國立高雄餐旅大學

NATIONAL KAOHSIUNG UNIVERSITY
OF HOSPITALITY AND TOURISM

「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-02-011**

版本編號：2.1

修定日期：113.09.12

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	100.04.01	資訊安全執行小組	初稿修訂	圖資館 副館長
1.0	100.07.26	資訊安全執行小組	首次發行	圖資館 副館長
1.2	101.08.27	資訊安全執行小組	新增 5.2.5	圖資館 副館長
1.3	108.08.14	資訊安全執行小組	新增 4.6、修訂 5.2、5.3	圖資處 圖資長
2.0	112.06.27	資訊安全執行小組	依據 112 年教育部稽核待改善事項新增 4.9、5.5-5.10，修訂 5.2-5.4，	資訊安全管理代表
2.1	113.09.12	資訊安全執行小組	新增 4.6	資訊安全管理代表

本程序書由資訊安全執行小組負責維護。

目錄：

1 目的

1.1 確保國立高雄餐旅大學（以下簡稱本校）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 本校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：審核本校「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 資訊安全小組：研擬資訊安全事件通報流程。

3.3 發現人員：所有人員（含：本校人員、約聘僱人員與委外駐點人員），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 資訊安全管理代表：督導資訊安全事件通報、處理及分析作業。

3.6 緊急處理組：

3.6.1 確定事件影響範圍，並評估損失。

3.6.2 協助資訊安全事件之通報、處理及分析作業。

3.7 支援單位：

3.7.1 內部單位：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 威脅情資

4.6.1 相同產業或其他組織受攻擊之攻擊手法、型式與細節。

4.6.2 組織內所採用相同系統或設備型號的攻擊資訊。

4.6.3 既有系統或既有設備之漏洞公告。

4.7 資訊安全事件等級區分為：

4.7.1 一級事件：

4.7.1.1 非核心業務資訊遭輕微洩漏。

4.7.1.2 非核心業務資訊或非核心資訊系統遭輕微竄改。

4.7.1.3 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，造成機關日常作業影響。

4.7.2 二級事件：

4.7.2.1 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。

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

4.7.2.3 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訊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。

4.7.3 三級事件：

4.7.3.1 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。

4.7.3.2 未涉及關鍵基礎設施維運之核心業務資訊或核心資訊系統遭嚴重竄改，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訊系統遭輕微竄改。

4.7.3.3 未涉及關鍵基礎設施維運之核心業務或核心資訊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訊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。

4.7.4 四級事件

4.7.4.1 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。

4.7.4.2 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訊系統遭嚴重竄改，或國家機密遭竄改。

4.7.4.3 涉及關鍵基礎設施維運之核心業務或核心資訊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。

4.8 一般事件：為一級或二級事件。

4.9 重大事件：為三級或四級事件。

4.10 資安預警事件：凡屬有待本校進行確認之資安事件皆屬於資安預警事件，說明如下：未確定事件或待確認事件單，來自各區教育學術資訊安全監控中心或縣市網資訊安全維運中心（X-SOC）使用之新型技術所產生之事件單，但正確性有待確認者。以及其他單位所告知教育部所屬單位所發生未確定之資安事件。

5 作業說明

5.1 威脅情資管理

5.1.1 情資蒐集

5.1.1.1 外部威脅情資蒐集來源為政府機關(如國家資通安全研究院)及供應商(如資安廠商、設備原廠)。

5.1.1.2 內部威脅情資蒐集來源為資安平台(SOC、SIEM、EDR、XDR…等)、設備警示、技術檢測結果、安全事件通報與日誌分析等資訊。

5.1.2 情資分析

5.1.2.1 應由資訊安全執行小組針對外部及內部威脅情資進行分析，評估其影響之範圍(如系統主機、網路設備或特定軟體等)。

5.1.3 情資處理

5.1.3.1 需至少每個月定期依情資分析結果建立「資訊安全情資管理表」，以研擬解決方案，如進行管理程序修正、技術脆弱性管理，並設定情資管理預訂完成時間及追蹤時間，持續追蹤至威脅情資處理完畢。

