TSC CAPITAL GROUP
The Bridge to the Asia Pacific Region

國立臺南大學

111年資訊安全暨個人資料管理規範導入顧問輔導服務案
課程名稱：資安及個資事件通報及應變

授課日期：111年7月6日
授課講師：德欣寰宇科技股份有限公司 資安顧問 吳懿仁

簡報大綱

一 資通安全及個資保護觀念及法規要求

二 本校資通安全事件通報及應變處理程序

三 本校個資安全事件通報及應變處理程序

四 案例分享與討論

tsc 海科 TSC CAPITAL GROUP
The Bridge to the Asia Pacific Region

資通安全及個資保護觀念及法規要求

資訊安全基本概念

- 何謂資訊？

  資訊是一種資產，像其他重要的組織資產一樣對組織**有價值**，而且需要**適當**的**保護**。

資訊是組織營運的資產

- 資訊是組織的重要資產並且也是所有業務流程的一部分。
- 包含營業秘密、專利、人員隱私和業務構想等。

它被視為組織的資產

建立資訊資產所需的成本、技術、時間及資源

資訊資產的資料分類是確保機密性及所有者

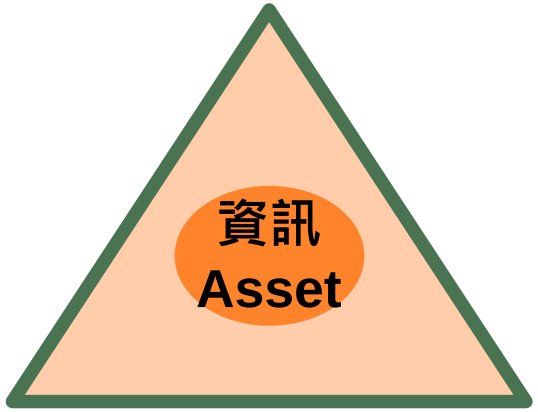
資料損失會**影響**組織在不同業務活動的**投資**

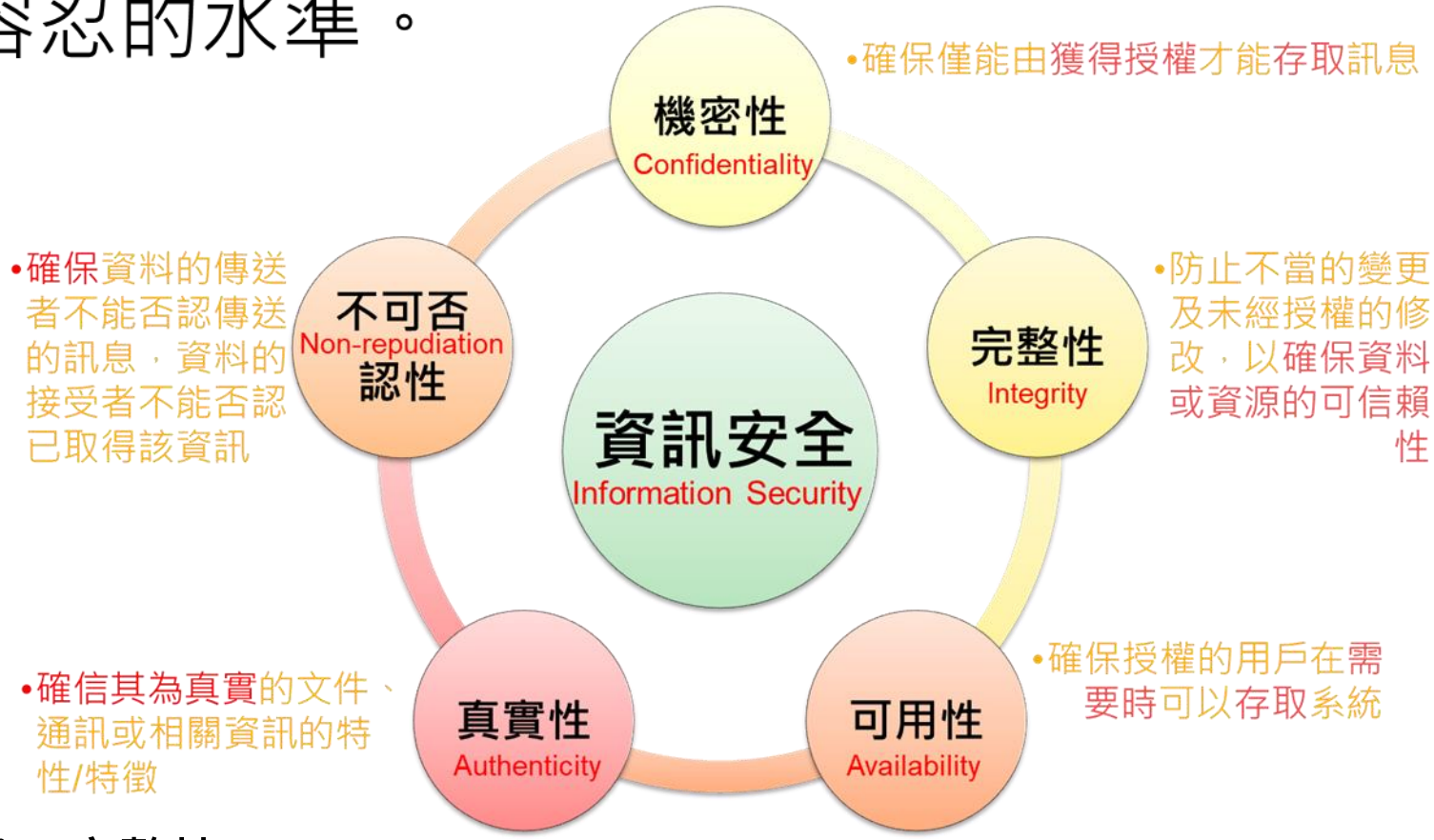
它是組織企業形象的一部分

資訊安全基本概念

- 資訊安全需在基礎設施及資訊間保持一個良好的平衡，在這樣的情況下資料或其服務在遭受竊取、竄改和破壞的情況應保持較低或可容忍的水準。

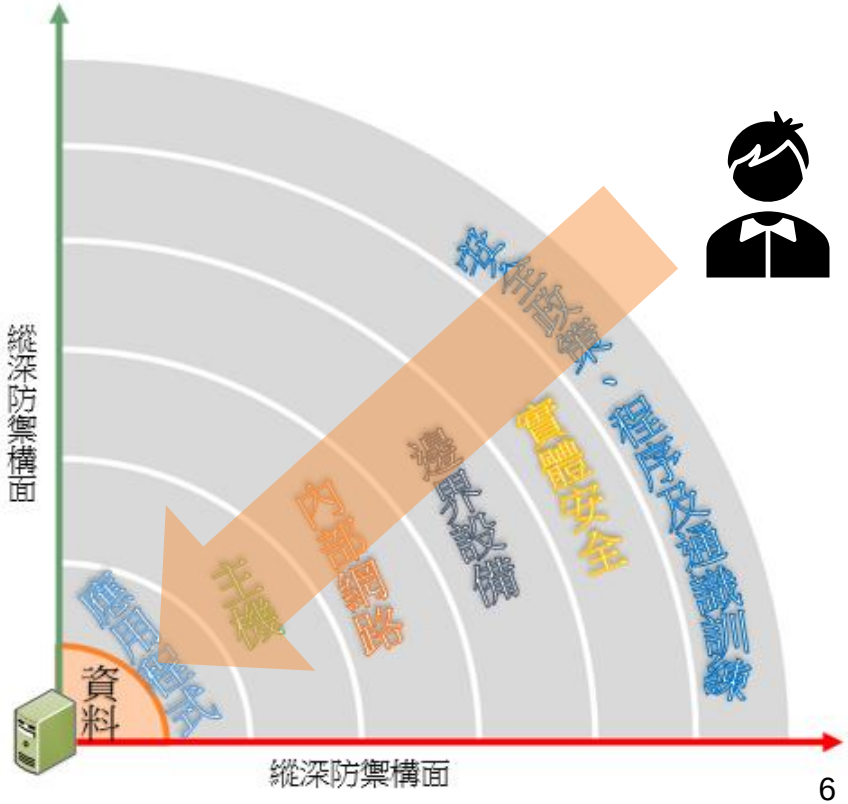
機密性、完整性及可用性常被作為資訊安全CIA的三角(維度)





