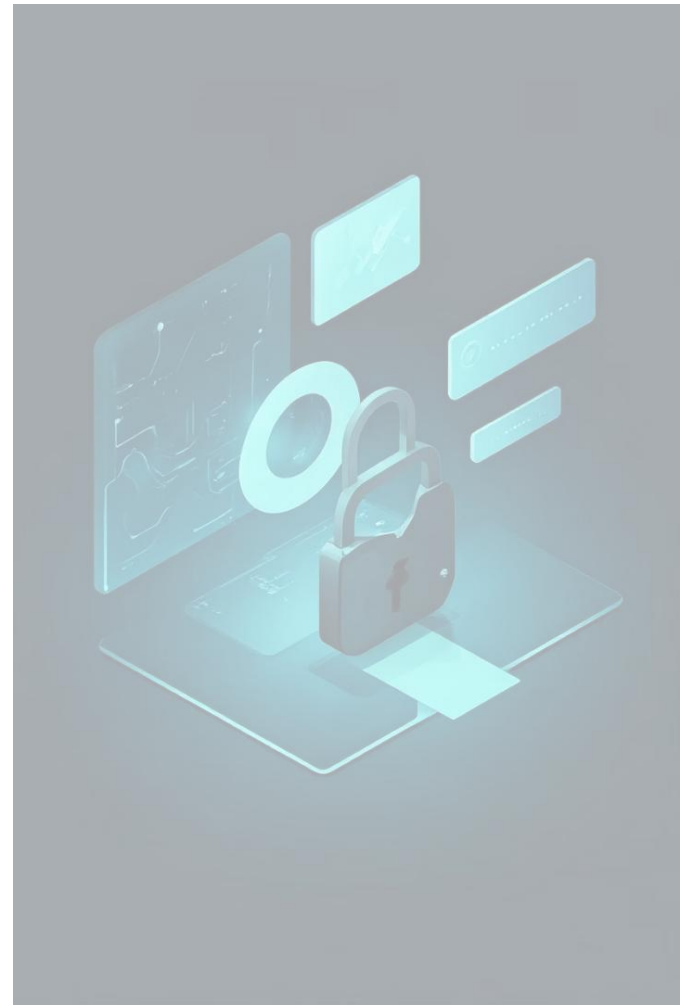




觀光署-115年度行政檢查計畫資安顧問服務案

季簡報

115年9月





目錄

一、共通性問題

二、個案問題分析

- 觀光業者個資外洩分享

- 近期事件分享

三、參考資料



一、共通性問題





一、共通性問題

- 本季稽核業者(旅行社)名稱如下：

項次	業者名稱	項次	業者名稱	項次	業者名稱
1	盈達旅行社	10	馨樂旅行社	19	天華旅行社
2	喜滿客旅行社	11	耀動國際旅行社	20	台灣近畿國際旅行社
3	遠達國際旅行社	12	海外台商旅行社	21	天意旅行社
4	晴天國際旅行社	13	京城天下旅行社	22	台灣英達旅行社
5	大榮國際旅行社	14	華府旅行社	23	偉輪旅行社
6	台北國際聯合旅行社	15	福洋國際旅行社	24	山水旅行社
7	歡樂旅行社	16	行邦旅行社		
8	金銀島旅行社	17	美最時旅行社		
9	新晨旅行社	18	鋼友旅行社		

