
雲林縣西螺鎮公所

監視與量測控制程序

文件編號： XLTG-02-004

版 次： V1.0

文件日期： 110 年 11 月 24 日

機密等級： 普通

目 錄

壹、	目的	1
貳、	適用範圍	1
參、	權責	1
肆、	定義	1
伍、	管理項目	2
一、	制定資訊安全監測項目清單	2
二、	監測與資料收集	2
三、	監測結果審查	3
四、	監測資料保存	3
陸、	參考文件	4
柒、	使用表單	4

壹、 目的

雲林縣西螺鎮公所(以下簡稱本所)對資訊安全管理系統(以下簡稱 ISMS)所採取之控制措施進行監視及量測，以確保 ISMS 的有效性，並作為管理與決策時的參考依據及流程持續改善之基礎，特訂定本監視與量測控制程序（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；凡屬控制措施的監視及量測活動均屬之。

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

無

伍、管理項目

為確保 ISMS 的有效性，並作為管理與決策時的參考依據及流程持續改善之基礎，應對 ISMS 所採取之控制措施群組進行監視及量測，以得知 ISMS 之實施狀態，並採取必要措施。

一、制定資訊安全監測項目清單

(一) ISMS 執行小組依據：

1. 本所資訊安全管理系統政策與目標。
2. 資訊安全相關的法令、法規和 ISO27001/CNS27001 標準的要求。
3. 資訊安全風險考量因素。
4. 重要資訊安全因素清單。

制定「資訊安全監視與量測項目清單」，並送 ISMS 執行小組組長審查。

(二) ISMS 執行小組組長應審查「資訊安全監視與量測項目清單」之監測項目、週期及其標準是否合宜。

二、監測與資料收集

(一) ISMS 執行小組組長將核定之「資訊安全監視與量測項目清單」指派適當人員收集所需之各項資訊。

(二) ISMS 承辦人應彙整所收集到之各項資訊，據以作為資訊安全管理的績效成果評估。

(三) 若委託廠商進行資通安全監測，則監測內容需符合資通安全法規的相關規定。

- (四) ISMS 承辦人應定期就核定之監測項目與監測值，提出當期之監測與分析結果，陳報 ISMS 執行小組組長審閱。對於不合適或須變更之監測項目與監測值亦應配合提出檢討。

三、 監測結果審查

- (一) ISMS 執行小組組長應定期審查監測結果，並評估監測結果是否符合資訊安全法規、資訊安全政策目標的要求，如不符合要求，應按「矯正措施處理程序」之規定辦理。
- (二) 審查工作應檢查所蒐集到之監測資料是否有以下之問題：
1. 資料遺漏。
 2. 不合理的資料值。
 3. 樣本取樣方式不符合統計假設。
 4. 不一致之量測基礎，例如不同時間基礎造成的偏差、不同的人員判斷原則、不同的度量單位…等情形。
- (三) 對於有問題之資料，ISMS 執行小組應設法予以更正、矯正或轉換，以確保監測資料之正確性與有效性。調整過程中應保留原始資料與調整後之資料，並敘明調整原因。

四、 監測資料保存

- (一) ISMS 監視及測量控制紀錄應指派適當人員妥為保存，並建立清單以利資料查閱管理。
- (二) 監測紀錄之保存及取用，應依「文件與紀錄管理程序」辦理。

陸、 參考文件

- 一、 矯正措施處理程序。
- 二、 文件與紀錄管理程序。

柒、 使用表單

- 一、 資訊安全監視與量測項目清單。
- 二、 資訊安全矯正措施處理表。