新光醫療財團法人
新光吳火獅紀念醫院
SHIN KONG WU HO-SU MEMORIAL HOSPITAL

新光吳火獅紀念醫院

資通安全事件通報及
危機處理作業程序書

－僅限本院同仁參閱－

新光醫療財團法人新光吳火獅紀念醫院

文 件 名 稱：資通安全事件通報及危機處理作業程序書

文 件 編 號：ISMS-2-07

制 定 單 位：資訊部

制 定 日 期：114 年 05 月 26 日

修 訂 紀 錄			
修訂日期	修訂內容摘要	頁次	版本
98.09.01	初版		1.0
104.09.01	修訂資安事件定義，並增述事故定義；資安事故歸類	1、2	1.1
110.01.28	依組織現行運作進行調整	全	1.2
112.04.19	依組織現行運作及流程進行調整	全	1.3
113.04.12	新增資通安全情資之評估及因應	6、7	1.4
113.06.06	新增緊急應變小組組織	1~10	1.5
114.05.26	因應 ISO27001:2022 轉版，相關內容改版	全	3.0
114.08.11	修正錯誤文字內容	全	3.1

新光醫療財團法人新光吳火獅醫院

文件編號	ISMS-2-07	文件名稱	機密等級	版本	3.1
制訂單位	資訊部	資通安全事件通報及危機處理作業程序書	內部使用	頁數	1/16

1 目的：

確保於資通安全事件發生時，能迅速依通報程序進行通報，並採取必要之應變措施，降低事件可能帶來之損害。

2 依據：

2.1 資通安全管理法

2.2 資通安全事件通報及應變辦法

2.3 ISMS-1-01 資訊安全政策

2.4 ISMS-2-03 資訊安全實施程序書

3 範圍：

本院作業環境中之資通安全事件。

4 權責

4.1 發現人：所有人員含正式員工與非正式員工（臨時員工或第三方派駐本院人員），發現疑似資通安全事件時，皆負有即時通報之責任。

4.2 資通安全管理委員會：督導本院之資通安全事件處理。

4.3 資安事件緊急應變小組：

4.3.1 小組人員詳如附錄 B。

4.3.2 發現資通安全事件後，進行分類及即時處理。

4.3.3 視資通安全事件之分類情況通知相關單位處理或通報資通安全管理委員會。

4.3.4 確定事件影響範圍並作損失評估。

4.3.5 協助資通安全事件分析、處理及通報。

4.3.6 依「資通安全情資分享辦法」之要求與中央目的事業主管機關進行情資分享。

4.4 支援單位：

4.4.1 本院內部單位：協助處理相關法律、人事懲處及採購等問題。

4.4.2 外單位：委外（第三方）廠商、上級主管機關、消防機關等。

5 定義

5.1 資通安全事件：於作業環境中，資訊之機密性、完整性、可用性遭受破壞之事件。

5.2 資通安全事件影響等級：依據「資通安全事件通報及應變辦法」辦理，將資通安全事件影響等級分為「一」、「二」、「三」、「四」四級，評定資安事件影響等級時，將以該事件造成之三面向(機密性、完整性及可用性)衝擊性，綜評該事件影響等級。

5.2.1 第一級：

- 非核心業務資訊遭輕微洩漏。
- 非核心業務資訊或非核心資通系統遭輕微竄改。
- 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。

5.2.2 第二級：

- 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。
- 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。
- 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。

5.2.3 第三級：

- 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。
- 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。
- 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。

5.2.4 第四級：

- 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。
- 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。
- 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。

