雲林縣西螺鎮公所

人員安全管理程序

文件編號： XLTG-02-008

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)，為確保資訊系統使用、建置及維運相關人員，了解並勝任其資訊安全角色及責任，運用人員審查、考核獎懲與異動管理等機制，並透過教育訓練活動之實施，使其能正確執行職務，降低竊盜、詐欺、設施誤用及人為錯誤的風險，特訂定本「人員安全管理程序」(以下簡稱本程序)。

貳、 適用範圍

本程序適用於本所全體人員，包括本所員工(含約聘僱人員、臨時人員等非編制內人員)、上級機關督導人員、承包商及第三方使用者等。

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。

肆、 定義

一、 員工：指本所編制內人員，以及約聘、約僱、臨時人員等非編制內人員。

二、 上級機關：指對本所業務有督導權責的機關，如中央機關等。

三、 承包商：指與本所有契約關係或依契約提供服務之廠商。

四、 其他使用者：即第三方使用者，指與本所無隸屬或契約關係的機關或人員。

伍、 管理項目

透過人員角色及責任識別，在人員上任前、業務執行中及業務終止或變更時，運用人員審查、考核獎懲及異動等管理機制與教育訓練活動，使其正確執行職務，降低竊盜、詐欺、設施誤用及人為錯誤的風險，以確保資訊安全。相關管理及教育訓練活動程序如下圖 5-1 所示：