一、共通性問題

- 本季查核家數24家，以下提出超過35%(約9家)以上業者不符合之問題，列為共通性問題討論。

項目
3.界定個人資料之範圍
4.個人資料之風險評估及管理機制
6.1資料蒐集、處理是否具備特定目的並具有法定要件？
6.2個人資料之利用，是否符合特定目的之範圍？
7.2是否依其業務特性、內容及需求，設定所屬人員接觸消費者個人資料之權限，並定期檢視其適當性及必要性？
8.1是否定期對實施所屬人員之個人資料保護與管理認知宣導及教育訓練？所屬人員是否明瞭上課內容？
10.1是否每年定期由適當組織執行資料安全內部稽核並提出評估報告？
10.2是否採取改善措施以持續改善資料安全維護？
11.3是否保存個人資料或儲存個人資料媒體之刪除、停止處理、利用或銷毀之原因、方法、時間及地點等紀錄？
11.5是否保存消費者個人資料之蒐集、處理及利用紀錄，以及自動化機器設備之軌跡資料？
12.1是否定期就個人資料安全維護議題召開會議並提出持續改善報告？
13.5是否要求受託者認委託機關之指示有違反本法、其他個人資料保護法律或其法規命令者，應立即通知委託機關？



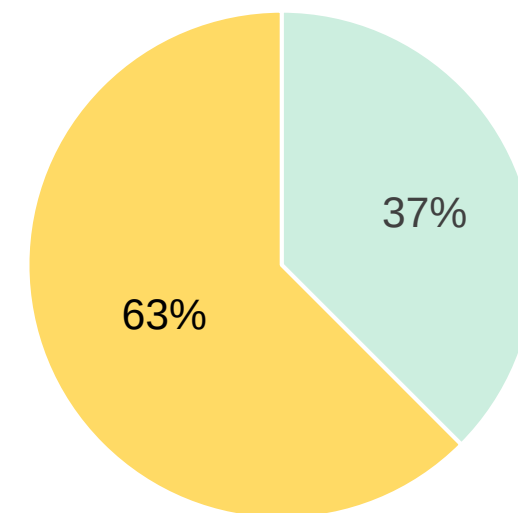
注意：上述查核項目均為法規要求事項，故有不符合應儘速進行改善。

一、共通性問題

查核項目：3.界定個人資料之範圍

查核內容：是否每年**定期清查**其所保有之個人資料檔案及其蒐集、處理或利用個人資料之作業流程，據以建立個人資料檔案清冊及個人資料作業流程說明文件？

■ 符合
■ 不符合



	- 個人資料檔案清冊。 - 個人資料作業流程說明文件。
佐證資料	
	- 公司業務流程中會碰到民眾個資之流程皆須盤點。 - 個人資料檔案清冊內容應包含蒐集目的、蒐集項目，以及完整個資生命週期(蒐集、處理、利用、儲存、銷毀)。
資料準備提醒	
	- 未「文件化」個人資料檔案清冊及個人資料作業流程說明文件。 - 僅盤點部分業務流程，未包含公司全部涉及個資之業務流程。 - 個人資料檔案清冊，蒐集目的及蒐集項目內容未依法規「個人資料保護法之特定目的及個人資料之類別」進行填寫。
常見不符合態樣	

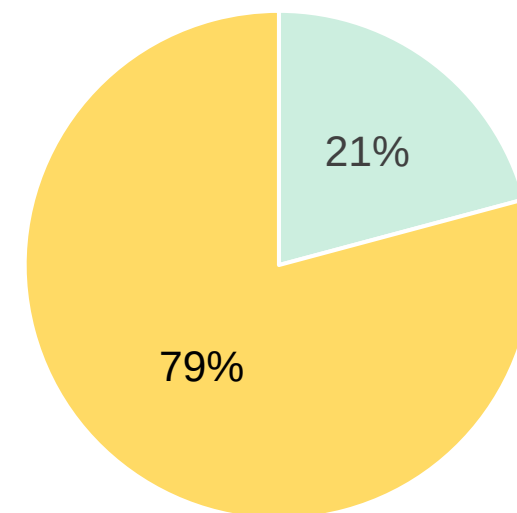
一、共通性問題

查核項目：4.個人資料之風險評估及管理機制

查核內容：是否每年**定期評估**其因蒐集、處理或利用個人資料可能面臨的法律或其他風險，並訂定適當之管控及因應措施？

■ 符合

■ 不符合



	1. 風險評估過程底稿。 2. 風險評鑑報告。 3. 風險處理計畫。
佐證資料	
	1. 應定義風險評估之方法論，並根據方法論訂定可接受風險值。 2. 如有超出可接受風險值之項目，應備有風險處理計畫或過程。
資料準備提醒	
	1. 未「文件化」風險評估過程底稿、風險評鑑報告及風險處理計畫等說明文件。 2. 未訂定可接受風險值或未針對超出可接受風險值項目進行風險處理。 3. 風險評估過程底稿與前項個人資料檔案清冊項目無法對應。
常見不符合態樣	

