tsc 德欣
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：個人資料保護法法律實務剖析

授課日期：111年8月12日、 9月2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 個人資料保護法介紹

二 個人資料保護法施行細則介紹

三 本校PIMS重點規範及社交工程防護宣導

四 個資管理常見問題與案例分享

五 課程結論

個人資料保護法介紹

個人資料保護法歷程

電資法→個資法 修正重點

- 擴大保護客體
- 普遍適用主體
- 增修行為規範
- 強化行政監督
- 促進民眾參與
- 調整責任內涵
- 除外適用條款

個人資料保護法架構

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)

個人資料保護法立法目的§1

規範個人資料之蒐集、處理及利用

避免人格權受侵害

促進個人資料合理使用

何謂個人資料?

一般個資§2

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。

特種個資§6 I

病歷、醫療、基因、性生活、健康檢查、犯罪前科

個資法所指行為定義 §2

當事人對自身個資之權利§3

當事人就其個人資料依本法規定行使之下列權利，不得預先拋棄或以特約限制之：

一. 查詢或請求閱覽。
二. 請求製給複製本。
三. 請求補充或更正。
四. 請求停止蒐集、處理或利用。
五. 請求刪除。

可拒絕當事人行使權利情形

一、妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益。
二、妨害公務機關執行法定職務。
三、妨害該蒐集機關或第三人之重大利益。

合理且適當使用個資-個人資料保護法§5

個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。

特種個人資料之蒐集、處理及利用-個人資料保護法§6

有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。但有下列情形之一者，不在此限：

- 一、法律明文規定。
- 二、公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施
- 三、當事人自行公開或其他已合法公開之個人資料。
- 四、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。
- 五、為協助公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。
- 六、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。

依前項規定蒐集、處理或利用個人資料，準用第八條、第九條規定；其中前項第六款之書面同意，準用第七條第一項、第二項及第四項規定，並以書面為之。

當事人同意-個人資料保護法§7

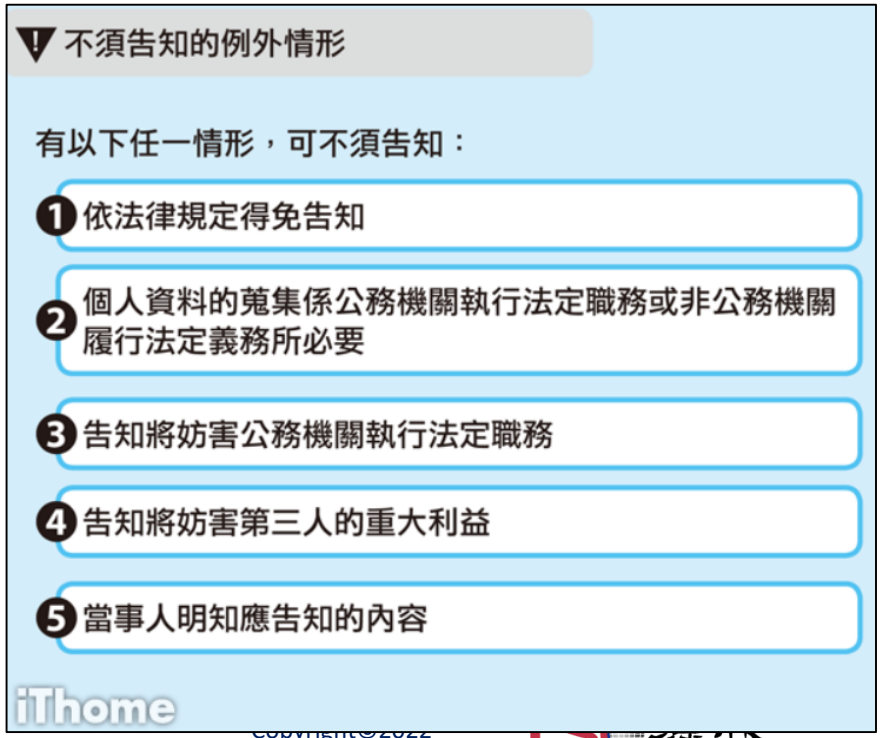
- 第十五條第二款及第十九條第一項第五款所稱同意，指當事人經蒐集者告知本法所定應告知事項後，所為允許之意思表示。
- 第十六條第七款、第二十條第一項第六款所稱同意，指當事人經蒐集者明確告知特定目的外之其他利用目的、範圍及同意與否對其權益之影響後，單獨所為之意思表示。
- 公務機關或非公務機關明確告知當事人第八條第一項各款應告知事項時，當事人如未表示拒絕，並已提供其個人資料者，推定當事人已依第十五條第二款、第十九條第一項第五款之規定表示同意。
- 蒐集者就本法所稱經當事人同意之事實，應負舉證責任。