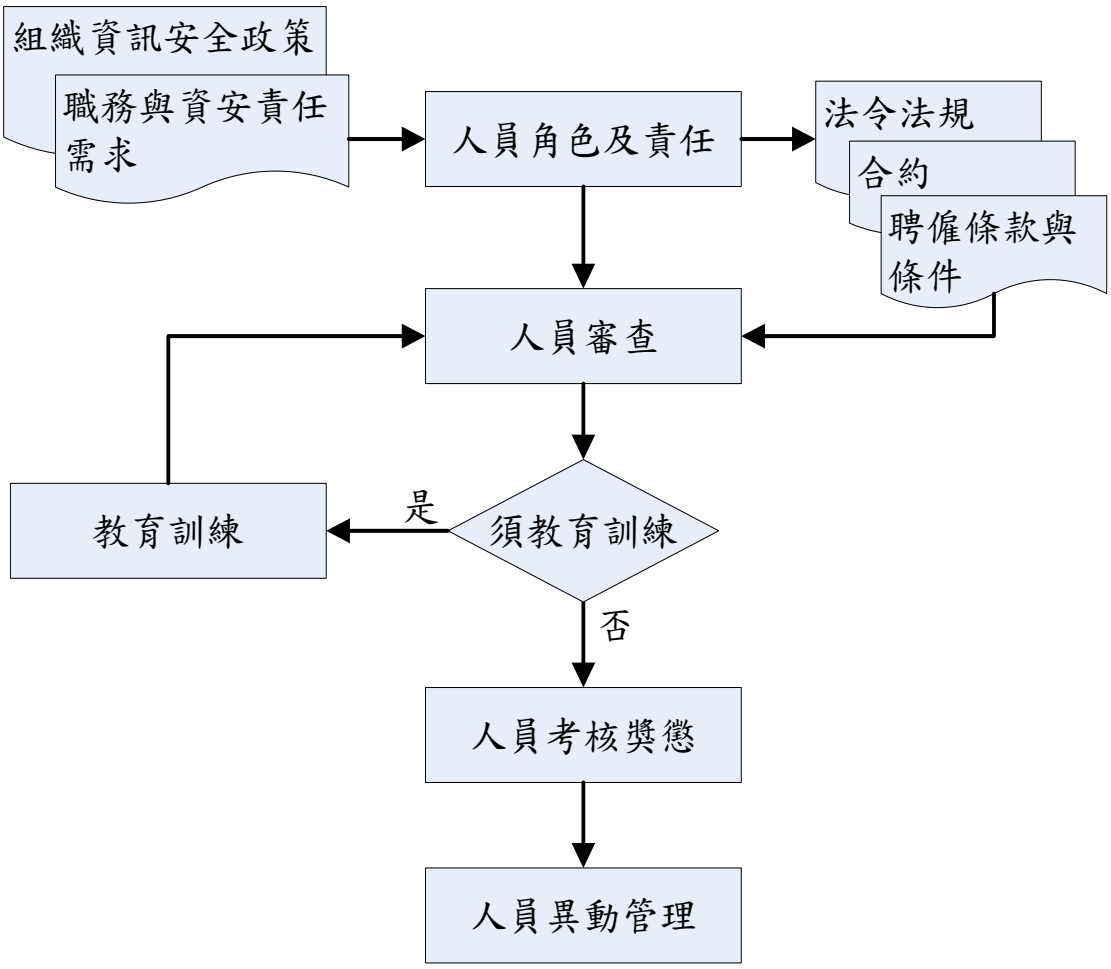

圖 5-1：人員管理及教育訓練活動程序圖

一、 人員角色及責任

資訊安全相關人員之角色及責任如下表 5-1 所示：

表 5-1：ISMS 角色及責任對照表

類別	角色	職務責任	資安責任					
			保密	正確操作使用	依授權使用	設備使用保管	資安通報	依法規或契約執行
員工	機房管理人員	辦理機房門禁及資訊設備管理業務，掌握各項設備維運狀態，確保設備正常運作。	V	V	V	V	V	V
	網路管理人員	辦理網路通訊服務基礎設施之帳號管理、故障管理、組態管理、效能管理、安全管理等，以確保網路效能及安全。	V	V	V	V	V	V
	應用系統管理人員	辦理應用系統管理，掌握應用系統維運狀態，確保應用系統正常運作。	V	V	V	V	V	V
	ISMS 執行小組成員	規劃與執行 ISMS 各項作業，確保 ISMS 之持續改善及有效運作。	V		V		V	V
	一般使用者	執行應用系統，確保業務正常運作。	V	V	V	V	V	V
上級機關	業務督導	對本所辦理資訊安全相關業務進行督導考核，以確保資訊安全之成效。	V		V		V	V
承包商	委外服務人員	依合約要求執行應用系統或資訊設備之建置、安裝、維護等事宜。	V	V	V	V	V	V
	供應商（電信、網路）	於本所通知時派員協助解決網路通訊相關疑義或排除障礙，確保網路通訊正常運作。	V				V	V
	供應商(電力)	於本所通知時派員協助解決電力相關疑義或排除障礙，確保電力正常運作。					V	V
	其他設備（非資訊設備）供應維護廠商	於本所通知限期內完成設備維護，確保設備正常運作。					V	V
	派遣人員	依合約要求執行相關事宜	V	V	V	V	V	V
其他使用者	一般民眾	依本所資訊安全政策之要求，正確使用本所所提供之各項資訊與服務。		V			V	
	其他機關與人員	依本所資訊安全政策及相關規定之要求，正確使用本所所提供之各項資訊與服務。		V	V		V	V

二、 人員審查及管控

於各角色任務開始前，透過下列機制，以確保相關人員明瞭其職務與資安責任，並勝任其角色：

（一）員工

1. 人員之任用及調派，應依照人事相關法規進行審查。
2. 人員進用時，應依其報到時所簽署之「公務人員服務誓言」，遵循「公務人員服務法」相關規定負保密之義務，並可以口頭或書面方式告知其職務責任與資安責任。
3. 擔任資訊安全管理系統職務的人員(如機房管理人員、網路管理人員、設備管理人員、應用系統管理人員及 ISMS 執行小組成員等)所應具備之能力，應從專業能力和學經歷等各方面進行評估，其進用之安全評估參考項目如下：
   (1)參與之熱誠與意願。
   (2)工作經歷。
   (3)學歷、專業能力及資格。
   (4)機密維護之責任。