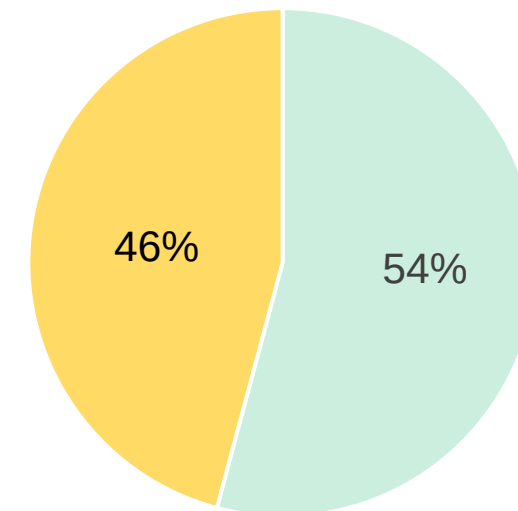
一、共通性問題

查核項目：6.蒐集、處理、利用作業

查核內容：6.1資料**蒐集、處理**是否**具備特定目的**並具有法定要件？

6.2個人資料之**利用**，是否**符合特定目的**之範圍？

■ 符合
■ 不符合



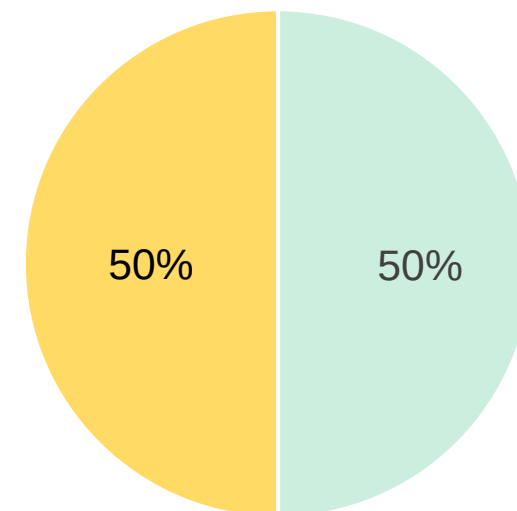
	1. 最新之個人資料檔案清冊。
佐證資料	
	1. 個資蒐集目的及蒐集項目內容應依法規「個人資料保護法之特定目的及個人資料之類別」進行填寫。
資料準備提醒	
	1. 未「文件化」個人資料檔案清冊。 2. 提供「未更新」之個人資料檔案清冊。 3. 個資蒐集目的及蒐集項目內容未依法規「個人資料保護法之特定目的及個人資料之類別」進行填寫。
常見不符合態樣	

一、共通性問題

查核項目：7. 資料安全管理及人員管理

查核內容：7.2是否依其業務特性、內容及需求，設定所屬人員接觸消費者個人資料之權限，並定期檢視其適當性及必要性？

■ 符合
■ 不符合



	1. 帳號權限清查紀錄。
佐證資料	
	1. 依個人資料檔案清冊盤點，了解是誰會碰到個資，相關資料夾或是系統權限均須進行帳號權限清查。
資料準備提醒	2. 帳號權限清查紀錄，至少包含但不限於「帳號名稱」、「權限」、「部門名稱」、「使用者」。
	1. 未「文件化」帳號權限清查紀錄。
常見不符合態樣	2. 帳號權限清查紀錄僅包含系統應用程式，遺漏清查作業系統、資料庫帳號。亦或者未清查可存放個資檔案之資料夾權限。

