雲林縣西螺鎮公所

資安事故管理程序

文件編號： XLTG-02-013

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 1

貳、 適用範圍 1

參、 權責 1

肆、 定義 2

一、 資訊安全事故來源及分類 2

二、 資訊安全事故等級 2

三、 異常徵兆 2

四、 資訊安全事故管理相關機構 4

伍、 管理項目 5

一、 準備與預防 5

二、 偵測與分析 6

三、 應變與通報 8

四、 存證與復原 11

陸、 參考文件 12

柒、 使用表單 12

壹、 目的

雲林縣西螺鎮公所(以下簡稱本所)為提供有關資訊安全事故之監控、通報、處理、檢討與學習等事宜，並規範相關人員之作業權責，以期當事故發生時，能迅速展開必要之應變處置，防止事故蔓延擴大，並於最短時間內回復正常運作，降低該事故可能帶來之損害，以維護資訊系統之安全，特訂定本「資訊安全事故管理程序」(以下簡稱本程序)。

貳、 適用範圍

本程序適用於本所發生重大資訊安全事故，或其他災害發生涉及資訊安全時之相關處理活動。

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、 資安聯絡人：由本所 ISMS 承辦人兼任，負責資訊安全事故發生時之聯繫及通報事宜。

六、 ISMS執行小組與主機房管理相關人員規劃及維護資訊安全管理系統(ISMS)，並防範資安事故發生；當事故發生時，執行緊急應變處理及資安事故通報。

七、 本所同仁：發現資安事故(或疑似資安事故)時，迅速通報主機房

管理相關人員或資安聯絡人。

肆、 定義

一、 資訊安全事故來源及分類

（一）內部危安事件：發現（或疑似）系統或設備遭人為惡意破壞毀損、作業不慎、設備故障（如空調失效）等事件。

（二）外來入侵事件，如病毒感染事件、或非法入侵（如駭客攻擊）事件等。

（三）天然災害或重大突發事件

1. 天然災害：如颱風、水災、地震等。
2. 重大突發事件：如火災、爆炸、核子事故、SARS、禽流感等。

二、 資訊安全事故等級

行政院國家資通安全會報107年11月21日訂頒「資通安全事件通報及應變辦法」，將資通安全事件等級分為四個級別。

（一）公務機關或特定非公務機關（以下簡稱各機關）發生資通安全事件，有下列情形之一者，為第一級資通安全事件：

一、非核心業務資訊遭輕微洩漏。

二、非核心業務資訊或非核心資通系統遭輕微竄改。

三、非核心業務之運作受影響或停頓，於可容忍中斷時間內回復正常運作，造成機關日常作業影響。

（二）各機關發生資通安全事件，有下列情形之一者，為第二級資通安全事件：

一、非核心業務資訊遭嚴重洩漏，或未涉及關鍵基礎設施維運之核心業務資訊遭輕微洩漏。

二、非核心業務資訊或非核心資通系統遭嚴重竄改，或未涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭輕微竄改。

三、非核心業務之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作，或未涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，於可容忍中斷時間內回復正常運作。

（三）各機關發生資通安全事件，有下列情形之一者，為第三級資通安全事件：

一、未涉及關鍵基礎設施維運之核心業務資訊遭嚴重洩漏，或一般公務機密、敏感資訊或涉及關鍵基礎設施維運之核心業務資訊遭輕微洩漏。

二、未涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭嚴重竄改，或一般公務機密、敏感資訊、涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭輕微竄改。

三、未涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作，或涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，於可容忍中斷時間內回復正常運作。