（二）上級機關

接獲上級機關辦理業務督導或資安攻防演練公文，應先予確認後，再由權責人員依業務實際需要，提供相關人員適當使用權限及認證機制。

（三）承包商

1. 對於承包商之職務、資安責任及相關人員應具備資格條件，應於招標文件或合約中敘明，合約中亦應考量資訊、通訊技術服務及

產品供應鏈關聯之資訊安全風險。

2. 承包廠商須簽定「資訊安全保密切結書（廠商）」外，參與該案之委外廠商員工，另須簽訂「資訊安全保密切結書（個人）」，以確保相關作業行為已受保密條款約束。

3. 對於電力、電信、網路及設備供應商之人員，應於作業前識別並確認其身分。

4. 如有廠商指派之駐點服務人員報到時，應填寫「駐點服務人員報到通知單」，由行政室權責人員賦予網路及資訊系統帳號及權限。

5. 權責人員應定期監視與審查由廠商提供的服務、報告及紀錄，若有廠商服務內容需變更時應重新評估其適切性。

（四）其他使用者

1. 對一般民眾提供資訊或服務時，可提供導覽、操作（或使用）說明等方式，確保其正確操作使用。

2. 對其他機關與人員提供資訊或服務時，除以人員身分識別外，得以提供操作手冊或教育訓練等方式，確保其正確操作使用。

3. 對參與投標廠商提供資訊或服務時，應於招標文件敘明提供資訊或服務之用途、使用及保密責任。

三、 考核獎懲

各角色任務執行期間，透過適當機制監督相關人員之資訊作業安全，防範不法及不當行為，並於違規時適時處理。

（一）員工

1. 重要資訊系統之管理、維護、設計及操作之人員，應妥適分工，

分散權責，並視需要建立制衡機制，實施人員輪調，建立人力備援制度。

2. 各單位於辦理各項業務訓練時，應將資訊安全教育納入課程，建立員工資訊安全認知，宣導資訊安全重要性。

3. ISMS 承辦人應依據執行 ISMS 之需求，對電腦機房、網路、資訊系統等相關管理人員，評估其對資訊安全相關認知與技術能力，施予適當之教育訓練。有關教育訓練之實施，依本程序「四、資訊安全教育訓練」規定辦理。

4. 單位主管應負責督導人員之資訊作業安全，防範不法及不當行為；每年並依據「職務說明書」之需求及安全項目，進行單位人員考核作業，評量其資格、能力及工作狀況。

（二）承包商

1. 委外服務廠商人員(如電力、電信、網路及設備供應商等之人員)進入本所時，應驗明身分，並換發臨時識別證後始得進入。

2. 如遇承包商指派駐點服務人員，應由承包商填寫「駐點服務人員報到通知單」並檢附相關資格證明文件，由權責單位人員驗明其身分後，視需求發給臨時識別證，除督導其日常作業外，並應負安全監控之責任，如有異常或不足，應予注意要求改善，倘有不適任情形，應依合約規定處理。

3. 承包商如有違反本所相關資安規定，造成本所權益受損，除依合約(供應商之服務契約或條款)規定處理外，並視情況依「政府採購法」相關規定辦理。

四、 資訊安全教育訓練

（一）每年應對人員進行資訊安全教育及訓練，促使其瞭解資訊安全的重要性及各種可能的資訊安全風險，以提高員工資訊安全意識，促其遵守資訊安全規定。

（二）應以人員角色及職能為基礎，針對不同層級的人員，進行適當的資訊安全管理之教育及訓練；資訊安全管理教育及訓練的內容應包括：ISMS 政策、資訊安全法令規定、資訊安全作業程序，以及如何正確使用資訊設備之訓練等。

