



因應新版個資法衝擊 教育體系如何應處？

交通部公路總局
王東琪主任



簡介

■ 學歷/考試

- 國立臺灣科技大學資管博士班
- 國立臺灣大學生態所博士候選人
- 美國紐約Fordham 大學資管所
- 100年公務人員高考二級考試「資訊處理類科」全國第1名
- 101年教育部公費留學考試「資訊與科技管理學門」全國第1名

■ 國際證照

- CCNA、SCJP、BS 10012 LA、ITIL、ISO 27001 LA

■ 工作歷練

- 教育部資科司分析師、科長
 - 推動教育體系個資管理制度
 - 推動教育部導入個資管理制度
- 檔管局設計師
- 明碁電通專案經理
- 資策會國防科技役

■ 經歷

- 考試院資安稽核委員
- 教育部資安稽核委員
- 交通部資安稽核委員
- 立法院主管資安講座
- 數位部智慧政府3.0 諮詢委員





大綱

一

近期業者個資外洩事件剖析

二

行政院精進措施

主管們如何協助營造資安文化

三

個資保護法修法重點

四

教育體系如何應處

五

結語



近期業者個資外洩事件剖析



iRent 40萬筆個資外洩！ 公總認定有疏失 開罰20萬限期改正

iRent資料庫暴露於公開網路不設防，引發大眾關注，配置錯誤問題應受更多重視

說明

6. 報導內容: iRent 數據庫個資外洩風險，和泰集團正式回應

7. 發生經過

擁有的
手機號

8. 因應措施

9. 其他說明

與和泰
無重大

和泰
之資料庫

iRent針對日前發生會員個資外流疑慮，引起廣大消費者不安與社會關注，向大眾致上萬分歉意。此事件發生原因為「內部用來記錄應用程式 Log 檔之暫存資料庫，因未適當阻擋外部連線，導致該資料庫可能遭外部專業資訊人員使用特定工具及技巧進入該資料庫內查詢近三個月的會員異動資料。」該暫存資料庫曾紀錄之個資包含會員姓名、電話、地址、經遮蔽之信用卡資訊(排除盜刷疑慮)、身分證、生日、Email、緊急聯絡人、申請會員上傳照片檔(經編碼)，有遭外部查詢之可能，



格上租車也傳個資外洩，1萬多人受害！ 格上火速回應：資料庫無異常下載

格上租車爆個資外洩！公總開罰10萬

格上租車表示，本次涉及存取共享車出租單之個資風險事件，經調整作業流程、強化資料防護機制後，已於2月7日將「出租單查詢功能」重新上線，提供共享車會員查詢及下載出租單使用。共享車出租單功能資訊安全改善措施包括：

1. 強化加密：開啟出租單前，需輸入密碼。
2. 檔案不落地：出租單不預先放置於儲存空間，調整為會員有檢視或下載需求時才產出，封閉外部存取可能。



事件剖析

兩大資料庫缺失

存取權控制失效

未設置存取權限，導致任何人都能連線進入資料庫。

資料處理不當

未對機敏資料進行**去識別化**，導致用戶真實資料外洩。



個資外洩事件層出不窮

個資外洩事件 數位部裁處蝦皮20萬元、誠品10萬元



博客來3000會員個資外洩元兇是境外駭侵 北檢簽結

微風遭駭 90萬用戶個資外洩

111年全年度民眾通報高風險賣場排名

高風險賣場報案排名

博客來網路書店
旋轉拍賣
蝦皮拍賣
誠品書局
迪卡儂

因電商錯誤設定
操作ATM解除

WARNING

如有接到假冒該類賣場要求謊稱設定錯誤，提到「操作ATM」、「購買遊戲點數」及「操作網路銀行」來解除「分期付款」、「訂單錯誤」等設定。請注意這一定是詐騙！
請立即撥打165反詐騙專線通報！



