

財政資訊中心暨各地區國稅局
資訊安全事故管理準則

版本 1.1

中華民國 102 年 1 月 4 日

文件編號	ISMS-209-01	資訊安全事故管理準則	版本	1.1
------	-------------	------------	----	-----

1.依據.....	1
2.目的	1
3.範圍.....	1
4.權責.....	1
5.定義.....	2
6.作業規範.....	2
7.相關資料.....	5
8.附件暨使用表單.....	6
9.角色權責分配表.....	6
附件 1、行政院國家資通安全會報通報與應變作業流程圖.....	8
附件 2、資安事故管理暨國家資通安全通報應變網站通報流程圖.....	9

文件編號	ISMS-209-01	資訊安全事故管理準則	版本	1.1
------	-------------	------------	----	-----

1. 依據

- 1.1 行政院頒定之『行政院及所屬各機關資訊安全管理規範』。
- 1.2 財政部頒定之『財政部暨所屬機關(構)資訊安全管理準則』。
- 1.3 行政院國家資通安全會報頒定之『國家資通安全通報應變作業綱要』。

2. 目的

財政資訊中心暨各地區國稅局(以下簡稱各機關)為確保與資訊系統相關的資訊安全事件與弱點發生時，相關處理與權責單位能在最短時間內，經由通報程序掌握資訊，即時作出研判並採取必要之應變措施，避免事件或事故擴大，降低可能帶來之損害，特制定本管理準則。

3. 範圍

各機關資訊作業環境發生資訊異常事件或資安事故。

4. 權責

4.1 各機關資訊作業環境內部與外部人員

發現或觀察到可疑的異常事件、資安事故或安全弱點時，皆負有即時通報並提供相關資訊之責任。

4.2 發生異常事件或資安事故之作業單位

應視狀況配合處理單位做即時適當之處理，並於事後配合進行評估、規劃及執行改善與預防措施計畫。

4.3 財政資訊中心資訊安全執行小組

4.3.1 接受各機關異常事件或資安事故通報，並蒐集與彙總相關資訊。

4.3.2 整體異常事件或資安事故通報流程之規劃與建議。

4.3.3 評估異常事件或資安事故範圍及其影響。

4.3.4 對資訊安全聯合執行小組呈報異常事件或資安事故及其處理狀況。

4.3.5 執行異常事件或資安事故偵測、預防、通報、分析及處理。

4.3.6 完整留存異常事件或資安事故相關紀錄。

4.3.7 督導並追蹤各單位之改善與預防措施計畫及執行進度。

4.3.8 彙整異常事件或資安事故之處理結果、改善與預防措施執行結果，並向資訊安全管理審查聯席會報呈報。

4.4 各機關資訊安全執行小組

4.4.1 評估各機關異常事件或資安事故範圍及其影響。

4.4.2 呈報資異常事件或資安事故及其處理狀況。

4.4.3 執行各機關異常事件或資安事故偵測、預防、通報、分析及處理。

4.4.4 完整留存異常事件或資安事故相關紀錄。

文件編號	ISMS-209-01	資訊安全事故管理準則	版本	1.1
------	-------------	------------	----	-----

4.5 其餘相關權責依據『資訊安全組織管理準則』附件1、資訊安全工作執行執掌表。

5. 定義

5.1 資訊安全事件(Information security event)

系統、服務或網路發生一個已識別的狀態，其指示可能的資訊安全政策違例或保護措施失效，或是可能與安全相關而先前未知的狀況等。

5.2 資訊安全事故(Information security incident)

單一或一連串有顯著機率可能危害營運作業與威脅資訊安全之非所欲或非預期的資訊安全事件；或未遵循資訊安全政策、管理準則或作業規範，造成損害之事件。

5.3 外部支援單位

委外廠商、司法警政及消防機關、政府網路危機處理中心(GSN-CERT/CC)、國家資通安全會報技術服務中心、台灣電腦網路危機處理暨協調中心(TWCERT/CC)等，聯繫資訊參見「資訊安全聯絡清單」中之外部單位。