（四）各機關發生資通安全事件，有下列情形之一者，為第四級資通安全事件：

一、一般公務機密、敏感資訊或涉及關鍵基礎設施維運之核心業務資訊遭

嚴重洩漏，或國家機密遭洩漏。

二、一般公務機密、敏感資訊、涉及關鍵基礎設施維運之核心業務資訊或

核心資通系統遭嚴重竄改，或國家機密遭竄改。

三、涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停

頓，無法於可容忍中斷時間內回復正常運作。

三、 異常徵兆

（一） 事故的徵兆(Sign)可分為兩類：前兆(Precursors)與跡象(Indications)：

1. 前兆乃未來可能會發生事故的徵兆，例如：

(1)Web 伺服器紀錄中發現有不明對象對網站進行弱點掃描。

(2)針對電子郵件伺服器弱點的新攻擊程式問世。

(3)駭客團體揚言要開始攻擊。

2. 跡象則是可能已經發生過或現在正發生的事故的徵兆，例如：

(1)網路型入侵偵測系統偵測到有不明對象對檔案傳輸(FTP)伺服器進行緩衝區溢位攻擊。

(2)防毒軟體偵測到某主機感染病毒。

(3)網頁伺服器當機。

(4)使用者抱怨上網很慢。

(5)主機房管理相關人員發現奇怪檔名的檔案。

(6)使用者回報收到具威脅性的電子郵件。

(7)主機中的稽核設定被變更過。

(8)應用程式的日誌中發現多次登入失敗。

(9)電子郵件管理者發現大量可疑的信件。

(10)主機房管理相關人員發現流量異常。

四、 資訊安全事故管理相關機構

（一） 行政院國家資通安全會報

行政院國家資通安全會報以下簡稱「安全會報」為掌握我國政

府機關及公民營事業機構資安事件，迅速雙向通報及緊急應變處置，負責國家資通訊安全相關事項之政策諮詢審議、協調及推動，其幕僚作業由行政院資通安全處辦理，安全會報下設網際防護及網際犯罪偵防等二體系，下設相關組。

（二）國家資通安全會報技術服務中心

以下簡稱「技服中心」，由財團法人資訊工業策進會建置及維運，主要係協助行政院資通安全處執行通報應變組之相關工作，並提供通報應變各分組下之政府機關（構）事前安全防護、事中預警應變、事後復原鑑識等技術服務。

（三）台灣電腦網路危機處理暨協調中心(TWCERT)

CERT(Computer Emergency Response Team)是由各個國家、組織或企業自行組成的組織，TWCERT 於民國 87 年 9 月於台灣地區成立，主要服務為提升電腦與網路系統的安全性、統籌運用台灣網路與電腦之相關資源、防止與處理資訊或網路安全危機事件、協助系統管理者診斷電腦網路安全漏洞、建置網站以提供電腦網路安全資源、以及舉辦網路安全宣導活動等。

伍、 管理項目

本所於遭遇資訊安全事故時，應迅速通報並進行緊急應變處置，以防止事件擴大造成更大之傷害。相關作業如下頁圖 5-1：資安事故管理流程圖所示。

一、 準備與預防

（一）ISMS 執行小組平日即須依「營運持續管理程序」執行即時偵防、監測預警工作，並藉由監測工具（如入侵偵測系統(IDS)等）或國家資通安全通報應變網站通報應變組通告等方式，以掌握最新的預警訊息，並適時對主機房管理相關人員及使用者發布警告訊息及控制發展趨勢，以減少資訊安全事故的發生頻率。

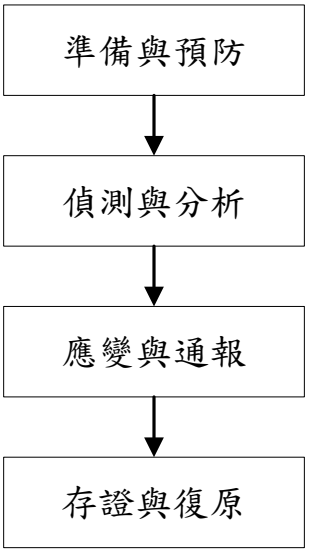

圖 5-1：資安事故管理流程圖

（二）ISMS 執行小組依「營運持續管理程序」，制定災害復原及營運持續計畫，並落實災害演練，熟悉各種可能之資安事故處理方式，以期當事故發生時，能迅速完成資訊系統之復原或維持基本運作能力。

