元智大學

資訊安全事件管理暨通報作業程序

機密等級：公開
文件編號：ISMS-P-12
版　　次：1.2
文件負責人：文管人員
發行日期：2025-10-30

修 訂 紀 錄				
版次	修訂日期	修訂頁次	修訂者	修訂內容摘要
1.0				初版
1.1	113.9.24	7,8	黃欣慧	6.3、附錄A，將「國家資通安全通報應變作業綱要」改為「資通安全事件通報及應變辦法」
1.2	114.10.15	1,3,4,5,7	黃欣慧	1. 適用範圍更改成全校，修改文件名稱，目的及適用範圍一併修正。 2. 修訂 5.1.1 流程、5.1.2~5.1.9 納為 5.1.1.1~5.1.1.8、改 5.1.10~5.1.14 為 5.1.2~5.1.6。 3. 安插「5.1.4」涉及個資通報與應變、新增「5.1.15」定期呈報年度資安事件資訊予主管。 4. 新增相關文件：元智大學個人資料檔案安全維護計畫。

核　　准	審　　查	制　　訂

目錄

資訊安全事件管理暨通報作業程序					
文件編號	ISMS-P-12	機密等級	公開	版本	1.2

1 目的

確保本校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，以降低事件可能帶來之損害。

2 適用範圍

本校作業環境中之資訊安全事件均適用之。

3 權責

3.1 事件發現人員

發現疑似資訊安全異常事件時，皆負有即時通報之責任。

3.2 權責單位

指資訊安全事件處理之權責單位，確定事件影響範圍並作損失評估，並執行資訊安全事件之分析及處理。

3.3 資訊安全管理小組

督導資訊安全事件分析、處理及通報等。

3.4 資訊安全工作小組

執行危機處理程序作業包含資訊安全事件分析、處理及通報等。

3.5 外部單位：協助資訊提供、資訊安全事件處理等。

4 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、可用性遭受破壞之事件。

4.2 資訊安全事故

資訊安全事件 3 級以上(事件等級請參照附錄 A)。

4.3 資訊安全事件分類

4.2.1 內部危安事件：發現（或疑似）遭人為惡意破壞毀損、作業不慎

等事件。

4.2.2 外力入侵事件：電腦病毒感染事件、駭客攻擊（或非法入侵）事件。

4.2.3 天然災害或突發事件

4.2.3.1 天然災害：颱風、水災、地震等。

4.2.3.2 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。

