教育部資通安全處理小組

作業說明

教育部電算中心

中華民國 101 年 10 月 16 日

壹、依據

一.依據中華民 90 年 1 月 17 日行政院第 2718 次院會通過「建立我國通資訊基礎建設安全機制計畫」。

二.依據中華民 92 年 1 月 28 日國家資通安全會報第七次工作小組會議決議執行資通安全第二階段推動方案。

三、依據中華民國 101 年 8 月 1 日行政院院臺護字第 1010138057A 號函「國家資通安全通報應變作業綱要」。

貳、前言

隨著網際網路之普及應用，如何建立安全及可信賴的資訊安全作業環境，有效防範電腦及網路犯罪，確保業務順利運作，已成為刻不容緩之重點工作，為使本部及教育體系各級機關學校資訊安全作業處理與通報機制順暢，訂定本要點。

參、目的

一.協助解決本部及教育體系各級機關學校所遭遇的資訊安全問題，確保安全及可信賴的作業環境，以保護資料、系統、設備及網路的安全。

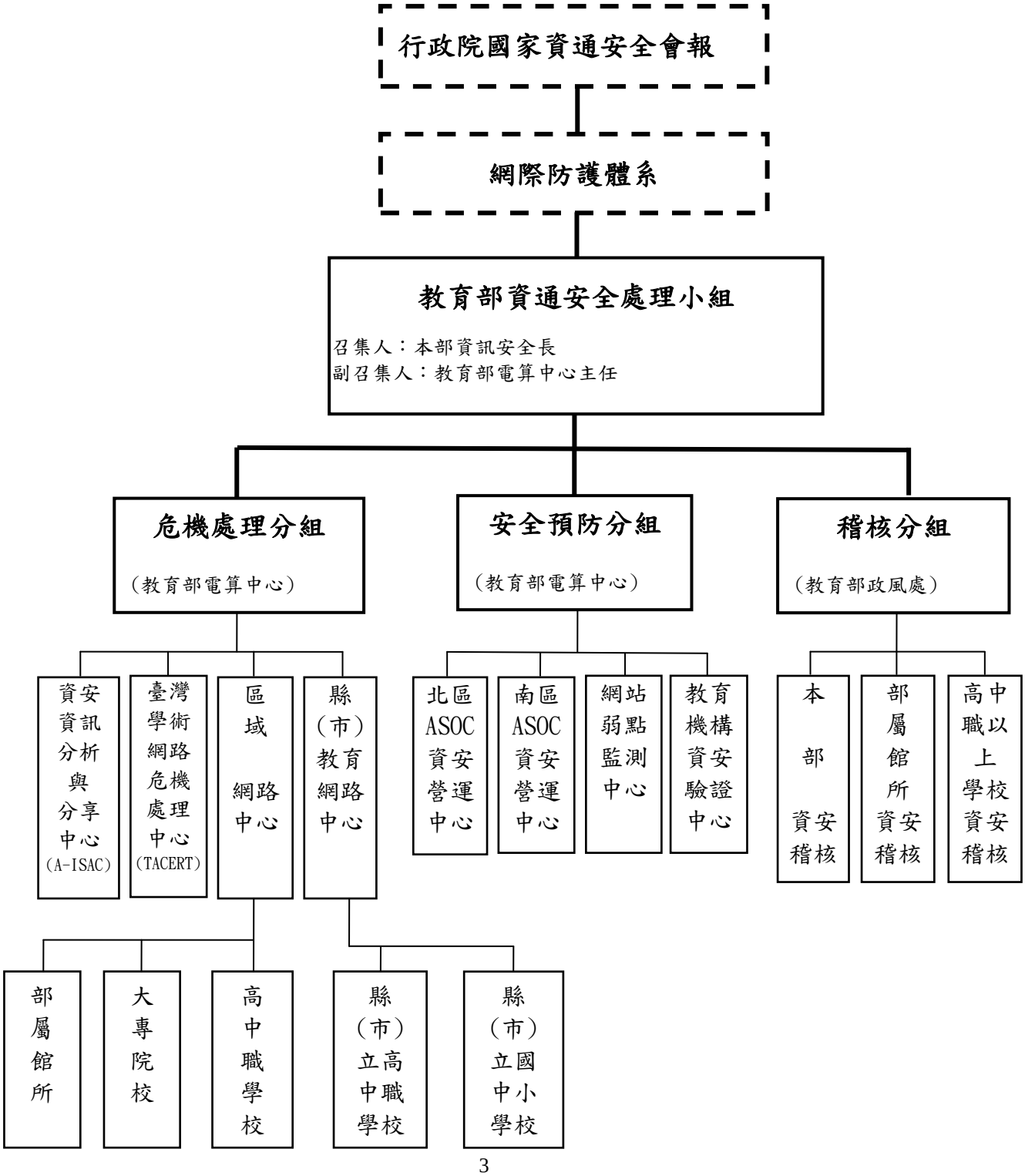
二.協助本部及教育體系各級機關學校資訊安全事件之通報與處置事宜。

三.落實本部及教育體系各級機關學校資訊安全管理制度。

肆、組織架構及職掌

一.本部為行政院國家資通安全會報網際防護體系之學術機構分組，本部

主責學校及研究機構，特訂定教育部「資通安全處理小組」組織,本小組設召集人一人(由本部資訊安全長擔任）、副召集人一人(由本部電算中心主任擔任),下設危機處理分組、安全預防分組與稽核分組相關組織架構如下圖：



二. 各分組職掌

各分組依業務需要，分別研訂相關職掌如下：

1. 危機處理分組: 負責規劃危機處理程序, 查明危機事件原因, 確定影響範圍, 執行應變措施, 辦理危機通報, 執行解決辦法等事項.

2. 安全預防分組: 負責搜集資通安全資訊, 培訓資通安全技術, 訂定系統安全等級, 建置資通安全措施, 執行資通安全監控等事項.

3. 稽核分組: 由本部政風室邀請專家學者擔任稽核委員, 主要負責「資通安全處理小組」實施稽核作業.

伍、教育體系機關(構)學校之資訊安全責任等級分級

一、依據行政院國家資通安全會報「資訊安全責任等級分級作業施行計畫」, 各類資安系統等級應執行之工作事項如下：