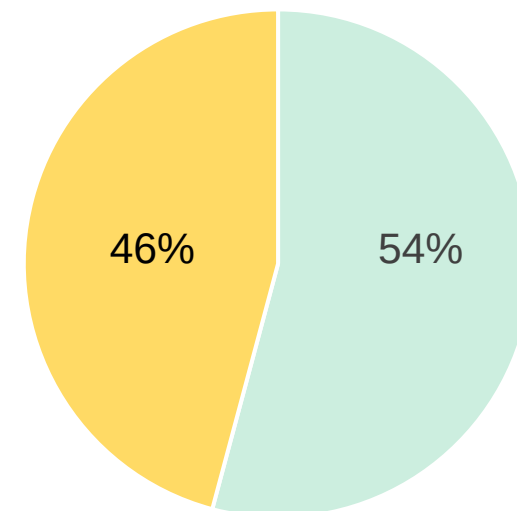
一、共通性問題

查核項目：8.認知宣導及教育訓練

查核內容：8.1是否定期對實施所屬人員之個人資料保護與管理認知宣導及教育訓練？

所屬人員是否明瞭上課內容？

■ 符合
■ 不符合



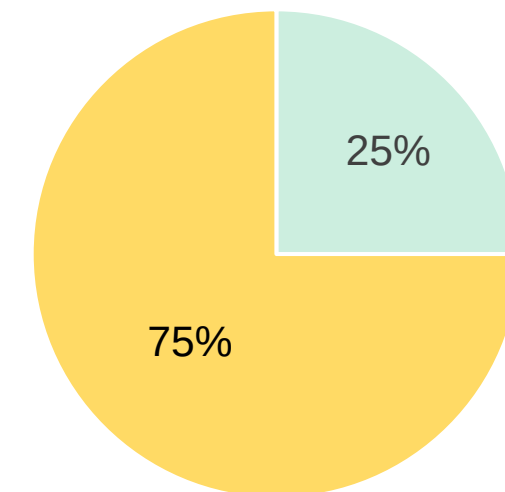
	1. 教育訓練課程內容。 2. 上課人員簽到表(需含授課日期)。
佐證資料	3. 課後測驗結果或同仁明瞭上課內容之佐證。
	1. 上課內容應包含個人資料保護相關法令之要求、人員之責任範圍及各項個人資料保護相關作業程序。
資料準備提醒	2. 有接觸到個資的同仁務必參與教育訓練。
	1. 僅提供教育訓練課程內容，未包含「簽到表」、「課後測驗結果」。 2. 教育訓練內容未包含個資保護、個資法令法規要求及人員責任範圍。
常見不符合態樣	3. 僅部分同仁代表接受教育訓練，未包含「所有接觸個資之同仁」。

一、共通性問題

查核項目：10. 資料安全稽核機制

查核內容：10.1是否每年定期由適當組織執行資料安全內部稽核並提出評估報告？

■ 符合
■ 不符合



	1. 內部稽核報告。
佐證資料	
	1. 資料安全稽核機制之作法建議寫在安全維護計畫中，且應包含「稽核之頻率」及「執行方式」。
資料準備提醒	2. 稽核報告內容須包含但不限於「日期」、「稽核範圍」、「稽核項目」、「稽核人員」。
	3. 稽核報告內容應提出是否有不符合事項或待改善事項。
	1. 稽核報告未呈現「稽核範圍」，無法確認有接觸到個資之單位是否都已納入稽核範圍。
常見不符合態樣	2. 稽核報告未呈現「稽核項目檢查結果」，僅說明本次稽核無不符合事項。

