數位經濟相關產業個資安維辦法及案例宣導

財團法人資訊工業策進會
科技法律研究所
2025

adipd@iii.org.tw
02-66311032

個資法要求業者採取個資安全維護措施

業者責任

(個資法第27條)

- 訂定個資安全維護計畫
- 採取適當個資安全維護措施，防止導致個資事故

主管機關行政檢查

(個資法第22條)

- 例行性行政檢查
- 個案外洩行政調查

違反義務之效果

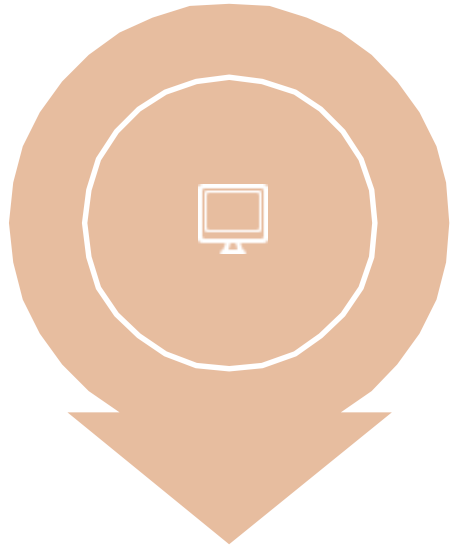
未定計畫、未採取適當安全措施、個資外洩

(個資法第48、50、25條)

- 首次違反裁罰2萬~200萬，並限期改正
- 情節重大案件，首次違反裁罰15萬~1500萬
- 逾期未改正，裁罰15萬~1500萬，並可按次連續處罰
- 可併罰代表人(與公司同一裁罰額度)
- 可公布公司名稱、代表人姓名、違反個資法情形

大綱

數位經濟相關產業
個資安維辦法宣導



安全維護措施
常見問題案例

數位經濟相關產業個資安維辦法簡介

- 本部於112年10月12日訂定「數位經濟相關產業個人資料檔案安全維護管理辦法」，提供適當安全維護措施採取標準，要求數位經濟相關產業業者加強個資保護措施

授權依據：個資法第27條第3項（§1）

適用對象：數位經濟相關產業（§2）

訂定安全維護計畫 (§3)	個資保護政策內容 (§4)	安全維護計畫內容 (§5~§17)	執行頻率分級管理 (§18)	受託者與委託者應遵循個資保護原則 (§19)

施行日（§20）

- 業者若未依本辦法採取適當安全維護措施致個資被竊取、竄改、毀損、滅失或洩漏，或未訂定安全維護計畫，本部將依個資法第48條裁罰

適用範圍

- **安維辦法第2條**

  鑒於數位發展部所管產業通常蒐集、處理或利用大量且重要之個資，其所負之安全維護責任應較嚴謹看待，因此不論蒐集之個資樣態、個資筆數或資本額多寡皆適用安維辦法

- **附表一**

行政院主計總處行業統計分類 分類編號及行業名稱		適用本辦法之行業說明
4871	電子購物及郵購業	從事以網際網路方式零售商品之行業（不含電視、廣播、電話等其他電子媒介及郵購方式）
582	軟體出版業	軟體出版業
620	電腦程式設計、諮詢及相關服務業	電腦程式設計、諮詢及相關服務業
6312	資料處理、主機及網站代管服務業	從事代客處理資料、主機及網站代管以及相關服務之行業（不含線上影音串流服務）
639	其他資訊服務業	其他資訊服務業
6699	未分類其他金融輔助業	第三方支付服務業（不含其他金融輔助業）

資服業者

訂定安全維護計畫

- **安維辦法第3條**
  業者應於本辦法施行之日起**3個月內**完成「個人資料檔案安全維護計畫及業務終止後個人資料處理方法」**(安維計畫)**之規劃及訂定，**納入符合第5條至第17條規定**之具體內容

1 **配置管理人員及相當資源**
(安維辦法第5條)

2 **界定個人資料範圍**
(安維辦法第6條)

3 **個人資料風險評估管理機制**
(安維辦法第7條)

4 **事故之預防通報應變**
(安維辦法第8條)

5 **個人資料蒐集、處理、利用內部管理程序**
(安維辦法第9、10條)

6 **個人資料之安全維護措施實作**
- 資料安全管理(安維辦法第11條)
- 人員安全管理(安維辦法第12條)
- 認知宣導及教育訓練(安維辦法第13條)
- 設備安全管理(安維辦法第14條)

7 **個人資料安全維護檢查與改善**
- 資料安全稽核機制(安維辦法第15條)
- 使用紀錄、軌跡資料及證據保存；業務終止後個資處理方法(安維辦法第16條)
- 個資安全維護整體持續改善(安維辦法第17條)

8 **其他**
- 執行頻率分級管理(安維辦法第18條)
- 受託業者與委託業者應遵循個人資料保護原則(安維辦法第19條)

分級管理：強化安全維護措施執行頻率(1/3)

- **安維辦法第18條**
  規模較大之業者(資本額1000萬以上或保有個資5000筆以上)，強化部分安全維護措施執行頻率(每12個月至少1次)

安全維護措施	執行內容	規模較小之業者	規模較大之業者
1.配置管理之人員及相當資源(安維辦法第5條)	配置管理之人員及相當資源	**隨時**	**隨時**
2.界定個資範圍(安維辦法第6條)	盤點(清查)個資檔案及筆數及界定個資範圍	**定期**	**每12個月**
3.個資風險評估及管理機制(安維辦法第7條)	進行風險評估，根據風險評估結果採取適當之安全措施	**定期**	**每12個月**
4.事故之預防、通報及應變機制(安維辦法第8條)	• 建立事故預防、通報及應變機制 • 事故發生72小時內通報	**隨時**	**隨時**

分級管理：強化安全維護措施執行頻率(2/3)

安全維護措施	執行內容	規模較小之業者	規模較大之業者
5.個資蒐集、處理或利用之內部管理程序 (安維辦法第9條)	訂有個資內部管理程序	**隨時**	**隨時**
	檢視個資蒐集目的是否已消失或期限是否屆滿	**定期**	**每12個月**
6.國際傳輸限制、告知及監督 (安維辦法第10條)	• 檢視國際傳輸限制 • 告知個資當事人國際傳輸區域	**隨時**	**隨時**
7.資料安全管理措施 (安維辦法第11條)	• 採取防止外部網路入侵對策 • 演練異常存取資料行為因應機制 • 檢測系統漏洞及修補 • 更新執行防毒軟體及檢測惡意程式 • 檢查資通系統使用狀況及存取情形	**定期**	**每12個月**
8.人員安全管理措施 (安維辦法第12條)	檢視個資存取權限	**定期**	**每12個月**

分級管理：強化安全維護措施執行頻率(3/3)