5.2 資訊安全事件之管理

5.2.1 應建立資訊安全事件之處理作業程序，並成立「資通安全事件應變與通報小組」，賦予相關人員必要責任，以便迅速有效處理資訊安全事件。

5.2.2 除正常應變計畫（如：系統及服務之回復作業），資訊安全事件之處理程序，應視需要納入下列事項：

5.2.2.1 導致資訊安全事件原因之分析。

5.2.2.2 防止類似事件再發生之補救措施。

5.2.2.3 電腦稽核軌跡及相關證據之蒐集。

5.2.2.4 與受影響之使用者進行溝通及說明。

5.2.3 電腦稽核軌跡及相關證據應以適當方法保護，以利下列管理作業：

5.2.3.1 作為研析問題之依據。

5.2.3.2 作為研析是否違反契約或資訊安全規定之證據。

5.2.3.3 作為與委外廠商協商如何補償之依據。

5.2.4 應依據「資訊安全事件通報與應變作業流程」處理資訊安全事件。相關作業程序應注意下列事項：

5.2.4.1 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。

5.2.4.2 向管理階層報告處理情形，並檢討、分析資訊安全事件。

5.2.4.3 限定僅授權之人員可使用回復後正常作業之系統及資料。

5.2.4.4 緊急處理步驟應詳實記載，以備日後查考。

5.3 內部通報程序

5.3.1 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，並副本告知直屬主管。本校權責單位為『圖書資訊處』，即「資通安全事件應變小組」，其聯絡資訊如下：

5.3.1.1 網址：https://lic.nkuht.edu.tw/

5.3.1.2 聯絡電話：電話為 07-8060505 分機 14203

5.3.1.3 電子郵件：nkuhtlic@live.nkuht.edu.tw

5.3.2 權責單位於收到通知後，應遵循本程序書附件「資訊安全事件通報與應變作業流程」進行後續通報與處理作業。

5.3.3 有關是否啟動營運持續運作計畫，依「營運持續運作管理程序書」辦理。

5.3.4 決策處理：

5.3.4.1 當事件影響較低、衝擊性較小，或僅涉及單位內部、受損程度輕微時（如：電腦病毒感染），由權責單位自行處理，並將處理後狀況通知單位主管及資訊安全管理代表。