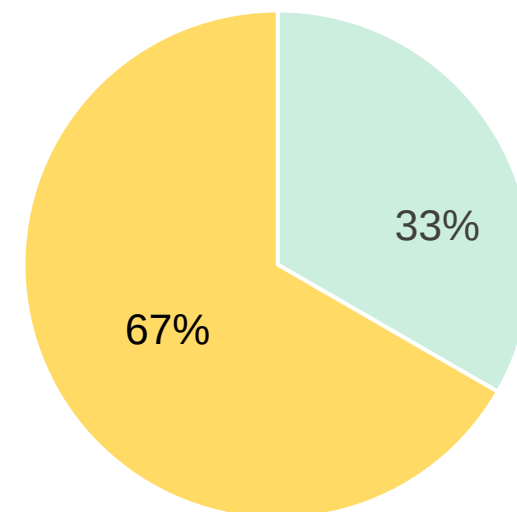
一、共通性問題

查核項目：10. 資料安全稽核機制

查核內容：10.2是否採取改善措施以持續改善資料安全維護？

■ 符合

■ 不符合



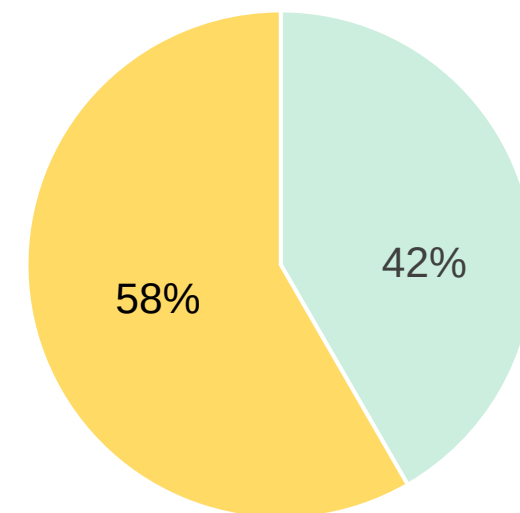
	1. 持續改善之作法相關紀錄。
佐證資料	
	1. 持續改善之作法建議寫在安全維護計畫中，應檢附「檢視或修正之紀錄」，如矯正單/追蹤紀錄。 2. 針對前項內部稽核結果提出之不符合項目或待改善項目進行持續改善。
資料準備提醒	
	1. 未「文件化」持續改善之作法或相關改善紀錄。
常見不符合態樣	

一、共通性問題

查核項目：11.使用紀錄、軌跡資料及證據保存

查核內容：11.3是否保存個人資料或儲存個人資料媒體之刪除、停止處理、利用或銷毀之原因、方法、時間及地點等紀錄？

■ 符合
■ 不符合



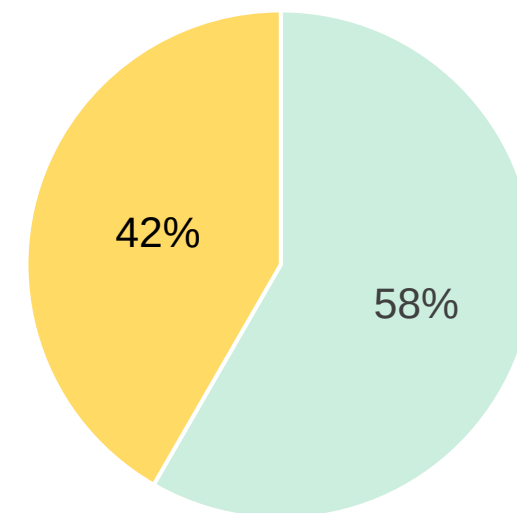
	1. 電子檔案銷毀、紙本檔案碎紙等之執行紀錄。
佐證資料	
	1. 銷毀紀錄應包含但不限於「原因」、「方法」、「時間」、「地點」。
資料準備提醒	
	1. 有執行銷毀，未留存「文件化」電子或紙本個資銷毀紀錄。
常見不符合態樣	