資訊安全的防禦縱深

- 縱深防禦是一種安全政策，是對要保護的資產設置了多個面向的防護。
- 此政策有助於避免攻擊者對資訊系統和資料的直接攻擊，某一面相受破壞只會讓攻擊面對接下一個面向的防禦。



資通安全管理法歷程

- 資通安全：指防止資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性、完整性及可用性。(資通安全管理法第3條第3項)

107年5月11日
三讀通過

→

107年6月6日
總統公告

→

107年11月21日
子法公告

→

108年1月1日
正式施行

→

108年8月26日
第1次子法修正

→

110年8月23日
第2次子法修正

立法目的及規範對象

➢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

以對人民生活、經濟活動及公眾或國家安全有重大影響者為納管對象。

公務機關	特定非公務機關
1.中央與地方機關(構) 2.公法人	1.關鍵基礎設施提供者 (電信、能源、銀行、財金、交通、供水及防救災) 2.公營事業(例如台糖) 3.政府捐助之財團法人（例如工研院）

tsc 遠東 TSC CAPITAL GROUP The Bridge to the Asia Pacific Region

資通安全管理法架構

資通安全管理法
(母法)

- 資通安全管理法施行細則(子法)
- 資通安全責任等級分級辦法(子法)
- 資通安全情資分享辦法(子法)
- 資通安全事件通報及應變辦法(子法)
- 特定非公務機關資通安全維護計畫(子法)
- 公務機關所屬人員辦理資通安全業務獎懲辦法(子法)

tsc 遠東 TSC CAPITAL GROUP
The Bridge to the Asia Pacific Region

資通安全管理法施行細則-§6-訂定資通安全維護計畫

第 6 條

1 本法第十條、第十六條第二項及第十七條第一項所定資通安全維護計畫，應包括下列事項：

一、核心業務及其重要性。

二、資通安全政策及目標。

三、資通安全推動組織。

四、專責人力及經費之配置。

五、公務機關資通安全長之配置。

六、資通系統及資訊之盤點，並標示核心資通系統及相關資產。

七、資通安全風險評估。

八、資通安全防護及控制措施。

九、資通安全事件通報、應變及演練相關機制。

十、資通安全情資之評估及因應機制。

十一、資通系統或服務委外辦理之管理措施。

十二、公務機關所屬人員辦理業務涉及資通安全事項之考核機制。

十三、資通安全維護計畫與實施情形之持續精進及績效管理機制。

2 各機關依本法第十二條、第十六條第三項或第十七條第二項規定提出資通安全維護計畫實施情形，應包括前項各款之執行成果及相關說明。

3 第一項資通安全維護計畫之訂定、修正、實施及前項實施情形之提出，公務機關經其上級或監督機關同意，得由其上級、監督機關或其上級、監督機關所屬公務機關辦理；特定非公務機關經其中央目的事業主管機關同意，得由其中央目的事業主管機關、中央目的事業主管機關所屬公務機關或中央目的事業主管機關所管特定非公務機關辦理。

