衛生福利部澎湖老人之家

「資訊安全管理系統」
安全事件管理程序書

機密等級：一般

編　　號：IS-PHSCH-02-011

版本編號：1.2

制訂日期：114.05.28

使用本文件前，如對版本有疑問，請與修訂者確認最新版次。

本文件歷次變更紀錄：

版次	修訂日	修訂者	說　　明	核准者
1.0	110.09.10	資訊安全執行小組	初版發行	召集人
1.1	112.05.22	資訊安全執行小組	修訂 5.3.4 重大資訊安全事件應保留事件發生之線索，如有需要得向~~國家資通安全會報技術服務中心~~國家資通安全研究院或檢警單位申請支援。	召集人
1.2	114.05.28	資訊安全執行小組	修訂 5.1.1 本家人員自行發現或經由外部通報(例如上級機關、委外廠商)疑似資訊安全事件發生時，應通報資訊安全執行小組，並告知直屬主管。	召集人

本程序書由資訊安全執行小組負責維護。

目錄：

1 目的

1.1 確保衛生福利部澎湖老人之家(以下簡稱本家)於資訊安全事件發生時，能迅速依程序進行通報，並採取必要之應變措施與建立事件學習機制，以降低事件所造成之損害。

2 適用範圍

2.1 本家資訊業務之資訊安全事件管理。

3 權責

3.1 資訊安全委員會：

審核本家「資訊安全事件通報與應變作業流程」，並督導資訊安全事件之管理作業。

3.2 資訊安全執行小組：

3.2.1 研擬資訊安全事件通報流程。

3.2.2 透過資通安全監控中心（SOC）、防毒軟體及系統釐清事件影響，並清查各單位受影響情形，據以完成資訊安全事件各階段通報，分享惡意程式 IoC 等。

3.3 發現人員：所有人員（含：正職人員、約聘（僱）人員、臨時人員與委外人員），發現疑似資訊安全事件時，皆負有即時通報之責任。

3.4 權責單位：資訊安全事件處理之權責單位，須執行資訊安全事件之分析及處理。

3.5 執行秘書：

3.5.1 督導資訊安全事件內外部通報、處理及分析作業。

3.5.2 負責綜整與定期更新訊息及擬定溝通計畫。

3.5.3 督辦緊急處理小組各項業務。

3.5.4 調度資訊及資通安全人員執行災害搶救及損害管制，防止次波攻擊及損害擴散。

3.6 緊急處理小組：

3.6.1 確定事件影響範圍，並評估損失。

3.6.2 依據事件情況研擬損害控制、復原作業及跡證保存計畫。

3.6.3 協助資訊安全事件之通報、處理及分析作業。

3.6.4 完成系統重建、弱點掃描或漏洞修補等事宜。

3.6.5 確保受害系統與相關系統及網路設備事件日誌之保存及管理。

3.6.6 依據系統保存跡證，完成鑑識分析，並追查防堵惡意中繼站。

3.6.7 依據事件調查根因，提出短、中、長期改善建議。

3.7 支援單位：

3.7.1 內部單位：負責辦理預算調撥及提供行政支援事宜，協助處理相關法律、人事懲處及採購等問題。

3.7.2 委外廠商：協助處理資訊安全事件。

4 名詞定義

4.1 資訊安全事件：凡於作業環境中，導致資訊資產之機密性、完整性、可用性遭受影響之事件。

4.2 內部危安事件：發現(或疑似)遭人為惡意破壞毀損、作業不慎等事件。

4.3 外力入侵事件：發現（或疑似）電腦病毒感染事件、駭客攻擊（或非法入侵）等事件。

4.4 天然災害：颱風、水災、地震等。

4.5 突發事件：火災、爆炸、重大建築災害及資訊網路系統骨幹(主幹寬頻)中斷事件等。

4.6 資訊安全事件等級區分為：

4.6.1 一級事件：

4.6.1.1 非核心業務資訊遭輕微洩漏。

4.6.1.2 非核心業務資訊或非核心資通系統遭輕微竄改。

4.6.1.3 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，造成本家日常作業影響。

4.6.2 二級事件：

4.6.2.1 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。

4.6.2.2 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。

4.6.2.3 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。

4.6.3 三級事件：

4.6.3.1 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。

4.6.3.2 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。