一、共通性問題

查核項目：11.使用紀錄、軌跡資料及證據保存

查核內容：11.5是否保存消費者個人資料之蒐集、處理及利用紀錄，以及自動化機器設備之軌跡資料？

■ 符合
■ 不符合



	- 消費者個人資料之蒐集、處理及利用紀錄。 - 自動化機器設備之軌跡資料。
佐證資料	
	確認自動化機器設備軌跡資料有留存操作紀錄，且保存時間至少滿五年。
資料準備提醒	
	- 自動化系統軌跡資料「未留存」，或「保存未滿五年」。 - 自動化系統軌跡資料僅留有「帳號登入、登出」，「未留存其他操作或使用紀錄」。
常見不符合態樣	

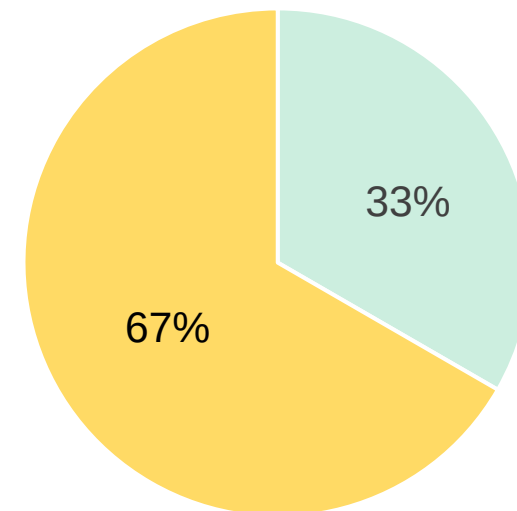
一、共通性問題

查核項目：12.個人資料安全維護之整體持續改善

查核內容：12.1是否定期就個人資料安全維護議題召開會議並提出持續改善報告？

■ 符合

■ 不符合



	1. 個人資料安全維護議題會議之紀錄。
佐證資料	
	1. 參與人員應包含接觸到個資之所有部門。
資料準備提醒	
	1. 未「文件化」召開個人資料安全維護會議之紀錄。 2. 自動化系統軌跡資料僅留有「帳號登入、登出」，「未留存其他操作或使用紀錄」。
常見不符合態樣	

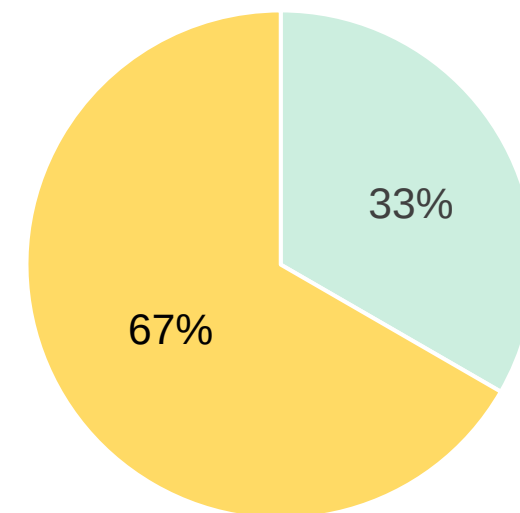
一、共通性問題

查核項目：13.委託作業

查核內容：13.5是否要求受託者認委託機關之指示有違反本法、其他個人資料保護法律或其法規命令者，應立即通知委託機關？

■ 符合

■ 不符合



	1. 個資委外之廠商清單及其合約文件，或其他地方明確告知委外廠商之證明文件。
佐證資料	
	1. 合約內容要明確寫出此規範。 2. 若未寫在合約內，係用其他證明文件應留有委外廠商明瞭且同意配合之紀錄(如：簽名或蓋章)。
資料準備提醒	
	1. 與委外廠商之合約內容未載明此項要求。 2. 已告知，但無「文件化」告知紀錄之佐證。
常見不符合態樣	