公私單位重大個資外洩事件

避免2023成個資外洩元年 國發會：月內提出個資專責機構籌備期程

台灣近年重大個資外洩事件	
公務單位 重大案件	民間單位 知名案件
2016年05月 「郵政商城」遭駭客侵入，逾1.7萬筆個資外洩。	2017年05月 「雄獅旅行社」遭駭客侵入，疑有逾36萬筆個資外洩，25位受害者於2018年透過消基會提出團體訴訟。後於2020年7月高等民事庭成立調解。
2016年07月 「勞動部就業通」網站遭駭客侵入，逾5.8萬筆求職者個資外洩。	2022年02月 「王品APP」遭駭案。
2019年06月 「銓敘部」個資遭販賣，逾20萬筆公務員個資外洩。	2023年01月 「iRent」個資外洩案。
2022年10月 「疑為全台戶政資料」遭販賣，逾2300萬筆台灣人個資外洩。	2023年02月 「格上租車」個資裸露案
2022年12月 「部立桃園醫院」系統疑遭駭。	
2023年01月 「健保署健保資料」遭內部人員竊取 「疑華航會員資料」遭國外論壇公布。	

近年民間公司團體個資外洩案例				
公司	時間	事件	後續	主管機關
和雲 (iRent)	2023年2月	外媒報導國外資安人員在和雲雲端伺服器發現資料庫，內有iRent約14萬會員全名、手機號碼、Email、信用卡等訊息。	<ul style="list-style-type: none"> 2/1 · 和泰車發布重大訊息 2/1 · 公路總局調查 2/4 · 和雲聲明會員資料未遭盜用並提出慰問方案 	交通部公路總局
博客來	2022年第二季	刑事局統計博客來個資外洩，接獲民眾通報遭詐騙全年達3,773件。	<ul style="list-style-type: none"> 官網加註反詐騙宣導警語、發送反詐騙宣導簡訊 	經濟部商業司
網軟	2021年7月	至少35個愛心協會及社福團體，因委託之資訊服務商網軟遭駭，導致大批捐款個資外洩。	刑事局接獲捐款民眾報案，調查後披露此事。	衛福部
誠品生活	2021年4月	「誠品線上」會員個資外洩，遭詐騙集團假冒誠品解除分期付款，刑事局統計全年反詐通報達940件。	<ul style="list-style-type: none"> 未發布重大訊息 	經濟部商業司
人力銀行	2020年10月	104約592萬筆、1111約有335萬筆求職者個資被放在中國暗網論壇販售。	104：報調查局偵查 1111：報刑事局偵查	勞動部

整理自媒體報導



行政院精進措施



防止非公務機關個資外洩精進措施

112年03月02日行政院第3845次會議

◆強化業者防護能力、完備法制、落實執法，提升個資保護

策略一

強化
聯繫會議功能

策略二

提高
個資法相關
罰則

策略三

設立
個資保護
獨立監督機關



策略一：強化聯繫會議功能(1/3)

事前

強化執法能量，提升防護能力

1 行政機關強化執法能量

- ✓ 各主管機關應成立常設之「個資行政檢查小組」，並由數位部適時行政協助。
- ✓ 各主管機關每年擬定行政檢查計畫，並對高風險業者，強化例行性行政檢查。

事中

2 業者提升個資防護能力

- ✓ 數位部協助各主管機關建立適當分級規範及技術規格。
- ✓ 各主管機關輔導所轄業者提升個資保護意識及防護措施，分階段輔導業者取得個資保護管理或資訊安全驗證。
- ✓ 金管會強化對上市櫃公司內稽內控要求，促請業者取得適當之個資保護管理或資訊安全驗證。

事後



策略一：強化聯繫會議功能(2/3)

