教育體系因應資安管理法之策略作為

教育部資訊及科技教育司

王東琪科長

簡報大綱

- 資通安全管理法
- 資通安全責任等級
- 資通安全維護計畫
- 資通安全通報及應變

資通安全管理法

資通安全管理法

- 總統107年6月6日公布**資通安全管理法**。
- 行政院107年11月21日發布相關子法：
  - 資通安全管理法施行細則
  - **資通安全責任等級分級辦法**
  - **資通安全事件通報及應變辦法**
  - 特定非公務機關資通安全維護計畫實施情形稽核辦法
  - 資通安全情資分享辦法
  - 公務機關所屬人員資通安全事項獎懲辦法
- 行政院107年12月05日函定自**108年1月1日施行**。

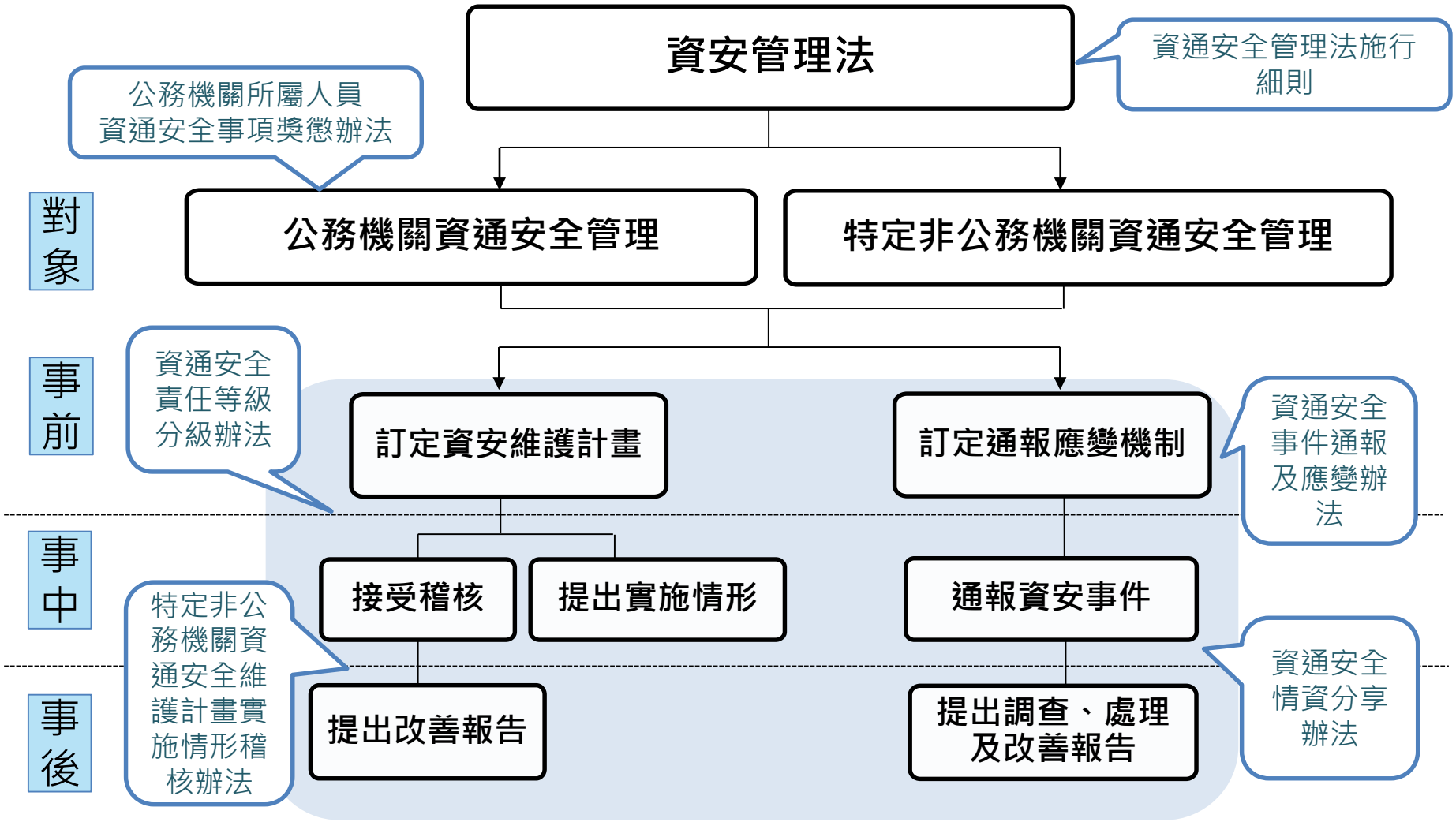
資通安全相關行政規則

- 政府機關（構）資通安全責任等級分級作業規定
  - 行政院104年1月20日院臺護字第1040121116號函修正發布
- 教育部與所屬機關(構)及學校資通安全責任等級分級作業規定
  - 教育部104年7月13日臺教資(四)字第1040059997號函發布
- 資訊系統分級與資安防護基準作業規定
  - 行政院104年7月31日院臺護字第1040141147號函
- 國家資通安全通報應變作業綱要
  - 行政院105年8月24日院臺護字第1050173756號函修正發布

資通安全相關行政規則

- ~~政府機關（構）資通安全責任等級分級作業規定~~
  - 行政院108年3月5日院臺護字第1080166960號函停止適用
- **教育體系資通安全責任等級分級作業規定(草案)**
- ~~資訊系統分級與資安防護基準作業規定~~
  - 行政院108年3月5日院臺護字第1080166960號函停止適用
- ~~國家資通安全通報應變作業綱要~~
  - 行政院108年3月5日院臺護字第1080166960號函停止適用
- **臺灣學術網路各級學校資通安全通報應變作業程序**
  - 教育部108年5月2日臺教資(四)字第1080063494號函訂定