5.3.4.2 處理過程中如發現造成之影響大於原先判定事件，權責單位應立即向資訊安全管理代表報告，重新執行事件分析辨識。

5.3.4.3 資訊安全管理代表應參考『臺灣學術網路各級學校資通安全通報應變作業程序』，並依據權責單位所提報之事件影響報告，決定是否進行外部通報作業。

5.4 外部通報作業：

5.4.1 資安事件需依據「臺灣學術網路各級學校資通安全通報應變作業程序」於 1 小時內完成對『教育機構資安通報平台』通報作業。

5.4.2 事件級別為一般事件需於 72 小時內完成損害控制或復原。

5.4.3 事件級別為重大事件需於 36 小時內完成損害控制或復原。

5.5 跡證保存

5.5.1 發生資訊安全事件時，本校應依下列原則進行跡證保存：

5.5.1.1 本校進行跡證保存時，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。

5.5.1.2 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。

5.5.1.3 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。

5.5.1.4 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。

5.5.2 簽訂資通系統或服務之委外契約時，應依第 5.2.1 及 5.2.2 規定於契約中定明紀錄保存及備份規定。

5.5.3 數位證據應以適當方法保護，以利下列管理作業：

5.5.3.1 作為研析問題及事件根因之依據。

5.5.3.2 作為研析是否違反契約或資訊安全規定之跡證。

5.5.3.3 作為與委外廠商協商如何補償之依據。

5.6 事件分析

5.6.1 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。

5.6.2 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。

5.6.3 分析結果應做成歷程紀錄，以結案時一併通報執行秘書。

5.6.4 重大資訊安全事件應保留事件發生之線索，如有需要得向檢警單位申請支援。

5.7 事件處理

5.7.1 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。

5.7.2 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。

5.7.3 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。

5.7.4 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。

5.7.5 限定僅授權之人員可使用回復後正常作業之系統及資料。

5.7.6 緊急處理步驟應詳實記載，以備日後查考。

5.7.7 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。

5.7.8 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。

5.8 結案

5.8.1 由資通安全事件應變小組進行外部通報結案。

5.8.2 與受影響之使用者進行溝通及說明。

5.8.3 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。

5.8.4 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：

5.8.4.1 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。

5.8.4.2 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。

5.8.4.3 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。

5.8.5 彙整相關文件並歸檔。

5.9 檢討改善

5.9.1 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。

5.9.2 檢討並改善處理步驟，進立處理標準程序，列入應變計畫。

5.9.3 向管理階層報告處理情形。

5.10 監督

5.10.1 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。

5.10.2 必要時，由資安長對外說明事件處理情形。

5.11 資通安全事件之學習

5.11.1 本校每年定期規劃辦理資安認知教育訓練，內容應包括本校曾發生之資安事件，以提升本校同仁資安意識，降低資安事件再發之可能性。

6 相關文件

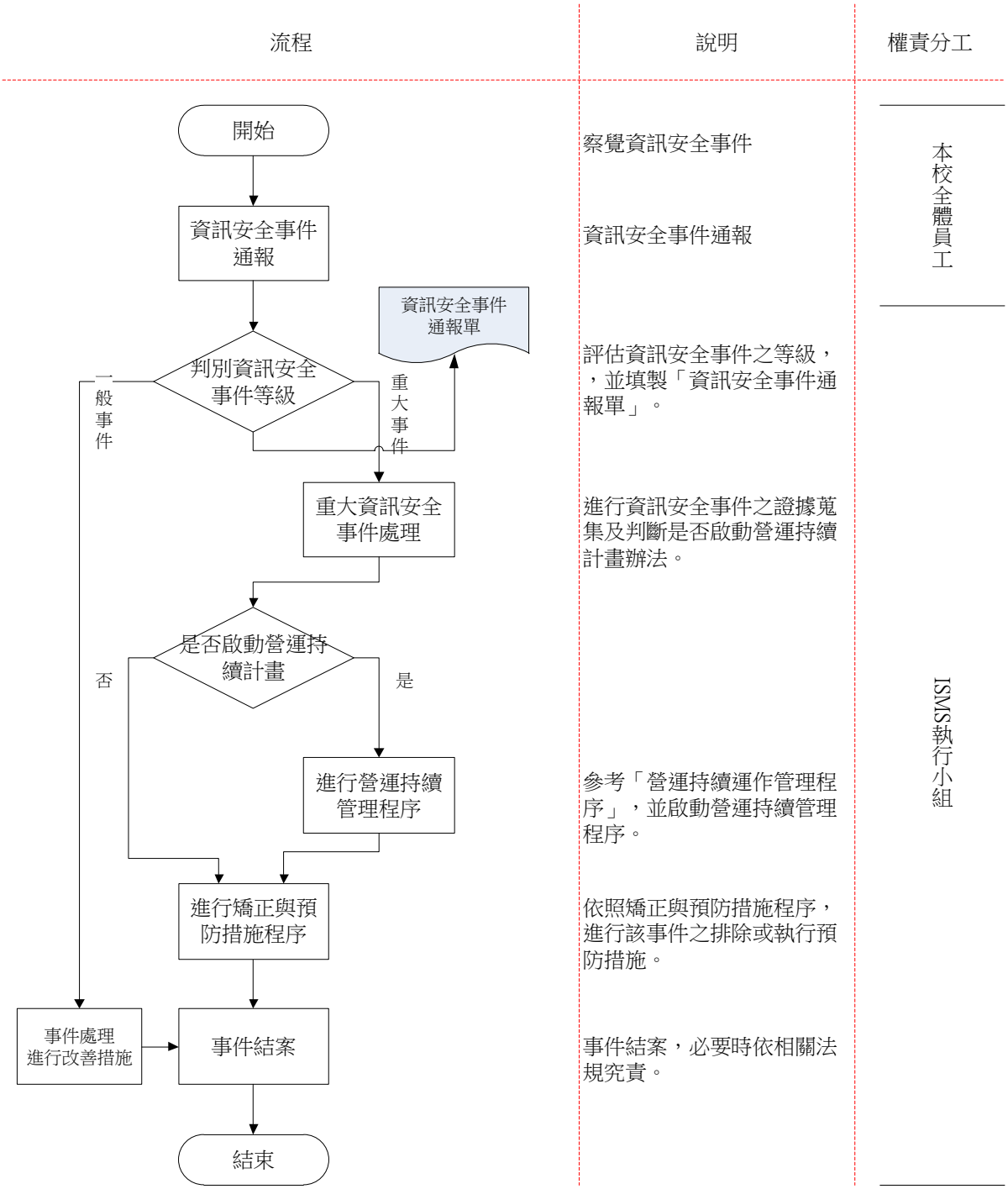
6.1 資訊安全事件通報與應變作業流程(附件)

6.2 資訊安全事件通報單

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 本校員工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 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」。

2.2.2 若為「一般事件」，直接進行改善作業後記錄並歸檔；若為「重大事件」，則依照下列重大資訊安全事件流程處理。

2.3 重大資訊安全事件處理：

2.3.1 證據蒐集：

2.3.1.1 當重大資訊安全事件發生時，若涉及行政或法律責任之追究，ISMS 執行小組應協助蒐集完整證據(如 Log、表單記錄、合約等)。

2.3.1.2 判斷是否啟動營運持續計畫作業指導書：

2.3.1.2.1 依照「營運持續運作管理程序書」內有關營運持續計畫作業指導書啟動條件，判斷是否啟動營運持續作業。

2.3.2 進行營運持續管理程序

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 進行矯正預防措施程序

2.3.3.1 依照「矯正預防措施管理程序書」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。