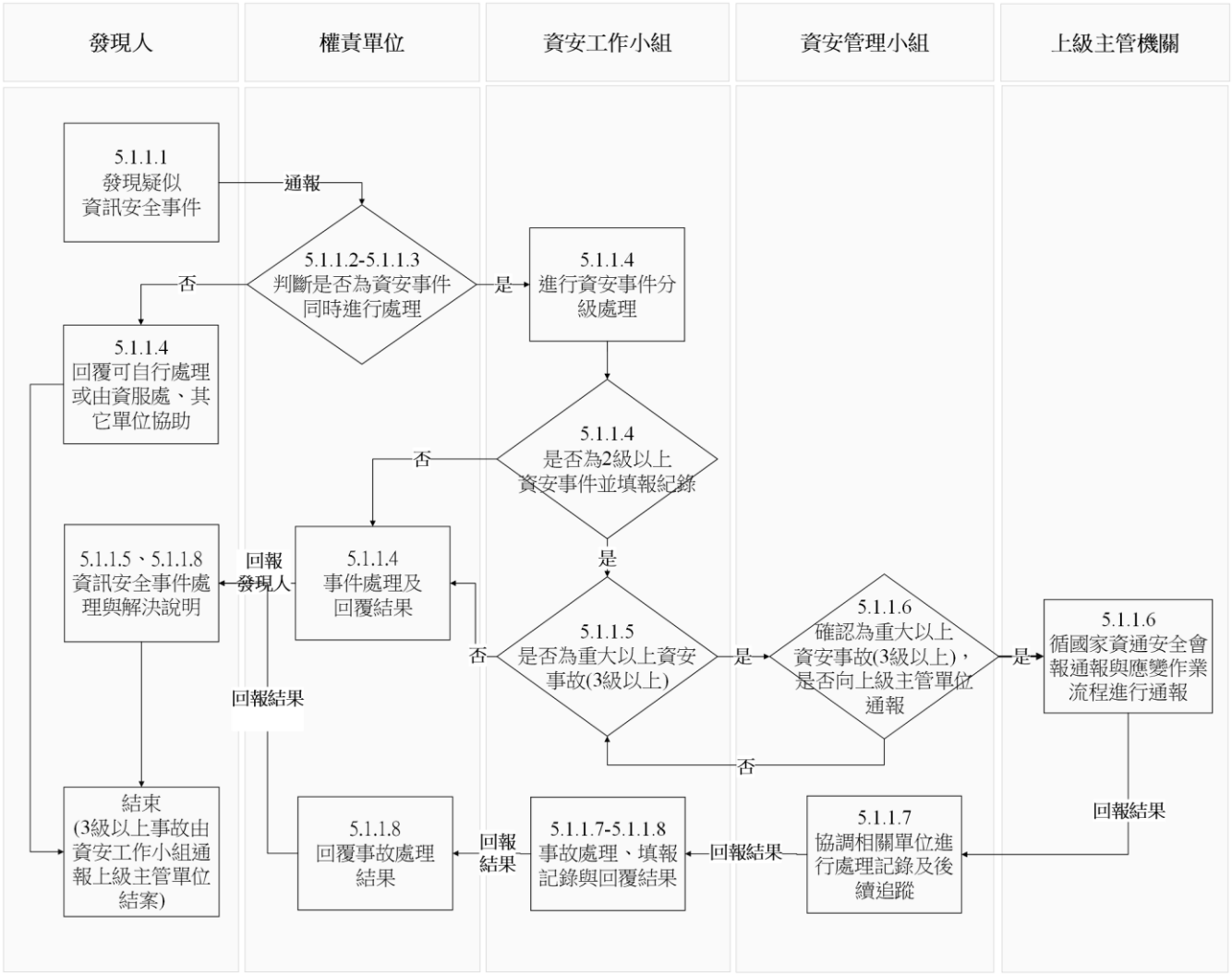
4.2 外部單位

委外(第三方)廠商、司法警政及消防機關、政府網路危機處理中心(GSN-CERT/CC)、負責國家資通安全及技術研究單位、台灣電腦網路危機處理暨協調中心(TWCERT/CC)、桃園區域網路中心、資訊及科技教育司等。

5 作業說明

5.1 事件通報及受理程序

5.1.1 流程



5.1.1.1 所有人員發現有資訊安全可疑事件時，需向「權責單位」進行資訊安全事件通報。

5.1.1.2 權責單位於收到通知後通報資訊單位，於第一時間研判是否為資訊安全事件，若判定為非資安事件時，將結果回覆事件發現人員。

5.1.1.3 當事件影響較低、衝擊性較小，僅涉及單位內且受損程度輕微時（如內部危安、電腦病毒感染），由權責單位處理，並將處理後狀況通知權責單位主管。

5.1.1.4 確定為資安事件後，由「資訊安全工作小組」進行分級，若判定為 2 級以上之資安事件時，由「資訊安全工作小

組」填寫「ISMS-F-34 資安事件通報紀錄表」，並判定是否為重大資安事故(3 級以上)。若判定為非2級以上資安事件，由權責單位處理後， 將結果回覆事件發現人員。

5.1.1.5 若判定為重大資安事故時，初估事件須處理時間，並通知「資訊安全管理小組」。若判定為非重大資安事故時，以2級資安事件處理及回覆。

5.1.1.6 若判定為重大資安事故且向上級主管單位通報。「資訊安全管理小組」得依據權責單位所提報之事件影響報告，決定是否向上級主管單位通報，若研判需通報，經單位主管確認後，則依據「資通安全事件通報及應變辦法」進行通報。

5.1.1.7 處理資安事件時，若需其他資源，則由「資訊安全管理小組」負責溝通協調作業，並適時提供「資訊安全工作小組」必要的協助。

5.1.1.8 「資訊安全工作小組」於處理資安事件時，應將事件發生之事實、可能影響之範圍、損失評估、判斷所需支援申請、採取之應變措施等事項，填報於「ISMS-F-33 資訊安全事件報告單」，並將結果回報權責單位由其回覆事件發現人員。

5.1.2 有關是否啟動業務持續計畫，依據「ISMS-P-21 業務持續營運管理程序書」辦理。

5.1.3 有關本校資訊設備發生異常則依「ISMS-P-17 資訊設備與媒體管理作業辦法」規定，進行通報與維修。

5.1.4 有關是否涉及個資事件，參考「元智大學個人資料檔案安全維護計畫」規定，進行通報與應變。

5.1.5 當重大資安事件發生需對外說明時，「資訊安全管理小組」須協助對外說明情況與處置方式，並向上級主管機關陳報。若非本校能力處理之資訊安全事件應適時尋求外部單位協力處理。