資通安全管理法架構


資安管理法
資通安全管理法施行細則
公務機關所屬人員資通安全事項獎懲辦法
對象
公務機關資通安全管理
特定非公務機關資通安全管理
事前
資通安全責任等級分級辦法
訂定資安維護計畫
訂定通報應變機制
資通安全事件通報及應變辦法
事中
接受稽核
提出實施情形
通報資安事件
特定非公務機關資通安全維護計畫實施情形稽核辦法
事後
提出改善報告
提出調查、處理及改善報告
資通安全情資分享辦法

立法目的與規範對象

- 立法目的
  - 為積極推動國家資通安全政策，加速建構國家資通安全環境，以保障國家安全，維護社會公共利益。
- 規範對象

公務機關

- 依法行使公權力之中央、地方機關(構)
- 公法人

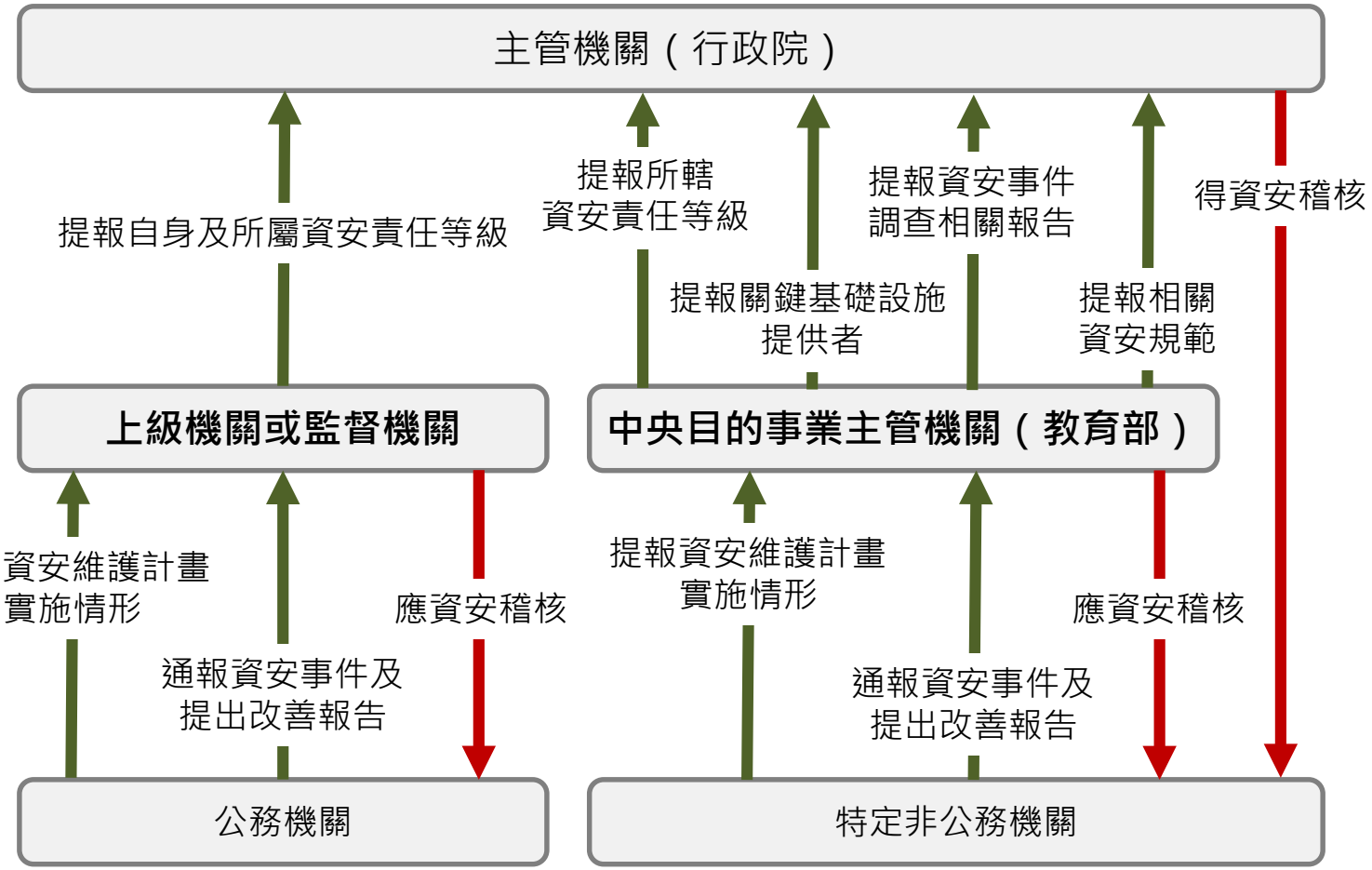
特定非公務機關

- 關鍵基礎設施提供者
- 公營事業
- 政府捐助之財團法人

教育體系規範對象

- 公務機關
  - 教育部及所屬機關(構)
  - 國家運動訓練中心
  - 各級公立學校及其附設機構(農林場、醫院等)
- 特定非公務機關
  - 財團法人大學入學考試中心基金會
  - 財團法人高等教育評鑑中心基金會
  - 財團法人社教文化基金會