安全維護措施	執行內容	規模較小之業者	規模較大之業者
9.認知宣導及教育訓練(安維辦法第13條)	實施教育訓練	**定期**	**每12個月**
10.設備安全管理措施(安維辦法第14條)	• 採取個資儲存物保存措施 • 採取適當進出管制措施	**隨時**	**隨時**
11.資料安全稽核機制(安維辦法第15條)	實施個資安全稽核	**定期**	**每12個月**
12.使用紀錄、軌跡資料及證據保存(安維辦法第16條)	保存紀錄至少5年	**隨時**	**隨時**
13.個人資料安全維護之整體持續改善(安維辦法第17條)	持續改善	**隨時**	**隨時**
	檢視及修正安維計畫	**定期**	**每12個月**

受託者責任(1/2)

受託者須遵循委託者應遵守之個人資料相關法規，以加強保護消費者

(個資法第4條意旨、安維辦法第19條第1項)

情境案例

委託者(如A醫院)委託資服業者B架設醫療資訊系統，B又複委託C。

資服業者責任

B與C所提供之醫療資訊系統(無論賣斷、租用、代管或雲端服務)，皆須遵守數位經濟相關產業安維辦法及A醫院應遵守之醫院個資安維辦法

醫療業者A

- 應遵守醫院個資安維辦法

資服業者B

B提供之服務應遵循：

- 數位經濟相關產業安維辦法，以及
- A適用之安維辦法，**提供具有委託者安維措施標準之系統**(安維辦法第19條)

資服業者C

C於受託範圍內應遵循：

- 數位經濟相關產業安維辦法，以及
- A及B適用之安維辦法(安維辦法第19條)

受託者責任(2/2)

蒐集個資主體(委託者)

- 零售業
  (經濟部商發署主管產業)
- 從事以網際網路方式零售商品之業者
  (數發部數產署主管產業)
- 觀光旅館業
  (交通部主管產業)
- 兒童課後照顧服務業
  短期補習班業
  (教育部主管產業)
- 食品、藥品批發零售業
  化粧品批發零售業
  社福團體
  (衛生福利部主管產業)

委託提供資訊系統服務

(受託者)

資訊服務業
(數發部數產署主管產業)

遵循法令及最佳實務

資服業應遵守法令

- 個人資料保護法及施行細則
- 行政院個資聯繫會議作業要點之資料安全管理措施
- 數位經濟相關產業個資安維辦法

受託者遵循委託方之個資法令

安維辦法第19條、個資法施行細則第7條

例如
- 零售業個資安維辦法
- 數位經濟相關產業個資安維辦法
- 觀光產業個資安維辦法
- 短期補習班個資安維辦法
- 食品業個資安維辦法
- 社會福利機構個資安維辦法
- 藥品、化粧品等個資安維辦法

可參考之最佳實務文件

例如
- ISO/IEC 27001、 27701
- TPIPAS

委外監督責任

零售業、旅宿業、餐飲業、社福團體等
蒐集、處理、利用消費者個資

委託
系統建置

資服業
受託處理消費者個資

複委託

資服業
受託處理消費者個資

■ 資服業者應接受委託者之監督(個資法施行細則第8條)，以及對複受託者為監督

監督內容(重點摘要)	監督方式建議
委託者預定委託資服業，蒐集、處理或利用個資之範圍、類別、特定目的及其期間	契約約定明確之個資蒐集、處理或利用相關條款
受託者(資服業者)是否採取之適當安全措施： 資服業者提供之系統服務功能是否符合個資法施行細則第12條、本部安維辦法、受託者應遵守之安維辦法的措施要求	• 委託者自行或委外稽核 • 委託者請資服業者自評(可參數發部指引附件3~5)
受託者(資服業者)違反個資相關法規時，應向委託者通知及採行補救措施	契約要求個資事故發生時，雙方於應變時之角色及責任分配(如通知通報、修補等)

■ 雖因受託者(資服業者)致個資外洩，但委託者監督不善時，委託者仍可能被主管機關裁罰

常見錯誤案例(1/2)：資安技術

常見錯誤案例	防範措施建議
誤觸社交工程導致之帳密外洩	• **社交工程識別教育訓練** • **雙因子或多因子認證**：登入時一律驗證，或陌生裝置登入時驗證均可
資料庫存取未設定身分驗證	• **雙因子或多因子認證** • **白名單**：限定登入存取IP、或限制境外IP進入
未安裝或未更新防火牆或應用程式防火牆(WAF)	**安裝並定期更新**
未定期檢測及修補漏洞(如遭受SQL Injection攻擊)	**定期進行弱點掃描、滲透測試等資安檢測**
資料庫內資料或傳輸資料未加密	**採取雙重加密**：資料庫內及傳輸之資料隱碼或加密(金鑰另外放置，不放在資料庫內)、資料庫及傳輸通道加密
閒置系統或過期資料未刪除	**定期檢查系統狀態、刪除閒置系統或過期資料**
未定期檢查系統狀態，參數跑掉遲未發現	
安裝系統後未修改預設密碼	• 測試帳號：應由資服業者修改帳密或刪除帳號 • 一般帳號：資服業者應強制客戶更換密碼
Web(網頁服務)、AP(應用程式)、DB(資料庫)、測試區、備份區等皆未區隔	• 各功能須放置於不同伺服器，或內部分割隔離 • web應置於防火牆外的非軍事區(DMZ)

常見錯誤案例(2/2)：個資管理

常見錯誤案例	防範措施建議
被認定為個資但未確實盤點及風險評估	以下個資皆須盤點: • 員工、供應商窗口、企業客戶窗口等聯繫資料皆為個資 • 提供代管服務、SaaS服務，客戶存放於伺服器內之個資
• **未於知悉資安事故72小時內通報主管機關** • **通知當事人之內容僅為防詐騙資訊** • **員工個資外洩未通知員工**	依照個資法第12條、個資法施行細則第22條、本部安維辦法第8條規定進行通知個資當事人及通報主管機關
隱私權政策：未確實告知傳輸地點、告知之傳輸對象過於空泛、使用目的過於廣泛、行銷目的之同意與其他目的包裹同意	隱私權政策及「個資當事人知情同意」之作法，建議由專業法律人員協助建立或確認
被拒絕行銷後又寄發行銷資訊	公司內部應建立受理刪除個資要求、拒絕行銷等相關內部標記管理機制
將員工健檢資料傳到Line群組或公開權限之共用區	應加強全體員工(包含管理階層)合法個資處理利用之教育訓練
員工教育訓練僅有資安內容，無「個資保護內容」	應加強代表人及相關管理人員相關認知教育訓練：「個資保護管理制度」不同於「資訊安全管理制度」
資料安全稽核僅有資安稽核，無「個資保護稽核」	
數位跡證(如LOG、軌跡紀錄等)未保存5年	應於租用防火牆、雲端伺服器或系統時加購延長LOG保存期限

大綱

數位經濟相關產業
個資安維辦法宣導

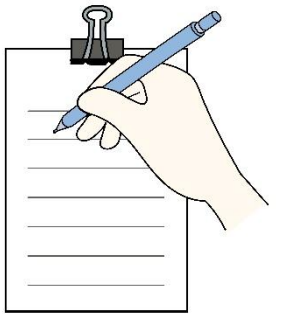
安全維護措施
常見問題案例

【安維辦法第3條】訂定安全維護計畫

Q1：公司內一定要備有一個名稱為「個人資料檔案安全維護計畫」的文件嗎?
還是有一套個資安全管理政策即可?