告知當事人義務-個人資料保護法§8

公務機關或非公務機關依第十五條或第十九條規定向當事人蒐集個人資料時，應明確告知當事人下列事項：

- 一、公務機關或非公務機關名稱。
- 二、蒐集之目的。
- 三、個人資料之類別。
- 四、個人資料利用之期間、地區、對象及方式。
- 五、當事人依第三條規定得行使之權利及方式。
- 六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響

如果是間接收集個資(非當事人提供)，應於處理前或利用前，向當事人告知**個人資料來源**及上述**第一項至第五項**所列事項。
(個人資料保護法§9)



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

個資當事人行使權利辦理期限§13

一. 公務機關或非公務機關受理當事人依第十條規定之請求，應於十五日內，為准駁之決定；必要時，得予延長，延長之期間不得逾十五日，並應將其原因以書面通知請求人。

查詢或請求閱覽
請求製給複製本

二. 公務機關或非公務機關受理當事人依第十一條規定之請求，應於三十日內，為准駁之決定；必要時，得予延長，延長之期間不得逾三十日，並應將其原因以書面通知請求人。

請求補充或更正
請求停止蒐集、處理或利用。
請求刪除。

公務機關對個資之蒐集、處理§15

- **公務機關對個人資料之蒐集或處理，除特種資料外，應有 特定目的，並符合下列情形之一：**

  -執行法定職務必要範圍內。

  -經當事人同意。

  -對當事人權益無侵害。

公務機關對個資之利用§16

公務機關對個人資料之利用，除特種資料外，應於執行法定職務必要範圍內為之，並與蒐集之特定目的相符。但有下列情形之一者，得為特定目的外之利用：

- 法律明文規定。
- 為維護國家安全或增進公共利益所必要。
- 為免除當事人之生命、身體、自由或財產上之危險。
- 為防止他人權益之重大危害。
- 公務機關或學術研究機構基於公共利益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。
- 有利於當事人權益。
- 經當事人同意。