事前

事中

事後

精進案件通報與監督程序

1 重大矚目案件強化監督流程

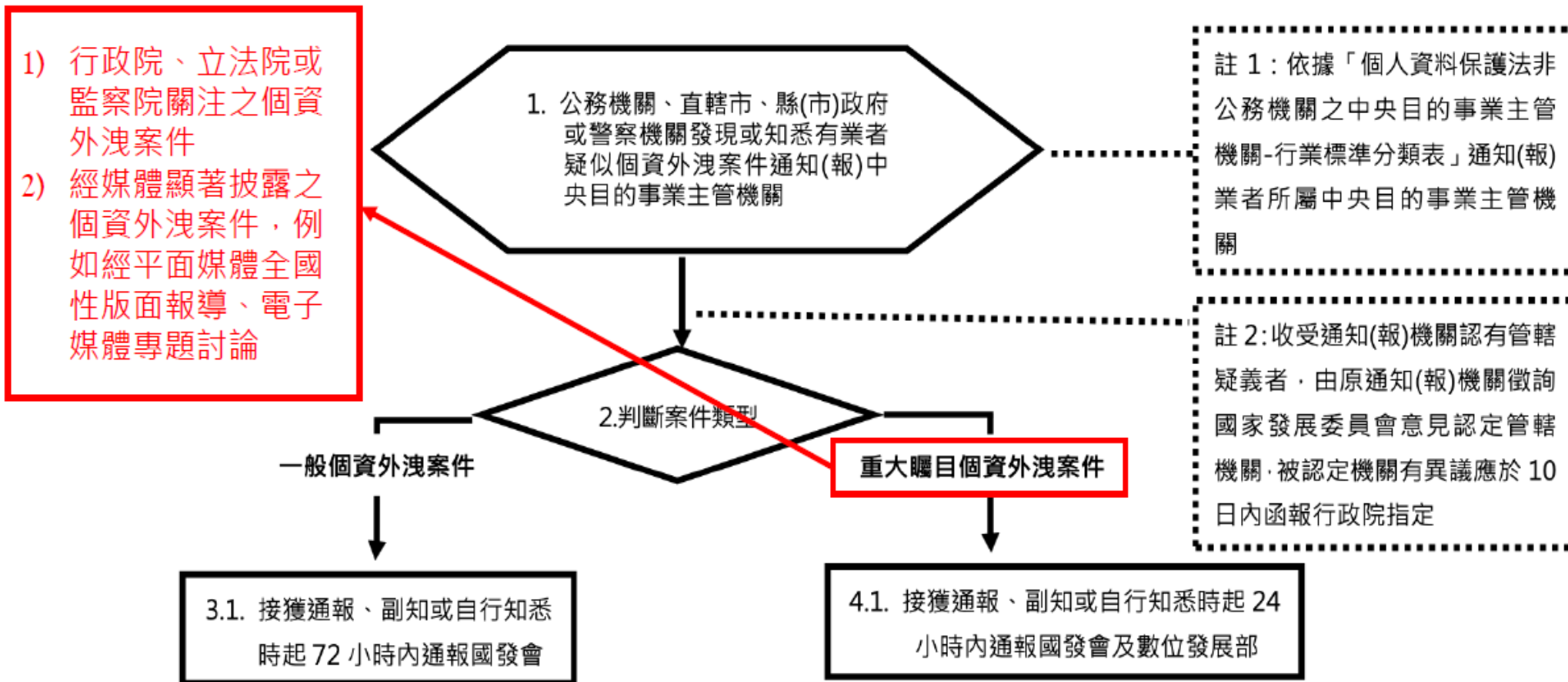
- ✓ 主管機關應於知悉後 24 小時之內通報國發會及數位部。
- ✓ 主管機關應於知悉後 3 日內進行行政調查、10 日內完成調查報告。
- ✓ 行政院於 2 週內召開會議，由主管機關說明行政調查辦理情形。

2 重大矚目案件提升行政調查能量

- ✓ 數位部參與行政調查，提供專業分析與鑑識技術協助。
- ✓ 必要時，請警政單位支援協同調查。



行政院及所屬各機關落實個人資料保護聯繫作業要點(112.05.29)





策略一：強化聯繫會議功能(3/3)

事前

事中

事後

落實執法及強化行政檢查

1 主管機關落實執法，要求業者提出改正計畫

- ✓ 非公務機關違反安全維護義務，主管機關應依個資法第 48 條規定作成命限期改正處分，要求提出改正計畫，逾期未改正，應予裁罰。
- ✓ 主管機關得依情節輕重及外洩事件造成之影響，評估適用個資法第 25 條規定。

2 高風險對象強化行政檢查

- ✓ 經濟部、衛福部、交通部、金管會及數位部，將擇定個資外洩高風險事業，於本年3~5月進行行政檢查。



策略二：提高個資法相關罰則

- 研議提高個人資料保護法相關罰則，並同步檢視其他相關法規罰則之合理性。

現況問題

- 非公務機關未採行適當安全措施防止個資外洩，應依個資法第48條，先命限期改正，屆期未改正，按次處罰新臺幣2萬元以上20萬元以下罰鍰。
 - ✓ 最高罰鍰金額上限僅為20萬
 - ✓ 須先命改正，未為改正方能處罰