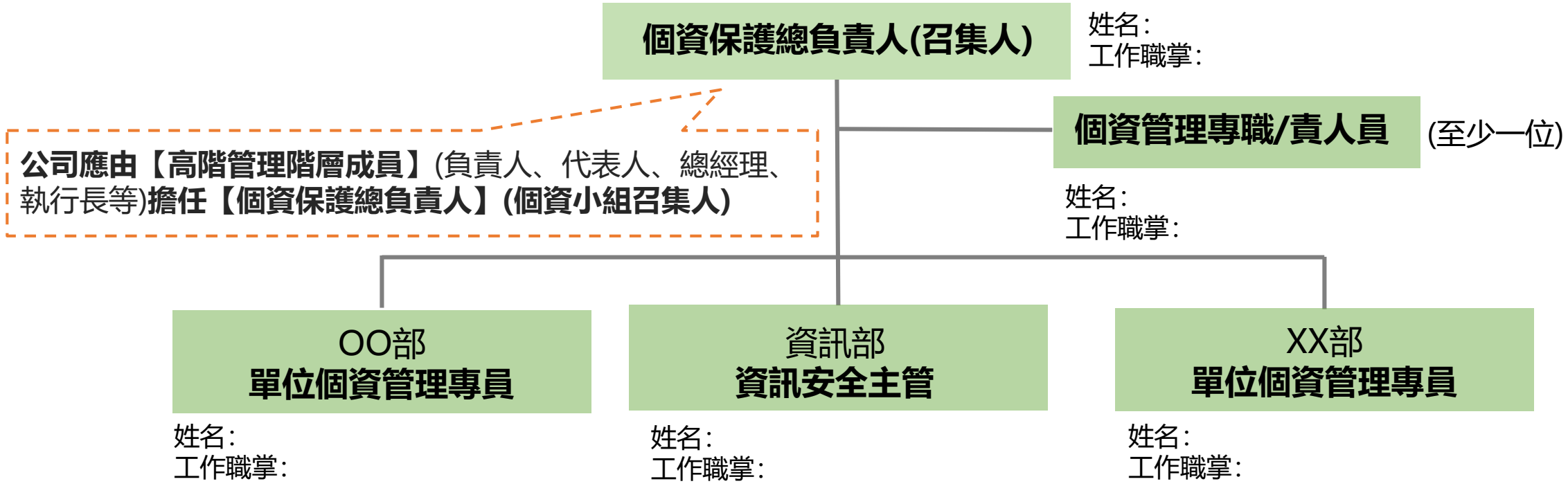
A：安維辦法第3條要求業者訂定「個人資料檔案安全維護計畫」，依照安維辦法所訂安全維護事項標準，訂定內部最高層級的個資安全管理政策

惟業者若已有一套完整的個資管理政策文件，只要該政策文件內容都有包含安維辦法的相關要求，即已訂定「個人資料檔案安全維護計畫」，不用重複作業另做一套名稱與法規相同之文件



【安維辦法第5條】配置管理之人員及相當資源

Q2：如何呈現管理人員配置？ A：繪製人員配置架構圖，並經公司代表人核定



Q3：集團子公司之個資管理執行人力，是否可由集團母公司管理成員及職員兼任?

A：個資管理執行人力(包含個資保護總負責人)應由子公司高階管理成員及職員擔任，以證明子公司具有獨立落實個資保護之能力

【安維辦法第6條】界定個人資料之範圍

Q4：公司也要針對客戶(業主)委託處理的個資進行盤點嗎?

A：為界定安全維護計畫的適用範圍，業者應確實盤點以公司自己名義保有，以及受客戶(業主)委託提供資訊服務所保有之個資數量及欄位名稱

範例

業務流程/個資檔案名稱	特定目的	個人資料類別及內容	預計處理或利用方式	處理或利用地區	處理或利用期間	資料筆數	處理及利用軌跡紀錄
員工資料	人事管理	識別個人資料(如姓名、地址、電話、電子郵件等資訊)	管理員工資料	例：台灣地區及本公司關聯方經營業務的其他國家或地區	例：至法規要求年限屆至**，或使用目的不復存在時	例：OOO筆	例：於OO系統保存資料處理及利用之行為紀錄
		辨識財務(如金融帳戶等)	給付薪資				
客戶之消費者資料	主機代管而代儲存個資	識別個人資料(如姓名、地址、電話、電子郵件等資訊)	受託儲存客戶之消費者資料	例：OO國(雲端伺服器資料中心所在地)	例：鑑賞期結束後(10日)	例：資料保存於客戶控制之資料庫*	例：於OO系統保存資料處理及利用之行為紀錄

*客戶之消費者資料保存於客戶控制之資料庫，但資料庫保存於資服業者(代)管理之伺服器時，**資服業者仍應將客戶消費者個資進行盤點，詳見Q5**

****訂有資料(涉及個資)保存年限的法規範例**

- **商業會計法**：會計帳簿及財務報表，於年度決算程序辦理終了後10年
- **職業安全衛生法**：一般體格健檢資料7年、特殊體格健檢資料10年以上
- **勞動基準法**：勞工名卡保存至勞工離職後5年；工資清冊、出勤紀錄5年

【安維辦法第6條】界定個人資料之範圍

Q5：界定公司個資範圍時，需盤點受託代營運系統或(代)管理伺服器內的個資嗎?

情境A

資服業者代維運網站或系統

資服業者須盤點代管個資

- 屬於「受委託蒐集、處理個資」情形，資服業者**須對該代管網站或系統所存取之個資進行盤點**
- 系統營運過程中，公司若會暫存系統內個資時亦屬之

情境B

資服業者受託(代)管理伺服器(含SaaS)

資服業者須盤點代管個資

- 系統及資料庫存於資服業者管理之伺服器(地端或雲端)，但資服業者通常「不具有伺服器內部資料的控制權」、「無法得知伺服器內是否含有個資」
- 由於個資仍儲存於資服業者(代)管理之伺服器內，**因此資服業者仍屬受託處理個資，負有保護伺服器安全、網路安全等義務**
- 資服業者**須對代管伺服器內儲存之個資進行盤點**，界定為安維計畫適用之範圍

情境C

資服業者賣斷系統後僅負責維護

資服業者不須盤點消費者個資

- 資服業者未受委託蒐集、處理或利用個資
- **但系統之開發政策(資安部分)仍應遵守個資法相關規範，建議可參考本部安維辦法規範以遵守個資法**

【安維辦法第7條】個人資料之風險評估及管理機制

Q6：如何做個資風險評估?