6 作業內容

6.1 資通安全事件之管理

6.1.1 資通安全事件之反應與處理作業程序應包含以下事項：

6.1.1.1 醫療系統電腦當機或服務中斷。

6.1.1.2 資通系統環境遭入侵或破壞。

6.1.1.3 業務資料不完整或錯誤，導致作業異常。

6.1.1.4 機密性資料遭未授權存取。

6.1.1.5 重要幹線中斷。

6.1.1.6 電力供應中斷。

6.1.2 主要網路設備或線路中斷時，除執行應變計畫（如系統及服務回復作業）外，資通安全事件之處理程序應納入以下事項：

6.1.2.1 分析事件發生原因。

6.1.2.2 規劃並執行防止類似事件再發生之補救措施。

6.1.2.3 蒐集電腦稽核軌跡及相關證據。

6.1.2.4 與使用者、受影響人員或系統回復負責人進行溝通與確認。

6.1.3 電腦稽核軌跡及相關證據應妥善保存，以利後續管理作業：

6.1.3.1 作為問題分析之依據。

6.1.3.2 作為確認是否違反契約或資通安全規範之證據。

6.1.3.3 作為與軟硬體供應商協商補償之依據。

6.1.4 資通安全事件處理作業程序應包括以下事項：

6.1.4.1 於最短時間內確認作業及安全控制系統是否完整與正確。

6.1.4.2 向資安長報告緊急處理情形，並進行事件檢討與改正。

6.1.4.3 限定授權人員方可使用已回復正常之系統及資料。

6.1.4.4 紀錄緊急處理過程，以供後續查考。

6.2 資通安全事件之通報

已註解 [陳1]: 通報機制???本作業說明書??

6.2.1 發現或懷疑資通安全事件時，應依本作業程序書規定之通報機制，迅速通知權責主管單位與人員進行處理。

6.2.2 員工及與本院簽訂保密協議之外部人員，應明確了解資通安全事件的反應及報告程序，確保依規範處理。

6.3 資通安全弱點之反映

6.3.1 應即時監控資通系統及服務設施內部之安全弱點與可能威脅，並迅速通報主管單位。

6.3.2 系統安全弱點應由專業人員處理，不得由使用者自行修正。

6.4 軟體功能不正常之反映

6.4.1 使用者發現軟體功能異常時，應立即通知資訊部、工務部或服務廠商處理。

6.4.2 應建立軟體異常反映與處理程序，包括：

6.4.2.1 紀錄螢幕訊息與異常徵兆。

6.4.2.2 立即停止使用設備並通知資訊部。

6.4.2.3 檢視異常設備，於重新啟動前以離線方式處理。

6.4.2.4 使用者不得自行移除異常軟體，系統回復作業應由受過適當訓練及具備經驗之人員執行。

6.5 資通安全事件偵測判定

6.5.1 一般使用者：遇到下則狀況，通知資安專責人員，或通知總機，由總機轉知資安專責人員，專責人員及聯絡方式標註於「ISMS-1-02-1 資通安全組織成員表」。

6.5.1.1 防毒軟體訊息通知，電腦疑似中毒。

6.5.1.2 應用系統無故中斷，連不到伺服主機。

6.5.1.3 無法連接網際網路，網路連線異常。

6.5.1.4 網頁疑似被綁架，彈出垃圾廣告。

6.5.1.5 收到疑似釣魚簡訊、郵件。

6.5.1.6 收到疑似勒索軟體通知。

6.5.1.7 資料異常，疑似資料庫損毀。

6.5.1.8 疑似郵件帳密被盜，發大量異常郵件。

6.5.2 資安專責人員：立即判斷可能原因，並著手處理錯誤。並依法規「資通安全事件通報及應變辦法」完成資通安全事件等級判斷。

6.6 通報程序

6.6.1 疑似資通安全事件發生時，由發現人依事件歸屬通報資訊部資安專責人員並副知直屬主管。

6.6.2 資訊部資安專責人員於收到通知後，研判是否資通安全事件。若：

6.6.2.1 判定為非資安事件時，將結果回覆發現人。

6.6.2.2 判定為資安事件時，初估事件處理時間，並通知資安事件緊急應變小組。

6.6.2.2.1 資安組各相關系統管理人員檢視系統問題及處理。

6.6.2.2.2 資通安全事件發生時，應將事件發生之事實、可能影響之範圍、損失評估、判斷支援申請、採取之應變措施等事項，立即填「ISMS-2-07-01 資通安全事件報告單」或使用電子簽核系統之「資訊安全事件通報報告單」。