後續推動

- 研議修正個資法第48條，參考相關國際立法例提高罰則。
- 各部會盤點所主管個資保護相關法規，並評估罰則之合理性。



策略三：設立個資保護獨立監督機關

● 推動獨立監督機關 必要性

- | | |
|--|---|
| 1
憲法判決：
建立統籌性
個資保護獨立
監督機制
(以114年8月為期限) | 2
落實國家人權
行動計畫：
設置獨立隱私
專責機關
(以113年5月為期限) |
| 3
國內實務監
管課題解決、
國際趨勢接
軌急迫需求 | 4
朝野立委、監
察院與各界倡
議期盼 |

● 國際以設置獨立監督機 關為趨勢

- 1** 各國普遍設置獨立監督機關
 - ✓ 至少70個國家設置個資保護獨立監督機關
- 2** 隱私相關國際組織需獨立機關方能入會
 - ✓ 如：全球隱私大會(GPA)入會會員須為具獨立性之個資保護機關
- 3** 獨立機關為取得GDPR適足性認定條件
 - ✓ 日、韓皆已成立獨立機關並取得適足性認定



個資保護法修正案



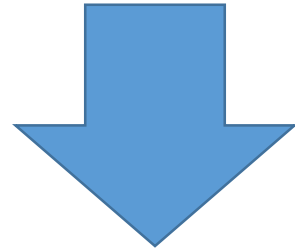
個資保護法修正案

- 112年5月16日立法院三讀通過個資法修正案。
- 促使非公務機關投入人力、技術及成本，落實保護民眾個人資料之責任，並有助於政府打擊詐欺相關政策推動。
- 另針對公務機關個資保護之強化，除落實現行資通安全管理法對於公務機關的管理規範外，未來個人資料保護委員會將以獨立專責機關的定位，整體規劃對於公務機關及非公務機關個資保護之監督機制。



修法重點(1)

- 個資法第四十八條，非公務機關違反第二十七條第一項或未依第二項訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法之裁罰方式及額度。

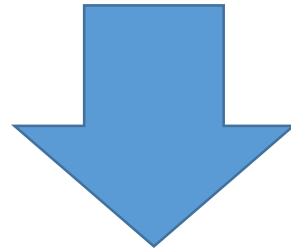


- 逕行處罰同時命改正，提高罰鍰上限，**新臺幣2萬元以上200萬元以下**。
- 情節重大者，**新臺幣15萬元以上1500萬元以下**。
- 屆期未改正者，按次處**新臺幣15萬元以上1500萬元以下**。



修法重點(2)

- 由「**個人資料保護委員會**」擔任個資法主管機關。
- 現行個資法並未設置單一專責機關。
- 落實憲法法庭判決，有關建立個資保護獨立監督機制之要求。



整合目前分屬於**中央目的事業主管機關**、**地方政府**及**國發會**的權責



修法前後比較

條文	修法前	修法後
增訂第1條之1規定	中央目的事業主管機關及地方政府 分散管理 ，並由國家發展委員會擔任個資法解釋機關	將由個資委員會擔任個資法的主管機關， 整合目前分屬的權責
增修第48條第2項及第3項規定	違反第二十七條第一項或未依第二項訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法者，中央目的事業主管機關或地方政府須 先限期命其改正 ，屆期未改正者，方得按次處新臺幣 2萬元至20萬元 罰鍰	<ul style="list-style-type: none"> ✓ 直接裁處新臺幣2萬元至200萬元罰鍰，毋須先限期命其改正； ✓ 情節重大者，罰鍰則可提高至新臺幣15萬元至1,500萬元； ✓ 屆期未改正者，按次處新臺幣15萬元以上1,500萬元以下罰鍰



違反個資法 - 行政責任

2萬-
20萬

- 先改再罰
- 蒐集個資沒有告知法定資訊
- 不讓當事人行使權利
- 違法行銷

5萬
-50萬

- 先罰再改
- 違法蒐集、處理、利用個人資料
- 違法國際傳輸個人資料

2萬-
1500萬

- 先罰再改
- 沒有做到適當安全維護
- 沒有訂定安全維護計畫
- 2萬 - 200萬
- 情節重大：15萬 -

代表人
一起罰

- 企業受罰時
- 代表人、管理人、有代表權人
- 受同額罰鍰處罰
- 除非能證明盡到防止義務



違反個資法 - 民事責任

要件

- 違反個資法規定，致個資遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。
- **除非能證明無故意或過失。**