A：先評估「個資檔案價值」（個資類別之數字＋個資屬性之數字的總合數字）及「可能風險類型」，再依據資料價值評估「風險處理對策」投入成本，提出合適的風險處理對策

範例

業者可評估資料價值以投入相應成本

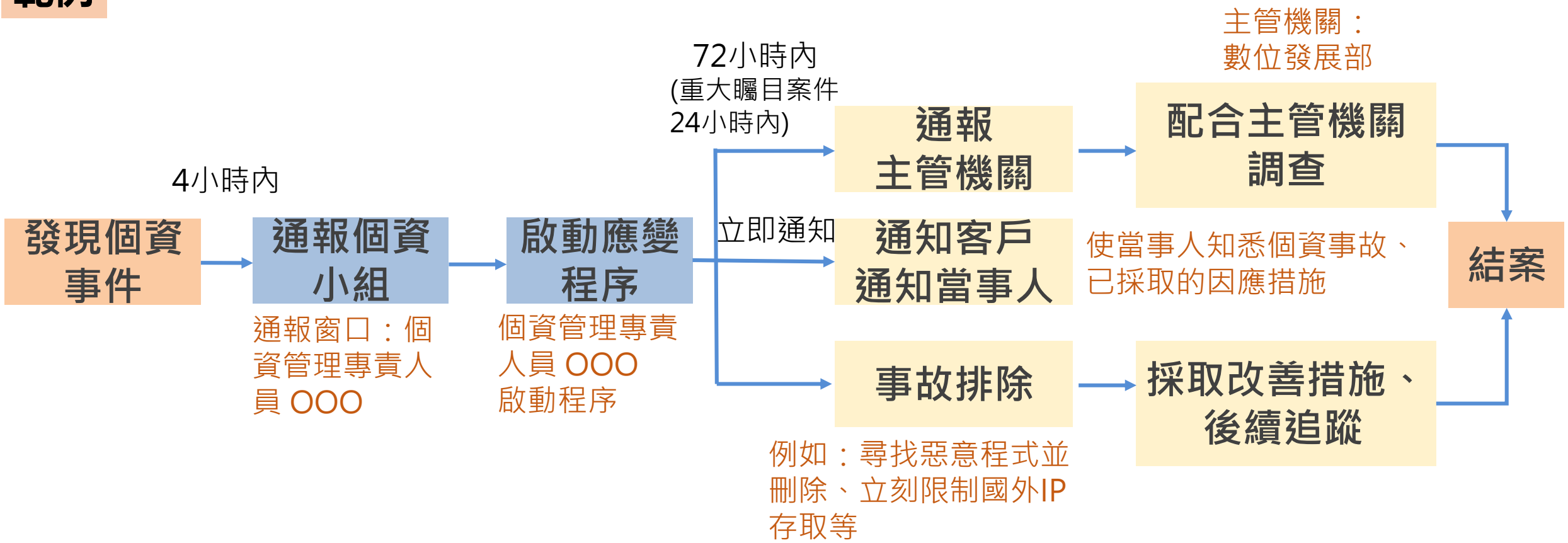
個資檔案	個資檔案價值				作業情境及內容	可能風險類型	風險處理對策
	A個資類別 1.一般 2.敏感(財務) 3.特種	B個資屬性 1.廠商 2.員工 3.消費者	C個資筆數 1.100筆以下 2.100~5000筆 3. 5000筆以上	個資檔案價值 (A+B+C, 數值越高越優先)			
例：消費者訂單	2	3	3 (OOO筆)	8	外部傳送(串接)	串接渠道有漏洞致外洩	1.尋找漏洞修正協定 2.傳輸資料隱碼
例：廠商聯絡資料	1	1	1 (OOO筆)	3	保管(地端資料庫)	中釣魚信件致資料庫遭攻擊及外洩	1.加強員工社交工程演練 2.資料庫內資料加密

【安維辦法第8條】事故之預防、通報及應變機制

Q7：事故因應流程應如何訂定?

A：發現事故後依序通報內部、通報主管機關、通知客戶及當事人、事故排除等。

範例



【安維辦法第8條】事故之預防、通報及應變機制

Q8：是否須通知客戶(業主)並協助通知消費者？通知消費者的內容為何不能只有防詐騙宣導?

A：為防止當事人2次傷害及損害擴大，請依個資法與施行細則規定通知當事人：

1、**資服業者通知客戶：**
資服業者作為受託者，發生個資外洩時，應於初步查明後，立即通知客戶發生情事及補救措施

2、**由第一線接觸消費者的客戶負責通知消費者：**
受託者應提醒客戶以符合個資法方式，初步查明後立即通知消費者，但亦可與客戶約定由資服業者負責通知

3、**通知內容：**應包括個資被侵害之事實及已採取之因應措施，僅有防詐騙宣導係違反個資法

【安維辦法第8條】事故之預防、通報及應變機制

Q9：如何通報主管機關?

	安維辦法第8條規定	數位產業署提醒
通報時點	事故發生72小時內	若屬重大矚目案件(例如媒體已大幅報導)，業者請協助於24小時內完成通報
通報條件	業者遇有個資外洩等事故，將危及其正常營運或大量當事人權益者	可參考警政署通報標準(30日內超過10件個資外洩通報可認為屬大量)
通報對象	數位發展部(數位產業署) • 電話：02-23808390 • 信箱：www-mailbox.adi.gov.tw	不宜僅報警
通報內容	利用安維辦法附表2(業者個人資料外洩通報表)	

【安維辦法第9條】個資蒐集、處理及利用之內部管理程序

Q10：隱私權政策應記載哪些內容才符合個資法?

A：公司應明確說明(1)非公務機關名稱、(2)特定目的、(3)個資類別、(4)個資利用期間、地區、對象及方式、(5)當事人依個資法第3條規定得行使之權利及方式、(6)當事人得自由選擇提供個資及不提供將造成權益影響

範例

OO公司隱私權政策

特定目的	個人資料類別(及內容)	預計蒐集、處理、利用方式	處理或利用地區	處理或利用期間
會員登入資料	識別個人資料（如會員之姓名、地址、電話、電子郵件等資訊）	取得基本資料以確認是否為本人登入使用服務	雲端伺服器(OO地區資料中心)	至使用目的不復存在時
提供商品及服務	辨識財務者（如信用卡或金融機構帳戶資訊）	購買商品或服務時付款之用	雲端伺服器(OO地區資料中心)	至使用目的不復存在時
行銷之分析	個人描述（例如：性別、出生年月日等）	客戶服務統計與研究分析	雲端伺服器(OO地區資料中心)	至使用目的不復存在時
OOO抽獎活動	識別個人資料（如會員之姓名、地址、電話、email等資訊）	行銷業務	台灣地區地端伺服器	至活動結束日

【安維辦法第10條】國際傳輸限制及告知

Q11：什麼情形下哪些業者須告知個資在境外蒐集、處理或利用的地點?