二、 偵測與分析

（一）發生異常徵兆時，發現人員應立即通知行政室人員或主機房管理相關人員到場查看，值班人員或主機房管理相關人員可視需要邀請相關人員共同會勘，以瞭解該異常發生之原因，並分析判斷是否為資安事故。

（二）如判斷非為資安事故，則由行政室人員協助處理，無須進行通報或

填寫「資通安全事故通報單」;若為資安事故，行政室人員或主機房管理相關人員應即通知資安聯絡人，並進行下列評估：

1. 影響範圍：例如那些設備、網路、系統、應用程式已受到影響。
2. 事故發生來源及如何發生。
3. 損失情形。
4. 所需支援。
5. 可採取之應變措施。

（三）資安聯絡人應將評估結果填寫於「資通安全事故通報單」，並通報ISMS 執行小組及 ISMS 執行小組組長後，按「三、應變與通報」之規定進行後續處理。

（四）ISMS 執行小組人員應於接獲事故或災害發生通知時，儘速到場協助進行緊急應變處置，除邀集相關系統維運管理及業務承辦人員，研判問題發生之原因及嚴重性（資安等級）外，並評估災害損失狀況，評估內容至少應包括：

1. 設備或系統損害情況。
2. 資料受損項目。
3. 作業影響範圍。
4. 作業延誤情況。
5. 估算資訊系統作業及資料回復所需時間。
6. 備援場所設備及人員支援狀況等。

（五）如判斷為非資安事故，資安聯絡人仍應持續予以監測，直到該異常徵兆已確實解除。

三、 應變與通報

（一） 緊急應變處理

1. 內部危安事件：發現（或疑似）遭人為惡意破壞毀損、作業不慎、重要設備故障等危安事件時，相關人員應迅速查明事件影響狀況、受損程度等，必要時，啟用備份資料、程式或啟動備援計畫相關措施，期儘速回復正常運作。

2. 病毒感染事件：

(1)資訊處理設備發現遭病毒入侵時，發現人員應立即通知行政室人員或主機房管理相關人員。

(2)處理人員應立即中斷該設備之網路連線，以隔離病毒，避免疫情擴散，

(3)儘速取得所需病毒清除程式，並按病毒修護程序，完成病毒清除及修護復原工作。

(4)必要時，可尋求防毒維護廠商或資訊安全事故管理相關機構之協助，以清除病毒，並掌握電腦病毒感染最新動態。

3. 非法入侵事件：

(1)資訊系統發現疑似或已被駭客入侵時，主機房管理相關人員應於第一時間隔離受入侵系統及拒絕入侵者任何存取動作，如切斷入侵者之實體連線或調整防火牆設定等，以阻絕駭客進一步入侵，並通知資安聯絡人。

(2)主機房管理相關人員應記錄系統被入侵情形、被駭統計分析及損失評估等資料，除供後續防護與預警之參考外，並由資安聯絡人循通報程序向主管機關反映，並移請相關偵辦業務單位循線追查處理。

(3)ISMS 執行小組於事故處理完畢後，應全面檢討網路安全防護措施、修補安全漏洞或修正防火牆之設定等具體改善補救措施，以防止類似入侵或攻擊情事再度發生。

4. 天然災害或重大突發事件應變處理：

(1)如遇颱風、水災、地震等天然災害，或火災、爆炸、核子事故、建築災害等重大意外事件，應按「營運持續計畫」之計畫內容辦理。

(2)如發現資訊設備或儲存媒體遭偷竊或被破壞時，發現人員應迅速通報資安聯絡人，資安聯絡人接獲訊息後，除按通報程序進行通報作業外，並移請相關偵辦業務單位循線追查處理。

(3)如遇資訊網路系統骨幹（主幹頻寬）中斷事件，應立即聯繫線路租用及網路維護廠商查明障礙點、影響區間及範圍，啟動應變機制，緊急調撥備援系統或替代路由，實施流量控管，執行搶修作業。