6. 作業規範

6.1 資訊安全事件與安全弱點通報

- 6.1.1 內部或外部人員發現或觀察到異常事件，應向資訊服務管理服務台進行通報；如確認為資訊安全事件則向各機關資安聯絡人進行資訊安全事件通報。
- 6.1.2 資訊安全監控平台自動告警之資訊安全事件，依「資訊安全通報單」(電子表單)相關流程進行管制。
- 6.1.3 發現資安事件時，宜同時採取下列正確行為：
 - 6.1.3.1 立即記錄所有重要細節(例如：未遵循或違反事件的型式、故障發生情形、螢幕上顯示的訊息、奇怪的行為)。
 - 6.1.3.2 不自己執行任何動作，但立即通報窗口。
 - 6.1.3.3 在任何情況下都不要嘗試去證明可疑的弱點。
- 6.1.4 各機關資安聯絡人於收到通報後，須通知相關管理人員進行事件處理並追蹤處理情形。
- 6.1.5 若通報事件由本地資訊服務管理服務台或二線人員根據『國家資通安全通報應變作業綱要』，依實際影響情形判定屬6.2定義之級別，除進行『資訊服務管理服務台管理程序手冊』及『事件管理程序手冊』之事件與通報處理，應依據SOC『緊急事件單通報流程』，通報至國家資通安全通報應變網站，並以傳真、電話或E-mail副知財政資訊中心資安窗口。

文件編號	ISMS-209-01	資訊安全事故管理準則	版本	1.1
------	-------------	------------	----	-----

6.2 資訊安全事件分級

6.2.1 依據『國家資通安全通報應變作業綱要』，資安事件影響等級區分為4個級別，由重至輕分別為「4級」、「3級」、「2級」、「1級」：

6.2.1.1 4級事件(符合下列任一情形者，屬4級事件)：

6.2.1.1.1 國家機密資料遭洩漏。

6.2.1.1.2 國家重要資訊基礎建設系統或資料遭竄改。

6.2.1.1.3 國家重要資訊基礎建設運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作。

6.2.1.2 3級事件(符合下列任一情形者，屬3級事件)：

6.2.1.2.1 密級或敏感業務資料遭洩漏。

6.2.1.2.2 核心業務系統或資料遭嚴重竄改。

6.2.1.2.3 核心業務運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作。

6.2.1.3 2級事件(符合下列任一情形者，屬2級事件)：

6.2.1.3.1 非屬密級或敏感之核心業務資料遭洩漏。

6.2.1.3.2 核心業務系統或資料遭輕微竄改。

6.2.1.3.3 核心業務運作遭影響或系統效率降低，於可容忍中斷時間內回復正常運作。

6.2.1.4 1級事件(符合下列任一情形者，屬1級事件)：

6.2.1.4.1 非核心業務資料遭洩漏。

6.2.1.4.2 非核心業務系統或資料遭竄改。

6.2.1.4.3 非核心業務運作遭影響或短暫停頓。

6.3 資訊安全事故處理程序

6.3.1 判定為1級(含)以上需通報至國家資通安全通報應變網站之事件，若處理過程中如發現事件造成影響大於原先判定等級，應立即更正事件分級；應通報應變網站之事件需進行以下作業：

6.3.1.1 立即評估事故處理時間。若判斷處理時間超過可容忍中斷時間，應通報各機關資訊安全執行小組組長，依據『營運持續管理準則』評估是否啟動營運持續作業，及適時尋求外部單位協助處理。

6.3.1.2 若為國稅平台共通資訊安全事件，財政資訊中心資訊服務管理服務台應通知資訊安全聯合執行小組組長，必要時召集相關成員協助各機關進行資安事故處理；若為3級(含)以上事件，並通知資訊安全管理審查聯席會報召集人。