角色與權責



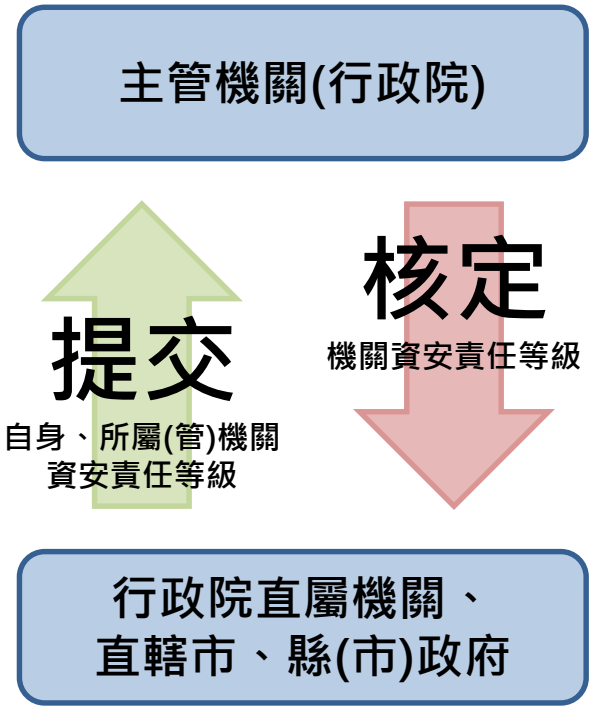
- 設置資安長
- 訂定及實施資安維護計畫
- 訂定資安事件通報及應變機制

- 訂定及實施資安維護計畫
- 訂定資安事件通報及應變機制

資通安全責任等級

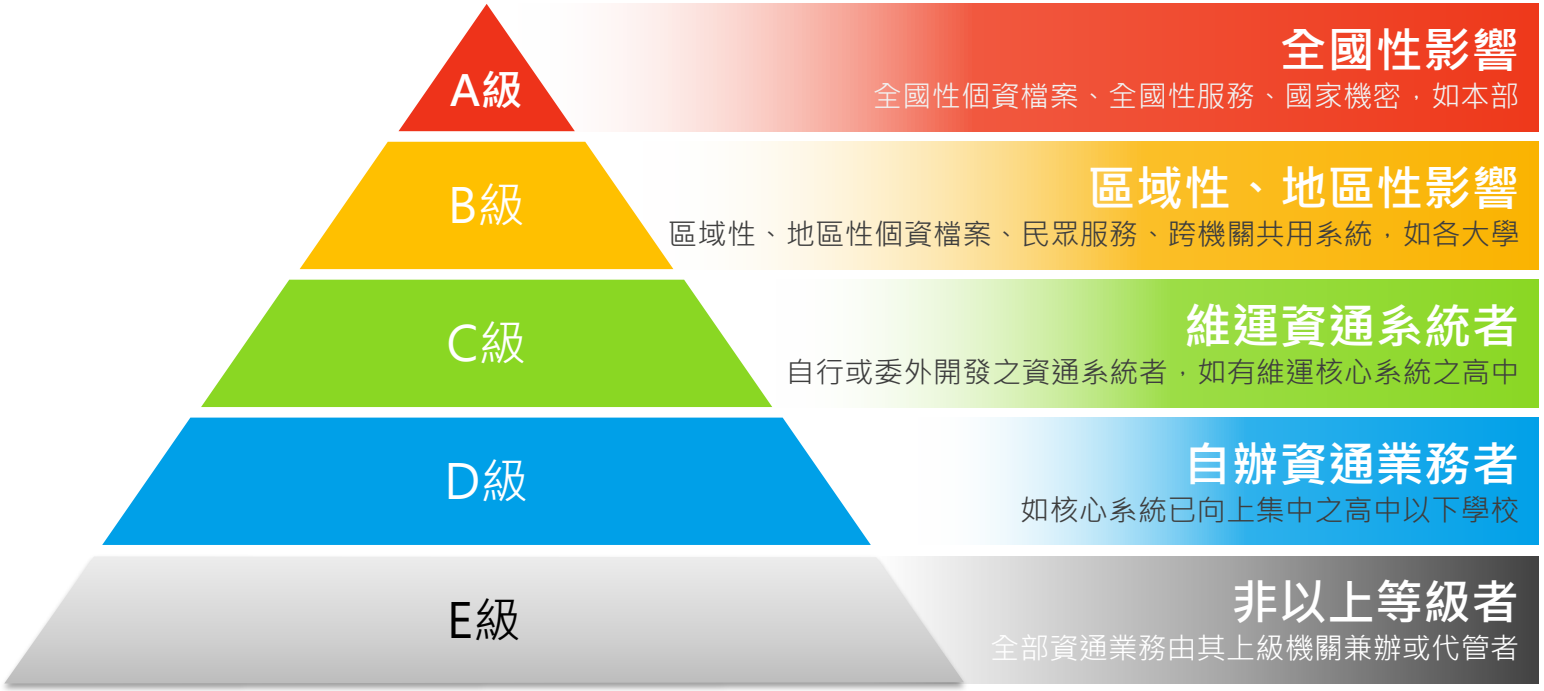
教育體系等級提交機關

- **提交機關**應每2年提交所屬責任等級，報行政院核定。
  - 教育部(行政院直屬機關)
    - 部屬機關、機構
    - 國立大專校院及其附設機構
    - 國立高級中等以下學校
    - 教育部主管政府捐助之財團法人
  - 各直轄市、縣（市）政府
    - 教育網路中心(二級單位)
    - 直轄市、縣(市)立各級學校



- 資通安全責任等級分級辦法第3條

資安責任等級分級原則


A級
全國性影響
全國性個資檔案、全國性服務、國家機密，如本部
B級
區域性、地區性影響
區域性、地區性個資檔案、民眾服務、跨機關共用系統，如各大學
C級
維運資通系統者
自行或委外開發之資通系統者，如有維運核心系統之高中
D級
自辦資通業務者
如核心系統已向上集中之高中以下學校
E級
非以上等級者
全部資通業務由其上級機關兼辦或代管者

分級作業辦法應辦事項-管理面

辦理事項	辦理內容	A	B	C
資通系統分級及防護基準	完成資通系統分級，並完成防護基準；每年至少檢視一次妥適性	1年內		2年內
ISMS之導入及通過公正第三方之驗證	2年內**全部核心資通系統**導入資訊安全管理系統。	3年內完成第三方驗證；並持續維持期驗證有效性。		O*
業務持續運作演練	**全部核心資通系統**	每年1次	每2年1次	
辦理內部資通安全稽核		每年2次	每年1次	每2年1次
資通安全專職(責)人員（1年內）		4人	2人	1人*
資安治理成熟度評估（公務機關）		每年1次		X

***C級單位因應措施**

- ISMS導入
  - 短期：資科司後續將與國教署協調規劃**輔導團隊**，輔導C級學校導入教版管理規範。
  - 長期：高級中等以下學校全部**資通系統向上集中**為共通系統，將責任等級降至D級。
- 專職(責)人員
  - 短期：本部同意高級中等以下學校得以專責人員配置，兼任資訊行政教師減授教學節數。
  - 長期：國教署配合修正「高級中等學校組織設置及員額編制標準」，資安人力法制化。