作業名稱 / 等級	防護縱深	ISMS 推動作業(註一)	稽核方式	資安教育訓練(一般主管、資訊人員、資安人員、一般使用者(註二))	專業證照	檢測機關網站安全弱點
A 級	NSOC 直接防護/SOC 自建或委外、IDS、防火牆、防毒、郵件過濾裝置	通過第三者驗証	每年至少 2 次內稽	1. 每年至少(3、6、18、3 小時) 2. 資訊人員、資安人員需通過資安職能鑑定	維持至少 2 張資安專業證照	每年 2 次
B 級	SOC(選項)、IDS、防火牆、防毒、郵件過濾裝置	通過第三者驗証	每年至少 1 次內稽	1. 每年至少(3、6、16、3 小時) 2. 資訊人員、資安人員需通過資安職能鑑定	維持至少 1 張資安專業證照	每年 1 次
C 級	防火牆、防毒、郵件過濾裝置	自行成立推動小組規劃作業	自我檢視	每年至少(2、6、12、3 小時)	資安專業訓練	每年 1 次

D 級	防火牆、防毒、郵件過濾裝置	推動 ISMS 觀念宣導	自我檢視	每年至少(1、4、8、2 小時)	資安專業訓練	每年 1 次

註一：驗證範圍應涵蓋機關（構）之核心業務資訊系統，並逐步擴大至全單位。

註二：

1、一般主管：擔任主管職務相關人員，如機關(副)首長、部門主管(含資訊主管)等。

2、資訊人員：負責資訊作業相關人員，如系統分析設計人員、系統設計人員、系統管理人員及系統操作人員等。

3、資安人員：負責資通安全業務相關人員，如資安管理人員、資安稽核人員等。

4、一般使用者：一般業務、行政、會計、總務人員等單位內資訊系統的使用者。

二、本部所屬機關(構)學校資訊安全依行政院資通安全會報劃分資訊安全責任分級為 A,B,C,D 四種等級

類別	內　　容
A 級 重要核心	・教育政策主管機關（教育部） ・教學醫院（台大醫院、成大醫院）
B 級 核心	・6 所入學考試常設機構 .117 所大學 ・13 個 TANet 區網中心 ・22 個縣(市)教育網路中心 .陽明大學附設醫院 .資安重點館所(國家教育研究院、國家圖書館、國立臺中圖書館)
C 級 重要	・30 所技術學院及 14 所專科學校 ・11 個部屬館所
D 級 一般	・491 所公私立高中、職學校 ・3,398 所國中小學