tsc 遠航 TSC CAPITAL GROUP
The Bridge to the Asia Pacific Region

資通安全事件通報及應變辦法-§9&§10-訂定資通安全事件通報及應變作業規範

第 9 條　公務機關應就資通安全事件之通報訂定作業規範，其內容應包括下列事項：

一、判定事件等級之流程及權責。

二、事件之影響範圍、損害程度及機關因應能力之評估。

三、資通安全事件之內部通報流程。

四、通知受資通安全事件影響之其他機關之方式。

五、前四款事項之演練。

六、資通安全事件通報窗口及聯繫方式。

七、其他資通安全事件通報相關事項。

第 10 條　公務機關應就資通安全事件之應變訂定作業規範，其內容應包括下列事項：

一、應變小組之組織。

二、事件發生前之演練作業。

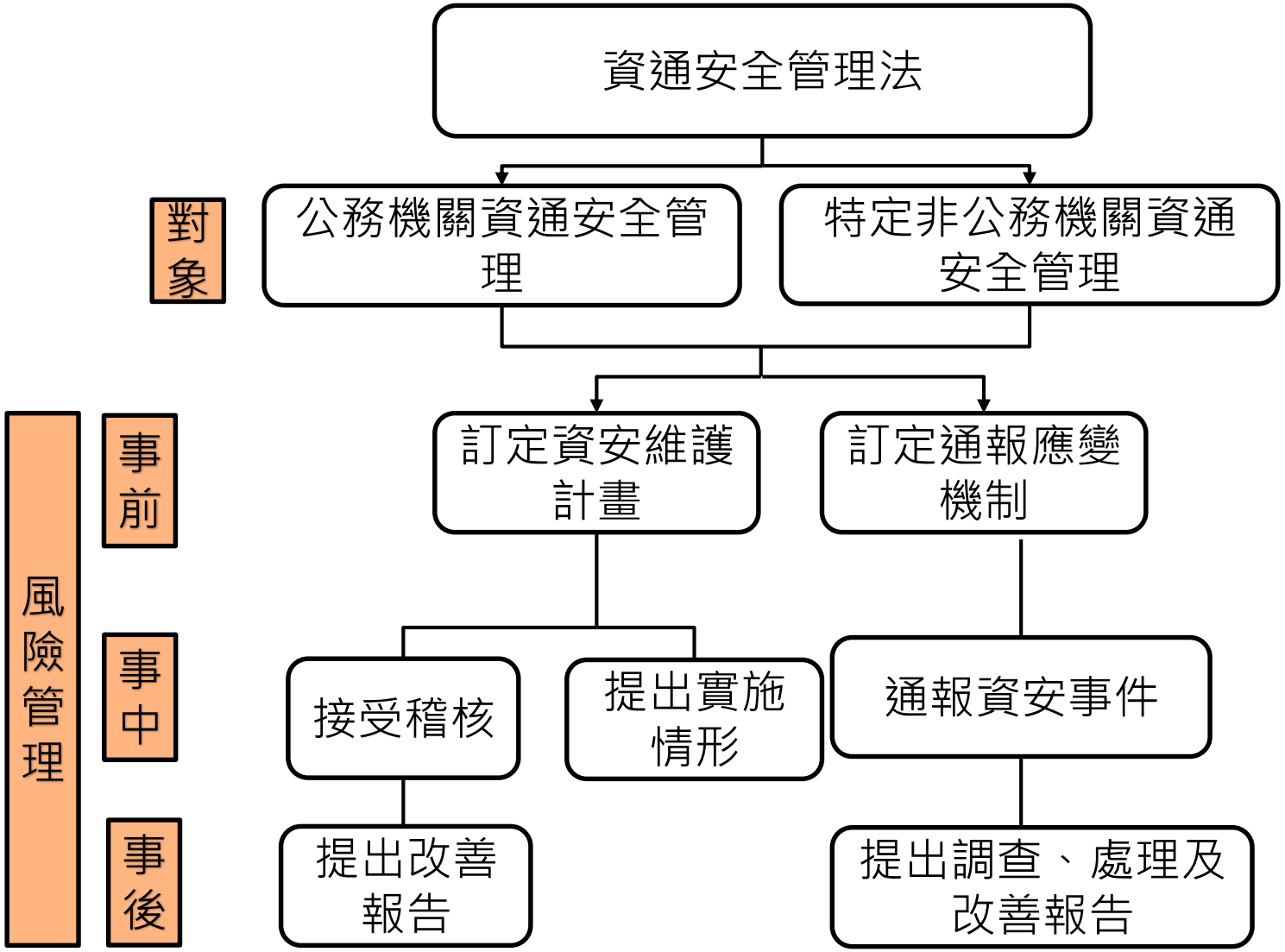
三、事件發生時之損害控制機制。

四、事件發生後之復原、鑑識、調查及改善機制。

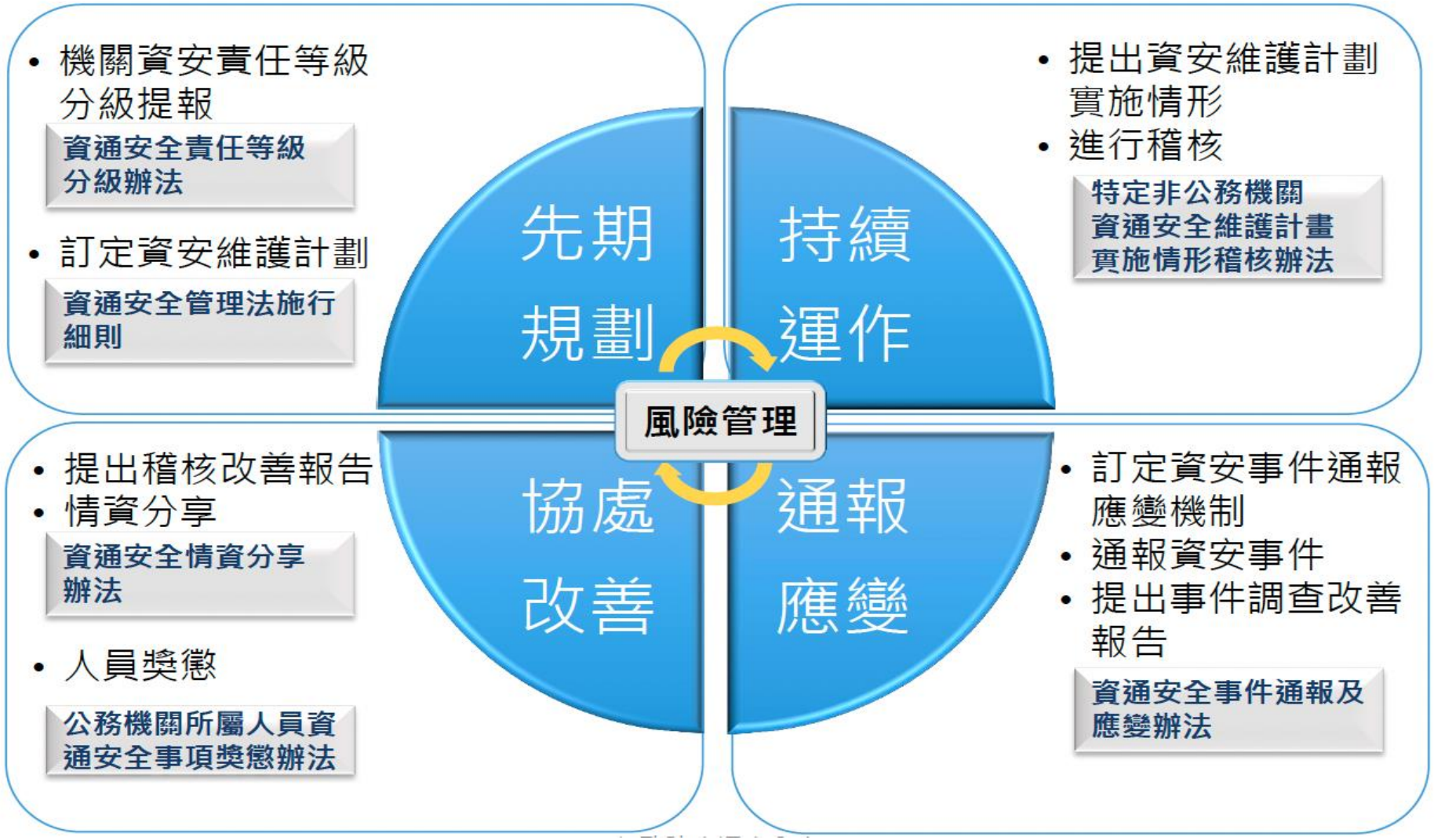
五、事件相關紀錄之保全。

六、其他資通安全事件應變相關事項。

風險管理角度之資安維護計畫及通報應變機制

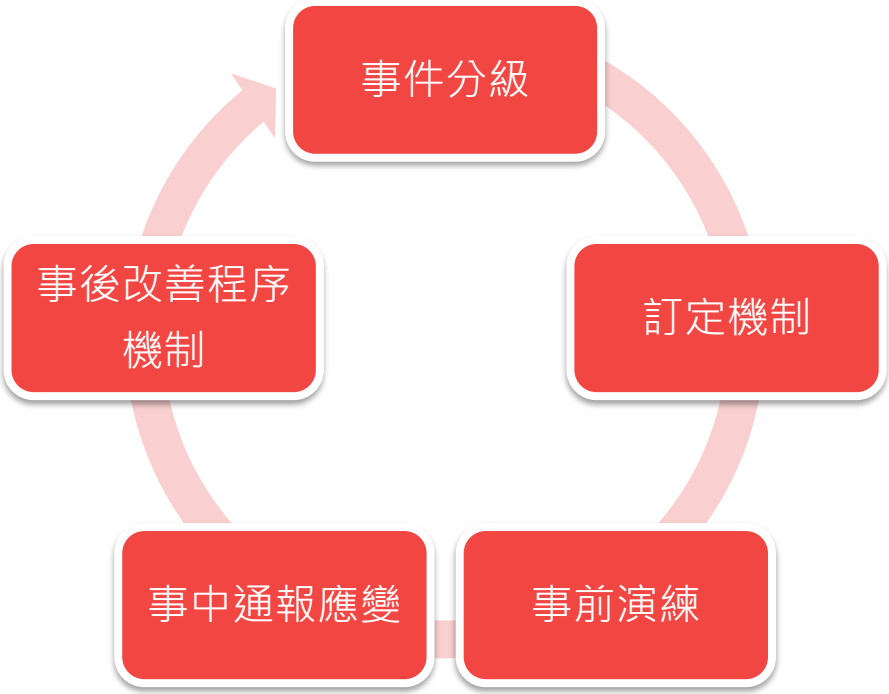


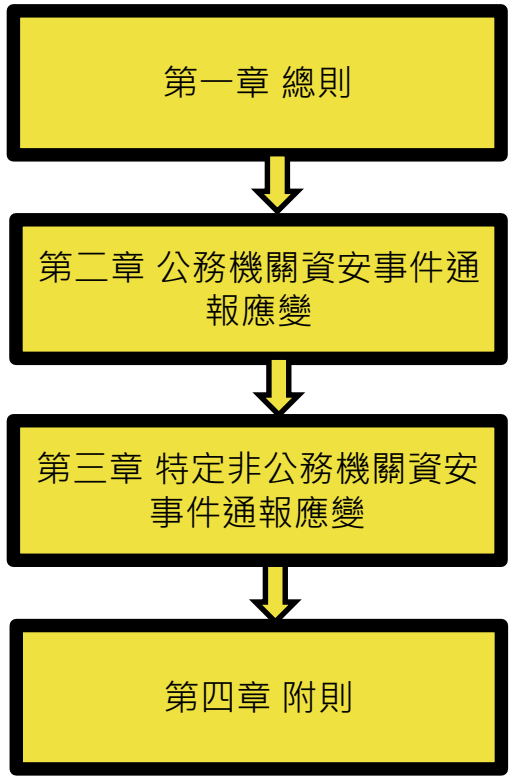
資通安全管理法與子法整體運作循環



資通安全事件通報及應變辦法

- 本辦法依資通安全管理法第14條第4項及第18條第4項規定訂定。
- 為強化各機關之資安事件之因應。
- 規範事件之分級、事前演練、事中通報及應變，以及事後改善之程序、機制。