A：

情境1：我國境內蒐集個資後國際傳輸

我國或國外業者，對我國人民或他國人民個資，於我國境內蒐集，再傳輸至我國境外時，須適用我國個資法規定，告知個資國際傳輸的地點

- 業者：我國或國外業者
- 個資當事人：我國人民或他國人民個資

情境2：於我國境外蒐集個資

於我國境外蒐集我國人民個資者，**僅限我國業者須適用我國個資法**(個資法第51條第2項、法務部法律字第10703502240號函)，告知個資蒐集、處理或利用之境外地點

- 業者：限我國業者
- 個資當事人：限我國人民

【安維辦法第10條】國際傳輸限制及告知

Q12：資料若存放在國外伺服器，是否需告知客戶或個資當事人？告知內容為何?

A：若有以下情形，**應將個資傳輸/存放區域明確方式告知當事人**：

- 系統商將受託代管的個資儲存於雲端服務，該雲端服務的實體設施於我國境外時，系統商應告知客戶，使客戶能告知個資當事人(消費者)

- 跨國集團位於我國的子/分公司，將所屬人員(員工、股東等)個資提供給國外之母/總公司，或將個資存放於國外伺服器時應告知

◆委託者可於契約中要求受託資服業者明確告知國際傳輸區域(例如資料儲存的伺服器在哪個國家區域)

【安維辦法第11條】資料安全管理

Q13：若被懷疑發生個資外洩事件，如何證明沒有發生個資外洩?

A：請提供以下三項之LOG紀錄分析是否異常作為證明：事故所涉期間的
(1)網頁系統登入LOG (2)防火牆 IP LOG (3)存放個資的資料庫之存取LOG

Q14：如何精進資料安全管理措施?

A：建議至少可採取以下資料安全管理措施

建議措施	**措施範例**
登入認證機制	雙因子、多因子認證
登入及存取權限控管	綁定登入IP、強制一人一帳戶、限制帳號數、限制境外IP進入
系統架構變更	網頁架設於DMZ非軍事區；前台網頁、後台正式區、備份區與測試區皆進行區隔(放置於不同伺服器或虛擬主機)
加密	傳輸之資料隱碼或加密、資料庫加密(金鑰另外放置，不放在資料庫內)
異常檢查功能	偵測新連線或新增檔案、限制圖檔上傳格式、上傳時檢查是否為真實圖檔

【安維辦法第11條】資料安全管理

Q15：如何執行個資隱碼機制?

A:

1、**個資隱碼機制，**可分為以下方式:

A. 去識別化

B. 加密：資料庫內資料加密(如AES-256加密技術)，及傳輸加密(如SSL憑證)

2、可**「評估使用情境」**決定是否及如何採行隱碼機制，舉例如下:

A. 個資交換(傳輸、介接等)：由於外洩風險較大，原則建議可評估採行隱碼機制

B. 使用者介面:

- 建議網頁訂單查詢或後台訂單查詢等使用者介面可評估採行隱碼機制，避免個資外洩後資訊被用於詐騙或詐刷信用卡
- 若服務模式無法讓所有使用者介面的個資呈現隱碼，建議可設定每日可存取的最高數量(例如50~100筆)

C. 僅供內網使用：如通訊錄，若已採取適當安全維護措施，或可評估不採行隱碼

【安維辦法第11條】資料安全管理

Q16：如何說明服務作業流程（個資傳輸過程）？

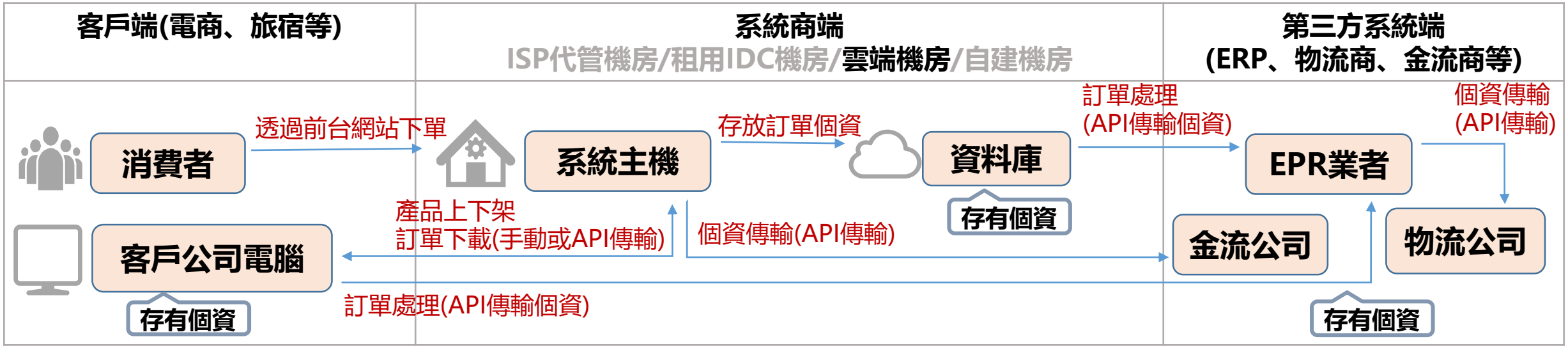
A：1、文字說明營運模式：例如

1) 系統商建置系統並提供服務給消費者

2) 系統商建置系統後賣斷但代管(或代維運)系統

3) 系統商建置系統並存放於雲端機房，或地端機房(自建機房、租用IDC機房等)

