教育部國教署｜115年度
亞洲大學｜陳偉嵩

校園資通安全專責人員知能研習

資訊委外作業安全及事件應變通報

三大主題

01

資訊委外安全

從選商、評估到維運，將資安要求納入全生命週期流程。

02

資安事件通報

面對資安事件之處理，分級管理、精準通報

03

應變作業規範

資安事件發生後、即時控制、服務復原與持續改善。

第一章

資訊委外
不是責任外包

安全要求必須一路跟著服務走

核心觀念

把工作委外辦理，就沒事了？

受託關係仍須受選任、監督、查核與事件管理的完整治理循環，法律責任不可轉嫁。

法規依循

委外安全的制度基礎

資通安全管理法第9條

資通安全管理法施行細則第7條

資安法常見FAQ

政府資訊服務採購作業指引

共通性資通安全基本要求

資訊服務採購契約範本

REGULATORY COMPLIANCE FRAMEWORK

LIFECYCLE MEASURES

資通系統籌獲各階段資安強化措施

CYBERSECURITY COMPLIANCE FRAMEWORK

需求階段：

規格與評選強化

確認系統防護等級(普、中、高)

編列資安經費5%以上

受託者資安作業納入評選權重10%且評選委員須含至少

建置階段：

外部專家與第三方驗證

維運階段：

持續稽核與事件應對

一位資安專家

核心資通系統應聘請外部專家協助檢視資安管理

若核心系統委託金額達1,000萬元以上，應評估辦理獨立驗證與認證(IV&V)

對高防護等級系統辦理廠商稽核

發生重大資安事件時應立即辦理稽核並將結果送交主管機關

採購流程

從選商到驗收：每一步都要留下紀錄

選商

廠商資格審查
資通系統服務建議書
廠商資安能力評估表

驗收

文件交付、功能測試、使用授權、安全檢測報告。

採購控制點

評估與履約的關鍵文件

評估　　系統評估、防護基準、專案時程與RFP需求規格。

履約　　執行團隊、查核點、保密切結、SSDLC文件。

PROCUREMENT CONTROL POINTS

維運治理

服務上線後，管理才真正開始

- 系統維運紀錄
- 廠商權限審查
- 系統演練作業
- 資料備份管理
- 異常與事件管理

OPERATIONAL GOVERNANCE

公共電視案例

維護廠商誤刪數位新聞資料

受災數量

42萬

自2017年起建檔之數位新聞資料畫面遭到完全刪除。

約32萬筆可由IBM磁帶檔及影音網站取回，但仍有近8萬筆珍貴新聞畫面永久遺失。

問題不只在一個錯誤指令

權限

維護作業是否具備最小必要權限?

備份

備份是否獨立、可驗證、可復原?

監督

機關是否持續監督受託業務?

案例二

484臺電腦資料遭誤刪

非駭客入侵，亦屬資安事故

工程師因程式碼撰寫錯誤導致系統指令誤執行。雖然並非外部攻擊，但內部作業疏失對營運影響巨大，所幸已透過復原機制完成還原。

核心啟示

「人員作業疏失，也是一種資安風險」

01

程序管控

強化程式碼審核 (Code Review) 與自動化測試流程，避免單一錯誤直接影響正式環境。

02

教育訓練

定期辦理技術人員資安意識與標準作業規範培訓，落實雙重確認機制。

03

制度檢視

檢視權限派發制度，落實最小權限原則，限制高風險指令的執行範圍。

勞發署高分署澄清稿｜113-08-28

資料外洩，可能轉化為現實傷害

案例三

消防報案系統遭駭

40,000+

民眾報案個資外洩

高雄市消防局報案系統遭駭客入侵，導致三年期間內，超過 40,000 筆 敏感個資遭竊取。

遭盜用的資料包含民眾傷病紀錄與聯繫資訊，並已在非法網路論壇進行販售與流通。

PRESENTATION 2026

事件通報與應變

基本流程

從知悉到改善，形成閉環

01

事前防禦

訂定應變機制與標準作業程序(SOP)。

02

事中處置

依法規時限進行通報、採證與控制。

03

事後優化

根因分析、改善報告與定期演練。

事件分級

級別取決於三個維度

資訊性質

核心業務、敏感資訊、一般公務機密、國家機密。

CIA衝擊

機密性、完整性、可用性。

四 級 制 度

資通安全事件：由1級至4級

1

輕微事件

非核心資訊輕微洩漏或竄改，且可於容忍時間內恢復正常。

2

中度事件

非核心資訊嚴重影響，或核心業務資訊遭輕微影響。

3–4

重大事件

核心或國家機密資訊遭重大洩漏，關鍵系統無法及時恢復。

先辨識資料，再判斷事件

個人資料

姓名、身分證號、醫療、財務與其他可識別個人的資料。

一般公務機密

除國家機密外，依法令負有保密義務的資訊。

國家機密

為確保國家安全或利益，依法核定機密等級的資訊。

機密性、完整性、可用性

C

機密性

依外洩資訊的性質與程度，由機關認定輕微或嚴重。確保資訊僅供獲授權者存取。

I

完整性

評估資訊遭未經授權竄改、刪除或損害之程度。確保資料的準確性與完整無缺。

A

可用性

評估能否在可容忍中斷時間內恢復。確保獲授權者在需要時能即時存取資訊。

第一級與第二級

第一級

非核心業務資訊輕微洩漏或竄改；非核心業務受影響但可於可容忍時間內恢復。

第二級

非核心資訊嚴重洩漏或竄改；或核心業務輕微影響並可及時恢復。

事件定義

第三級與第四級

第三級

核心業務嚴重洩漏或竄改；核心服務受影響且無法於容忍時間恢復。

第四級

敏感資訊嚴重洩漏或竄改；國家機密遭洩漏；關鍵系統無法恢復。

完整通報應回答的關鍵問題

- 哪個機關發生事件?
- 何時發生或知悉?
- 狀況與影響範圍為何?
- 事件等級如何評估?
- 是否需要外部支援?
- 已採取哪些初步措施?