6.6.2.3 資安事件等級區分應依「資通安全事件通報及應變辦法」之要求辦理。

6.6.2.3.1 經判定為第一、二級時，應由資安專責人員通報單位主管、部主任。

6.6.2.3.2 經判定為第三、四級時，應由資安專責人員通報單位主管、部主任、資安長。

6.6.2.3.3 完成損害控制或復原作業後由資安長判定，依主管機關規範進行通報。

6.6.3 決策處理：

6.6.3.1 第一級由資訊部資安專責人員處理，資安組組長辦理必要之決策，並將處理後狀況通知資訊部主任。

6.6.3.2 第二級由資訊部資安專責人員、資安組組長辦理必要之處理，並由資訊部主任做決策。

6.6.3.3 第三、四級由資訊部資安專責人員、資安組組長、資訊部主任辦理必要之處理，並陳資通安全管理委員會主任委員(資安長)決策。

6.6.3.4 處理過程中如發現造成之影響大於原先判定事件，資訊部主任應立即向資通安全管理委員會主任委員(資安長)報告，重新執行事件分析辨識，判定事件等級。

6.6.3.5 資安專責人員確認事件等級後，先以口頭通報資安長。

6.6.3.6 資安長確認後於 1 小時內完成 H-ISAC 通報。

6.6.3.7 事件後續處理情形，需定期向資通安全委員會報告。

6.6.4 處理資安事件時，若需其他資源，則由資通安全管理委員會主任委員(資安長)負責溝通協調作業，並適時提供資安事件緊急應變小組必要的協助。

6.6.5 有關是否啟動營運持續計畫，依「ISMS-3-04 營運持續管理作業說明書」辦理。

6.6.6 有關本院之資訊設備發生異常則依「ISMS-3-01 實體與環境安全工作說明書」進行通報與維修。

6.6.7 當資安事件發生需對外說明時，資訊部主任應會同本院相關單位向資通安全管理委員會主任委員(資安長)陳報，並協助本院發言人對外說明情況與處置方式。

6.6.8 如遇資通安全事件危及人員生命或設備遭到破壞時，情況緊急需當下處理時，由資安事件緊急應變小組即時通知相關單位請求處理。

6.7 危機處理程序

6.7.1 本院電腦機房業務、資訊部之資通安全危機處理包括事前建置安全防護機制、事中主動預警緊急應變及事後復原追蹤鑑識偵查等步驟。說明如下：

6.7.1.1 事前建置安全防護機制：

6.7.1.1.1建置資通安全系統及整體防護架構，增加防禦能力，以減少事件發生；事前完備的防護機制，可增進處理事件之應變速度及減少損害程度。

6.7.1.1.2規劃建置資安系統及網路安全整體防護環境。

6.7.1.1.3彙整資安文件：安全相關文件應齊備，以利資通安全事件發生時可參考使用。

6.7.1.1.4規劃及執行模擬情境演練，以優化緊急應變程序及強化人員熟悉度

6.7.1.2 事中主動預警、緊急應變：

6.7.1.2.1事件辨識：其目的為辨識事件之歸屬及採取之對策為何，屬內部危安事件、外力入侵事件、天然災害或突發事件，並決定問題處理的方法與程序。

6.7.1.2.2事件控制：依據各類事件危機處理之程序，進行事件傷害控制，降低影響的程度及範圍。

6.7.1.2.3問題解決：事件處理權責單位或管理者須將問題徹底解決。例如在處理電腦病毒的擴散時，採用掃毒軟體來移除主機上的病毒。

6.7.1.2.4恢復作業：問題解決後，將系統恢復至事件發生前的正常運作狀態。

6.7.1.3 事後復原追蹤鑑識偵查：

6.7.1.3.1後續追蹤的精神在於檢討原事件是否會重複發生，並審視現有環境的漏洞，藉研析相關資料以釐清事件發生的原因與責任。

6.7.1.3.2受損單位依復原程序實施災後復原重建。

6.7.1.3.3資安事件應保留事件發生之線索，如有需要得向檢警單位申請數位鑑識（電腦、網路鑑識）。

6.7.1.3.4為有效追蹤，檢討事件原因，應審視現有環境的漏洞，由權責單位於「ISMS-2-07-01 資通安全事件報告單」或電子簽核系統之「資訊安全事件通報報告單」，詳述事件發生原因、處理經過、因應對策、檢討暨改善建議及持續追蹤事項。