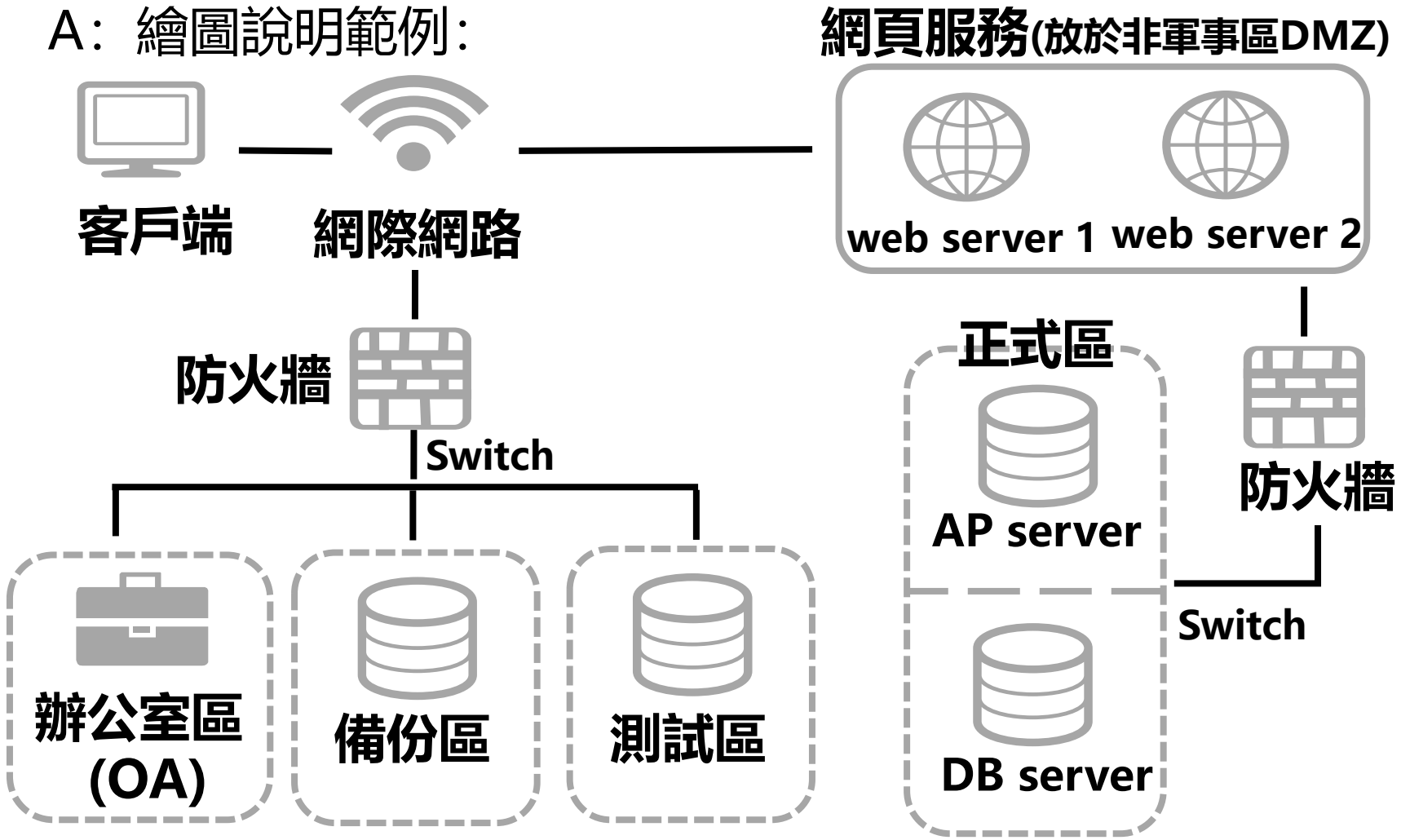
2、繪圖說明服務作業流程（個資傳輸過程），例如系統商於雲端建置系統為例：



【安維辦法第11條】資料安全管理

Q17：應如何架構系統較為安全？如何說明服務系統或網路架構圖？

A：繪圖說明範例：



系統各區宜區分隔離，使各流量不會互相接觸，例如：

1、正式區、測試區及備份區皆應放置於不同的(虛擬、雲端)伺服器，若只有一個伺服器則應在內部隔離

2、提供代管服務(或透過SaaS服務提供購物或訂房等系統)時，應將不同客戶之系統各別放置於不同伺服器內

3、網頁服務應移出Switch之外並放置於網路及防火牆間的「非軍事區(DMZ)」

【安維辦法第13條】認知宣導及教育訓練

Q18：個資保護認知宣導及教育訓練包含哪些內容?

A:

1、認知宣導與教育訓練內容應至少:

1) 個人資料保護相關法令之規定
2) 所屬人員之責任範圍
3) 業者訂定之個資安維計畫內容、各項管理程序、機制及措施等

2、認知宣導與教育訓練方式，例如:

1) 內部宣導訓練(可委託外部專家講習)，或指派人員參與外部課程
2) 社交工程(釣魚信件)演練或識別方式教學
3) 寄發宣導電子報

3、上述宣導及教育訓練紀錄應留存備份

如宣導內容、教材、參加人員簽到表、測驗成績等

【安維辦法第13條】認知宣導及教育訓練

Q19：安維辦法第13條第2項
1、業者只要對代表人、負責人或第五條所稱管理人員中任一人為教育訓練即可嗎?
2、「依安全維護計畫所擔負之任務及角色」，具體訓練內容可能有哪些呢?

A:

1、公司代表人、負責人及個資管理人員三者皆應受訓
尤其是代表人及負責人，有分配人力和資源的最高權限，若不清楚個資保護是什麼、公司個資政策有哪些，沒採取的嚴重性等，可能將不會給予公司足夠的人力及資源，該業者的個資管理可能會產生缺失

2、代表人、負責人及個資管理人員另就其於安維計畫所擔負之任務及角色受訓
例如個資法相關規範、如何主導及撰擬該公司之安維計畫內容、如何配置個資管理人員及相當資源以支持公司之個資管理等

【安維辦法第14條】設備管理措施

Q20：若想允許員工使用非公務電腦設備執行公務，要如何訂定管控機制(BYOD自帶設備政策)?

A：採行BYOD時，須注意行動裝置存取公司內部資料的過程，尤其是裝置身分識別、網路存取等級以及行動應用系統的管理措施。建議可從下列方式訂定BYOD政策：

訂定內部安全機制	• 訂定員工使用規範：例如明定存取方式、加強密碼強度 • 訂定設備管理政策：例如指定支援某幾種行動裝置、可遠端連線到哪些公司資源 • 訂定BYOD員工離退機制：例如公司使離職員工不再能遠端連線，並刪除公司資料
提供員工使用手冊與員工教育	• 可提供員工使用手冊或利用員工教育落實員工的資安觀念
試辦BYOD	• 執行 BYOD 初期， 建議先採取小範圍試辦計畫，待施行一 段時間後，視評估結果、影響範圍及衝擊，再考慮是否擴大或施行

【安維辦法第15條】資料安全稽核機制

Q21：一定要花錢委託第三方辦理稽核嗎?