二、個案問題分析

- 觀光業者個資外洩說明
- 近期事件分享

觀光業者AA公司個資外洩說明

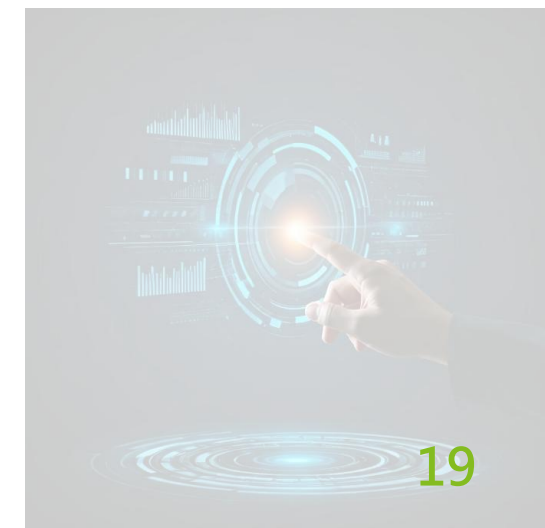
觀光業者AA公司個資外洩原因及後續處理情形





AA公司個資外洩說明-事件說明

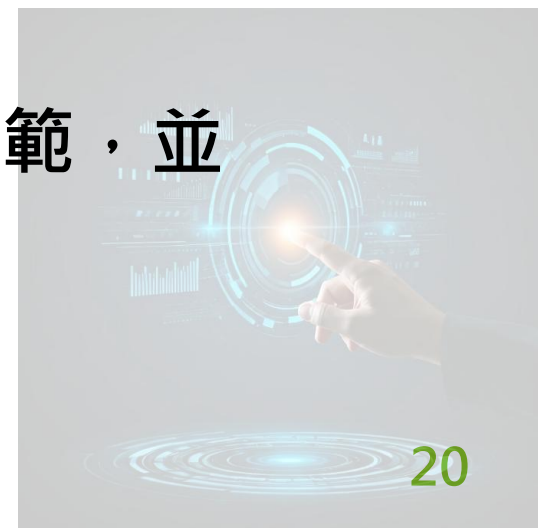
- AA公司接獲法務部調查局通知,資訊設備疑似遭駭客侵,經法務部調查局至該公司逐台電腦檢查後,發現為一台電腦點選了某大學客戶發來的email詢價單有後門程式,所以該台電腦可能導致個資洩漏發生。
- 1.經訪查單位個人電腦經調查局逐台檢視後，針對有問題的電腦重新汰換與設定。
- 2.加強員工資訊安全認知，除需核銷之資料外，其他敏感資料不留存於電腦。
- 3.規劃建置ISMS與PIMS管理制度。





AA公司個資外洩說明-後續可精進之作為

- 定期執行個人資料盤點作業：
 - 確認公司可觸到個人資料之部門及人員。
- 定期執行個人資料風險評估：
 - 針對個人資料盤點結果，進行風險評估，並針對高風險或不可解受風險項目採行風險處理計畫。
- 定期執行內部稽核：
 - 透過稽核確認同仁皆已遵守公司訂定之個人資料保護管理相關規範，並落實執行。



近期事件分享

蒐集7-9月國內外備受關注的重大個資外洩事件。





B公司CC平台疑個資外洩

🕒 時間：

今年5月底，國內資訊服務業者B公司旗下CC平台疑似遭駭客攻擊，除造成服務一度中斷，也傳出用戶個人資料疑似外洩。

🔍 調查：

🔍 公司初步判斷為伺服器硬碟資料毀損，後續偵測到部分系統出現異常，於是啟動資安事件應變機制，並委請資安公司進行數位鑑識與事件調查，同時向法務部調查局完成報案程序。

📌 結果：

☑ 經後續調查，最終認定B公司違反《個人資料保護法》第27條第1項規定。依該條規定，數發部因此依法對B公司及代表人分別裁處100萬元罰鍰，共200萬元，並要求限期改正。