不適用個資法規定§51

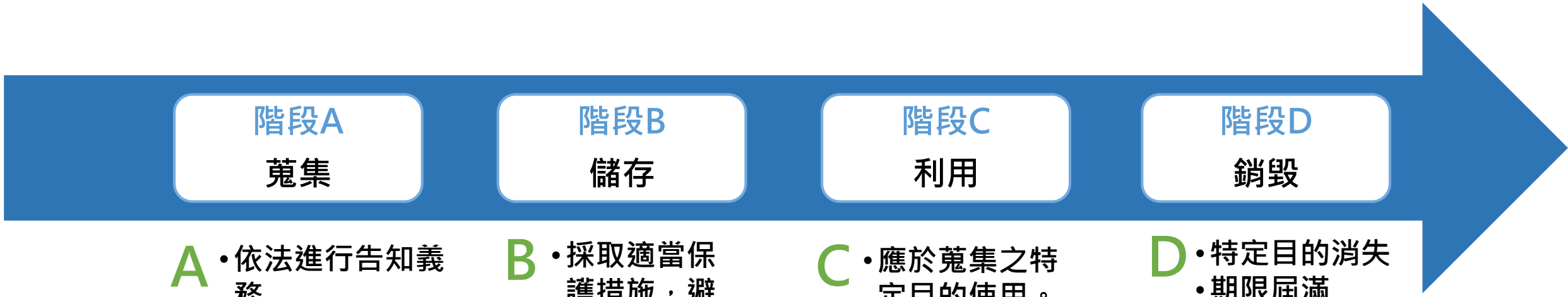
自然人為單純個人或家庭活動之目的，而蒐集、處理或利用個人資料。

於公開場所或公開活動中所蒐集、處理或利用之未與其他個人資料結合之影音資料。

Ex.社交活動、喜帖、親友通訊錄、活動照片/影片

個人資料保護法施行細則介紹

蒐集、儲存、利用、銷毀



A
- 依法進行告知義務
- 取得書面同意

B
- 採取適當保護措施，避免個人資料被竊取、竄改或銷毀

C
- 應於蒐集之特定目的使用。
- 特定目的外之使用應另取得書面同意

D
- 特定目的消失
- 期限屆滿
- 當事人要求

特種個資定義-個資法施行細則§4

類別	對應個資法	內容定義
醫療 (C111健康紀錄)	醫療	指以治療、矯正或預防人體疾病、傷害、殘缺為目的 ，所為的診察、診斷及治療；或基於診察、診斷結果，以治療為目的，所為的處方、用藥、施術或處置等行為全部或一部之總稱。
	病歷	依醫療法第六十七條所定之病歷應包括下列各款之資料： 一、醫師依醫師法執行業務所製作之**病歷**。 二、各項檢查、檢驗報告資料。 三、其他各類醫事人員執行業務所製作之紀錄。
基因 (C113種族或血統來源)	基因	指由人體一段去氧核醣核酸(DNA)構成，為人體控制特定功能之遺傳單位訊息。
性生活 (C112兩性生活)	性生活	指所有與性行為有關之活動之總稱，如性傾向、性慣行等。
身心健康狀況 (C66健康與安全紀錄) (C111健康紀錄)	健康檢查	指非針對特定疾病進行診斷或治療之目的，而以醫療行為施以檢查所產生之資料，如**健康檢查報告、身心輔導報告**等。
犯罪前科 (C115其他裁判及行政處分)	犯罪前科	指經緩起訴、職權不起訴或法院判決有罪確定、執行之紀錄。

告知當事人方式-個人資料保護法施行細則§16

依本法第八條、第九條及第五十四條所定告知之方式，得以言詞、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。

安全維護事項-個人資料保護法施行細則§12

本法第六條第一項但書第二款及第五款所稱適當**安全維護措施**、第十八條所稱**安全維護事項**、第十九條第一項第二款及第二十七條第一項所稱**適當之安全措施**，指公務機關或非公務機關為防止個人資料被竊取、竄改、毀損、滅失或洩漏，採取技術上及組織上之措施。

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

Check

9.資料安全稽核機制
10.使用紀錄、軌跡資料及證據保存

Action

11.個人資料安全維護之整體持續改善

個資法施行細則§12-安全維護事項(1/2)

一、配置管理之人員及相當資源:成立個資保護組織（個資管理委員會）、設置個資保護聯繫窗口並指定各單位個資保護專人、提供足夠之個資保護資源及承諾。

二、界定個人資料之範圍：個資盤點清查(紙本、電子檔案、系統)

三、個人資料之風險評估及管理機制：需進行個資風險評估，並對違法事項或高風險項目訂定風險處理計畫

四、事故之預防、通報及應變機制：事故發生時包含內部通報、主管機關通報、當事人的權益通報程序、應變處理程序都應該明訂。

五、個人資料蒐集、處理及利用之內部管理程序：應訂定及實施個人資料蒐集、處理及利用之內部管理程序。

六、資料安全管理及人員管理：應建立及實施個人資料保護管理機制及人員安全管理。

個資法施行細則§12-安全維護事項(2/2)