A:

1、安維辦法第15條沒有限定稽核方式，因此業者可評估自身條件，選擇
   - 員工採取「自我檢查」後繳回自檢表(可參考資服業個資指引附錄4自檢表)
   - 個資管理小組進行「內部稽核」
   - 委請第三方進行「外部稽核」
2、稽核範圍為本部安維辦法第5~17條要求之措施

資服業者落實個人資料安全維護計畫自我檢查/內部稽核表		
公司名稱	檢查/稽核時間	檢查/稽核人員
編號	自我檢查/內部稽核項目	自我檢查/內部稽核說明
1.配置管理之人員及相當資源		
1.1配置個資保護總負責人		
1.1.1	由高階管理者擔任個資安全總負責人	□由_____擔任 □訂定公司內部權責 □檢驗措施皆正確執行
1.2建立個資小組及配置個資管理專員		
1.2.1	建立個資小組	□建立個資小組 □修訂安全維護計畫
1.2.2	配置管理人員(一位或以上)	□有配置管理人員 □(建議)為專責人員

【安維辦法第16條】個資使用紀錄、軌跡資料及證據保存

Q22：業者若租用雲端伺服器服務蒐集、處理或利用個資，如何保存相關LOG紀錄?

A：

1. 請務必向雲端服務提供者申請加值服務，以保存相關LOG
2. 若雲端服務提供者提供之LOG保存期間，未達法規要求期限(如數位經濟相關產業安維辦法規定保存5年)，則業者須自行隨時下載LOG，並保存放於其他設備(如地端設備)

Q23：為何相關LOG紀錄要保存5年?

A：為督促業者留存相關LOG紀錄，以利於疑似個資外洩事件的調查或訴訟審理中進行舉證，因此參考個資法第30條損害賠償責任時效期間，規定相關LOG紀錄應至少留存5年，以利業者自身、委託客戶或主管機關進行相關監督稽核

【安維辦法第16條】業務終止後個人資料處理方法及紀錄

Q24：業務終止後不處理閒置個資、設備、網頁系統，可能造成的結果及處理方式

A：

	可能事故	預防事故之處理方式
網頁系統	閒置網頁之可能漏洞遭SQL Injection攻擊	閒置網頁刪除，或隔離至不會接觸到外網之空間
設備	閒置機台若仍連接內網，可能因其他OA設備誤觸社交工程而被駭客接觸	閒置機台不連網，或盡快報廢消磁
	過期之紙本資料、公用可攜式設備等遺失，或被離職員工帶到新任職單位	• 提供新版本之資料及設備時，繳回或刪除舊版本 • 離職員工應繳回所有設備、銷毀資料
個資	利用期限已屆滿之個資，被駭客竊取進而不法利用	• 時常檢視個資蒐集目的是否已消失或期限是否屆滿 • 已消失或屆滿之個資須刪除

【安維辦法第18條】強化安全維護措施執行頻率

Q25：哪些規模大的業者，需要於多久時間內至少執行一次安全維護措施?

規模較大之業者(資本額1000萬以上或保有個資5000筆以上)，強化部分安全維護措施執行頻率(每12個月至少1次)

安全維護措施	執行內容	規模較小之業者	規模較大之業者
1.配置管理之人員及相當資源(安維辦法第5條)	配置管理之人員及相當資源	隨時	隨時
2.界定個資範圍(安維辦法第6條)	盤點(清查)個資檔案及筆數及界定個資範圍	定期	每12個月
3.個資風險評估及管理機制(安維辦法第7條)	進行風險評估，根據風險評估結果採取適當之安全措施	定期	每12個月
4.事故之預防、通報及應變機制(安維辦法第8條)	• 建立事故預防、通報及應變機制 • 事故發生72小時內通報	隨時	隨時

【安維辦法第18條】強化安全維護措施執行頻率

安全維護措施	執行內容	規模較小之業者	規模較大之業者
5.個資蒐集、處理或利用之內部管理程序 (安維辦法第9條)	訂有個資內部管理程序	隨時	隨時
	檢視個資蒐集目的是否已消失或期限是否屆滿	定期	每12個月
6.國際傳輸限制、告知及監督 (安維辦法第10條)	• 檢視國際傳輸限制 • 告知個資當事人國際傳輸區域	隨時	隨時
7.資料安全管理措施 (安維辦法第11條)	• 採取防止外部網路入侵對策 • 演練異常存取資料行為因應機制 • 檢測系統漏洞及修補 • 更新執行防毒軟體及檢測惡意程式 • 檢查資通系統使用狀況及存取情形	定期	每12個月
8.人員安全管理措施 (安維辦法第12條)	檢視個資存取權限	定期	每12個月

【安維辦法第18條】強化安全維護措施執行頻率

安全維護措施	執行內容	規模較小之業者	規模較大之業者
9.認知宣導及教育訓練 (安維辦法第13條)	實施教育訓練	定期	每12個月
10.設備安全管理措施 (安維辦法第14條)	• 採取個資儲存物保存措施 • 採取適當進出管制措施	隨時	隨時
11.資料安全稽核機制 (安維辦法第15條)	實施個資安全稽核	定期	每12個月
12.使用紀錄、軌跡資料及證據保存(安維辦法第16條)	保存紀錄至少5年	隨時	隨時
13.個人資料安全維護之整體持續改善(安維辦法第17條)	持續改善	隨時	隨時
	檢視及修正安維計畫	定期	每12個月

【安維辦法第18條】強化安全維護措施執行頻率

Q26：安維辦法第18條關於個人資料的筆數，其定義為何?

A：個資法未定義個資筆數的計算方式，實務上也無特定計算方式。建議可依公司自身業務流程，或公司實際個資檔案保存方式等作法，以自然人為基準計算，例如：

1、依公司自身業務流程：以每一自然人之每一蒐集特定目的計算

- 「王小明_20歲_電話09********」用於A特定目的算一筆資料
- 「王小明_20歲_電話09********」用於B、C特定目的則算兩筆資料

2、個資檔案保存方式計算：

- 個資分散儲存於不同檔案：若2個檔案內皆有同一自然人王小明的個資，計2筆
- 所有個資已彙整於同一檔案：同一自然人，不論欄位和特定目的，皆以1筆計

【安維辦法第19條】受託者應遵循委託者適用之法規

Q27：資服業者受託開發系統服務蒐集、處理或利用個資時，須遵守哪些個資法規範?

A：受託開發系統蒐集、處理或利用個資時，應同時遵守以下法規之要求及標準：

- 個資法及個資法施行細則
- 數位經濟相關產業個人資料檔案安全維護管理辦法
- 委託者的中央目的事業主管機關所訂定之個資安維辦法

情境案例

醫療業者A

- 應遵守醫院個資安維辦法

資服業者B

B提供之服務應遵循：

- 數位經濟相關產業安維辦法，以及
- A適用之安維辦法，**提供具有委託者安維措施標準之系統**

資服業者C

C於受託範圍內應遵循：

- 數位經濟相關產業安維辦法，以及
- **A及B適用之安維辦法**

【安維辦法第19條】受託者應遵循委託者適用之法規

數位發展部 數位產業署
Administration for Digital Industries, moda

Q28：資服業者與委託客戶間的契約應如何約定個資相關條款?