D品牌會員資料外洩事件

事件時間

2026年7月遭受未授權第三方入侵。

影響範圍

臺灣、香港、英國、南韓、土耳其等多個國家

外洩資料

會員之姓名、電話、電子郵件、性別、國籍及購買偏好等消費紀錄。

社會影響

引起全球關注D品牌在資安與跨境監控上的潛在風險。

E公司預約平台個資外洩

事件時間

2026 年 9 月初。

影響範圍

南韓、日本、泰國、中國等多個國家，也包含台灣4,281人。

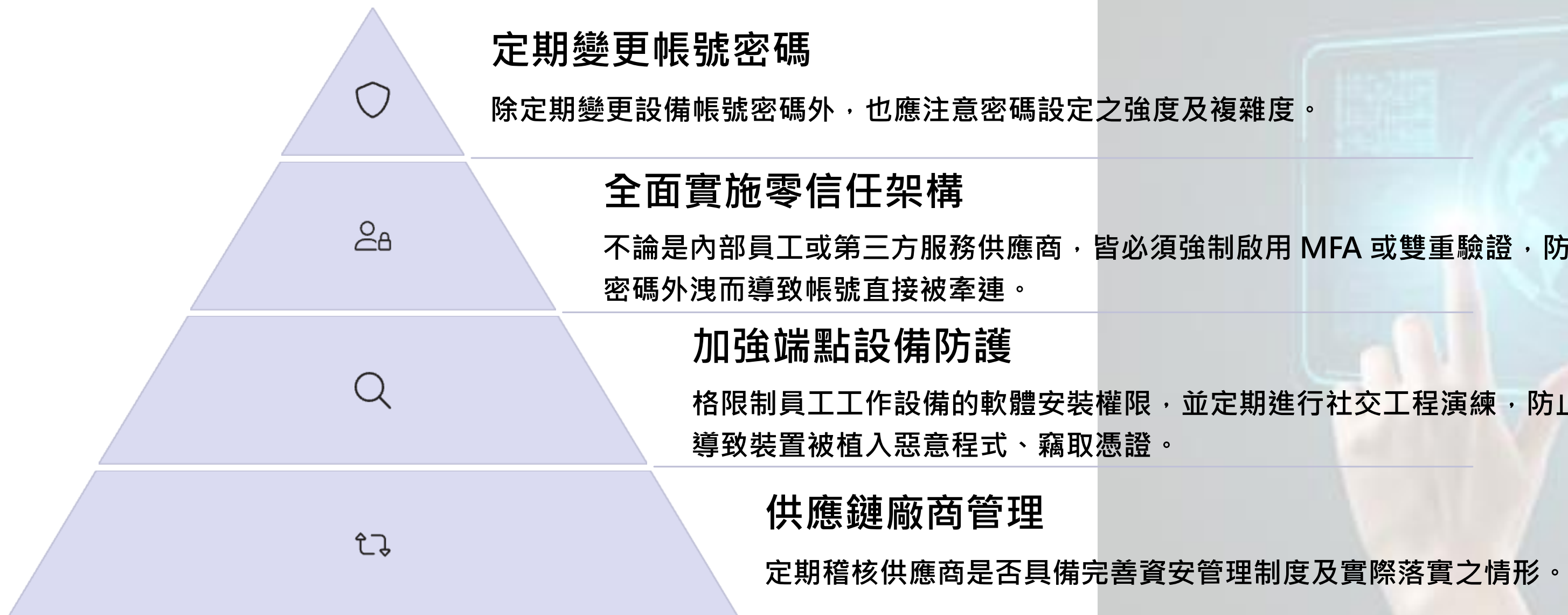
外洩資料

姓名、電話號碼、電子郵件、出生年月日、性別、社群帳號 ID、術前面部/部位照片、諮詢的預約動機、預約醫院與醫生姓名、實際施作的療程與手術名稱、付款紀錄及金額。

社會影響

E公司提供查詢功能，讓使用者可以在一定期間確認自己哪些資料受到影響。

針對7-9月資料外洩事件之資安防護建議



三、參考資料

- 經濟部個資作業手冊
(https://www.moea.gov.tw/mns/colr/content/SubMenu.aspx?menu_id=7783)。