種類

- 財產損害
- 精神損害
- 回覆名譽

範圍

- 不容易或不能證明實際損害額時，可請求法院依照侵害情節，以每人每一事件500元以上2萬元以下計算。
- 同一事件 + 多數受害人，賠償上限2億元



違反個資法 - 刑事責任

意圖為自己或第三人不法（財產）利益 或 意圖損害他人（各種）利益

違法蒐集、處理
或利用個人資料

非法變更、刪除，或以其他非
法方法妨害個資檔案正確性

足生損害於他人

處5年以下有期徒刑，
可併科100萬元以下罰金

處5年以下有期徒刑、拘役或科或併科
100萬元以下罰金



教育體系個資外洩頻仍

教育學程報名系統疑個資外洩 台大：已修復補強

台灣好報 | 2.3k 人追蹤 ☆ 追蹤

2021/6/3 18:45

0 Like

(中央社記者許秩維台北3日電) 前台大學生會長師培中心教育學程報名系統個資外洩；台大校方表示學校將檢討並強化資安和個資保護。



台灣大學前學生會長吳奕柔在臉書發文指出，昨日學程網路報名系統，發現只要輸入任何台大在學身分證字號、生日、手機電話、戶籍地址等個人資

廠商涉妨害個資法 大專院校新生個資外洩波及全台



鄧至傑 / 澎湖

2022年6月10日



搜尋公告

【400級新生注意】請不要再相信來路不明之住宿用具用品訂購單



私立專科以上學校及私立學術研究機構 個人資料檔案安全維護計畫實施辦法(110.12 28)



個資保護規劃



個資管理程序



稽核與改善



個人資料檔案安全維護

學校得指定或設管理單位或指定專人，負責個人資料檔案安全維護

推動

規劃、訂定、修正與執行本計畫，包括業務終止後個人資料處理方法等相關事項

報告

定期就執行情形向管理人報告

矯正

依據稽核人員就執行之評核進行檢討改進，並向管理人及稽核人員提出書面報告

訂規

訂定個人資料保護管理政策，將其所蒐集、處理及利用個人資料之依據、特定目的及其他相關保護事項，公告使其所屬人員均明確瞭解

訓練

定期對所屬人員施以基礎認知宣導或專業教育訓練，使其明瞭個人資料保護相關法令之規定、所屬人員之責任範圍及各種個人資料保護事項之方法或管理措施



安全維護事項有哪些可做

個資管理PIMS

組織資源配置	界定個資範圍
風險評估機制	通報應變機制
內部管理程序	資安人員管理
認知教育訓練	設備安全管理
安全稽核機制	資料紀錄保存

計畫持續改善

資安管理ISMS

資安管理政策	資訊資產管理
風險評鑑管理	實體安全管理
通信作業管理	存取控制管理
系統開發管理	委外業務管理
資安事件管理	業務持續管理
內部稽核管理	矯正改善管理

人員安全與教育訓練



ISMS/PIMS規範導入事項比較

選定控制措施





委外廠商責任由委託機關負責

電腦至阿達 | 13k 人追蹤 ☆ 追蹤

日本社福承包人員醉倒後弄丟了一個存放了 46 萬位市民個資的隨身碟

2022年6月25日 週六 下午8:32

BBC 網站在報導中引述了日本當地的報導，表示這位不具名的承包人員在下班前將這份隨身碟收到了自己的公事包中，並前往了位於大阪市西北方的尼崎市，他在當地的居酒屋喝了數個小時的酒，最終在離開後直接醉倒在路邊。當他終於酒醒後，他發現了這個重要的隨身碟早已連同自己的公事包一起不翼而飛。

尼崎市政府當局在公開聲明中表示這份隨身碟中除了包含著全體市民的名字、出生日期以及地址等基本資料之外，還記錄了許多更加機密的資訊，像是稅務細節、銀行帳號以及受社會安全局保護的家庭資訊，都是可能侵犯個人隱私的重要資訊。不過值得慶幸的是，尼崎市政府證實了存放在隨身碟中的個人資料都有進行額外的加密保護，並以一個密碼鎖上，同時也強調到目前為止還沒有出現任何試圖存取這些重要資訊的跡象或記錄。