4.6.3.3 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。

4.6.4 四級事件：

4.6.4.1 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。

4.6.4.2 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。

4.6.4.3 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。

5 作業說明

5.1 事件通報

5.1.1 本家人員自行發現或經由外部通報(例如上級機關、委外廠商)疑似資訊安全事件發生時，應通報**資訊安全執行小組**，並告知直屬主管。

5.1.2 **資訊安全執行小組**於收到通知後，立即研判是否為資訊安全事件。若：

5.1.2.1 判定僅為資訊安全異常事件而非資訊安全事件時，則將判定結果回覆予發現人員，並於期限內處理完畢。

5.1.2.2 判定為資訊安全事件時，應啟動內部通報程序及外部通報程序。

5.1.3 內部通報程序

5.1.3.1 疑似資訊安全事件發生時，發現人員應依事件歸屬通報權責單位，並告知直屬主管。

5.1.3.2 權責單位於收到通知後，應遵循本程序書附件「資訊安全事

件內部通報與應變作業流程」進行後續通報與處理作業。

5.1.4 外部通報程序

5.1.4.1 發生資訊安全事件時，應遵循「資通安全事件通報及應變辦法」進行外部通報作業。

5.1.4.2 權責單位確認發生資訊安全事件時，應於 1 小時內於「國家資通安全通報應變網站」完成通報作業。

5.1.4.3 對於一般事件，權責單位應於知悉事件後 72 小時內完成損害控制或復原作業之辦理，並應留存紀錄；於重大事件，權責單位應於知悉事件後 36 小時內完成損害控制或復原作業之辦理，並應留存紀錄。

5.2 跡證保存

5.2.1 依據「政府機關（構）資安事件數位證據保全標準作業程序」進行數位證據蒐集。

5.2.2 發生資訊安全事件時，機關應依下列原則進行跡證保存：

5.2.2.1 機關進行跡證保存時，應優先採取隔離機制，包含設備關機、網路連線中斷或隔離、關閉服務、限制連線、限制權限、有限度修補漏洞等方式，以降低攻擊擴散。

5.2.2.2 若系統無備援機制，應備份受害系統儲存媒介（例如硬碟、虛擬機映像檔）後，以乾淨儲存媒介重建系統，於完成系統

測試後提供服務。

5.2.2.3 若系統有備援機制，應將服務切換至備援系統提供服務，並保留受害系統及設備，於完成事件根因分析或完整備份後重建系統，經系統測試後切換至原系統提供服務。

5.2.2.4 若備援設備亦為受害範圍，於重建受害系統時應以維持最低限度對外運作為原則，保存受害跡證。

5.2.3 簽訂資通系統或服務之委外契約時，應依第 5.2.2.1 及 5.2.2.2 規定於契約中定明紀錄保存及備份規定。

5.2.4 數位證據應以適當方法保護，以利下列管理作業：

5.2.4.1 作為研析問題及事件根因之依據。

5.2.4.2 作為研析是否違反契約或資訊安全規定之跡證。

5.2.4.3 作為與委外廠商協商如何補償之依據。

5.2.5 本家與各地所於日常維運資通系統時，應依自身資通安全責任等級保存日誌（Log），並定期備份於外部設備，其保存範圍及項目依據「通信與作業管理程序書」日誌保存規範辦理。

5.3 事件分析

5.3.1 應複製數位證據後再以複本進行事件分析，以免異動數位證據。

5.3.2 分析事件之歸屬及採取之對策，如內部資安事件、外力入侵事件、天然災害或重大突發事件等，並決定處理的方法與程序。

5.3.3 分析結果應做成歷程紀錄，以結案時一併陳核執行秘書。

5.3.4 重大資訊安全事件應保留事件發生之線索，如有需要得向國家資通安全研究院或檢警單位申請支援。

5.4 事件處理

5.4.1 考量單位資源，於最短的時間內，確認回復後之系統及相關安全控制是否完整及正確。

5.4.2 確認具體受害範圍，並優先恢復對外服務及核心資通系統運作，防止次波攻擊及擴散情形。

5.4.3 評估各系統是否於可容忍中斷時間內恢復服務及對利害關係人之影響，決定是否對外公告事件之相關內容。

5.4.4 依據分析結果，若為已紀錄之各類事件危機處理之程序，立即進行事件傷害控制，降低影響的程度及範圍。必要時依「營運持續運作管理程序書」啟動營運持續運作計畫。

