德明財經科技大學

資訊安全事件通報管理規定

機密等級：一般

文件編號：Takming-ISMS-B-011

版　次：V 1.2

初版日期：107.12.25

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	107.12.25	N/A	執行小組	初版
1.1	109.02.07	3	執行小組	5.2.3 刪除”2 級以上(含)”
1.1	109.02.07	3	執行小組	5.2.4 刪除”2 級以上(含)”
1.1	109.02.07	3	執行小組	資訊安全等級區分參考從“行政院國家資通安全通報應變作業綱要”改成”臺灣學術網路各級學校資通安全通報應變作業程序”
1.1	109.02.07	4，5	執行小組	事件等級內容修改
1.1	109.02.07	5	執行小組	將”國家資通安全會報通報與應變作業流程”改成”臺灣學術網路各級學校資通安全通報應變作業程序”
1.2	112.01.04	5	執行小組	刪除”參考「行政院及所屬各機關資訊安全管理要點、管理規範」”

1. 目的

確保德明財經科技大學(以下簡稱本校)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. 適用範圍

本校作業環境中之資通安全事件均適用之。

3. 名詞定義

3.1. 資通安全事件

是指系統、服務或網路發生一個已識別的狀態，其指示可能的資通安全正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。

3.2. 資通安全事故

單一或一連串有顯著機率可能危害營運作業與威脅資通安全之非所欲或非預期的資通安全事件。

3.3. 資通安全事件分類

3.3.1. 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。

3.3.2. 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。

3.3.3. 天然災害或突發事件

3.3.3.1. 天然災害：颱風、水災、地震等。

3.3.3.2. 突發事件：火災、爆炸、核子事故、重大建築災害等。

3.3.3.3. 網路系統骨幹(主幹寬頻)中斷事件等。

3.4. 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)、國家資通安全科技中心、台灣電腦網路危機處理暨協調中心(TWCERT/CC)、台北區域網路中心、教育部資訊科技司等。

4. 權責

4.1. 事件發現人員

發現疑似資通安全異常事件時，皆負有即時通報之責任。

4.2. 通報窗口

指資通安全事件處理之通報窗口，須執行資通安全事件之分析及處理。

4.3. 資通安全推動小組召集人

督導資通安全事件分析、處理及通報等。

4.4. 緊急事件應變小組

4.4.1. 確定事件影響範圍並作損失評估。

4.4.2. 執行危機處理程序作業包含資通安全事件分析、處理及通報等。

4.5. 內部單位

協助處理相關法律、人事獎懲及採購等問題。

4.6. 外部單位

協助資訊提供、資通安全事件處理等。

5. 要求事項

5.1. 資通安全事件管理責任及程序

5.1.1. 建立不同的程序以處置不同型式的資通安全事故，包括：

5.1.1.1. 資通系統失效與服務的減損。

5.1.1.2. 惡意碼。

5.1.1.3. 阻絕服務。

5.1.1.4. 不完全或不準確的營運資料所產生的錯誤。

5.1.1.5. 機密性和完整性的損壞。

5.1.1.6. 資通系統的誤用。

5.1.2. 資通安全事件及事故處理相關責任

5.1.2.1. 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校人員)，發現疑似資通安全異常事件時，皆負有即時通報之責任。

5.1.2.2. 通報窗口

資通安全事件或事故處理之通報窗口，執行資通安全事件或事故之分析及處理。

5.1.2.3. 資通安全推動小組召集人

督導資通安全事件或事故分析、處理及通報。

5.1.2.4. 資通安全推動小組

5.1.2.4.1. 訂定系統安全等級。

5.1.2.4.2. 蒐集資通安全資訊。

5.1.2.4.3. 建置資通安全措施。

5.1.2.4.4. 培訓資通安全技術。

5.1.2.5. 緊急事件應變小組

5.1.2.5.1. 執行組織資通安全事件或事故之處理。

5.1.2.5.2. 確定影響範圍並作損失評估。

5.1.2.5.3. 執行解決辦法。

5.1.2.5.4. 規劃危機處理程序。

5.1.2.5.5. 執行資通安全監控。

5.1.3. 保持與特殊利害相關團體的聯繫

5.1.3.1. 組織為有效落實資通安全管理制度、獲取資通安全技術及產品資訊與知識；處理資通安全事件或執行系統

修補資訊等，應隨時與相關團體維持聯繫。

5.1.3.2. 將資訊建立於「外部單位聯絡清單」。

5.2. 通報資通安全事件

5.2.1. 所有人員發現有資通安全可疑事件時，依「資通安全事件通報流程」向通報窗口進行資通安全事件通報。

5.2.2. 通報窗口於收到通知後需研判是否為資通安全事件，若判定為非資安事件時，將結果回覆事件發現人員。

5.2.3. 若判定為資安事件時，由通報窗口初估事件須處理時間並通知「緊急事件應變小組」，由「緊急事件應變小組」判定是否為重大資安事件，並填寫「資通安全事件報告單」。

5.2.4.「緊急事件應變小組」於處理 2 級以上(含)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，立即填具「資通安全事件報告單」。

5.2.5. 資通安全等級區分，參考「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，由重至輕分別為「4 級」、「3 級」、「2 級」及「1 級」，另新增資安預警事件類別。

5.2.5.1.「4 級」事件，符合下列任一情形者：

5.2.5.1.1. 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。

5.2.5.1.2. 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通系統遭嚴重竄改，或國家機密遭竄改。