委外監督

個資法委外監督

個資範圍、類別、目的、期間

受託者應採行的適當安全維護

複委託之受託者約定

受託者違法應通知事項及補救

委託者保留指示之事項

結束後個資之返還與刪除

定期確認執行狀況+記錄結果

資安管理法委外監督

完善資安管理措施或第三方驗證

配置專業人員

複委託與否、範圍、安全措施

涉及國安的適任性查核、管制出境

安全性檢測證明、授權證明

違法應通知及補救

結束後資料返還與刪除

其他資通安全相關措施

定期或知悉事件時執行稽核或確認



委外監督可以怎麼做



事前—明確約定

- 委託目的、類別、範圍、期間
- 權利&義務
- 安全措施
- 補救&通知事項
- 退場機制



事中—執行監督

- 低強度
—廠商自評
- 中強度
—機關提出項目，廠商提出符合性
- 高強度
—機關執行稽核



事後—退場機制

- 資料返還
- 資料銷毀
- 資料遷移？
- 你被廠商「鎖定」了嗎？



資訊廠商選擇與管理-數位部資通安全署

數位發展部資通安全署
Administration for Cyber Security, moda

關於資安署 ▾ 資安法規專區 ▾ 業務專區 ▾ 行政院國家資通安全會報 ▾ 訊息公告 ▾

首頁 > 資安法規專區 > 資安法常見問題 > 辦理受託業務-受託者之選任及監督

資安法規專區

- 資通安全管理法及子法
- 重點消息
- 資安法常見問題 **▾**
 - 納管對象及範圍
 - 資通安全責任等級分級
 - 資通安全責任等級分級之應辦事項-資安專職人力及證照
 - 資通安全責任等級分級應辦事項-其他
 - 資通安全維護計畫撰寫及實施情形填報
 - 辦理受託業務-受託者之選任及監督

辦理受託業務-受託者之選任及監督

資通安全管理法FAQ PDF

- 6.1. 委外注意事項何時要納入？ +
- 6.2. 資安法施行前已存在的委外契約，是否適用委外管理之規定？ +
- 6.3. 受託者是否必須通過第三方驗證，第三方驗證之範圍？ +
- 6.4. 何謂完善的資通安全管理措施？ +
- 6.5. 如何判斷廠商之資通安全管理措施是否"完善"由誰來判斷？（是採購單位、業務單位、資訊單位還是稽核單位）？ +
- 6.6. 若廠商通過第三方驗證，如何判斷辦理受託業務之相關程序及環境有無含括在驗證範圍？ +
- 6.7. 客製資通系統開發，是否須第三方安全性檢測？ +
- 6.8. 第三方安全性檢測包含哪些事項？ +



資訊廠商選擇與管理-國家資通安全研究院

附件 2 政府資訊委外資安檢核表

1. 委外作業資安要求

參考指引名稱		政府資訊作業委外資安參考指引			指
項次	查核項目	是否完成	對照章節	常見	
				顧問輔導	稽審
1	機關是否具備基礎資安管理意識、認知及控管措施，其資安控管措施是否(至少)包含下列項目：	N/A	3.資訊委外各階段資安要求	N/A	N
1-1	了解資訊委外所應遵循之法律、法規、命令、相關標準及指引等？		3.資訊委外各階段資安要求	○	○
1-2	具備依 ISO/CNS 27001 或其相似標準所制定之資通安全政策？		3.資訊委外各階段資安要求	○	○
1-3	具備依 ISO/CNS 27001 或其相似標準所制定之相關資安規範與程序，以便機關進行資訊委外資安需求識別時，有穩固參考基礎？		3.資訊委外各階段資安要求	○	○

