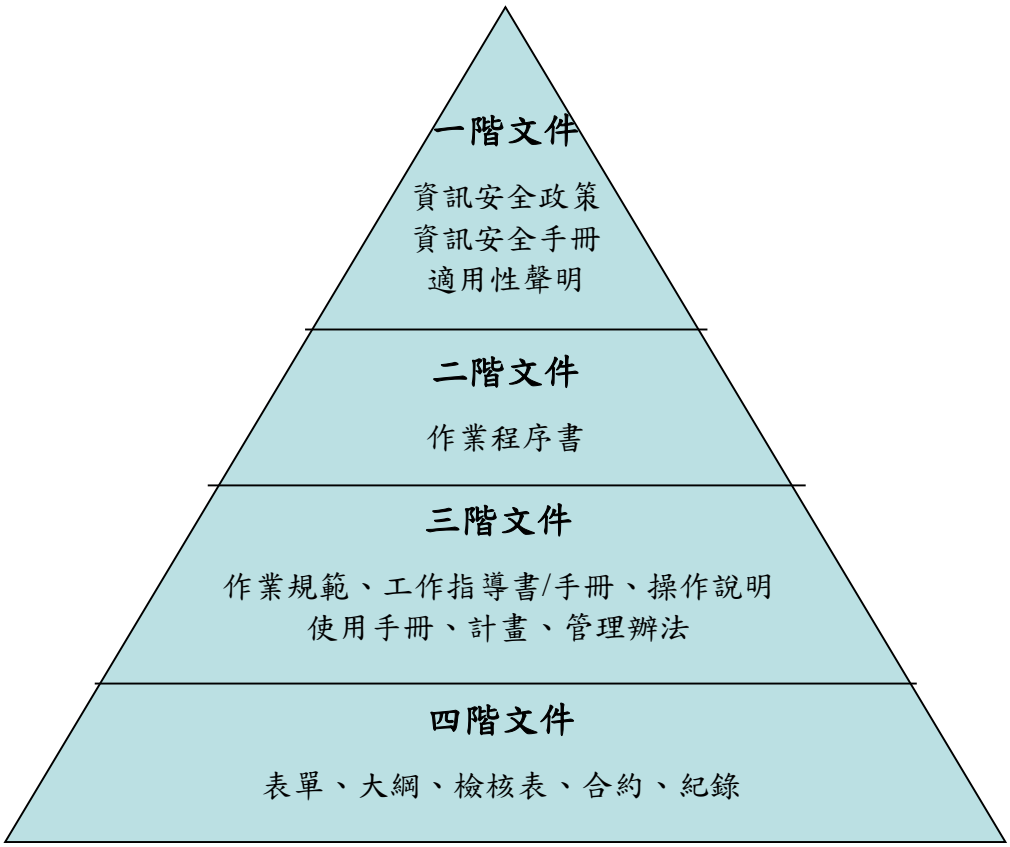

圖 2-2：ISMS 文件架構圖

（一） 一階文件

包含本所資訊安全政策、資訊安全手冊及適用性聲明文件，提供本所資訊安全管理系統一個整體性的描述，說明本所 ISMS 實施之範圍、ISMS 政策、相關程序與文件、並描述本所各項流程間之交互關係。所有與 ISMS 相關之人員，均應熟悉本政策文件之政策及執行目標，並將其運用為各種程序、方法及工作規範之指導原則。

（二） 二階文件

依據 ISO27001/CNS27001 標準之管理原則、本所資訊安全政策及資訊安全手冊所制定之各項程序文件，規劃及發展資訊安全相關之各項活動與服務所需之組織運作流程，並詳述於各程序文件中。

每一流程可能包含數項相關之程序，程序書中將再依其作業特性，建立一到數份之程序，以分別說明每一作業之執行程序。

（三） 三階文件

為確保本所資訊安全政策及資訊安全手冊中各項資訊安全規劃、維運及支援作業(Operation Support)工作於必要時能有適當之指引，針對流程中之關鍵技術或作業另訂說明文件，如作業指導書(或手冊)、作業規範、操作說明(或使用手冊)、計畫、管理辦法等，以作為相關作業執行時之指導。

（四） 四階文件

為利於落實本所各項作業，並達到制度化與一致化之目的，對於 ISMS 之各項要求，於流程執行過程中提供細部之表單、大綱、及查核表等，以利相關人員依照規定之表單及資料執行各項作業，並記錄作業執行結果。此類表單，可以採用電子媒體方式處理，但仍必須保留該表單必要之資料。

肆、 ISMS 文件之核定

一、 ISMS 一階文件，除「資訊安全政策」外，可由 ISMS 執行小組研提，經資訊安全管理委員會審查核定後實施，修正時亦同;「資訊安全政策」由 ISMS 執行小組研提，經資訊安全管理委員會審查及鎮長核定後公告實施。

二、 ISMS 第二、三、四階文件，由資訊安全管理委員會授權 ISMS 執行小組研提，並由資安長或其授權人審查核定後實施。

伍、 ISMS 內部稽核

ISMS 稽核分組應規劃內部稽核作業，將稽核範圍、準則、項目、方法及前次稽核的結果納入考量,每年至少辦理一次內部稽核,以判定 ISMS 控制目標、控制措施、過程及程序是否符合下列要求：

一、 符合 ISO27001/CNS27001 條文要求。

二、 相關外部、內部法規及程序規範。

三、 符合已知的資訊安全要求。

四、 選用之控制措施確實執行與維護。

五、 依照預定時程落實執行。

稽核時所發現不符合項目，須填寫「資訊安全矯正措施處理表」,受稽核單位應進行改善措施並如期完成，ISMS 稽核小組應持續追蹤控管改善措施之落實。詳見「資訊安全稽核程序」及「矯正措施處理程序」。

陸、 ISMS 之改進

本所 ISMS 之持續改進，應於日常作業中不斷累積經驗，並依據以下各程序所規範之關鍵時點予以檢討，以維持 ISMS 之適用性及有效性。

一、 依「監視及測量控制程序」，審查監控及量測結果，判定控制措施的有效性。

二、 依「矯正措施處理程序」針對 ISMS 所產生的異常狀況或潛在問題，採取適當處理及研擬改善措施。

三、 依內部稽核結果，評估 ISMS 之管理控制，確保 ISMS 政策和目標的適宜性。

四、 依「營運持續管理程序」確保資訊業務能因應重大資訊安全事故，採取適當應變措施。

五、 依「資訊安全組織管理程序」實施管理審查，以確保 ISMS 之政策和目標的適宜性和有效性。

六、 依「法規遵循性管理程序」識別法規之適用性，以避免違反任何法律、行政命令、契約、標準、安全技術等規範。

七、 實施 ISMS 所選用之各項控制措施及其所對應之程序文件，詳見「適用性聲明(SOA)」。