分級作業辦法應辦事項-技術面

辦理項目	辦理內容	A	B	C
安全性檢測 全部核心資通系統*	網站安全弱點檢測	每年2次	每年1次	每2年1次
	系統滲透測試	每年1次	每2年1次	
資通安全健診*	網路架構檢視、網路惡意活動檢視、使用者端電腦惡意活動檢視、伺服器主機惡意活動檢視、目錄伺服器設定及防火牆設定檢視	每年1次	每2年1次	
資通安全威脅偵測管理機制*	完成威脅偵測機制建置，並持續維運	1年內		X
	依行政院指定方式提交監控管理資料	O	O	X
資通安全防護 （啟用，並持續使用及適時進行軟、硬體之必要更新或升級）	防毒軟體、網路防火牆、具有郵件伺服器者，應備電子郵件過濾機制	1年內		
	IDS/IPS、具有對外服務之核心資通系統者，應備應用程式防火牆（WAF）	1年內		X
	APT攻擊防禦	1年內	X	
政府組態基準 （GCB）	依主管機關公告之項目，完成GCB導入作業，並持續維運（公務機關）	1年內		X

分級作業辦法應辦事項-認知與訓練

辦理事項	辦理內容	A	B	C
資通安全教育訓練	資通安全及資訊人員，每人每年各接受12小時之資通安全專業課程訓練或資通安全職能訓練*	至少4人	至少2人	至少1人
	一般使用者及主管，每人每年至少接受之一般資通安全教育訓練	每人3小時		
資通安全專業證照及職能訓練證書	初次受核定或等及變更後之一年內，資通安全專職（責）人員總計應持有之**資通安全專業證照**，並持續維持證照之有效性	4張以上	2張以上	1張以上
	資通安全專職人員總計應持有之**資通安全職能評量證書**，並持續維持證照之有效性（公務機關）	4張以上	2張以上	1張以上

***資通安全專業課程訓練或資通安全職能訓練**：
本部將請**教育體系資安團隊**協助辦理資安相關教育訓練課程，後續將公告於TACERT及A-ISAC網站。

分級作業辦法應辦事項-D、E級

面向	辦理項目	辦理細項	D	E
技術面	資通安全防護	防毒軟體、網路防火牆、具有郵件伺服器者，應備電子郵件過濾機制	1年內	X
認知與訓練	資通安全教育訓練	一般使用者及主管，每人每年至少接受之一般資通安全教育訓練	每人3小時	

前瞻建構綠能雲端資料中心計畫

教育體系部分：

規劃目標

國中小校園機房向上集中至所屬縣市網路中心		高中職校園機房向上集中	
108年	109年	108年	109年
13縣市	20縣市	50%	80%

- 向上集中工作重點
  - 改善PUE、可靠度及資安
  - 推動及輔導各縣市依需求及特色提出全縣市或跨縣市集中之核心系統，如：學校首頁、網域名稱、電子郵件系統、校務行政系統、公文系統、會計系統等

- 教育體系資訊資源集中效益
  - 減輕行政負擔
  - 提高軟硬體資源利用率
  - 減少系統重複開發
  - 持續改善機房PUE
  - 減少設備維運及維護成本
  - 提升機房可用率達99.95%

前瞻建構綠能雲端資料中心計畫

- 針對134個國立高中職，為協助資通安全責任等級降為D級的申請條件，本部也會輔導媒合有意願學校辦理核心系統(例如校務行政系統)向上集中
- 媒合直轄市及離島國立高中職，並補助教育網路中心協助
- 委託國家高速網路中心協助辦理其他縣市國立高中職向上集中至國網代管資料中心

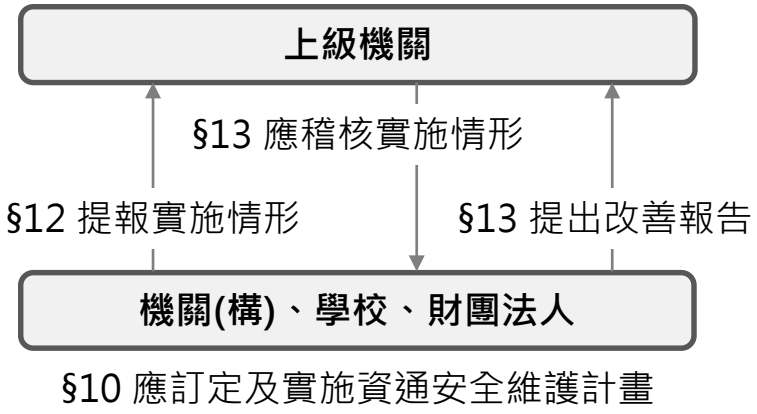
應辦事項配套措施

應辦單位	辦理項目		因應措施
A、B級	資通安全威脅偵測管理機制		臺灣學術網路連線單位可結合**臺灣學術網路資安監控系統(南、北SOC, Mini-SOC)**進行威脅偵測機制。
A、B、C級	核心資通系統	網站安全弱點檢測	由**成功大學網站防護團隊**協助辦理。
		滲透測試	教育體系資安檢核技術服務計畫協助辦理。
	資通安全健診		請**北、南區學術資訊安全維運中心**協助辦理相關教育訓練課程。
	資通安全專業證照		委託教育機構資安驗證中心(國立中興大學)開設ISO 27001:2013 LA、BS 10012:2017 LA 證照專班。
	資通安全職能評量證書		後續教育體系委託政治大學協助辦理相關教育訓練，由國家資通安全會報技術服務中心考試評量。