資通安全事件通報及應變辦法-第5條

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。

前項資通安全事件等級變更時，公務機關應依前項規定，續行通報。

公務機關因故無法依第一項規定方式通報者，應於同項規定之時間內依其他適當方式通報，並註記無法依規定方式通報之事由。

公務機關於無法依第一項規定方式通報之事由解除後，應依該方式補行通報。

什麼是資安事件？(1/2)

- 資通安全事件係指系統、服務或網路狀態經鑑別而顯示可能有**違反資訊安全政策**或**保護措施失效**之狀態發生，可能影響資通系統機能運作，構成資通安全政策之威脅。(資安法第1章第3條第4款)

什麼是資安事件？(2/2)

- 資訊安全事故是在機密性、完整性和可用性會影響到網路設備或系統主機上儲存資料安全性的活動。
- 可能是在主機系統或網路環境中**真實或疑似**的不良**事件**。
- 這是一種**違反政策或應立即處理**的威脅，對電腦安全政策、可能接受的使用策略或是標準的安全作業具有潛在的衝擊。

資訊安全事故的類型

1. 惡意代碼或內部威脅攻擊
2. 未經授權的存取
3. 未經授權的使用服務
4. 電子郵件的濫用
5. 間諜活動
6. 詐騙與竊盜
7. 員工惡意濫用與破壞
8. 網路與資源的濫用
9. 資源錯誤設定的濫用

資安事件影響等級評定方式

- 資安事件影響等級評定須考量三面向衝擊性
  - 「機密性」衝擊。
  - 「完整性」衝擊。
  - 「可用性」衝擊。

綜合評估資安事件造成之三面向衝擊，評定影響等級。

- 資安事件影響等級由輕至重分「1」、「2」、「3」、「4」四個級別

	機密性	完整性	可用性
4			
3			
2	✓		
1		✓	
無			✓

2級事件

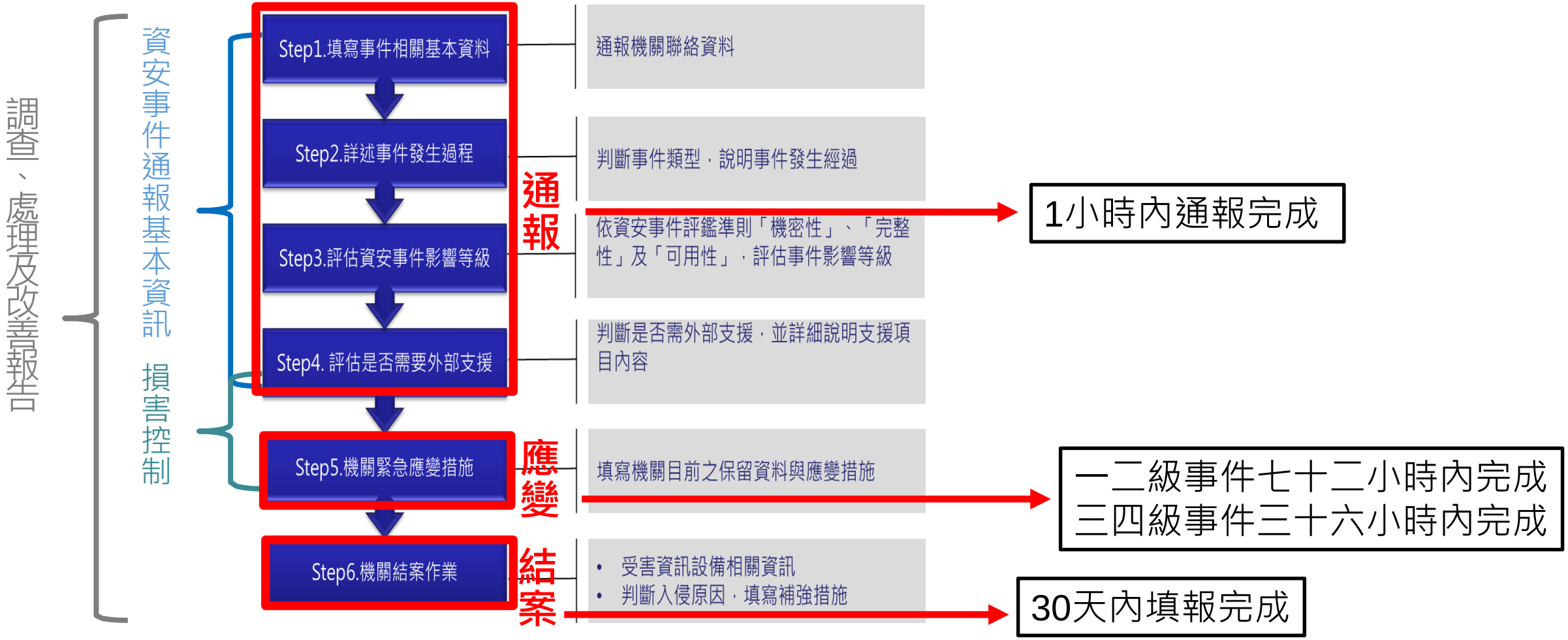
資安事件等級綜合評估表(1/2)

	機密性 資訊洩漏		完整性 資訊/資通系統遭竄改		可用性 業務/資通系統運作遭中斷	
	資訊性質	影響程度	業務資訊/資通系統	影響程度	業務/資通系統	可否於可容忍中斷時間回復
1級	非核心業務	輕微	非核心	輕微	非核心	可
2級	非核心業務	嚴重	非核心	嚴重	非核心	不可
	核心業務 (未涉及CI維運)	輕微	核心 (未涉及CI維運)	輕微	核心 (未涉及CI維運)	可
3級	核心業務 (未涉及CI維運)	嚴重	核心 (未涉及CI維運)	嚴重	核心 (未涉及CI維運)	不可
	核心業務 (涉及CI維運)	輕微	核心 (涉及CI維運)	輕微	核心 (涉及CI維運)	可
	一般公務機密、敏感資訊	輕微	一般公務機密、敏感資訊	輕微		
4級	核心業務 (涉及CI維運)	嚴重	核心 (涉及CI維運)	嚴重	核心 (涉及CI維運)	不可
	一般公務機密、敏感資訊	嚴重	一般公務機密、敏感資訊	嚴重		
	國家機密	-	國家機密	-		

資安事件等級綜合評估表(2/2)

	機密性 資訊洩漏		完整性 資訊/資通系統 遭 竄改		可用性 業務/資通系統運 作 作遭中斷	
影響程度 業務性質/資通系統別	洩漏程度		竄改程度		可否於可容忍時間內回復	
	輕微	嚴重	輕微	嚴重	可	不可
非核心業務	1級	2級	1級	2級	1級	2級
非核心資通系統			1級	2級	1級	2級
未涉及CI維運之核心業務	2級	3級	2級	3級	2級	3級
未涉及CI維運之核心資通系統			2級	3級	2級	3級
涉及CI維運之核心業務	3級	4級	3級	4級	3級	4級
涉及CI維運之核心資通系統			3級	4級	3級	4級
一般公務機密、敏感資訊	3級	4級	3級	4級		
國家機密	4級		4級			

資安事件通報資訊



※完成通報登錄、應變處置、結案登錄(Step1-6)即表示完成調查、處理及改善報告

公務機關與特定非公務機關資安事件作業比較

項目		公務機關	特定非公務機關
相同	通報作業流程	於時限內完成「事件通報作業」、「損害控制」及「調查、處理及改善報告」作業	
	制定資安規範	• 訂定資安事件之通報作業規範 • 訂定資安事件之應變作業規範	
相異	事件通報對象	上級/監督機關、主管機關	中央目的事業主管機關
	配合上級/監督機關資安演練	• 社交工程演練每半年一次 • 資安事件通報演練每年一次	無特殊規定
	配合主管機關資安演練作業	• 社交工程演練 • 資安事件通報及應變演練 • 網路攻防演練 • 情境演練 • 其他必要之演練	• 網路攻防演練 • 情境演練 • 其他必要之演練

tsc 海科 TSC CAPITAL GROUP The Bridge to the Asia Pacific Region

各機關資通安全事件通報及應變處理作業程序

事件通報

- 事件通報及應變小組：指揮官、情資及計畫組、應變執行組、後續調度組
- 3、4級資通安全事件，各 機關除規定通報外，應另以**電話通知**上級機關或中央目的事業主管機關