5.1.6 如遇資訊安全事件危及人員生命或設備遭到破壞，情況緊急需當下處理時，由「資訊安全工作小組」即時通知相關單位請求處理，並通報「資訊安全管理小組」同時參考5.2危機處理程序應變。

5.1.7 彙整年度資安事件資訊，定期呈報資訊安全管理小組召集人與資通安全暨個人資料保護推動委員會召集人，供後續檢討與決策參考。

5.2 危機處理程序

5.2.1 資訊單位在資訊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：

5.2.2 事前建置安全防護機制

5.2.2.1 建置資訊安全系統(例人員安全管理、資產分類與控管、實體與環境安全管理、系統開發與維護等安全機制等)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。

5.2.2.2 參考「行政院及所屬各機關資訊安全管理要點、管理規範」規劃建置資安系統及網路安全整體防護環境。

5.2.2.3 彙整資安文件

資訊安全相關文件應齊備，以利資訊安全事件發生時可參考使用。

5.2.3 事中主動監控、緊急應變

5.2.3.1 主動監控

利用系統、人員執行主動監控作業。

5.2.3.2 事件辨識

其目的為辨識事件之歸屬及採取之對策，辨識屬內部危安事件、外力入侵事件、天然災害或重大突發事件，並決定處理的方法與程序。

5.2.3.3 事件控制

依據各類事件進行事件傷害控制，降低影響的程度及範圍。

5.2.3.4 問題解決

事件處理權責單位或負責人須將問題徹底解決。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等。

5.2.3.5 保全證據、紀錄與蒐證

處理資安事件過程，需保留相關紀錄與證據，包含資安事件發生時的系統狀態、網路流向與帳號存取紀錄等，以便進行事後鑑識作業。

5.2.3.6 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。

5.2.4 事後復原追蹤鑑識偵查

5.2.4.1 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，藉由研析相關資料以釐清事件發生的原因與責任歸屬。

5.2.4.2 受損單位依復原程序實施災後復原重建。

5.2.4.3 重大資安事件應保留事件發生之線索(如記錄等)，如有需要得向「國家資通安全會報技術服務中心」或檢警單位申請數位鑑識（電腦、網路鑑識）。

5.2.4.4 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-F-33 資訊安全事件報告單」，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。

5.3 資訊安全事件懲處

資安事件若由本校教職員生不當行為造成，得依照教育部頒訂之「台灣學術網路管理規範」、「元智大學網路使用管理辦法」、「ISMS-F-11 刑法關於電腦犯罪部份條文」等相關規定辦理。

5.4 資訊安全目標管理

依據「ISMS-P-01 資訊安全政策」以保護資訊資產之機密性、完整性、可用性、適法性為目標。

5.5 威脅情資

每季整合區網中心資安通報、台灣學術網路危機處理中心通報、國家資通安全研究院安全技術報告，並分享給組織人員。

6 相關文件

6.1 行政院及所屬各機關資訊安全管理要點、管理規範。

6.2 台灣學術網路管理規範。

6.3 資通安全事件通報及應變辦法。

6.4 元智大學網路使用管理辦法。

6.5 元智大學個人資料檔案安全維護計畫。

6.6 ISMS-P-01 資訊安全政策。

6.7 ISMS-P-21 業務持續營運管理程序書。

6.8 ISMS-P-17 資訊設備與媒體管理作業辦法。

6.9 ISMS-F-11 刑法關於電腦犯罪部份條文。

6.10 ISMS-F-33 資訊安全事件報告單。

6.11 ISMS-F-34 資安事件通報紀錄表。

附錄A

資訊安全等級區分，依據「資通安全事件通報及應變辦法」辦理，安全事件等級概分為四級：

『1』級事件，符合下列任一情形者，屬 1 級事件：

- 非核心業務資料遭洩漏。
- 非核心業務系統或資料遭竄改。
- 非核心業務運作遭影響或短暫停頓。

『2』級，符合下列任一情形者，屬 2 級事件：

- 非屬機密級或敏感之核心業務資料遭洩漏。
- 核心業務系統或資料遭輕微竄改。
- 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。

『3』級，符合下列任一情形者，屬 3 級事件：

- 機密級或敏感公務資料遭洩漏。
- 核心業務系統或資料遭嚴重竄改。
- 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。

『4』級，符合下列任一情形者，屬 4 級事件：

- 國家機密資料遭洩漏。
- 國家重要資訊基礎建設系統或資料遭竄改。
- 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。