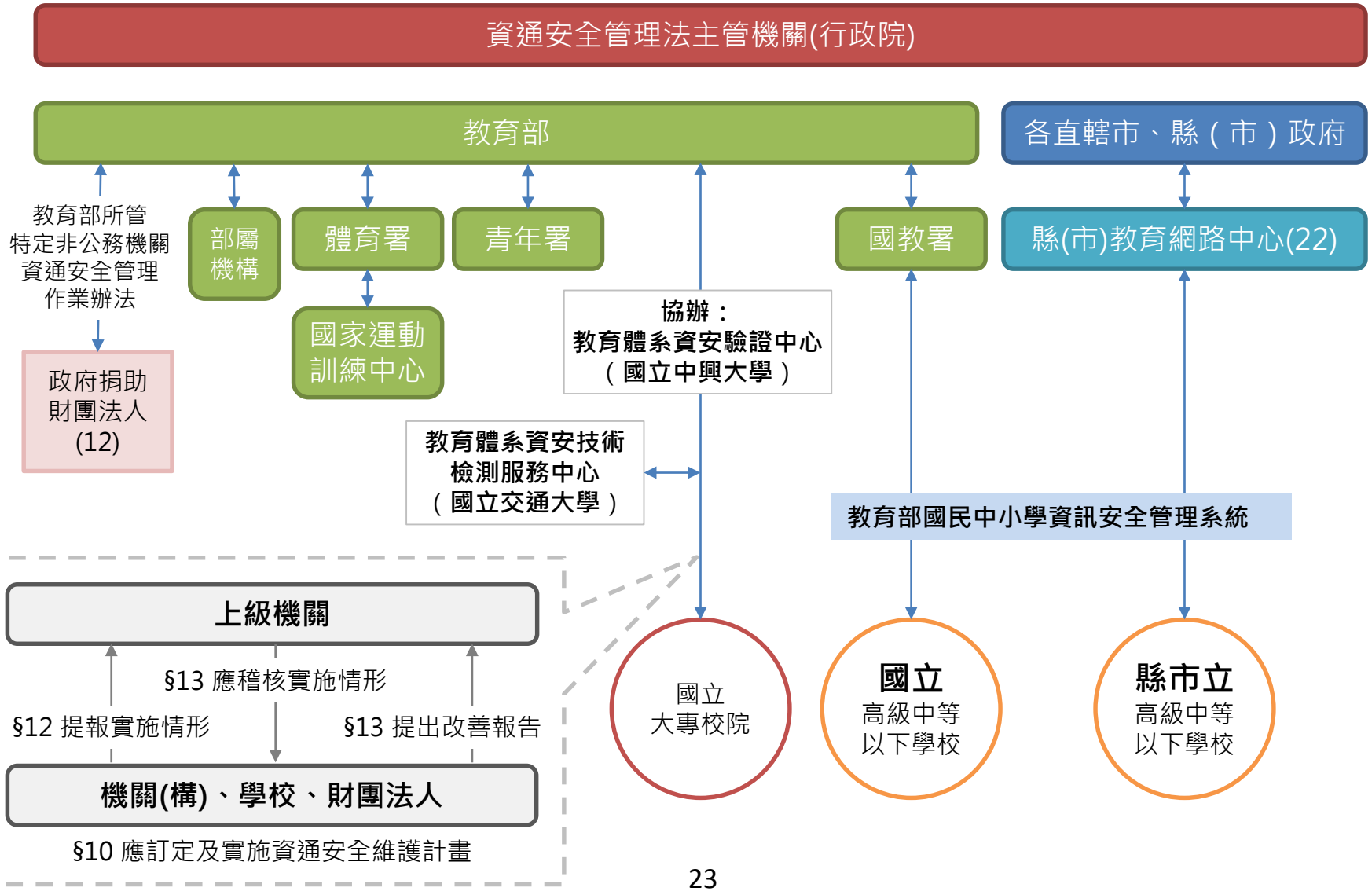
資通安全維護計畫

資通安全維護計畫

- 本法第10條，公務機關應訂定及實施資通安全維護計畫。
- 本法第12條，公務機關應每年向上級提出資通安全維護計畫實施情形。
- 本法第13條，公務機關應稽核其所屬機關之資通安全維護計畫實施情形。



教育體系稽核作業


資通安全管理法主管機關(行政院)
教育部
各直轄市、縣（市）政府
教育部所管特定非公務機關資通安全管理作業辦法
部屬機構
體育署
青年署
國教署
縣(市)教育網路中心(22)
國家運動訓練中心
協辦：教育體系資安驗證中心（國立中興大學）
政府捐助財團法人(12)
教育體系資安技術檢測服務中心（國立交通大學）
教育部國民中小學資訊安全管理系統
上級機關
§13 應稽核實施情形
§12 提報實施情形
§13 提出改善報告
機關(構)、學校、財團法人
§10 應訂定及實施資通安全維護計畫
國立大專校院
國立高級中等以下學校
縣市立高級中等以下學校