6.7.2 資通安全事件通報與危機處理流程，詳如附錄 A。

6.7.3 外力入侵事件危機應變參考程序，詳如附錄 C。

6.8 資通安全情資之評估及因應

本院接獲資通安全情資(數發部提供漏洞警訊情資、HISAC 及委外公司、SOC 提供之威脅情資及資安新聞)，應由資安專責人員評估該情資之內容，並檢視如果對本院有影響，應決定最適當之因應方式，並做成紀錄。

6.8.1 資通安全情資之分類評估

本院接受資通安全情資後，應指定資通安全專責人員進行情資分析，並依據情資之性質進行分類及評估，責由相關管理人員進行防護因應，情資分類評估如下：

嚴重等級：高

- 影響本院核心系統運作。

- 已被公開或地下組織公佈程式碼/工具的漏洞。
- 經利害關係團體研判對本院有重大資安疑慮。

嚴重等級：中

- 影響本院非核心系統運作。
- 已被公開或地下組織公佈程式碼/工具的漏洞
- 經利害關係團體研判對本院有資安疑慮。

嚴重等級：低

- 對本院營運相關系統無直接影響。
- 非本院重要營運系統有資安疑慮。

6.8.2 資通安全情資之因應措施

本院於發現資通安全之相關情資後，由本院資訊部資安專責人員進行資通安全情資分類評估後(必要時得委專家或廠商協助分析處理)，應針對情資之等級進行相應之控制措施。

6.8.2.1 評估為「高」嚴重等級之情資若已影響內部相關服務與作業時，應依據「5.2 通報程序」辦理，以資安事件標準判定後續處置方式。

6.8.2.2「中」嚴重等級以下則視需要以信件或其他得以留下紀錄之方式通知當責單位評估修補，並應於接獲通知後儘速分派相關人員進行處理，並將評估結果及預計處理方式回覆資訊部，後續由資訊部彙整追蹤處理結果。

6.8.2.3 情資處理時效

6.8.2.3.1「高」嚴重等級：須於 30 天內完成分析及改善。

6.8.2.3.2「中」嚴重等級：須於 60 天內完成分析及改善。

6.8.2.3.3「低」嚴重等級：須於 90 天內完成分析及改善。

6.8.2.4 情資處理原則

6.8.2.4.1評估影響之範圍及攻擊手法，提出相關矯正預防措施、依照弱點等級進行修補作業及時程安排及評估現有的防禦能力及技術，確認是否足以防禦此威脅，若無法防禦應提出相關強化之解決方案。

6.8.2.4.2威脅情資應納入每年風險評估作業進行考量。

6.8.2.4.3 資訊部應每月檢視 HISAC、VANS、SOC 報告中與重要及本院有相關情資，填註威脅情資管理紀錄。

6.8.2.4.4 資安委員會會議定期提報與本院有相關情資之統計數據及因應。

6.8.2.4.5 若因其他因素導致系統無法進行修補作業，應將無法修補之弱點、影響之系統、預計剩餘風險、無法修補之原因(視需要會同系統開發單位提供佐證)及風險控制補償措施提報評估後，並取得主管核准後始得排外。