5.2.5.1.3. 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。

5.2.5.2.「3 級」事件，符合下列任一情形者：

5.2.5.2.1. 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。

5.2.5.2.2. 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。

5.2.5.2.3. 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。

5.2.5.3.「2 級」事件，符合下列任一情形者：

5.2.5.3.1. 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。

5.2.5.3.2. 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

5.2.5.3.3. 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

5.2.5.4.「1 級」事件，符合下列任一情形者：

5.2.5.4.1. 非核心業務資訊遭輕微洩漏。

5.2.5.4.2. 非核心業務資訊或非核心資通系統遭輕微竄改。

5.2.5.4.3. 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。

5.2.5.5. 資安預警事件：凡屬有待受害單位進行確認之資安事件皆屬於資安預警事件，說明如下：

5.2.5.5.1. 未確定事件或待確認事件單：來自北區教育學術安全監控中心(N-ASOC)、南區教育學術資訊安全監控中心(S-ASOC)、縣市網資訊安全維運中心(MINI-SOC)使用之新型技術所產生之事件單，但正確性有待確認者。

5.2.5.5.2. 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。

5.2.5.6. 其他：非屬以上事件，事件發生不影響業務進行，可立即修復。

5.3. 通報安全弱點

5.3.1. 系統使用者發現系統有不正常之情形，應立即透過報修管道通知系統負責人進行問題處理，依據「資訊應用系統安全管理規定」以記錄問題發生的原因及排除的狀況。

5.3.2. 弱點管理依據「網路安全管理規定」辦理。

5.4. 資通安全事件評估與決策處理原則

5.4.1. 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「緊急事件應變小組」處理。

5.4.2. 處理過程中如發現造成之影響大於原先判定事件，「緊急事件應變小組」應立即向「資通安全推動小組」召集人報告，重新執行事件分析辨識。

5.4.3. 「資通安全推動小組」召集人得依據「緊急事件應變小組」所提報之事件影響，向資安長進行報告，並由資安長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」進行事件等級分類並通報。

5.4.4. 處理資安事件時，若需其他資源，則由「資通安全推動小組」負責溝通協調作業，並適時提供各單位必要的協助。

5.4.5. 有關是否啟動業務持續計畫，依據「資訊安全營運持續管理規定」辦理。

5.4.6. 有關本校資訊設備發生異常則依「資訊資產管理規定」，進行通報與維修。

5.4.7. 當重大資安事件發生需對外說明時，「資通安全推動小組」召集人須協助對外說明情況與處置方式，並向上級主管機關陳報。

5.4.8. 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「緊急事件應變小組」即時通知相關單位請求處理。

5.4.9. 若非本校能力處理之資通安全事件應適時尋求外部單位協力處理。

5.5. 資通安全事件危機處理程序

5.5.1. 事前建置安全防護機制

5.5.1.1. 建置資通安全系統(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。

5.5.1.2. 規劃建置資安系統及網路安全整體防護環境。

5.5.1.3. 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。

5.5.2. 事中主動監控、緊急應變機制

5.5.2.1. 利用系統、人員執行主動監控作業。

5.5.2.2. 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，並評估決定處理的方法與程序。

5.5.2.3. 依據各類事件進行事件傷害控制，降低影響的程度及範圍。

5.5.2.4. 緊急事件應變小組須將問題徹底解決。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。

5.5.2.5. 問題解決後，將系統恢復至事件發生前的正常運作狀態。

5.5.3. 事後復原追蹤鑑識偵查

5.5.3.1. 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，藉由研析相關資料以釐清事件發生的原因與責任。

5.5.3.2. 受損單位依復原程序實施資安事故後之復原重建。

5.5.3.3. 重大資安事件應保留事件發生之線索，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)。

5.5.3.4. 為有效追蹤，檢討事件原因，應審視現有環境的漏洞，由緊急事件應變小組於「資通安全事件報告單」，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。

5.6. 從資通安全事故中學習

5.6.1. 組織應由資通安全事故所得的資訊，識別其重複發生或其影響程度，利用會議、內部網站或電子郵件等方式，對組織內員工加強宣導，避免事故重覆發生。

5.6.2. 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「台灣學術網路使用規範」、「德明財經科技大學校園網路使用規定」等相關規定辦理。

5.7. 證據的收集

5.7.1. 為預防資安事故發生後，若需做為民事或刑事訴訟事件的相關鑑識證據，例如：遵照電腦誤用或資料保護法。組織應將事故發生過程中的相關紀錄或資料保存。

5.7.2. 資安事件發生後，組織內為了處置懲處行動之目的而收集和呈現證據時，證據收集法則應涵蓋：

5.7.2.1. 證據的可採用性：此項證據是否可以在法庭上使用。

5.7.2.2. 證據的證據力(weight)：證據的品質與完全性。為達到證據的可採用性，組織宜確保其資訊系統遵循可採用證據產生方法的相關已公告標準或作業規範。

5.7.3. 組織可根據以下條件建立有力的證據存底：

5.7.3.1. 紙本文件：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要妥為保管，任何調查都宜確

保原始文件未遭竄改。

5.7.3.2. 關於電腦媒體上的資訊：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(若不可能，至少一份鏡像或複本)，並使其不被變動。

5.7.4. 資通安全事件證據資訊的保護

5.7.4.1. 所有鑑識工作只宜在證據資訊的複本上執行。

5.7.4.2. 應保護所有證據材料的完整性。

5.7.4.3. 證據資訊的複製宜由值得信賴的人員監督，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應予以存錄。

6. 參考文件

6.1. 資通安全事件通報流程。

6.2. 行政院及所屬各機關資訊安全管理要點、管理規範。

6.3. 台灣學術網路使用規範。

6.4. 德明財經科技大學校園網路使用規定。

6.5. 資訊安全政策。

6.6. 資訊安全營運持續管理規定。

6.7. 資訊應用系統安全管理規定。

6.8. 網路安全管理規定。

6.9. 資訊安全事件報告單。

6.10.外部單位聯絡清單。

6.11. 資訊資產管理規定。

6.12.資通安全事件通報及應變辦法。