文件編號	ISMS-209-01	資訊安全事故管理準則	版本	1.1
------	-------------	------------	----	-----

- 6.3.1.3 若為各機關個別之資訊安全事件，各機關資訊服務管理服務台應通知資訊安全執行小組組長，必要時召集相關人員或協調財政資訊中心人員處理資訊安全事件；若為3級(含)以上事件，並通知各機關資訊安全長。
- 6.3.1.4 於一小時內向「國家資通安全通報應變網站」通報，相關通報流程如「行政院國家資通安全會報通報與應變作業流程圖」(詳附件1)。
- 6.3.1.5 4、3級事件須於發現資安事件36小時內復原或完成損害管制，2、1級事件須於發現資安事件72小時內復原或完成損害管制。
- 6.3.1.6 資訊安全事件危及人員生命或設備遭到破壞等涉及民、刑事案件時，應由政風室通報檢調單位請求處理。
- 6.3.2 處理資安事故時，由資訊安全執行小組組長負責協調相關單位提供必要資源。
- 6.3.3 必要時資訊安全執行小組組長應負責或指派專人對外說明資安事故處理進度。
- 6.3.4 外部通報流程可參考「國家資通安全通報應變網站通報流程圖」(詳附件2)。
- 6.4 資訊安全事故檢討與學習
- 6.4.1 應辨識資安事故根因並採取有效對策，依據資安事故分類，研擬改善未來事故處理的方法與程序。
- 6.4.2 資訊安全執行小組應定期將資安事故統計資訊提交資訊安全管理審查會報，以利資訊安全管理制度之持續改善。
- 6.4.3 資訊安全事故依『資訊安全矯正及預防管理準則』及『問題管理程序手冊』進行矯正與預防步驟。
- 6.4.4 資訊安全事故處理結果應定期彙整，並在無牽涉個人隱私與業務機密之情況，可公告於內部網站，描述事件發生原因、過程、處理方式與改善與注意事項建議等，做為資安宣導及資安事件預防之參考資訊。
- 6.5 資訊安全事故證據蒐集
- 6.5.1 於資安事故處理過程中，若涉及民、刑事法律行動，應進行蒐證與證據保留，必要時得協調外部支援單位或檢警單位協助處理。
- 6.5.2 於證據蒐集完成前，相關電腦應儘量避免重新開機，以保全完整證據，必須重新開機，則應於重新開機前保留系統稽核紀錄檔案。

文件編號	ISMS-209-01	資訊安全事故管理準則	版本	1.1
------	-------------	------------	----	-----

6.5.3 必要時，宜根據以下原則建立證據存底：

- 6.5.3.1 紙本文件：妥為保管記錄發現者、發現地點、發現時間及發現時在場證人的原始文件，任何調查都宜確保原始文件未遭竄改。
- 6.5.3.2 電腦媒體上的資訊：所有可移除式媒體、硬碟上或記憶體中的資訊宜製作鏡像(Mirror image)或複本(依適用性與要求)，以確保可用性；複製過程的所有活動宜保留日誌，且過程宜有見證；宜以安全方式保持原始媒體與日誌(若無法做到，至少保存一份鏡像或複本)，並使其不被變動。
- 6.5.3.3 所有鑑識工作宜只在數位證據的複本上執行。
- 6.5.3.4 宜保護所有數位證據的完整性。
- 6.5.3.5 數位證據的複製宜由授權人員監督，執行複製過程的時間、地點、執行複製活動的人員、利用的工具和程式等資訊宜予以存錄。