A：至少於契約中盡可能明確約定以下內容：

1、資服業者權利義務

1) 資服業者將配置於系統之各項安全維護措施；若因客戶預算考量而欲排除預設的安全維護措施，也應載明清楚

2) 資服業者可存取、處理個資之權限(並遵守最小化原則)

2、委託客戶權利義務

1) 委託客戶應具備之設備規格(安全維護環境，如安裝防毒軟體或防火牆、定期更換密碼且有一定強度、自備伺服器時作業系統達一定等級、有防範釣魚信件之訓練等)

2) 客戶可至資服業者處稽核，或要求資服業者定期繳交稽核報告及資安檢測報告

3、發生個資外洩時，雙方於應變時之角色及責任分配(如通知通報、修補等)

【安維辦法第19條】受託者應遵循委託者適用之法規

Q29：安維計畫如何包含委託者適用法規之內容?

A:

1、先分別盤點公司針對以下情境，各自應遵循的規範標準

- 資服業者以自己名義蒐集、處理或利用個資時，公司自身應遵循的規範標準
- 資服業者受託蒐集、處理或利用個資時，委託者應遵循的規範標準
- 資服業者受託建置系統時，委託者應遵循的規範標準

2、再分別將符合各個自應遵循的規範標準，訂於公司之安維計畫中

- 可選擇將所有應遵守標準訂於一套安維辦法
- 亦可針對不同專案情境，各別另訂安維計畫或系統開發政策

【安維辦法第19條】委託者應監督受託者

Q30：資服業者如何監督(複)受託者?

A：資服業者身為乙方，若想再複委託時，依個資法施行細則第7、8條規定，監督丙方(複受託者)，於受託範圍內遵循：

- 數位經濟相關產業安維辦法
- 資服業者之委託者(甲方、業主)適用之個資安維辦法及其他個資、資安相關規範

甲方(業主)
蒐集、處理、利用消費者個資

委託

資服業(乙方)
受託處理消費者個資

複委託

資服業(丙方)
受託處理消費者個資

項次	自評內容	自評結果	說明
個資保護政策與安全維護計畫			
1	是否訂定個人資料保護管理政策，並對內公開周知？	□符合 □不符合 □不適用	
2	是否訂定個人資料檔案安全維護計畫或適當安全維護措施或建置通過第三方驗證之資訊安全管理系統並公布施行？	□符合 □不符合 □不適用	
個人資料生命週期行為規範			
3	對於個人資料之蒐集、處理或利用之範圍、類別、特定目的與期間是否明確律定？	□符合 □不符合 □不適用	
4	對於個人資料之蒐集、處理、利用、傳輸或刪除，是否訂定管理作業程序並公布施行？	□符合 □不符合 □不適用	
個人資料盤點與風險管理			
5	對所保有之個人資料，是否定期實施	□符合	

【其他】系統開發政策

Q31：系統開發政策該如何訂定?

A:

1、客戶使用的系統可能接觸個資時，系統的安全維護措施應遵守個資法相關規範，因此資服業者宜訂定系統開發政策(包含資安維護部分)

2、系統開發政策可參考SSDLC(安全的軟體發展生命週期)及本部安維辦法第11條

需求	設計	開發	測試	部署維運
例如: • 系統防護需求分級 • 遵守本部安維辦法及客戶適用法規	例如: • 考量資安威脅，進行「威脅建模分析」，分析及分類程式資安風險	例如: • 預防OWASP TOP 10 常見漏洞 • 建置權限控管、加密、LOG等機制	例如: • 源碼檢測(靜態分析) • 弱點掃描或滲透測試(動態分析)	例如: • 安裝後刪除或修改測試帳號 • 軟體的(最新)版本控制及更版機制 • 異常行為監控預警 • 備份機制

按讚、加入粉絲專頁

JOIN ADI FB！

掃描 QR CODE

數位發展部數位產業署

感謝聆聽　Thank You!

【附件1】數位經濟相關產業適用對象及本署聯絡窗口

分類編號及行業名稱		適用本辦法之行業說明	本署聯絡窗口
4871	電子購物及郵購業	從事以網際網路方式零售商品之行業（不含電視、廣播、電話等其他電子媒介及郵購方式）	平臺經濟組 電話：02-23808315
582	軟體出版業	軟體出版業	【線上遊戲】平臺經濟組 楊銘澤 視察 電話：02-23808331 【套裝軟體】數位服務組 電話：02-23808011
620	電腦程式設計、諮詢及相關服務業	電腦程式設計、諮詢及相關服務業	【資服產業】數位服務組 尤振宇 視察 電話：02-23808035 【資安產業】新興跨域組 謝書華 技正 電話：02-23808414 【實境體感】平臺經濟組 王雅萱 專員 電話：02-23808333
6312	資料處理、主機及網站代管服務業	從事代客處理資料、主機及網站代管以及相關服務之行業（不含線上影音串流服務）	
639	其他資訊服務業	其他資訊服務業	
6699	未分類其他金融輔助業	第三方支付服務業（不含其他金融輔助業）	平臺經濟組 蘇凌平 科員 電話：02-23808323

【附件2】法遵資源

- **個資法** https://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=I0050021
- **安維辦法：**數位經濟相關產業個人資料檔案安全維護管理辦法
  https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=K0010162
- **指引：**資訊服務業者落實個人資料保護暨資訊安全參考指引
  https://www-api.moda.gov.tw/File/Get/adi/zh-tw/QlNCZLlBl7xoF5G

- **範本：**安全維護計畫範本word檔 & 常見問題QA
  https://stli.iii.org.tw/model.aspx?no=179
- **宣導影片：**https://youtube.com/playlist?list=PLzHI_Rr862REDf4DjRLx-GmpchCjyiMTz&si=40McwCR6M9e0l7n4
- **線上諮詢：**個資安維計畫線上健檢諮詢報名
  https://stli.iii.org.tw/news-detail.aspx?no=16&d=126
- **聯絡窗口：**
  adipd@iii.org.tw **02-66311032**

安全維護計畫範本WORD檔

【附件3】其他參考資源

- **臺灣電腦網路危機處理暨協調中心(TWcert/CC)**

  申請加入會員/訂閱資安事件訊息

  https://www.twcert.org.tw/tw/mp-1.html

- **數位發展部 網路詐騙通報查詢網APP**

  網路上看到疑似詐騙訊息，可將訊息網址貼到APP中，查詢或通報詐騙

  - 安卓版：https://play.google.com/store/apps/details?id=com.fraud.buster.prod
  - iOS版：https://apps.apple.com/tw/app/網詐通報查詢網/id6587570857

- **內政部警政署 165全民防騙網**

  提供近期民眾遭遇詐騙之事件、防詐宣導資源

  https://165.npa.gov.tw/#/