教育體系稽核作業

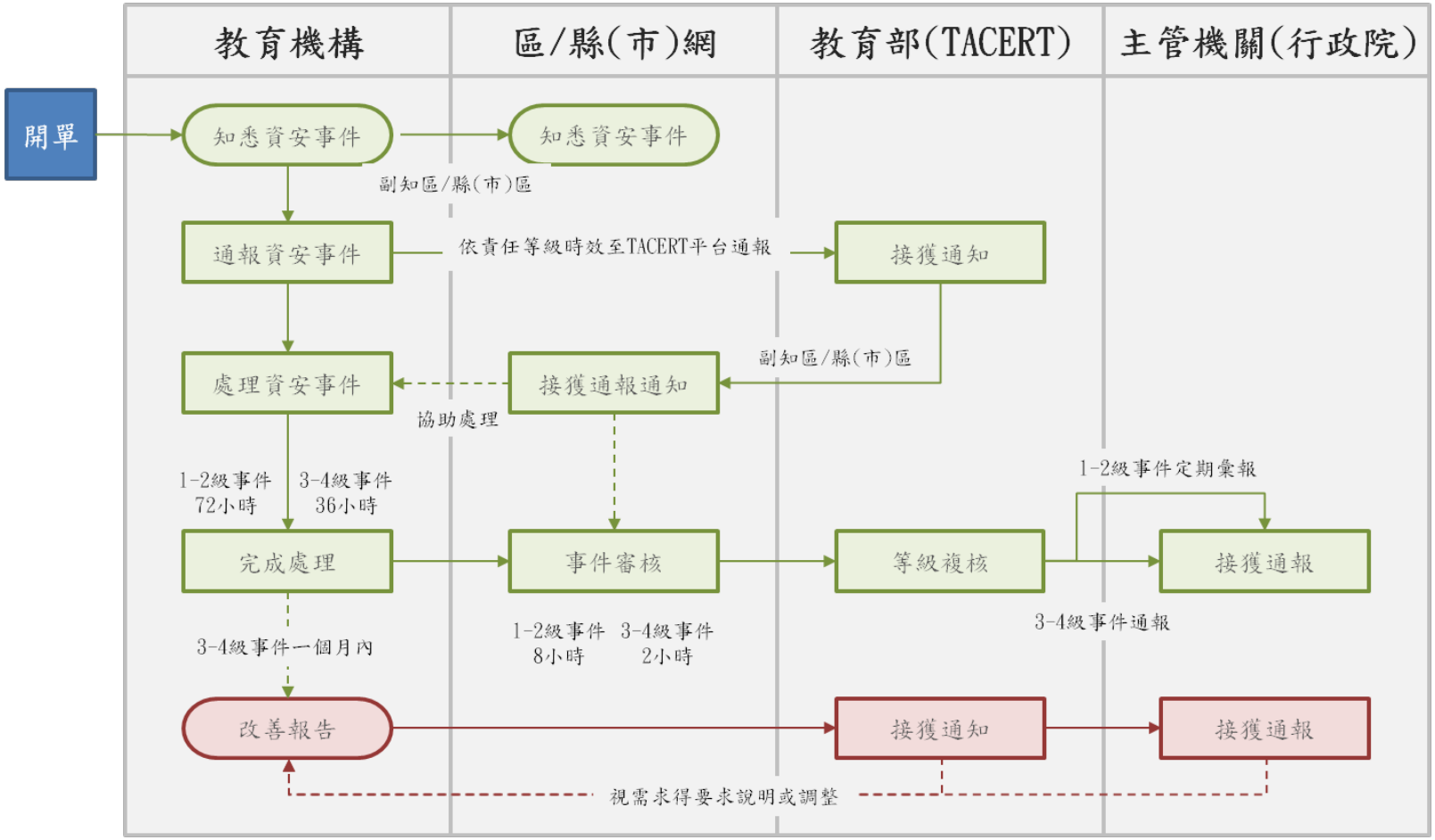
- 大專校院
  - 委託「教育機構資安驗證中心」協助辦理相關稽核作業。
    - 制度面：教育部本部。
    - 管理面：教育機構資安驗證中心（國立中興大學）。
    - 技術面：教育體系資安技術檢測服務中心（國立交通大學）。
- 高級中等以下學校
  - 補助新北市政府教育局開發「資訊安全管理系統」。
    - 訂定維護計畫：學校填報上傳「資通安全維護計畫」。
    - 學校提報實施情形：學校填報實施情形題目。
    - 稽核實施情形：評量人員線上評量審查，到校輔導訪視。

資通安全通報及應變

臺灣學術網路各級學校資通安全通報應變作業程序

- **資通安全事件通報及應變辦法第20條**
  - 公務機關於本辦法施行前，已針對其所屬公務機關，自行同訂定資通安全事件通報及應變機制，並實施一年以上者，得經主管機關核定後，與其所屬公務機關繼續依該機制辦理資通安全事件之通報及應變。
- 本部108年5月2日修正發布「**臺灣學術網路各級學校資通安全通報應變作業程序**」，各級學校依前開作業程序辦理通報及應變。

各級學校通報及應變流程



修正重點

新增「確認時間」

- 於通報流程中新增「**確認時間**」欄位，以利記錄事件確認時間。

新增「改善措施」

- 於應變流程中新增「**改善措施**」欄位，以利處理人員填寫事件改善措施。

新增「事件列印」

- 於事件通報應變完成後，於「**歷史通報**」中新增「**事件列印**」功能，以利處理人員列印事件內容送呈單位主管

修正時程

- 此次修正項目預計於**108年07月01日(一)**上線，上線後依據相關修正進行通報應變作業。

修正依據

資通安全事件通報及應變辦法

- 依據資通安全管理法之資通安全事件通報及應變辦法**第二章第四條**規定：
  - 公務機關**知悉**資通安全事件後，應於**一小時**內依主管機關指定之方式及對象，進行資通安全事件之通報
- 依據資通安全法之資通安全事件通報及應變辦法**第三章第十一條**規定：
  - 特定非公務機關**知悉**資通安全事件後，應於**一小時**內依中央目的事業主管機關指定之方式，進行資通安全事件之通報