附件 12 委外廠商查核項目表

○○○ (機關名單) 委外廠商查核項目表

編號：○○

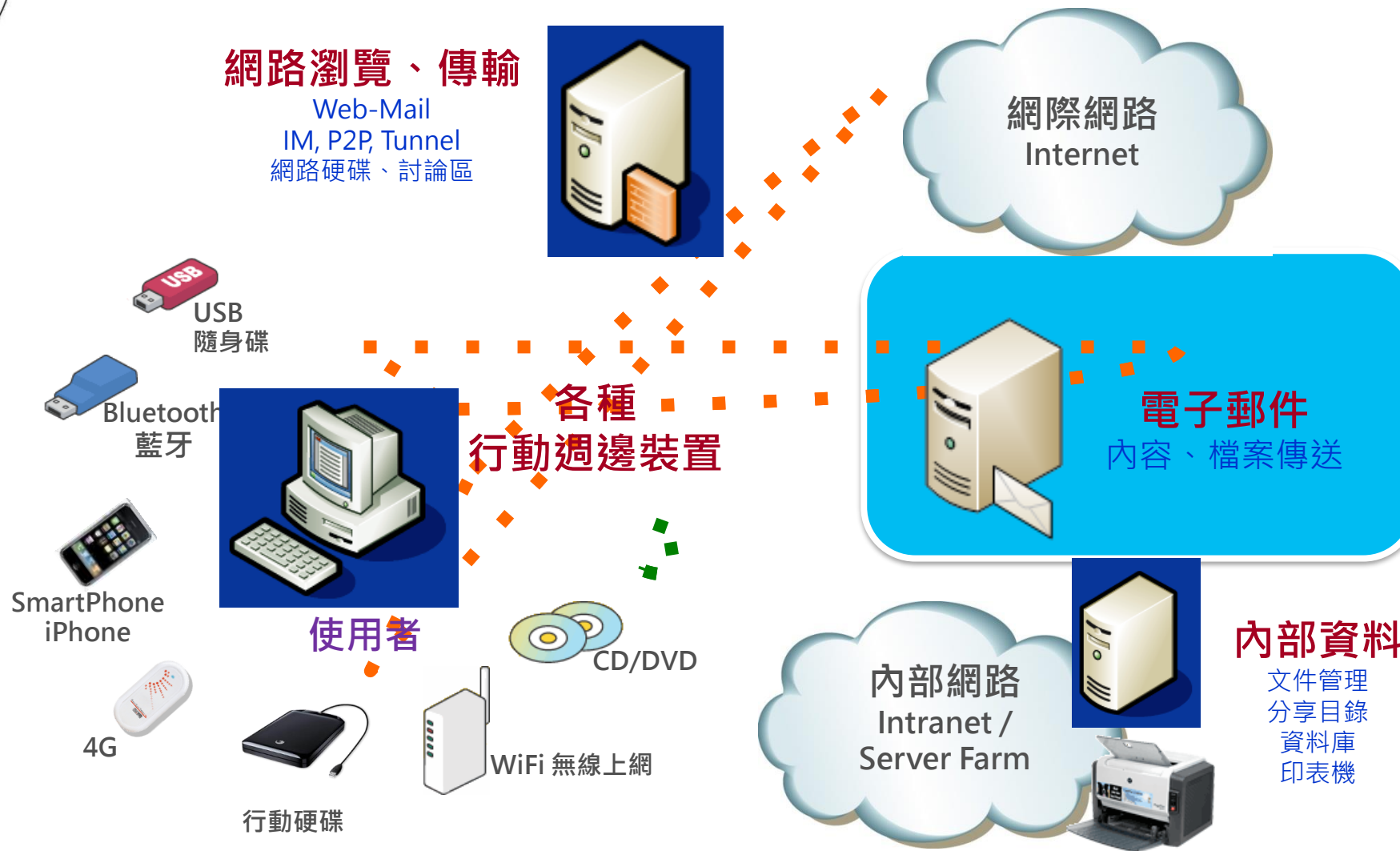
填表日期：○○○年○○月○○日

查核人員：○○○

查核項目	查核內容	查核結果			說明
		符合	不符合	未適用	
1. 資通安全政策之推動及目標訂定	1.1 是否定義符合組織需要之資通安全政策及目標？	■	□	□	已訂定資通安全政策及目標。
	1.2 組織是否訂定資通安全政策及目標？	■	□	□	政策及目標符合機關之需求。
	1.3 組織之資通安全政策文件是否由管理階層核准並正式發布且轉知所有同仁？	■	□	□	依規定按時進行教育訓練之宣達。
	1.4 組織是否對資通安全政策、目標之適切性及有效性，定期作必要之審查及調整？	■	□	□	定期進行政策及目標之檢視、調整。
	1.5 是否隨時公告資通安全相關訊息？	■	□	□	將資安訊息公告於布告欄。
2. 設置資通安全推動組織	2.1 是否指定適當權責之高階主管負責資通安全管理之協調、推動及督導等事項？	■	□	□	指派副首長擔任資安長。



個人資料可能外洩管道風險





自我檢視重點(資安面向)