事件應變會議

- 3、4級資通安全事件，資安長應**召開會議**研商相關事宜
  1.資通安全事件概況
  2.評估受影響範圍
  3.其他必要之討論事項

損害控制或復原措施

- 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
- 評估是否對外公告
- 依規定完成通知作業

各機關資通安全事件通報及應變處理作業程序

根因分析

- 除設備故障外，應保存跡證， 督導進行根因調查，並提出紀錄分析；若發現惡意程式，應上傳Virus Check檢測，並送防毒或資安公司檢測
- 評估**短、中、長期**資安管理改善策略

tsc 海航 TSC CAPITAL GROUP The Bridge to the Asia Pacific Region

各機關資通安全事件通報及應變處理作業程序

改善追蹤

- 各機關進行事件改善追蹤時，應召開會議，並據以辦理下列事項:

1.評估改善作為期程。

2.評估執行成效，並據以調整改善策略。

3.配合上級機關、中央目的事業主管機關或主管機關辦理相關改善作為。

4.第三級或第四級資通安全事件，應由執行秘書將各階段**改善措施執行成效定期回報**事件指揮官至完成各項改善措施為止，並由機關資通安全專責人員彙整送交上級機關或中央目的事業主管機關，無上級機關者，應送交主管機關。

5.依會議決議及主管機關或中央目的事業主管機關指定之 方式，送交調查、處理及改善報告;第三級或第四級資通安全事件，應另以**密件公文**將該報告送交主管機關及上級或監督機關。

6.機關送交調查、處理及改善報告後，相關改善事項應納 入機關現行定期追蹤管考機制。

注意通報時間

項次	時間名稱	填入方式	說明
1	事件發現時間	**自行填寫**	事件發現時間需由機關**自行填寫**，平台限制該時間不得晚於通報時間
2	通報時間	系統填寫	以通報機關「通報登錄」時間為通報時間
3	完成損害控制或復原時間	系統填寫	通報平台以**「事件發現時間」**起算**36/72小時**內完成損害控制或復原時間
4	結報時間	系統填寫	以通報機關「完成損害控制或復原時間」起算**1個月(日曆天數30天)**內完成結報
5	通報送出時間	系統填寫	以通報機關「通報單填寫完成」時間為通報送出時間

個人資料保護法歷程

84年

- 公布［電腦處理個人資料保護法］

99年

- 公布「個人資料保護法」

101年

- 公布［個人資料保護法］施行

104年

- 公布修正之「個人資料保護法」部分條文

105年

- 修正之「個人資料保護法」部分條文施行

有限適用範圍 → 全面適用

tsc 遠東 TSC CAPITAL GROUP
The Bridge to the Asia Pacific Region

個人資料保護法目的與架構

- §1，為規範個人資料之蒐集、處理及利用，以避免人格權受侵害，並促進個人資料之合理利用，特制定本法。

第一章 總則(§1~§14)

第二章
公務機關對個人資料之蒐集、處理及利用
(§15~§18)

第三章
非公務機關對個人資料之蒐集、處理及利用
(§19~§27)

第四章
損害賠償及團體訴訟
(§28~§40)

第五章
罰則
(§41~§50)

第六章
附則
(§51~§56)

何謂個資? §2

一般個資	特種個資
自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指 紋、婚姻、家庭、教育、職業、聯絡 方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。	病歷、醫療、基因、性生活、健康檢查、犯罪前科

個人資料保護法 第6條

特種個資不得隨意蒐集處理利用，但有下列情形之一者，不在此限

1.法律明文規定。

2.執行法定職務或履行法定義務所必要，且事前或事後有適當安全維護措施。

3.當事人自行公開或其他已合法公開的個人資料。

4.公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。

5.經當事人書面同意。但逾越特定目的之必要範圍或其他法律另有限制不得僅依當事人書面同意蒐集、處理或利用，或其同意違反其意願者，不在此限。

個人資料保護法§12-個資事件發生後通知當事人

第 12 條　公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。

親愛的消費者/會員您好：

非常抱歉，（公司或網站名稱）因（原因）發生個人資料外洩事故，且已有消費者接獲詐騙集團電話。提醒您，詐騙集團通常於週末或下班時間以（手法）誆騙消費者。如接獲疑似詐騙電話，請不要聽從指示操作 ATM 或提供任何個人資料，並立即通報 165 警政署反詐騙專線。

針對這次事件，本公司已（改善措施），未來也會持續加強資訊安全與個人資料保護管理，以降低消費者個資被侵害之風險。

如有關於訂單或本次個資事故之疑問，請於（上班時間）與本公司客服人員聯絡（電話）；上班時間以外請以（提供其他可行方式）聯絡本公司。

（公司名稱）　敬上

通知資訊3重點！！！！！
1.個資當事人個人資料被侵害之事實
2.已採取之因應措施(處理情形)
3.後續供當事人查詢之專線與其他查詢管道

tsc 遠東 TSC CAPITAL GROUP The Bridge to the Asia Pacific Region

個人資料保護法施行細則§22-適當方式通知當事人

第 22 條　1　本法第十二條所稱適當方式通知，指即時以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之。但需費過鉅者，得斟酌技術之可行性及當事人隱私之保護，以網際網路、新聞媒體或其他適當公開方式為之。

2　依本法第十二條規定通知當事人，其內容應包括個人資料被侵害之事實及已採取之因應措施。

銓敘部個資外洩通知

本部於108年6月22日接獲外部情資知悉國外網站揭露疑似本部所掌理之個人資料餘59萬筆，本部依個人資料保護法第12條及施行細則第22條規定通知當事人相關事項如下：

一、影響範圍：94年1月1日至101年6月30日間中央及地方機關公務人員送審人員歷史資料，實際影響人數為243,376筆，欄位包含身分證字號、姓名、服務機關、職務編號、職稱。

二、已採取因應措施：

(一) 依資通安全管理法向行政院國家資通安全會報技術服務中心進行資安事件通報。

(二) 疑似外洩資料之資訊系統早已於104年3月下線，為求審慎，本部即刻對本案現行運作相關資通系統進行弱點檢測及重新檢視防護措施。

針對本事件，本部已協請行政院資通安全處協助進行根因調查及全機關全面性資通安全檢測，本部將確實檢討改進，並依資通安全管理法及個人資料保護法持續精進各項資通安全及個資保護相關作為。

銓敘部108年個資外洩事件

tsc 遠航 TSC CAPITAL GROUP The Bridge to the Asia Pacific Region

個資法施行細則§12-安全維護事項

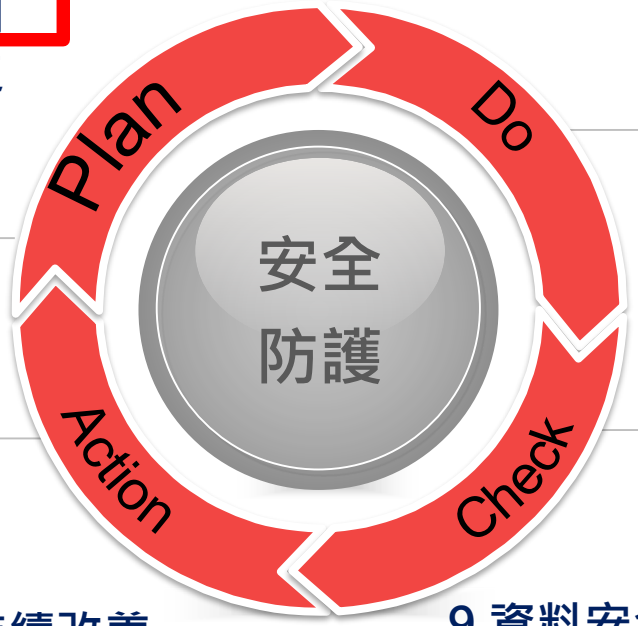
個資法§6、18、19、27

Plan

1. 配置管理之人員及相當資源
2. 界定個人資料之範圍
3. 個人資料之風險評估及管理機制
4. 事故之預防、通報及應變機制
5. 個人資料蒐集、處理及利用之內部管理程序