臺灣學術網路各級學校資通安全通報應變作業程序

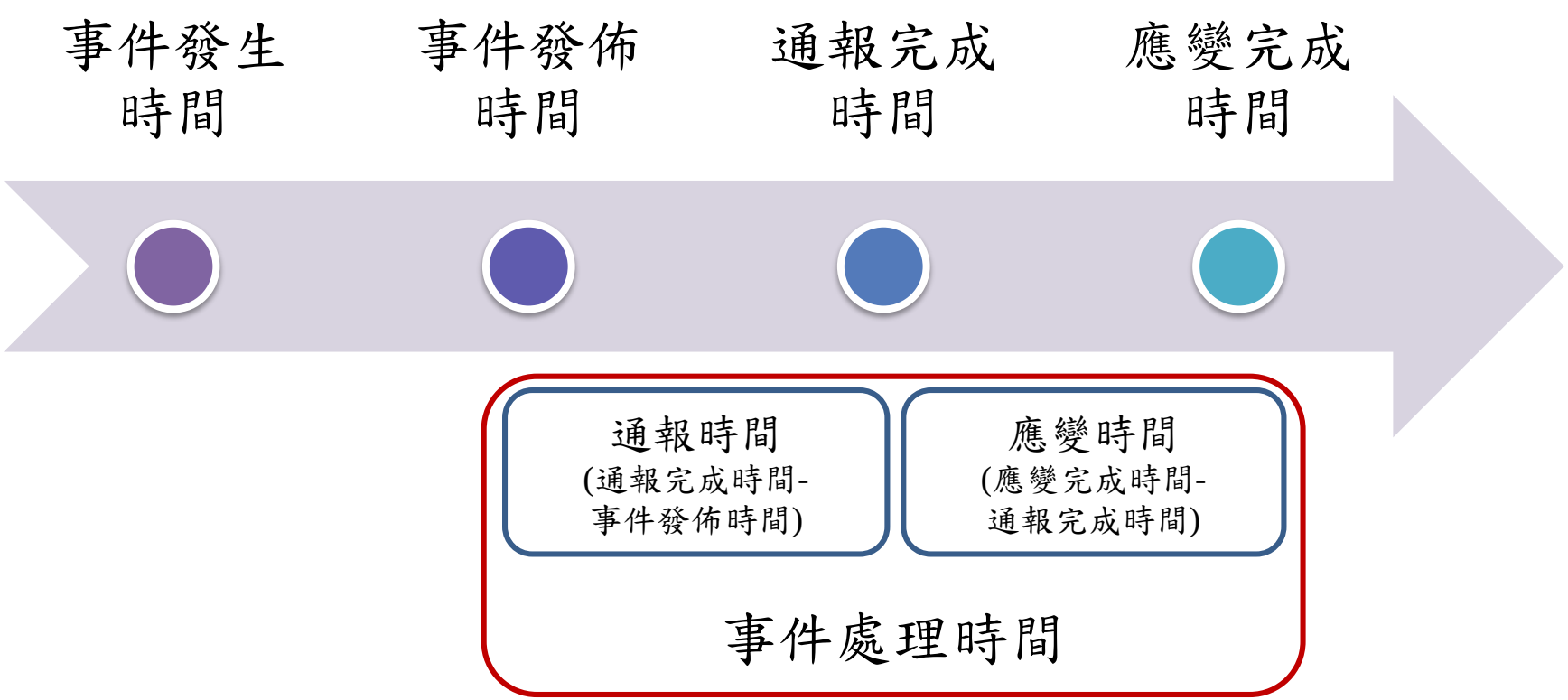
- 依據臺灣學術網路各級學校資通安全通報應變作業程序第三章第一節第二條規定：
  - 各連線單位發現資安事件後可先進行事件確認，經確認為資安事件後，須於**一小時**內，至通報應變網站通報登錄資安事件細節、影響等級及是否申請支援等資訊，並評估該事件是否影響其他連線單位運作。

確認時間修正說明

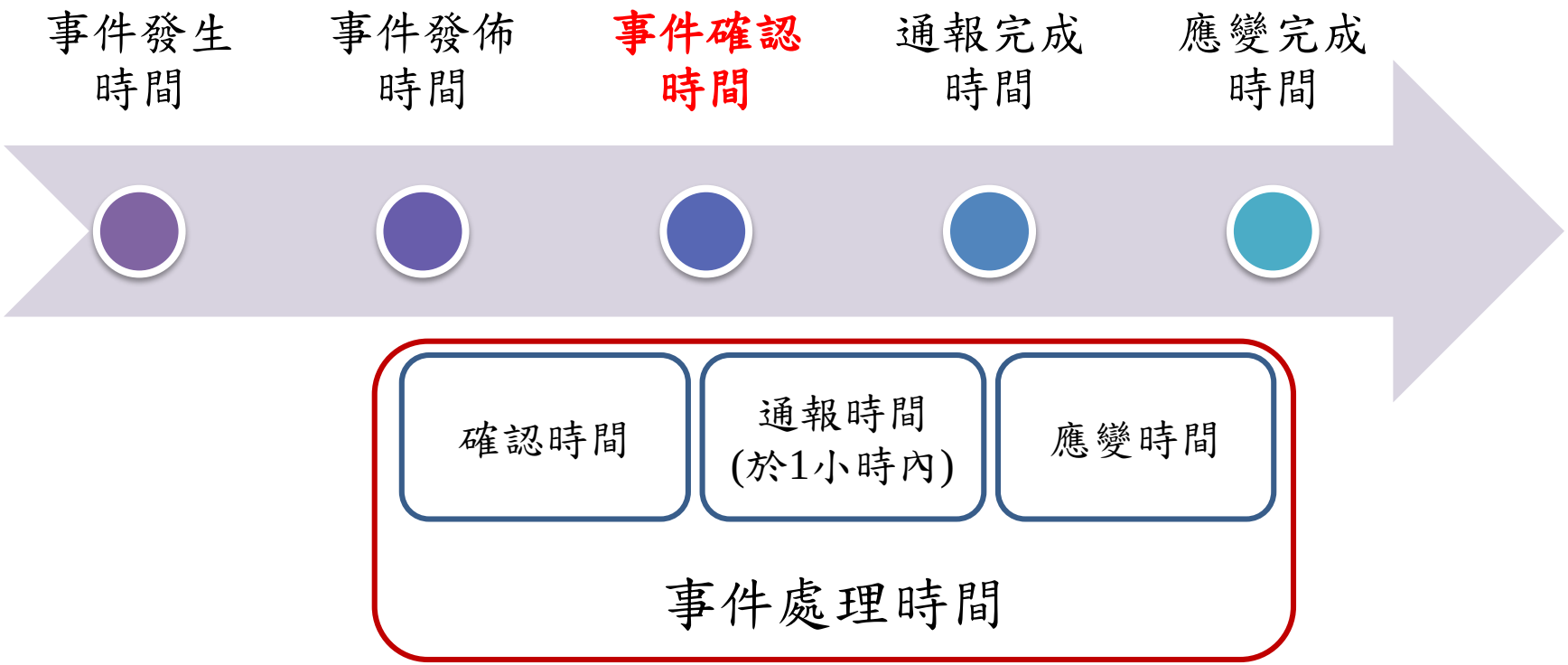
新增「確認時間」

- 於現行通報流程填寫欄位新增「**確認時間**」欄位
- 確認時間指各連線單位發現資安事件後可先進行事件確認，經確認資安事件條件成立之時間
- 事件通報流程需於確認時間後**1小時內**完成
- 事件通報應變時效不因新增確認時間而改變，
  「1」、「2」級事件需於**72小時內**完成；
  「3」、「4」級事件需於**36小時內**完成。