5.4.5 限定僅授權之人員可使用回復後正常作業之系統及資料。

5.4.6 緊急處理步驟應詳實記載，以備日後查考。

5.4.7 處理過程中如發現造成之影響大於原先判定事件，資安工作小組應立即向執行秘書報告，重新執行事件分析辨識。

5.4.8 倘涉及個人資料外洩，應評估通知當事人之適當方式，依個人資料保護法第十二條規定辦理。

5.5 結案

5.5.1 由資安執行組進行外部通報結案。

5.5.2 與受影響之使用者進行溝通及說明。

5.5.3 對外單位請求協助時，應以其結案為條件；委外廠商協助時，應請委外廠商製成報告以為結案依據。

5.5.4 依據事件結案紀錄，應評估短、中、長期資安管理改善策略，其內容如下：

5.5.4.1 短期：完成可立即性修補項目之調整，例如更換密碼或修補程式弱點等。

5.5.4.2 中期：依據事件根因提出 3 至 6 個月內完成之強化作為，例如盤點單位老舊設備，並訂定汰換期程。

5.5.5 長期：依據事件受害情形，視需要提出 2 年內完成之管理改善建議，例如培養資安人員能力。

5.5.6 彙整相關文件並歸檔。

5.6 檢討改善

5.6.1 後續追蹤檢討相關資訊安全事件是否會重複發生，並審視現有環境漏洞，透過研析相關資料，以釐清事件發生之原因與責任。

5.6.2 檢討並改善處理步驟，進立處理標準程序，列入應變計畫。

5.6.3 向管理階層報告處理情形。

5.7 監督

5.7.1 由執行秘書進行監督並通知資安長，重大事件由資安長召開事件應變會議。

5.7.2 必要時，由資安長對外說明事件處理情形。

6 相關文件

6.1 資訊安全事件通報與應變作業流程(附件)