6.5.4 參考之蒐證類別與內容如下：

- 6.5.4.1 電腦設備：作業系統及資料庫之日誌檔、系統變更歷程紀錄、維護紀錄等。
- 6.5.4.2 機房設施：人員與物品進出機房紀錄、電腦機房工作日誌、環境監控系統日誌檔、監視錄影紀錄、門禁刷卡紀錄、維護紀錄等。
- 6.5.4.3 軟體：軟體日誌檔、程式變更歷程紀錄、程式測試紀錄、應用系統異動與執行紀錄、資料變更歷程紀錄等。
- 6.5.4.4 文件：引用文件版本、來源、發行、借閱、銷毀紀錄等。
- 6.5.4.5 人員：人員進出辦公場所紀錄、職務分配表、輪班表、差勤紀錄、訓練紀錄等。
- 6.5.4.6 服務：契約、服務人員名冊(含下包商服務人員)、人員與物品進出紀錄、服務紀錄等。
- 6.5.4.7 組織聲譽：媒體報導、利害關係人公文書等。

6.6 資訊安全事件通報演練

6.6.1 應配合國家資通安全會報實施以下演練：

- 6.6.1.1 通報演練：主要測試聯絡電話與所有通報聯絡人之 E-mail 與簡訊發布有效性。
- 6.6.1.2 模擬攻防演練：主要模擬實際駭客入侵作為實施入侵檢驗，應按規定通報及辦理相關因應處置。

7. 相關資料

文件編號	ISMS-209-01	資訊安全事故管理準則	版本	1.1
------	-------------	------------	----	-----

- 7.1 『資訊安全組織管理準則』
- 7.2 『營運持續管理準則』
- 7.3 『資訊安全矯正及預防管理準則』
- 7.4 SOC 『緊急事件單通報流程』
- 7.5 資訊服務管理流程說明書之『資訊服務管理服務台管理程序手冊』
- 7.6 資訊服務管理流程說明書之『事件管理程序手冊』
- 7.7 資訊服務管理流程說明書之『問題管理程序手冊』

8. 附件暨使用表單

- 8.1 附件 1、行政院國家資通安全會報通報與應變作業流程圖
- 8.2 附件 2、資安事故管理暨國家資通安全通報應變網站通報流程圖
- 8.3 資訊安全通報單 (電子表單)

9. 角色權責分配表

資訊安全事故管理主要活動角色權責分配表(A- Accountable 負責角色、R- Responsible 執行角色、C- Consulted 受諮詢角色、I- Informed 被告知角色)：