調查、處理及改善報告

時間軸	發生、知悉、損害控制與復原時間。
損害評估	影響範圍、損害程度與控制歷程。
根因改善	根因分析、改善措施、時程與追蹤機制。

時限規範

時間是應變的關鍵

知悉通報

1小時

知悉資安事件後，必須於60分鐘內完成向上通報作業。

上級審核

1、2級事件：8小時內完成。

3、4級事件：2小時內完成。

動態調整

事件等級不是永遠固定

調查過程若發現影響範圍擴大，應提出等級變更申請並說明原因。

1個月

調查、處理及改善報告原則上於1個月內提交；特殊情況可申請延後。

建立可執行的應變作業規範

通報規範

機關內部必須先有清楚的作業程序

判定等級

流程清楚，權責明確。

建立窗口

提供緊急聯繫方式。

通知受影響方

定義通知方式與對象。

五項制度化能力

- 應變小組組織與角色分工
- 事前演練作業
- 損害控制機制
- 事後復原與調查
- 事件紀錄保全

應變目標

處理事件的三個核心目標

01

降低中斷時間

最小化業務與網路服務影響。

02

精準提供資訊

在關鍵時刻提供及時且準確的資訊。

03

確保合規性

保障政策與法律要求的權利。

六大程序

資安事件處理的完整循環

01

準備

02

識別

03

封鎖

04

根除

05

復原

06

經驗學習

CYBERSECURITY INCIDENT RESPONSE FRAMEWORK

第一階段

準備：在事件發生前做好規畫

組織

建立跨部門應變小組。

程序

設計標準化處理步驟。

資源

備妥工具、人力、預算並反覆演練。

CSIRT

黃金陣容：跨領域協作

技術部門	IT、資安與系統管理者。
法務部門	合規、證據保全與訴訟。
公關與人資	內外溝通、聲譽與人員議題。

第二階段

識別：先確認，再採證

可疑跡象

不明帳號或檔案、IDS警報、異常防火牆紀錄、服務不穩定。

證據取得

建立完整映像、記錄採證過程，維持Chain of Custody。

第三階段

封鎖：阻止損害擴大

1. 識別可信任來源與合法使用者。
2. 避免驚動入侵者，保護證據。
3. 在安全環境中開始證據分析。
4. 變更權限、阻擋惡意IP、關閉非必要服務。

第四階段

根除：清除威脅，也修補防線

決定移除或回存

評估惡意程式能否完全清除，並確認備份資料乾淨。

強化防禦機制

增加偵測與防禦措施，提升稽核紀錄並掃描其他系統。

復原：恢復服務，啟動新監控週期

安全、有序地將業務與服務恢復正常運作。

執行重點

針對本次攻擊手法建立客製化入侵偵測規則。

在網路、主機及應用程式層級強化日誌記錄。

第六階段

經驗學習：把事件變成能力

「那些不能記取歷史教訓的人，注定要重蹈覆轍。」

召開事後檢討會議，彙整技術與管理漏洞，轉化為政策修訂與防禦增強的依據。

證據必須可信，也必須可追溯

資料來源
檔案、日誌、網路傳輸記錄。

偵查用途
確認或否定犯罪行為的推斷。

法庭價值
支持或反駁法律主張。

數位鑑識四大程序，守住證據完整性

01

證物查封

安全地扣押並保護證據來源，嚴格防止任何形式的物理接觸或數位竄改，確保原始狀態不受破壞。

02

證據取得

使用鑑識級工具建立原始資料的完整位元流映像 (Bit-stream Image)，確保副本與原始媒介的內容完全一致。

03

證據分析

深入掃描檔案系統，搜尋並提取關鍵資訊、隱藏檔案與數位跡證，以還原事件的真實經過。

04

報告撰寫

詳實記錄鑑識過程、所用工具與分析結果，將關鍵發現彙整為具備法律效力的正式鑑定報告。

核心原則
CORE PRINCIPLES

數位鑑識核心原則：維護證據法律效力

01

完整性原則 (Integrity)

在鑑識過程中，嚴禁對原始儲存媒介進行任何寫入或修改，確保數位證據維持其原始狀態。

02

監管鏈原則 (Chain of Custody)

詳實記錄證物從發現、扣押至分析的每一步流程與經手人，確保证據的連續性與不可竄改性。

03

可重現性原則 (Repeatability)

鑑識過程必須標準化，使第三方在相同條件下能重複執行操作並獲得一致的分析結果。

總結

委外不委責，管理是核心；即時應變通報為上策