註：承辦全國性入學考試業務學校、機關(構)比照 B 級單位

陸、分組之任務及負責單位

一、危機處理分組：(負責單位：教育部電算中心)

1.辦理資通安全通報

(2)確認危機事件影響範圍與損失評估:與資訊安全事件通報單位合作評估相關影響程度。

(3)執行緊急應變措施:依資訊安全事件發生等級採行相關應變措施。

(4)查明危機事件原因:分析資訊安全事件成因以為未來防範。

(5)執行解決辦法:提供解決資訊安全事件之必要支援。

二、安全預防分組：(負責單位：教育部電算中心)

(1)蒐集資通安全資訊: 負責蒐集彙整資通安全相關資訊。

(2)培訓資通安全人才:辦理各級資訊安全教育訓練與觀念宣導。

(3)建置資通安全措施:協助各單位資訊安全軟硬體之建置。

(4)執行資訊系統監控:對於各重要系統監視與掌控,以維持正常運作。

三、稽核分組：(負責單位：教育部政風處)

(1) 落實學術機構分組 A、B 級機關學校導入資訊安全管理制度，並取得第三方外部稽核認驗證通過。

(2) 協助學術機構分組 C、D 級機關學校導入資訊安全管理制度，並不定期辦理資訊安全稽核作業。

柒.資安事件影響等級及資安通報應變處理流程

一、資安事件影響等級

資安事件影響等級分為4個級別,由重至輕分別為「4級」、「3級」、「2級」及「1級」。

(一)4級事件

符合下列任一情形者，屬4級事件：

1. 國家機密資料遭洩漏。

2. 國家重要資訊基礎建設系統或資料遭竄改。

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。

(二)3級事件

符合下列任一情形者，屬3級事件：

1. 密級或敏感公務資料遭洩漏。

2. 核心業務系統或資料遭嚴重竄改。

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。