6.8.2.5 情資分享對象及方式

本院如有資安情資，依據主管機關衛福部律定情資分享方式通報。

7 實施與修訂

本程序書奉　資訊安全委員會副主任委員核定後實施，修正時亦同。

8　相關文件

ISMS-3-01_實體與環境安全工作說明書。

ISMS-3-05_營運持續管理作業說明書。

9　使用表單

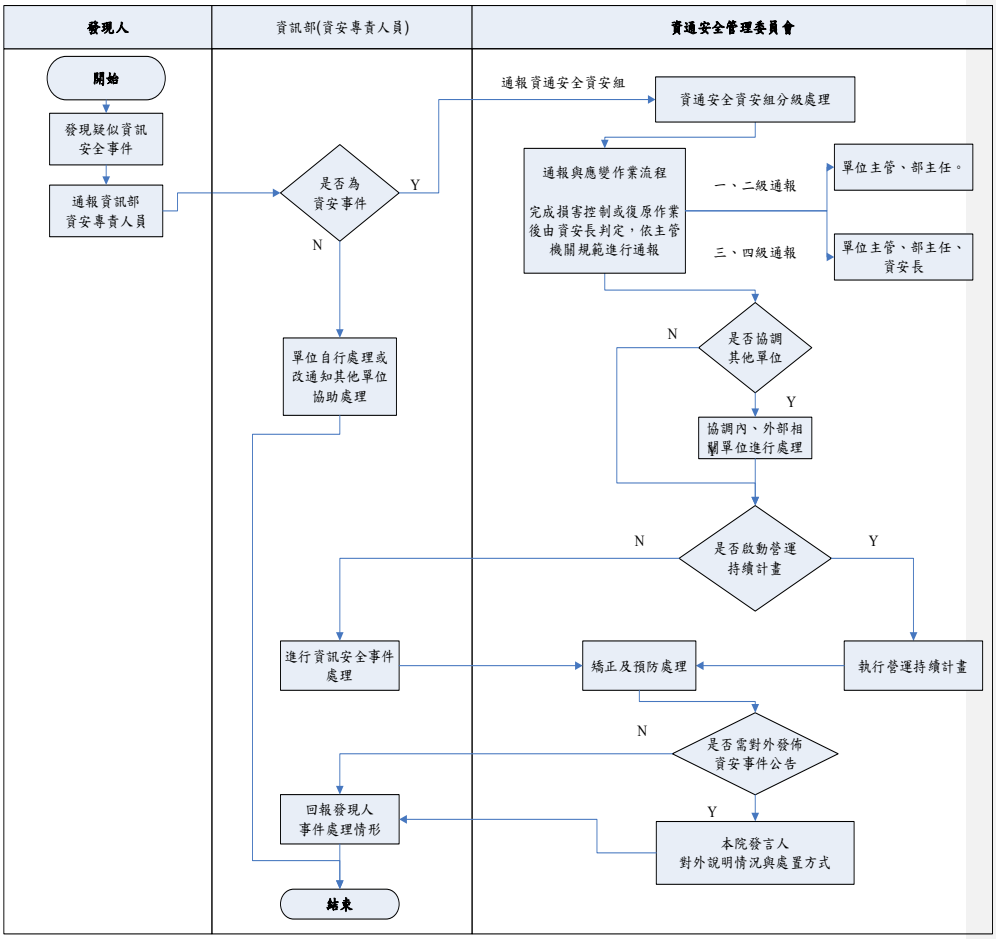
ISMS-1-02-01_資通安全組織成員表。

ISMS-2-07-01_資通安全事件報告單。

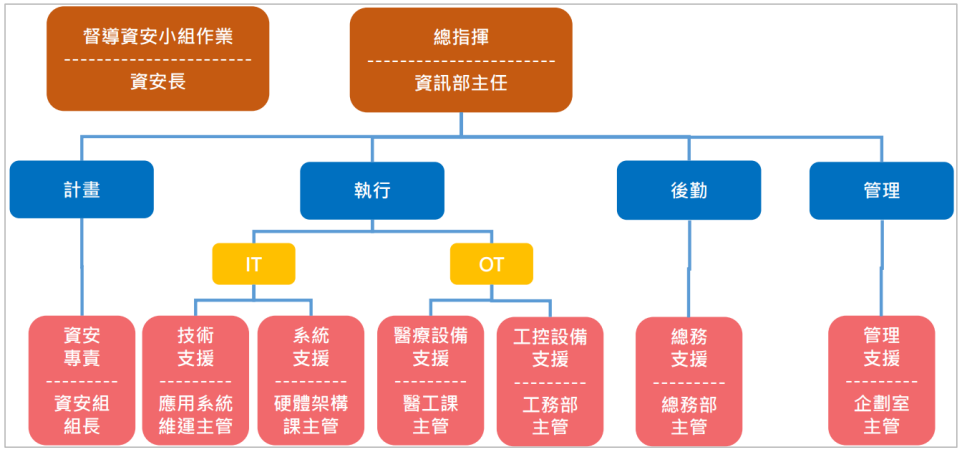
新光醫療財團法人新光吳火獅醫院

文件編號	ISMS-2-07	文件名稱	機密等級	版本	3.1
制訂單位	資訊部	資通安全事件通報及危機處理作業程序書	內部使用	頁數	11/16

附錄A、資通安全事件通報與危機處理流程



附錄B、資安事件緊急應變小組



附錄C、外力入侵事件危機應變參考程序

C.1、病毒及蠕蟲程式：

病毒及蠕蟲程式處理應變步驟如下：

C.1.1、第一步：隔離系統－當系統遭受攻擊時，由該系統管理者迅速自網路移除，但在移除前，須先審慎考量相關修補程式或解藥程式是否可以安裝。在處理時必須要詳細紀錄下所有的步驟。為防止病毒破壞或相關入侵證據遺失，勿強行中斷主機電力或將其重新開機。如果擴散的速度過快，系統管理者應立即將網路線移除，以確保蠕蟲病毒不會向外或向內擴散。此時應保留一條向外的通訊管道（如撥接網路），以備於必要時下載升級程式或病毒定義檔（病毒碼）。在未確定蠕蟲或病毒完全被控制之前，不得將 Internet 的網路線重新置回。

C.1.2、第二步：通知相關人員處理－如果事件仍持續擴大，系統管理者須通報單位主管、資訊部主管、資通安全資安組。經資通安全資安組協助，並決策通報資通安全管理委員會，由資通安全管理委員會決議，由召集人啟動緊急處理分組之機制。