現行通報應變時程

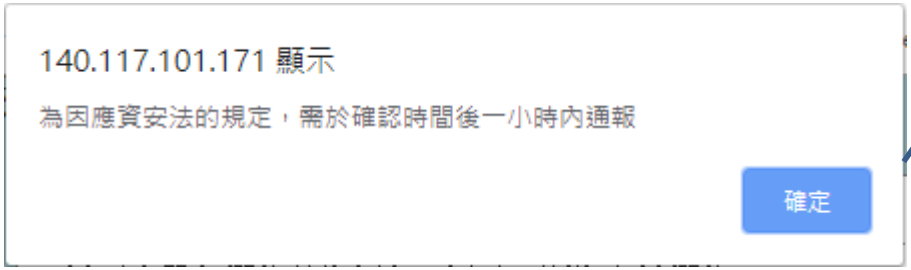

事件發生時間
事件發佈時間
通報完成時間
應變完成時間
通報時間
(通報完成時間-事件發佈時間)
應變時間
(應變完成時間-通報完成時間)
事件處理時間

修正後通報應變時程


事件發生時間
事件發佈時間
事件確認時間
通報完成時間
應變完成時間
確認時間
通報時間(於1小時內)
應變時間
事件處理時間

確認時間畫面


通報流程
各機關因受外在因素所產生資通安全事件時通報事項：
以下表單各欄位若為紅色◎標示，則為必填欄位
欄位中不得輸入特殊符號，例如：「;」、「"」、「'」、「$」、「&」、「%」、「!」、「^」、「*」、「<」、「>」、「_」、「|」、「-」
1.通報型態:
告知通報
2.◎事件發生時間：
2019-04-30 14:47:31
3.◎確認時間:
2019-05-30 09:17:50


140.117.101.171 顯示
為因應資安法的規定，需於確認時間後一小時內通報
確定

提示訊息

改善措施修正說明

新增「改善措施」

- 於現行應變流程填寫欄位新增「**改善措施**」欄位
- 改善措施指**各連線單位於完成通報應變後，針對事件發生提出相關改善措施，以完備事件處理流程及預防事件重覆發生**
- 改善措施包含「**改善辦法**」及「**改善時間**」欄位

改善措施畫面


應變流程
◎1. 緊急應變措施
已中斷網路連線，待處理完成後再上線
已停止伺服器之服務，待處理完成後再上線
直接處理完成，解決辦法詳見【解決辦法】
其它
◎2. 解決辦法：
(文字勿超過200中文字, 標點符號請用全形)
◎3. 解決時間：
改善措施
◎改善辦法：
(文字勿超過200中文字,標點符號請用全形)
依資通安全相關管理規範進行改善措施
◎ 改善時間：
2019-05-24 14:37:36

事件列印修正說明

新增「事件列印」

- 依據臺灣學術網路各級學校資通安全通報應變作業程序第三章第一節第六條規定：
  -「2」、「1」級資安事件通報應變完成後，應至通報應變網站列印單件，**每月彙整**送呈單位主管；
  「4」、「3」級資安事件需於事件發生後**36小時內**，通報送陳單位資通安全長(副校長或校長)。
- 於登入「教育機構資安通報平台」後，左側「**歷史通報**」中即可套表列印貴單位事件單以利送呈簽核

事件列印畫面


教育機構資安通報平台
Ministry of education information & communication security contingency platform
聯絡資訊
回首頁
修改個人資料
登出
通報
通報/應變
自行通報
事件單處理狀態
歷史通報
帳號管理
事件附檔下載
資安預警事件
事件統計
演練資訊
情資資料下載
事件單編號
發佈時間
距通報時間(小時)
流程
Page 1/1
台灣學術網路危機處理中心(TACERT)

事件列印畫面


教育機構資安通報平台
Ministry of education information & communication security contingency platform
聯絡資訊
回首頁
修改個人資料
登出
通報
通報/應變
自行通報
事件單處理狀態
歷史通報
帳號管理
事件附檔下載
資安預警事件
事件統計
演練資訊
情資資料下載
開始日期:
結束日期
查詢
匯出EXCEL
第一頁 |上一頁 |下一頁 |最終頁
事件單編號 | 單位 | | 來源 | 等級 | IP | 發佈時間 | 結案時間
120553 | 列印 | 1級 | 2017-09-03 13:40:19 | 2017-09-05 16:00:48
119749 | 列印 | 1級 | 2017-08-22 14:10:24 | 2017-08-23 14:38:13
53335 | 列印 | N-ASOC | 1級 | 2015-04-24 10:11:12 | 2015-04-24 16:29:07
39053 | 列印 | N-ASOC | 1級 | 2014-06-10 10:38:05 | 2014-06-10 11:58:30
32023 | 列印 | N-ASOC | 1級 | 2014-01-02 | 2014-01-02
台灣學術網路危機處理中心(TACERT)

事件列印畫面

◎緊急應變措施：
已中斷網路連線，待處理完成後再上線
解決辦法：
系統重灌，再上線
解決時間：　2015-04-24 11:52:22
◎改善措施：
改善辦法：
改善時間：　1999-01-01 00:00:00

資安長官：	單位主管：	承辦人：

套表簽核欄位

重點整理

新增「**確認時間**」並於事件確認**後一小時內**完成通報流程

新增「**改善措施**」以完備事件處理流程

新增「**事件列印**」以利送呈簽核

修正項目於**108年07月01日(一)**上線

重點提醒

因應「**資通安全管理法**」及其相關辦法與「**臺灣學術網路各級學校資通安全通報應變作業程序**」進行相關修正作業

各單位務必掌握時效依照相關規定完成通報應變作業，以避免相關刑事、民事及行政相關責任。

TACERT連絡方式

- 如有任何問題可透過下列方式連絡TACERT團隊協助
  - 網站：https://cert.tanet.edu.tw
  - 服務信箱：services@cert.tanet.edu.tw
  - 電話：(07)525-0211
  - 網路電話：98400000

感謝指導