(三)2級事件

符合下列任一情形者，屬2級事件：

1. 非屬密級或敏感之核心業務資料遭洩漏。

2. 核心業務系統或資料遭輕微竄改。

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。

(四)1 級事件

符合下列任一情形者，屬 1 級事件：

1. 非核心業務資料遭洩漏。

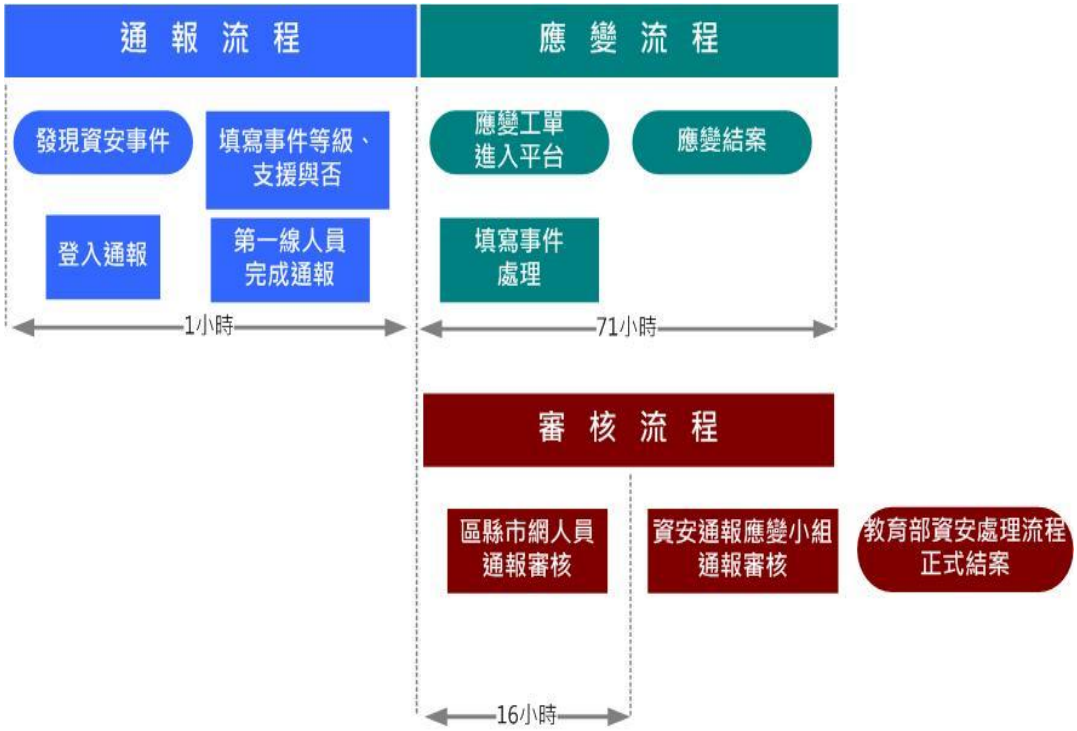
2. 非核心業務系統或資料遭竄改。

3. 非核心業務運作遭影響或短暫停頓。

二、本部及教育體系各級機關學校資訊安全通報應變程序如下

教育體系各級機關學校通報應變流程規劃為三層架構，架構圖如下所示:

(1) 教育體系各級機關學校發現1、2級資安事件時，應於1小時內登入「教育機構通報平台」進行通報。



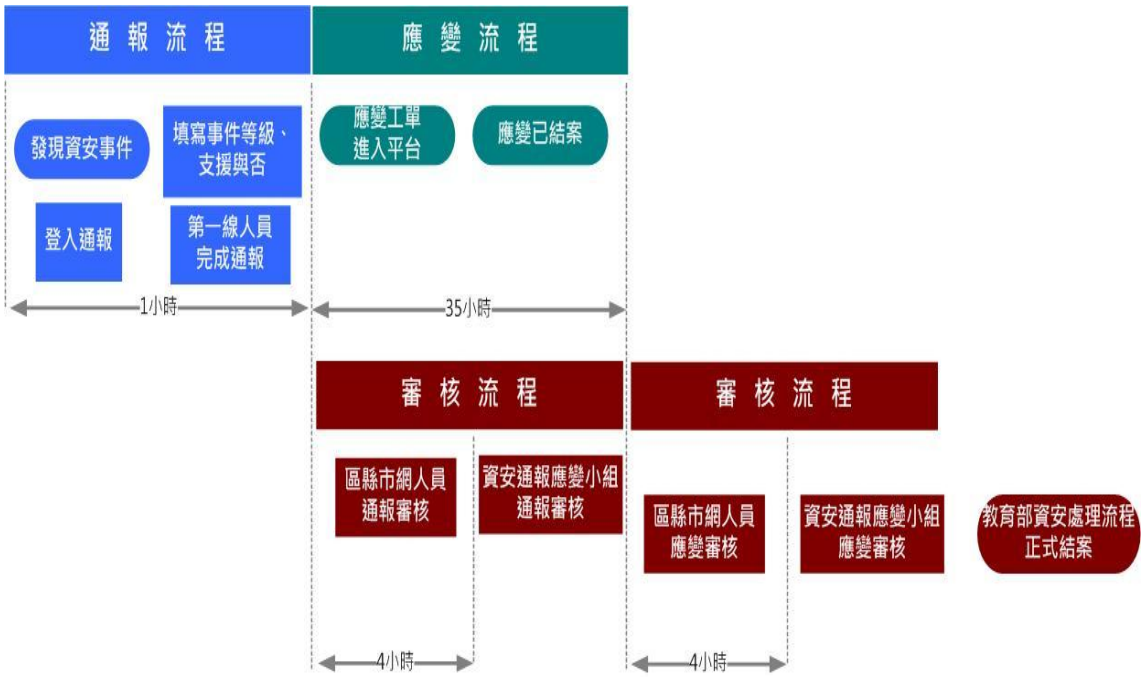
網址：https://info.cert.tanet.edu.tw

TACERT(臺灣學術網路危機處理中心)

服務電話：(07)525-0211

E-mail：service@cert.tanet.edu.tw

(2) 教育體系各級機關學校發現重大3、4級資安事件時，應於1小時內登入「教育機構通報平台」進行通報，並向教育部電算中心通報。



網址：https://info.cert.tanet.edu.tw

教育部資通安全處理小組

服務電話：(02)7712-9008

(3) 教育部本部各單位發現資安事件時(包含1、2、3、4級)，應於1小時內向教育部電算中心通報。

教育部資通安全處理小組

服務電話：(02)7712-9008

(4) 本部及教育體系各級機關學校如遇資訊安全事件涉及民、刑事責任者，除依通報程序進行通報外，應請求檢調單位協助處理。