（三）對人員進行資訊安全管理教育及訓練之政策，除適用 ISMS 系統管理人員外，對 ISMS 系統相關的使用者，亦一體適用。

（四）資訊安全教育訓練管理

1. 教育訓練規劃

(1)辦理依據：配合上級機關規定以及 ISMS 相關維運需求，由 ISMS 執行小組規劃資訊安全年度教育訓練計畫，包括課程、對象、時間等，並據以實施。

(2)師資：由 ISMS 執行小組委請本所內熟悉資訊安全運作之人員，或聘請外界資訊安全專業人士擔任講師。

(3)教育訓練內容：依照工作職務區分，教育訓練需求至少應有下列教育訓練內容：

A. 工作所需的管理課程。

B. 工作所需的管理標準(如 ISO27001/CNS27001)或實作指引(如 ISO27002/CNS27002 等)。

C. 工作職務相關的新技能、設備操作課程。

D. 工作職位相關技能、設備操作對資訊安全的影響及要求。

2. 教育訓練實施

(1)外部教育訓練：由單位主管指派，或由受訓人員向單位主管提出教育訓練申請，經核可後參訓，參訓之相關紀錄以專卷保存。

(2)內部教育訓練：ISMS 承辦人依據 ISMS 推動情形，配合本所業務人員專業教育訓練期程，辦理資訊安全教育訓練相關行政及調訓事宜。

(3)辦理內部教育訓練時，須由主辦單位填寫「資通安全教育訓練檢核表」。

3. 教育訓練紀錄管理

本所內、外教育訓練及宣導結束後，其相關資料(如簽到表、講義或宣導資料、課程滿意度調查、成效評量結果等)應專卷保存，並由主辦單位、ISMS 承辦人、或指派專人統一保管。

4. 教育訓練實施成效評量

(1)教育訓練實施之成效評量，以測驗方式為主，並輔以其他評量方法(如講師評估、繳交心得報告等)，或由主管評估確認方式（填寫「資通安全教育訓練成效評估表」）來進行，ISMS 承辦人應於每次教育訓練結束後將評量結果進行彙整。

(2)年度教育訓練實施結束後，ISMS 承辦人應統計年度之評量結果，並由 ISMS 執行小組組長陳報資訊安全管理委員會審查執行成效。

(3)ISMS 承辦人總結教育訓練實施情況和績效，可作為後續辦理教育訓練時之參考。

(4)於內部稽核時查驗資訊安全之實施情形，以評估教育訓練辦理成效。

五、 人員異動管理

（一）新進人員報到時，由人事室掌管員工到離職業務人員賦予員工編號，並以派令副本知會行政室。使用者視業務需要以書面向行政室申請系統權限、帳號、密碼使用，資訊人員設定完成後，由該新進人員自行辦理密碼變更。

（二）人員離退職或調離本所，人事室掌管員工到離職業務人員應於生效日前以派令副本知會行政室，異動人員應填寫「西螺鎮公所離職人員交待清單」會辦行政室，由行政室資訊承辦人立即停用/刪除其帳號及權限，同時將所停用/刪除之帳號及權限以表格形式複印，並移交其所保管的資產。

（三）當本所人員職務調整或異動時，人事室掌管員工到離職業務人員應於生效日前以派令副本知會資管科，權責人員應按該異動人員所辦理之業務，檢視並調整其帳號權限。

（四）如遇本所員工長期不在本所時(如長期借調支援、出國進修、長期病假、產假、留職停薪等)，帳號管理權責人員應視實際需求，決定是否暫停其網路帳號或調整其使用權限。

（五）委外服務廠商駐點服務人員如因合約到期或離職，應填寫「駐點服務人員撤駐報告單」，並歸還於專案內所保管的資產，依程序由權責人員立即刪除其帳號及權限。

陸、 參考文件

一、 公務人員服務法。

二、 政府採購法。

柒、 使用表單

一、 公務人員服務誓言。

二、 資訊安全保密切結書（廠商）。

三、 資訊安全保密切結書（個人）

四、 職務說明書。

五、 駐點服務人員報到通知單。

六、 駐點服務人員撤駐報告單。

七、 資通安全教育訓練檢核表。

八、 資通安全教育訓練成效評估表。

九、 西螺鎮公所離職人員交待清單。