C.1.3、第三步：辨識問題－應列出與病毒相關的檔案或系統程序，並予以清除或隔離。在處理時必須要詳細紀錄下所有的步驟，以利日後分析。如無法辨識，應聯繫防毒軟體廠商，提供解決的方法。

C.1.4、第四步：移除及預防病毒－將有問題的系統程序終止或移除，並利用廠商所提供的修補程式或解毒程式來移除病毒。所有系統，不論是否遭受攻擊，應同時進行掃毒及預防的工作。

C.1.5、第五步：恢復運作－在將系統恢復至正常運作狀態時，須逐步實施，並通知使用者恢復作業的進行。應要求各使用者或系統管理者密切注意系統復原狀況，發現任何異常，應立即停止所有復原程序進行查錯。若毫無任何升級或修補程式可用，則應利用事件發生前無瑕疵的系統備份來作恢復的工作

C.1.6、第六步：後續檢討－當事件處理完畢，系統恢復至正常運作狀態後，應作後續的檢討，並評估或修改既有不合時宜的程序。所作成的報告在彙整之後可作為範例或教案分發給相關人員。

C.2、入侵：發現或被入侵時，處理步驟如下：

C.2.1、第一步：通知相關人員－即刻通知系統管理者或應用程式管理者到場協助處理。

C.2.2、第二步：辨識問題－從系統事件紀錄檔及進行中的網路連線中找出攻擊的出處。系統管理者或應用程式管理者應儘快連絡相關網管人員，嘗試找出入侵者 IP 位址。

C.2.3、第三步：控制問題－強制將入侵者所建立的連線中斷，或鎖定有心人士所使用的帳號，強迫其自系統登出，或乾脆將網路線自系統移除。如果決定保持入侵者的連線以搜集證據，系統管理者或應用程式管理者，以及網管人員應將營運停頓及資料外洩的風險納入考量。一旦確定証據蒐集已備齊，應即刻中斷入侵者連線。如果事件仍持續擴大，系統管理者須通報單位主管、資訊部主管、資通安全資安組。經資通安全資安組協助，並決策通報資通安全管理委員會，由資通安全管理委員會決議，由召集人啟動緊急處理分組之機制。

