雲林縣西螺鎮公所

矯正措施處理程序

文件編號： XLTG-02-003

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「資訊安全管理系統」(以下簡稱 ISMS)實施過程中所發生的異常及不符合事件,得以適當處理及改善，並達成持續改善的目標，特訂定本「矯正措施處理程序」(以下簡稱本程序)。

貳、 適用範圍

本程序適用於本所「資訊安全管理系統」實施範圍內，有關資訊安全方面的異常或不符合事項之矯正措施管理相關事宜。

參、 權責

一、 資安長或其授權人核定、發布本程序。

二、 ISMS 稽核小組組長審查本程序，並督導本程序之執行。

三、 ISMS 稽核小組研擬、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、 事件權責單位主管：

(一)分析問題之重要性程度，並排定優先順序。

(二)指派相關人員，進行問題解決。

(三)評估並決定可行之矯正措施。

(四)評估矯正措施的成效。

六、 事件權責單位承辦人員：執行並記錄矯正措施之執行過程及執行結果。

七、 ISMS 稽核小組驗證與追蹤矯正措施之確認完成。

肆、 定義

一、 不符合事項

（一）輕微不符合事項：未能完全遵循一項或多項 ISMS 之要求，但為單一事件者。

（二）嚴重不符合事項：未能執行一項或多項 ISMS 之要求，或同一輕微不符合事項多次發生。

二、 觀察事項(潛在不符合事項)：稽核時未能判定為符合或不符合，但未來有可能成為不符合之事項。

三、 矯正措施：為消除已經發生的不符合及潛在可能發生的不符合事項所採取的措施。

四、 持續改善：採取矯正措施，使實施範圍內之 ISMS 能依循規劃、執行、檢查與改善的模式持續改進。

伍、 管理項目

ISMS 於實施過程中，當發生異常或不符合標準或程序文件要求等事件時，應予適當處理並尋求有效改善措施，以避免類似情形再次發生，並達成持續改善的目標。

一、 啟用時機

ISMS 實施範圍內之各單位遇有下列情事時，應啟動矯正措施：

（一） 資訊安全管理審查時所提示之各項需改善事項。

（二）接獲稽核人員於稽核時發出之「資訊安全矯正措施處理表」，要求執行相關改善作業或需進一步觀察時，詳見「資訊安全稽核程序」。

（三）發現任何會使本所資訊業務或安全議題暴露於可接受風險值以上的事件。

（四）當發現各項影響資訊安全控制措施有效性的事件或有可能發生時。

（五）流程實施過程中，發現各種可能之改善機會時。

二、 擬定矯正措施

（一）當發現符合矯正措施啟動條件之各項事件時，發現人員應將發現事實記錄於「資訊安全矯正措施處理表」後，轉交事件權責單位進行處理。

（二）接獲「資訊安全矯正措施處理表」之事件權責單位主管可召集相關人員進行討論，分析不符合事件問題發生之原因及影響程度，並識別潛在的各項不符合事項。

（三）就各項不符合事件，研擬矯正措施或改善的方法(可分為短期方案和長期方案)，並排定優先處理順序及時程，以防止類似事件再次發生。

（四）對於觀察事項(潛在不符合事件)，可視需要研擬管控措施，以防止潛在不符合事件的發生。

（五）事件權責單位主管可指派適當人員，將評估後決定實施的矯正措施填入「資訊安全矯正措施處理表」中，並可視需要簽報資訊安全管理小組，以取得所需資源。

三、 執行矯正措施

（一）受指派之處理人員或相關單位，依據擬定的矯正措施進行問題解決或各項改善作業。

（二）事件權責單位主管應評估改善措施的執行成效，並要求受指派之處理人員記錄矯正措施之執行過程及執行結果於「資訊安全矯正措施處理表」。

四、 追蹤與查核

（一）事件權責單位主管應將已完成改善工作之「資訊安全矯正措施處理表」，送交原開立該表之發現人員，以確認所發現問題確實已獲得改善。

（二）開立「資訊安全矯正措施處理表」之人員應確認改善情形並填具審查意見後，將該「資訊安全矯正措施處理表」送交 ISMS 稽核組複核。

（三）ISMS 稽核小組除確認矯正措施執行之成效外，尚需審查是否有衍生其他問題，並檢討程序文件是否需配合修訂。

（四）ISMS 稽核小組半年應至少進行 1 次追蹤查核，以掌握所有應執行之「資訊安全矯正措施處理表」的狀態，直到確認已辦理完成並同意簽結。

（五）如矯正措施尚未完成，ISMS 稽核小組應持續進行追蹤，直到確認完成為止。

（六）確認已完成矯正工作之「資訊安全矯正措施處理表」，交由 ISMS 稽核小組留存備查。

（七）ISMS 稽核小組應指派具備稽核員資格之人員，對於矯正完成或矯正中之「資訊安全矯正措施處理表」進行驗證稽核，以確認矯正結果與狀態，如有不符合情事，仍以開立「資訊安全矯正措施處理表」

方式，按矯正措施規定辦理。

（八）完成驗證確認之「資訊安全矯正措施處理表」，由稽核員陳報 ISMS 稽核小組組長審核，審核確認之「資訊安全矯正措施處理表」，交由 ISMS 稽核小組留存備查。

（九）待矯正事項若短期內無法完成或執行困難者，應進行風險評估，並經資訊安全管理委員會核可後，視為已完成該矯正事項之處理。

陸、 參考文件

一、 資訊安全稽核程序。

二、 資訊安全文件與紀錄管理程序。

柒、 使用表單

資訊安全矯正措施處理表。