6.2 資訊安全事件通報單

6.3 「資通安全管理法」

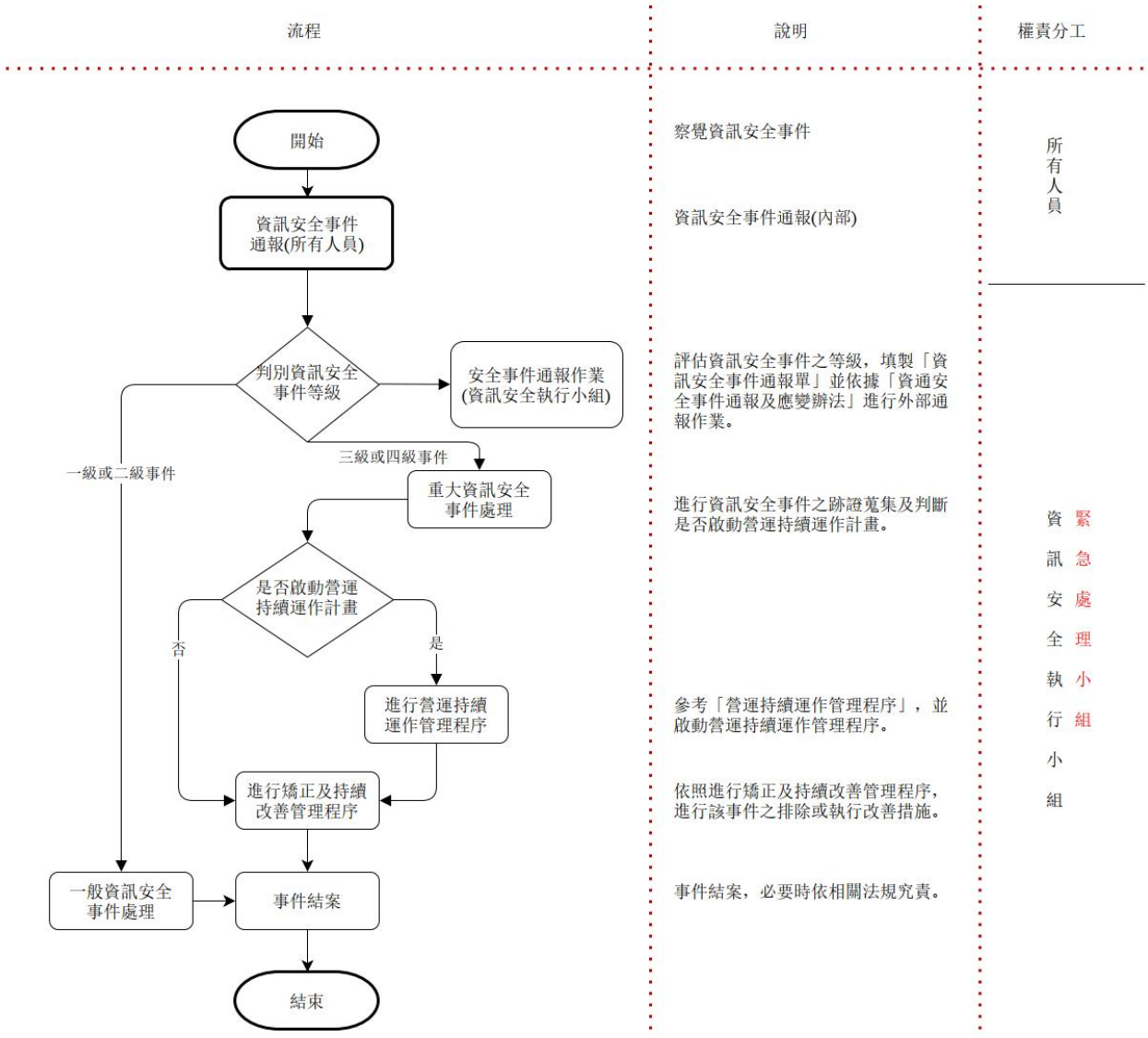
6.4 「資通安全事件通報及應變辦法」

6.5 「政府機關（構）資安事件數位證據保全標準作業程序」

附件：

資訊安全事件通報與應變作業流程

1 流程圖：



2 流程說明：

2.1 資訊安全事件通報：

2.1.1 本家所有人員於業務處理過程中發生資訊安全事件，或發現與資

訊安全有關之潛在風險時，應向資訊安全通報窗口通報。

2.2 判別資訊安全事件等級：

2.2.1 權責單位於收到通知後，研判是否為資訊安全事件。若：

2.2.1.1 判定為非資訊安全事件時，則將結果回覆予發現人員。

2.2.1.2 判定為資訊安全事件時，初估事件處理時間，釐清僅須紀錄或立即進行處理因應作業，並通知權責主管及執行秘書。

2.2.2 資訊安全通報窗口於收到通報後，應立即進行該事件等級評估，並填寫「資訊安全事件通報單」。

2.3 資訊安全事件處理：

2.3.1 跡證蒐集：

2.3.1.1 各級資安事件發生時，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。

2.3.1.2 前項調查、處理及改善報告送交之時限，得經上級或監督機關及主管機關同意後延長之。

2.3.1.3 當三級或四級資訊安全事件發生時，若涉及行政或法律責任之追究，資訊安全執行小組應協助蒐集完整證據(如 Log、表單記錄、合約等)。

2.3.1.4 判斷是否啟動營運持續運作計畫：

2.3.1.4.1 依照「營運持續運作管理程序書」內有營運持續運作計畫啟動條件，判斷是否啟動營運持續運作管理程序。

2.3.2 進行營運持續運作管理程序

2.3.2.1 依照「營運持續運作管理程序書」之流程處理。

2.3.3 進行矯正及持續改善管理程序

2.3.3.1 依照「矯正及持續改善管理程序書」之流程處理。

2.3.4 事件結案

2.3.4.1 資訊安全事件必須確實排除後始得結案。