資安政策與程序

應評估公司的資訊安全政策是否完整並符合法規、行業標準等相關要求，並確認是否有建立適當的資安程序以確保資訊安全。

組織與職責

應評估公司內部的組織架構是否適當，各個職責是否明確，是否有專人負責資安事宜。

存取控制

應評估公司的存取控制制度是否完整，確保資訊系統的存取權限僅限於需要的人員。

系統及應用程式開發

應評估公司的系統及其應用程式開發流程，確保開發過程中有適當的資安控制。

網路安全

應評估公司的網路安全措施是否符合相關要求，確保網路資源的安全性。

物理安全

應評估公司的物理安全措施是否適當，包括機房設備安全、門禁控制等。

災害復原計畫及演練

應評估公司是否有適當的災害復原計畫，並定期進行演練，以確保在發生災害時能及時恢復資訊系統。

事件通報與應變流程

應評估公司的資訊安全事件處理流程是否完善，並定期進行演練，確保在發生個資事件時能夠及時、適當地處理。



自我檢視重點(個資面向)

☑ 個資蒐集與處理

應評估公司蒐集、處理個人資料的適法性、適當性及正確性，確保個人資料的合法性。

☑ 個人資料保護

應評估公司是否遵循相關的個人資料保護法規，確保個人資料的保密性及安全性，確保個人資料不被洩露、竊取或濫用。

☑ 個資利用目的

應評估公司使用個人資料的合法性，確認使用個人資料的目的是否明確，是否經過事前告知並獲得同意。

☑ 個資存取控制

應評估公司的個人資料存取控制措施是否完善，確保只有經授權的人員能夠存取相應的個人資料。

☑ 個資資料安全

應評估公司的個人資料安全措施是否適當，包括個資的加密、傳輸安全、存儲安全等。

☑ 個資保留及維護

應評估公司個人資料的保留期限是否符合相關法規和政策，並定期維護保留之個資，避免違反相關法律法規。

☑ 個資事件通報

當發生個資外洩事件時，是否有通報管道可以連絡相關負責人員並採取適當的應變措施，以減少損失和風險。

☑ 個資洩漏事件處理流程及演練

應評估公司的個資安全事件處理流程是否完善，並定期進行演練，確保在發生個資事件時能夠及時、適當地處理。



自我檢視重點(系統安全)

☑ 系統架構檢查

檢查系統架構是否符合安全設計原則，是否存在單點故障、漏洞和風險等問題。

☑ 系統設置檢查

檢查公司資訊系統的安全設置，包括系統設置是否符合相關安全標準和要求，是否設置了必要的安全措施。

☑ 網路安全檢查

檢查公司網路安全是否符合相關安全標準和要求，包括防火牆、入侵檢測和防範措施等。

☑ 資料加密檢查

檢查公司資料加密技術的使用情況，確保個人資料得到有效保護。

☑ 存取控制檢查

檢查公司存取控制機制的有效性，是否按照相關規定授權訪問權限，以及記錄存取日誌等。

☑ 安全測試檢查

檢查公司資訊安全測試的情況，包括滲透測試、弱點掃描、安全評估等，以確保資訊安全風險得到有效控制。

☑ APP檢測

檢查公司是否有對公司APP進行漏洞掃描和安全檢測，發現潛在的漏洞和安全問題。

☑ 修補紀錄

檢查公司的修補紀錄，包括已知漏洞的修補措施、修補時間、修補人員等。



結語



務求法遵合規，善盡良善管理責任

- 個資法適用範圍涵蓋公私立學校，且分別負有行政、民事及刑事等責任，教育體系應嚴加重視。
- 公立學校除落實現行資通安全管理法對於公務機關的管理規範外，應強化個資保護，尤其委外管理更應著重。
- 依個資法第27條及教育部個資安維計畫實施辦法第6條規定，私立專科以上學校應訂定及執行安全維護計畫，包括業務終止後個人資料處理方法。



結合資安推動個資保護，以收綜效

- 各校可評估結合現有資安管理(ISMS)及適度導入個資管理制度(PIMS)，避免重複資源投入以達到雙贏。
- 建議未來高教深耕計畫(資安專章)應同時併入個資防護自檢表，並透過實地訪視督導各校落實情況。



感謝聆聽 · 敬請指導

THANK YOU