C.2.4、第四步：移除問題－終止所有執行中的程序，並移除任何有心人士所留下的帳號、檔案或目錄。如果只有一個帳號為有心人士所使用，則此帳號的密碼須加以更改，如果是超過一個以上的帳號為有心人士所使用，則最好強迫所有使用者更改密碼。聯絡軟體廠商提供修補程式以修復系統的安全漏洞。

C.2.5、第五步：恢復運作－在將系統恢復至正常運作狀態時，須逐步實施，並通知使用者恢復作業的進行。應要求各使用者或系統管理者密切注意系統復原狀況，發現任何異常，應立即停止所有復原程序進行查錯。

C.2.6、第六步：後續檢討－當事件處理完畢，系統恢復至正常運作狀態後，應作後續的檢討，並評估或修改既有不合時宜的程序。所作成的報告在彙整之後可作為範例或教案分發給相關人員。

C.3、人員進出管制：

若有未經授權進入的閒雜人等在管制區中徘徊，平日該關閉的門窗無故開啟等，這些皆會對資安環境形成潛在的威脅。人員進出管制的處理步驟如下：

C.3.1、第一步：辨識問題－如有不明人士在管制區中徘徊而無陪同人員在場，發現者應要求對方提出識別証明及來訪的事由。當發現者感覺到人身受到威脅，切勿嘗試獨自與對方接觸。

C.3.2、第二步：移除問題－若對方未能提出有效證明，發現者應陪同對方至警衛處。如果對方未能遵從指示，發現者必須立即通報警衛或通知資通安全資安組聯絡警察單位處理。不明人士進入的方式及時間必須調查清楚。

C.3.3、第三步：後續檢討－當事件處理完畢，資通安全資安組應作後續的檢討。檢視相關的人員出入紀錄，比對不明人士進入的方式及時間，並且利用此機會來評估或修改既有不合時宜的程序。

C.4、阻斷服務攻擊（DOS）：

阻斷服務攻擊的處理步驟如下：

C.4.1、第一步：辨識問題－從系統的事件紀錄辨識攻擊的形態、範圍、本質，辨識攻擊者所使用方法是利用應用程式，封包遞送過程，或者是通訊協定的安全漏洞。往連線上游找出被控制的阻塞點，或找出攻擊的源頭。

C.4.2、第二步：通知相關人員－即刻通知系統管理者、應用程式管理者或連線服務提供廠商協助處理。

C.4.3、第三步：控制問題－系統管理者、應用程式管理者或連線服務提供廠商可立即修改路由器上的 ACL（Access Control List）來限制惡意封包的通過。也可運用防火牆或其他封包過濾工具來阻擋攻擊的進行。如果決定將自攻擊來源的連線強制中斷，系統管理者、應用程式管理者應將營運中斷的風險納入考量。如果事件仍持續擴大，系統管理者須通報單位主管、資訊部主管、資通安全資安組。經資通安全資安組協助，並決策通報資通安全管理委員會，由資通安全管理委員會決議，由召集人啟動緊急處理分組之機制。

C.4.4、第四步：移除問題－與連線服務提供廠商合作來過濾攻擊來源的連線。移除不必要的服務埠或調整軟體參數以避免過多 session 同時啟動。聯絡軟體廠商提供修補程式以修復系統的安全漏洞。

C.4.5、第五步：恢復運作－在將連線恢復至正常運作狀態時，須逐步實施，並通知使用者恢復作業的進行。應要求各使用者或系統管理者密切注意連線復原狀況，發現任何異常，應立即停止所有復原程序進行查錯。

C.4.6、第六步：後續檢討－當事件處理完畢，連線恢復至正常運作狀態後，應作後續的檢討。