Do

6. 資料安全管理及人員管理
7. 認知宣導及教育訓練
8. 設備安全管理



Action

11.個人資料安全維護之整體持續改善

Check

9.資料安全稽核機制
10.使用紀錄、軌跡資料及證據保存

本校資通安全事件通報及應變處理程序

NUTN-ISMS-B011資通安全事件管理程序書-事件管理

1.應建立資通安全事件之處理作業程序，並賦予相關人員必要責任，以便迅速有效處理資通安全事件。
2.除正常應變計畫（如：系統及服務之回復作業），資通安全事件之處理程序，應視需要納入下列事項：
  2.1導致資通安全事件原因之分析。
  2.2防止類似事件再發生之補救措施。
  2.3電腦稽核軌跡及相關證據之蒐集。
  2.4與受影響之使用者進行溝通及說明。
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：
  3.1作為研析問題之依據。
  3.2作為研析是否違反契約或資通安全規定之證據。
  3.3作為與委外廠商協商如何補償之依據。
4.應依據「資通安全事件通報與應變作業流程」處理資通安全事件。相關作業程序應注意下列事項：
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。
4.2向管理階層報告處理情形，並檢討、分析資通安全事件。
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。
4.4緊急處理步驟應詳實記載，以備日後查考。

NUTN-ISMS-B011資通安全事件管理程序書-通報程序

1.疑似資通安全事件發生時，發現人員應依事件歸屬通報權責單位，並副知直屬主管。

2.權責單位於收到通知後，研判是否為資通安全事件。若：

2.1判定為非資通安全事件時，則將結果回覆予發現人員。

2.2判定為資通安全事件時，初估事件處理時間，並通知資通安全官。

2.3資通安全事件等級依照略....(此段後續會做程序書修正，將依據資通安全事件通報及應變辦法修整)