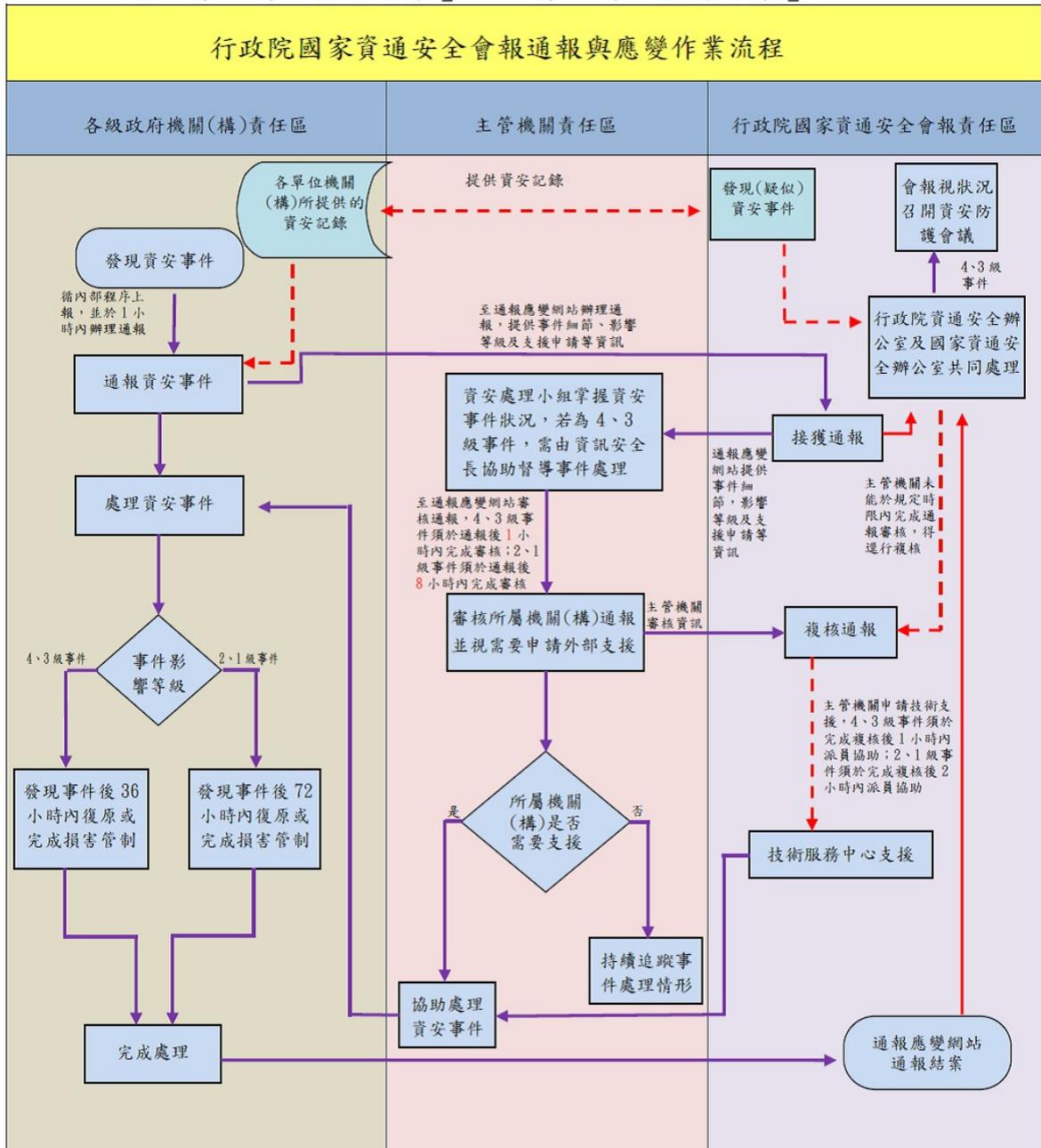
負責單位	聯合資安組織		各機關權責人員：		
重要資訊安全事故工作事項	資訊安全管理審查 聯席會報	資訊安全 聯合執行 小組	資訊安全長 與資安管理 審查組織	資訊安全 執行小組	資訊服務 管理服務 台
事件處理及通報處理				A	R
填寫資安事件通報單			I	A	R
評估事故處理時間			I	A	R
通報聯合執行小組組長/聯席會報召集人	I	I	I	A	R
通報各機關執行小組組長/資訊安全長			I	I	R/A
處理共通	A	R			I

文件編號	ISMS-209-01	資訊安全事故管理準則	版本	1.1
------	-------------	------------	----	-----

負責單位	聯合資安組織		各機關權責人員：		
	資訊安全管理審查 聯席會報	資訊安全 聯合執行 小組	資訊安全長 與資安管理 審查組織	資訊安全 執行小組	資訊服務 管理服務 台
資安事故					
處理各機關 資安事故			I	A	R
進行國家資通 安全會報通報	I	I	I	A	R
各機關共通資 安事件之檢討 及監督	A	R	I		
各機關個別資 安事件之檢討 及監督		I	A	R	

文件編號	ISMS-209-01	資訊安全事故管理準則	版本	1.1
------	-------------	------------	----	-----

附件 1、行政院國家資通安全會報通報與應變作業流程圖



文件編號	ISMS-209-01	資訊安全事故管理準則	版本	1.1
------	-------------	------------	----	-----

附件 2、資安事故管理暨國家資通安全通報應變網站通報流程圖

資安事故管理暨國家資通安全通報
應變網站通報流程圖