5. 主機房管理相關人員若懷疑事故影響範圍會因網路或系統開機而持續擴大，應立即封鎖資訊系統之使用，如關機、中斷網路連線、停止特定服務等。

（二）資安事故通報

1. 發現人員應立即通知行政室人員或主機房管理相關人員到場查看，如確認為重大資安事故時，資安聯絡人應立即填寫「資通安全事故通報單」，說明事故發生之事實，並就可能影響之範圍、損失情形、判斷支援申請、可採取之應變措施等事項進行評估，並通知 ISMS 執行小組組長，經 ISMS 執行小組組長確認後，通報至「國家資通安全通報應變網站」。依

據國家資通安全會報規定，知悉資通安全事件後，應於一小時內依主管機關指定之方式及對象，進行資通安全事件之通報。

2. 資安事故完成處理後，資安聯絡人填寫「資通安全事故通報單」，經 ISMS 執行小組組長確認後，陳報「國家資通安全通報應變網站」辦理結案。

3. 如該資安事故屬危及人員生命或設備遭到破壞、資料外洩等涉及民、刑事案件時，應由 ISMS 執行小組組長確認，並報請鎮長或其授權人同意後，通知主管機關，並移請相關偵辦業務單位循線追查處理。

4. 資通安全事件「第一級」發生時，資安聯絡人視其影響程度，評估是否通報 ISMS 執行小組組長，並依需要召集主機房管理相關人員召開會議，以便處理發生狀況。

5. 當資通安全事件達到「第二級」時，由資安聯絡人通報 ISMS 執行小組組長，並即刻召集主機房管理相關人員召開緊急應變會議處理。

6. 當資通安全事件達到「第三級」以上時，相關人員除立即進行緊急應變處置外，ISMS 執行小組組長應將事故全盤狀況陳報資安長核備。

7. 第一級或第二級資通安全事件，應於知悉該事件後七十二小時內內復原或損害管制；第三級或第四級資通安全事件，應於知悉該事件後三十六小時內復原或損害管制，各等級資安事件完成損害控制或復

原作業後，應持續進行資通安全事件之調查及處理，並於一個月內依主管機關指定之方式，送交調查、處理及改善報告。

8. 當事故發生導致資訊系統服務中斷時間達規定的時限，應由 ISMS 執行小組組長取得資安長同意後，宣布啟動營運持續作業。

四、 存證與復原

（一）ISMS 執行小組於完成緊急應變處置作業後，召集相關系統、設備供應或維護廠商，按「營運持續管理程序」規定，儘速依災難損害回復處理步驟，實施災後復原重建工作。

（二）當危機解除後，參與事故處理之相關人員(如系統管理人員、設備供應或維護廠商等)，應將災害應變處置復原之過程完整紀錄，並予建檔管制，以利爾後查考使用。相關記錄事項如下：

1. 事故發生原因分析及檢討改善方案。
2. 防止類似事件再次發生之具體方案。
3. 稽核軌跡及蒐集分析相關證據等。

（三）發生重大資安事故或有需要時，相關處理人員應保留事件發生之線索，移請相關偵辦業務單位循線追查處理，或經 ISMS 執行小組組長轉陳資安長同意後，由資安聯絡人向技術服務中心或檢、警、調單位申請追蹤鑑識與偵查支援，藉由研析稽核紀錄或入侵活動偵測等相關資料，釐清事件發生的原因與責任，並找出防護系統之漏洞，尋求補強保護方法，避免事件再度發生。

陸、 參考文件

一、 資通安全責任等級分級辦法政府機關（構）資訊安全責任等級分級作業施行計畫。

二、 國家資通安全技術服務與防護管理計畫。

三、 行政院及所屬各機關資安事件通報應變作業規範。

四、 行政院國家資通安全會報「各機關處理資通安全事件危機通報緊急應變作業注意事項」。

五、 營運持續管理程序。

六、 資通安全事件通報及應變辦法國家資通安全通報應變作業綱要。

柒、 使用表單

資通安全事故通報單