3.權責單位於發生資通安全事件時，應立即填具「資通安全事件報告單」。

4.決策處理：

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通安全官。

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通安全官報告，重新執行事件分析辨識。

4.3資通安全官應參考「教育機構資安通報應變手冊」，並依據權責單位所提報之事件影響報告，決定是否向上級主管單位通報。若需要通報，應由單位主管確認後執行。

5.有關是否啟動業務永續運作計畫，依「業務永續運作管理程序書」辦理。

NUTN-ISMS-B011資通安全事件管理程序書-危機處理

本校資通安全危機處理包括事前建置安全防護機制、事中主動預警與緊急應變，以及事後復原追蹤鑑識偵查等步驟。說明如下：

1.事前建置安全防護機制：

1.1建置資訊安全管理系統及整體防護架構。

1.2彙整及備妥資通安全相關文件。

2事中主動預警與緊急應變：

2.1事件辨識：辨識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。

2.2事件控制：依據各類事件危機處理之程序，進行事件傷害控制，降低影響的程度及範圍。

2.3　問題解決：事件處理權責單位或負責人須將問題解決。必要時，應向資通安全委員會提出建議方案。

2.4恢復作業：問題解決後，系統需恢復至事件發生前之正常運作狀態。

3.事後復原追蹤鑑識偵查：

3.1後續追蹤之精神乃係檢討相關資通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。

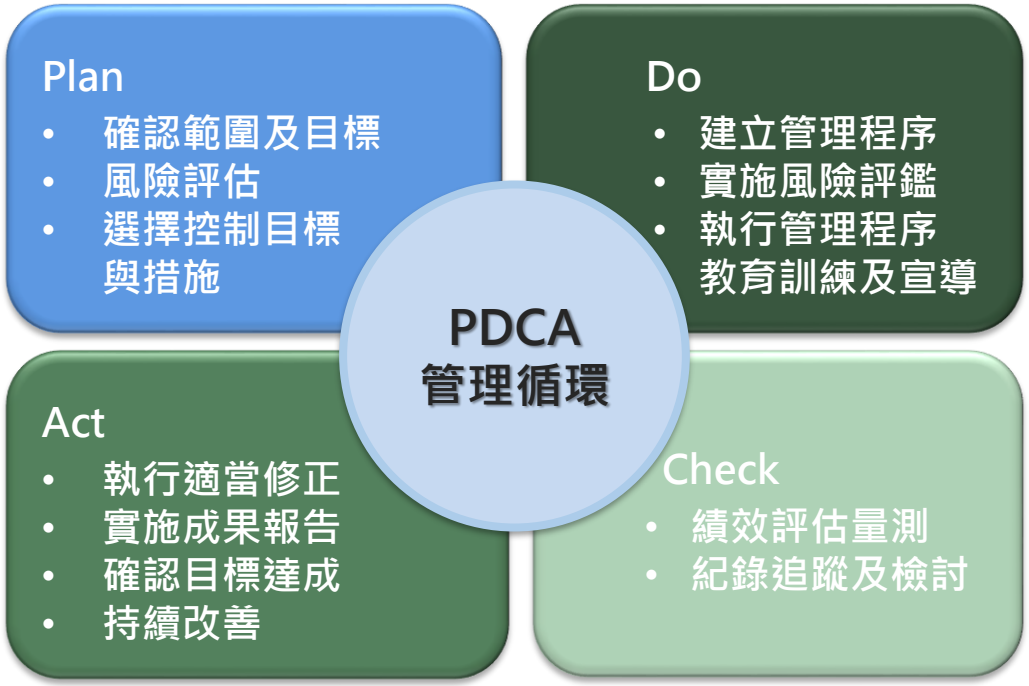
3.2受損單位依復原程序實施災後復原重建。

3.3資通安全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）。

NUTN-ISMS-B011資通安全事件管理程序書-檢討與改善

1.安全事件確認處理完成後，權責單位應檢討現行管理措施之完整性，並適當修訂相關作業管理規範或建置控制措施。必要時，應召開檢討會議。

2.權責單位應依「矯正管理程序書」規定處理，以避免類似安全事件重複發生。



NUTN-ISMS-D035 資通安全事件報告單

一、發現資通安全事件之單位聯絡資料：

單位名稱：_____通報人：_____

電話：_____傳真：_____E-mail：_____

二、資通安全事件通報事項：

1.事件發生時間：____年____月____日____時____分

2.設備資料：

◎IP 位址(IP Address)：_____（無；可免填）

◎網際網路位址(Web-URL)：_____（無；可免填）

◎設備廠牌、機型：_____

◎作業系統名稱、版本：_____

◎已裝置之安全機制：_____

3.資通安全事件資料：

◎系統安全等級：□4 級；□3 級；□2 級；□1 級

◎影響等級：4 級：影響國家資訊建設　　3 級：系統停頓，業務無法運作

2 級：業務中斷，影響系統效率　1 級：業務短暫停頓，可立即修復

◎事件分類：□非法入侵；□感染病毒；□阻斷服務；□其他：_____

◎破壞程度：□系統當機；□資料庫毀損；□網頁遭篡改；□其他：_____

◎事件說明：

◎可能影響範圍及損失評估：

◎應變措施：

三、期望支援項目：

四、解決辦法：

□已填寫 D019 異常事件紀錄表(紀錄編號：_____) □不須填寫 D019 異常事件紀錄表

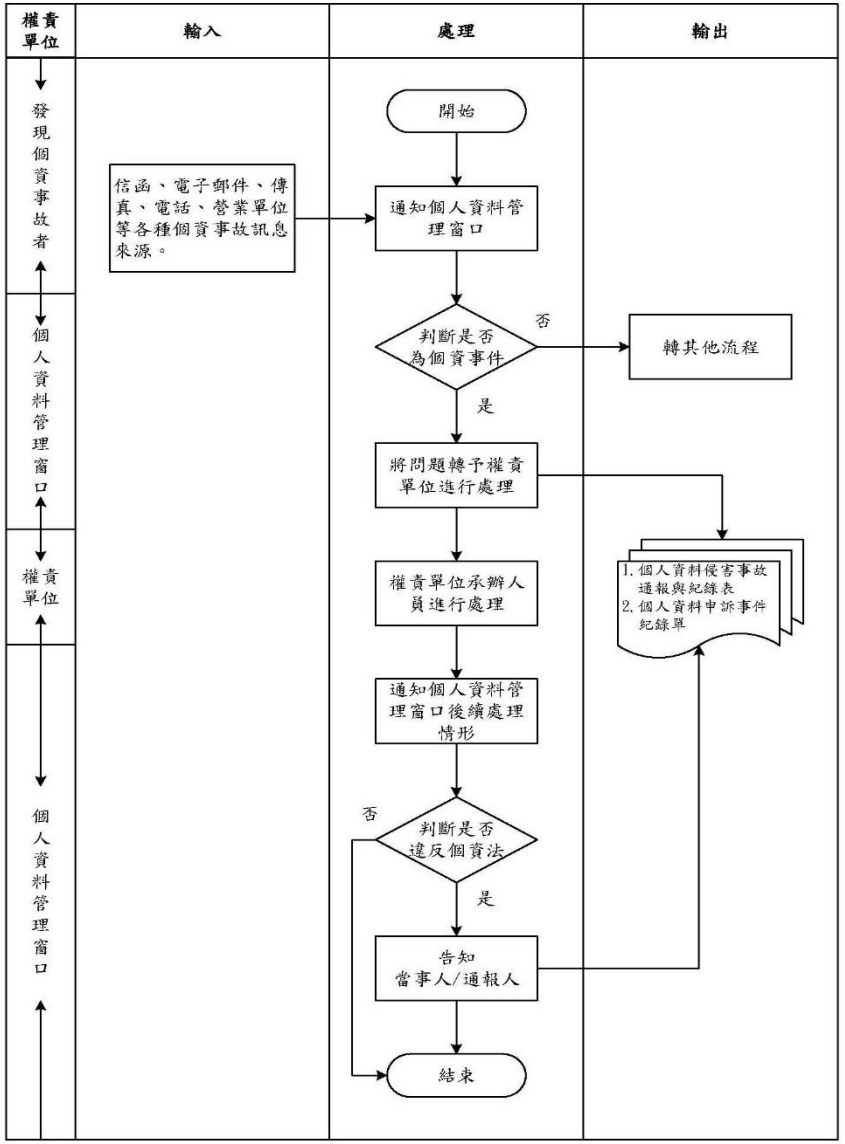
五、完成時間：____年____月____日____時____分

承辦人簽章	單位主管	資通安全官

填寫時須確認是否為最新版本表單，避免誤用造成填寫資料差異，延誤通報應變流程。

本校個資安全事件通報及應變處理程序

NUTN-PIMS-C002 個人資料保護緊急應變處理作業說明書



1.各單位於發現個資遭侵害時，應通知個人資料管理窗口，由個人資料管理窗口與個資保護執行小組判斷是否發生個資事故。

2事故發生時，應依下列個人資料事故通報及受理流程進行通報，以便即時處理與解決。

3.通報原則

3.1個資事故發生時，應依通報順序逐級陳報。

3.2當上述任何一層級人員無法依層級順序被通報時，負責通報人員應往上一層級逕行陳報，以確保通報程序之即時性。

4.判斷個資事故

4.1個人資料管理窗口接獲相關個資案件通知時，應立即協同相關人員蒐集相關跡證，初步判斷是否發生個資事故及其影響程度與範圍。

4.2若經判斷為個資事故，事故處理之業管單位應立即依據「個人資料事故通報及受理流程」，啟動個資應變措施相關處理作業。

4.3個人資料管理窗口應將相關異常通知、事故判斷及處理情形等相關資訊，確實記錄於「個人資料侵害事故通報與紀錄表」，並陳報權責單位主管審核。

NUTN-PIMS-C002 個人資料保護緊急應變處理作業說明書

5.記錄個資事故，啟動應變措施

個資應變措施應符合限制、處理、復原等三階段的事故處理原則，說明如下：

5.1.針對可即時解決之個資事件，業務權責單位陳報主管審核後，並通報個人資料管理窗口。

5.2.若個資遭到人為竄改或失竊等涉及民、刑事案件時，應即時通報警政或檢調單位請求處理。

5.3.事故處理作業所留存之相關紀錄應至少保留1年備查或依據本校「個人資料文件管理程序書」規定控管。

5.4.為提高個資侵害發生時之處理效率及應變能力，計畫內容包含計畫之說明、系統架構、緊急連絡人員清單、協力廠商清單及作業程序（含備援及復原程序）說明。

5.5若因個資事故連帶影響其他系統或資訊基礎建設運作時，應依據本校「個人資料稽核作業程序書」填寫「個人資料管理制度矯正處理單」進行後續處理。

NUTN-PIMS-C002 個人資料保護緊急應變處理作業說明書

6.確認狀況排除

6.1個資事故處理人員於處理完成後，應確認應變措施之有效性，並回報個人資料管理窗口及業務權責單位主管，視情況調整應變措施。

6.2個資事故發生之業務權責單位主管於初步認定事故排除後，仍應嚴密監控相關資訊，並進行必要之安全清查，防止潛伏之可疑行為再發生。

6.3個資事故確認排除後，業務權責單位應再回報個人資料管理窗口後續處理情形，且由其通知本校受事故影響之相關單位或回報上級單位。

6.4個人資料管理窗口應留存紀錄，並決定是否通報主管機關或要求業務權責單位通知當事人。

6.5業務權責單位應儘速將損失彙整後通知個人資料管理窗口，由個人資料管理窗口提供予個人資料管理規範導入工作小組，負責協助本校召集人對外說明情況與處置方式。

NUTN-PIMS-C002 個人資料保護緊急應變處理作業說明書

7.檢討及改善

7.1個資事故確認處理完成後，事故發生單位應檢討現行安全控制措施之完整性，並適當修訂相關作業管理規範或建置控制措施，且於必要時召開檢討會議。

7.2事故發生單位應於事故處理完畢後，進行相關矯正預防措施，避免同類型之個資事故重複發生。

7.3各單位權責主管應監督個資事故之後續處理及安全控制之有效性。

7.4個資事故之發生單位應為個人資料稽核作業之重點，並列入追蹤管理。

7.5由個人資料管理窗口彙整「個人資料侵害事故通報與紀錄表」，並在無牽涉個人隱私與本校業務機密之情況，將事件發生原因、過程、處理方式、注意事項及改善建議等內容，以網站或電子郵件等方式提供予本校員工，以做為內部個人資料保護安全宣導及事故預防之參考。

NUTN-PIMS-D033 個人資料侵害事故通報與紀錄表(1/2)

一、通報單位基本資料

通報人基本資料	單位		電話	
	姓名		傳真	
	職稱		E-mail	

二、發生情形

發現日期	____年____月____日____時____分
簡述發生經過與內容	
事故原因	☐ 個人資料檔案遭遇竊取、竄改毀損滅失或洩漏等相關事故。 ☐ 洩漏個人資料或違反政策的故意行為重大疏失。 ☐ 販賣個人資料圖利。 ☐ 個人資料檔案遭受誤用。 ☐ 超過蒐集之特定目的處理或利用。 ☐ 未經同意蒐集個人資料。 ☐ 個人資料未應當事請求修改、刪除停止使用製給複本及閱覽權利。 ☐ 其他：

NUTN-PIMS-D033 個人資料侵害事故通報與紀錄表(2/2)

四、業務權責單位處理情形

處理人員資料	單位：＿＿＿＿＿＿＿＿＿＿ 職稱：＿＿＿＿＿＿＿＿＿＿ 姓名：＿＿＿＿＿＿＿＿＿＿ 電話：＿＿＿＿＿＿＿＿＿＿	
簡述經過及結果		
承辦人	組長	單位主管

五、本校個人資料管理窗口覆核

依 C002 個人資料保護緊急應變處理作業說明書之 5 作業守則，本事故□免通報□通報主管機關(教育部)。 結案日期____年____月____日		
本校個人資料管理窗口	組長	單位主管

1、 緊急連絡電話：秘書室 06-2133111#111。
2、 本單所通報事件若非為個資事故，陳核至權責單位主管。
3、 本單需由通報單位親自持會受事故影響單位，各受會單位需落實代理人制度，相關層級負責人員不在即由代理人或該單位主管代簽並做必要處置，再轉知負責人員，以加速通報時效。
4、 本單原稿批示後存於本校個人資料管理規範導入工作小組。

案例分享與討論

案例1.日本外包業者弄丟46萬個資隨身碟

日本兵庫縣尼崎市發生市府外包業者遺失存有46萬名市民個資等資料的USB隨身碟事件，雖然最後順利找回且資料看似未外流，但幾天來逾萬市民致電市府表達不滿等，網友也罵翻。

日本富士新聞網報導，尼崎市長稻村和美6月24日傍晚在記者會上說，裝有USB隨身碟的包包已被尋獲，造成全體市民感到困擾及擔心，「由衷致上歉意」。

這起隨身碟遺失事件發生在6月21日，當天外包公司配合廠商的一名40多歲男員工，帶著這顆存有尼崎市所有市民個資、稅務資料及受領生活補助金等資料的隨身碟外出，並在餐飲店喝完酒後遺失自己所攜帶的包包。

外包公司表示，男子並未在第一時間回報公司，而是請了一天假自己去找包包，但因為遍尋不著，最後向警方求助。

為避免隨身碟內資料外洩，警方罕見動員了約30人協助尋找遺失物，最後在大阪府吹田市內一處大樓入口處尋獲。由於包包內有行動電話，研判行動電話位置資訊在尋找過程中發揮作用。

#委商管理 #資料管理 #事件管理

資料來源：https://udn.com/news/story/6812/6415288

案例2.政院資安月報 機關密碼用鍵遭入侵

根據政院最新一期資安月報，某機關4月被發現電子郵件帳號密碼外洩，經調查後發現，外洩帳號的密碼多採用鍵盤位置排序，如1qaz@WSX，雖然符合設置密碼的長度及複雜度要求，仍遭駭客破解。

最新一期資安月報指出，蒐整今年4月政府機關的資安聯防情資共6萬9964件，比例最高為外對內連線大量阻擋事件及外部主機執，帳號持續登入失敗行掃描探測攻擊達62%；其次是網頁攻擊行為及國外IP攻擊行為的入侵攻擊類，占16%；另外的政策規則類也占15%。

另外，月報也分享4月資安事件，某機關電子郵件帳號密碼外洩，經調查後發現，外洩帳號的密碼多採用鍵盤位置排序，如1qaz@WSX，雖然符合長度及複雜度要求，仍易遭駭客暴力破解。

月報表示，政府機關規定使用者密碼設定須符合複雜度原則，駭客常採用密碼暴力破解，機關應加強宣導，避免採用鍵盤排序設定密碼或常見字符轉換的字母，降低密碼遭破解的風險。

密碼問題屢次成為資安重點，根據資安月報整理，去年政府機關多次發生因使用身分證字號、生日、電話，抑或是123456等簡單規則的弱密碼，導致資通系統遭破解、機敏資訊外洩，要求各機關資通系統應禁止使用弱密碼，並依循GCB密碼原則。

密碼仍是已知弱點，建議服務設置或開啟善用雙因子/多因子認證(Two-Factor/Multi-Factor Authentication，2FA/MFA）或動態密碼（One-Time Passwords，OTP）

#存取管理 #密碼管理 #資料管理

資料來源：https://tw.news.yahoo.com/政院資安月報-機關密碼用鍵遭入侵-115539878.html

案例3. Volvo汽車遭駭導致研發資料外洩

汽車大廠Volvo Cars上周公告，今年稍早網路遭駭，致使公司研發資料被竊。

事件發生時間不明，Volvo Cars僅說檔案資料庫遭第三方人士非法存取，並有「少量」研發資產遭竊。發現事件後，Volvo已經切斷駭客存取管道，也通報相關單位。

根據現有資訊Volvo Cars周五證實入侵事件可能對公司營運產生影響。但Volvo表示目前沒有跡象顯示客戶車輛或個資受到影響。

Volvo Cars並未提供任何事件描述，不過Bleeping Computer報導，元兇可能是勒索軟體。Snatch勒索軟體駭客組織宣稱是其所為，他們宣稱11月底成功入侵且竊走Volvo檔案。這幫歹徒還張貼了檔案螢幕截圖，並釋出近36MB的資料。

不過Volvo Cars對法新社否認此次是勒索軟體攻擊事件。

圖片來源：Volvo Cars

#資料管理 #事件公告

資料來源：https://www.ithome.com.tw/news/148328

案例4.委外廠商出包 高中職學習歷程檔案毀損遺失

高中學習歷程檔案驚傳出包意外，國教署委託開發的「校內學生歷程檔案紀錄模組」，因委外廠商操作出錯，導致其中3台硬碟裡，118所高中職學生，9月4日後上傳的資料遺失。以桃園武陵高中為例，約有300多筆資料不見，立即校內補救，不想造成實質影響，教育部則表示，已請廠商全力救援硬碟。

高中職學生從高一開始，可以上傳學習成果和多元表現，109學年第二學期受疫情影響，延後上傳到9月30日。但使用國教署委託開發，校內檔案紀錄模組的學校，9月23日夜間起陸續接獲通知，部分檔案遺失或毀損。

根據委外廠商聲明，是一開始模式設定錯誤，系統更新重新開機後，硬碟被還原，約有118校要進行資料搬移，目前已重新設定硬碟並掛載，預估今（25）日周六完成。國教署高中組組長張永傑表示：「初步掌握資料，硬碟並沒有損壞，會朝著儘快將硬碟中的相關檔案，回復的方式來處理。」

資料來源：https://news.pts.org.tw/article/546373

#委商管理 #備份管理 #營運持續

案例5.財政部國稅局爆發記帳士個資外洩 行政院列資安事件

財政部國稅局傳出資安事件。財政部中區國稅局一名承辦人在建置記帳士查詢名冊時，疑人為疏失，誤將記帳士個資檔案傳輸上網，導致身分證字號、地址、出身年月等個資全都露，目前有國外網站將這些記帳士資料備份庫存，法界人士憂心，若資料被駭客拿去「暗網」兜售，後果相當嚴重，行政院目前將此事列為資安事件處裡。

備份財政部中區國稅局資料的網站是「台灣公開資訊網」，此網站在美國註冊，設立目的想讓民眾方便搜尋政府公開資料，但沒想到卻發生誤將記帳士個資上傳一事，目前中區國稅局已緊急將資料更新下架，但「台灣公開資訊網」庫存頁面依然存在，且該網站無聯絡人，想要對方下架恐非易事，除中區國稅局外，其他分區並無此情況發生。

目前該服務已無法讀取，但DNS cache尚存在。

資料來源：https://udn.com/news/story/7314/5927958

#人員管理 #資料管理 #事件管理

tsc 遠東 TSC CAPITAL GROUP The Bridge to the Asia Pacific Region

TSC CAPITAL GROUP
The Bridge to the Asia Pacific Region

問題與討論

請掃描QR code填寫課後評量

https://forms.gle/N1nfrHPMRQWXZSRU8

TSC CAPITAL GROUP

The Bridge to the Asia Pacific Region

感謝您的參與

歡迎於活動後與講師討論您的任何疑問

本公司的臉書粉絲團及部落格可以找到更多資訊

TSC – FB Site

TSC – Blog Site