七、認知宣導及教育訓練：應辦理個資認知宣導及相關專業訓練。

八、設備安全管理：主要是針對各種保存個資的設備或系統，應該要做完善的安全保護（資訊安全作業）。

九、資料安全稽核機制：應定期實施個資安全稽核。99年8月份法務部函文政風單位須將個資檢查納入年度內稽。

十、使用紀錄、軌跡資料及證據保存：IT設備或紙本資料個資存取、使用、流向的記錄、日誌檔（Log）等，都必須完整保留，因為這些都是舉證的證據力(善盡保管之責任)。

十一、個人資料安全維護之整體持續改善：針對個資保護不足之處持續更新(PDCA)。

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

本校PIMS重點規範及社交工程防護宣導

本校PIMS制度文件清單-1~3階

政策　程序書、規程、手冊　作業規範、說明書

序號	階層	文件編號及名稱
1	一階	A001個人資料保護管理政策
2	二階	B001個人資料保護組織程序書
3		B002個人資料文件管理程序書
4		B003個人資料檔案風險評鑑與管理程序書
5		B004個人資料蒐集、處理、利用與安全管理程序書
6		B005個人資料當事人之權利聲明
7		B006個人資料稽核作業程序書
8		B007個人資料保護矯正管理程序書
9		B008個人資料檔案安全維護計畫
10		B009業務終止後個人資料處理方法
11	三階	C001個人資料安全控管作業說明書
12		C002個人資料保護緊急應變處理作業說明書

本校PIMS制度文件清單-4階

表單、紀錄、清冊、計畫、報告

序號	編號及名稱
1	D001個人資料保護組織成員表
2	D002人員職掌清冊
3	D003外來文件一覽表
4	D004適用法規清單
5	D005外部單位聯絡表
6	D006目標達成計畫與量測表
7	D007個人資料保護管理審查會議紀錄
8	D008文件調閱申請單
9	D009文件修訂建議表
10	D010個人資料管理制度文件列表
11	D011個人資料檔案清冊
12	D012個人資料檔案威脅暨弱點分析評分構面表
13	D013個人資料檔案威脅及弱點評估表
14	D014個人資料檔案風險評鑑彙整表

序號	編號及名稱
15	D015個人資料檔案風險處理計畫
16	D016個人資料提供同意書
17	D017私權政策聲明
18	D018個人資料使用資訊服務申請表
19	D019個人資料紀錄銷毀申請單
20	D020個人資料申訴事件紀錄單
21	D021個人資料特定目的範圍變更需求同意書
22	D022個人資料管理制度內部稽核計畫
23	D023個人資料管理制度內部稽核表
24	D024個人資料管理制度有效性量測表
25	D025個人資料管理制度內部稽核報告

序號	編號及名稱
26	D026個人資料管理制度矯正處理單
27	D027員工個人資料保密切結書
28	D028合約商保密切結書
29	D029資訊服務申請表
30	D030帳號清查紀錄表
31	D031帳號清查結果報告
32	D032校務系統密碼變更申請表
33	D033個人資料侵害事故通報與紀錄表
34	D034個人資料管理會議紀錄
35	D035校務資訊系統資料整合應用申請表
36	D036教育訓練簽到表
37	D037個人資料侵害事故應變演練計畫

個人資料蒐集之基本管控重點

- 個資蒐集不逾越特定目的。
- 個資蒐集須符合個資法有關蒐集之法定要件。
- 個資蒐集須履行當事人之告知義務。**(參考本校NUTN-PIMS-D016)**

個人資料提供同意書		
文件編號：NUTN-PIMS-D016	版次：1.0	機密等級：一般
紀錄編號：	填表日期：　年　月　日	

本同意書說明國立臺南大學（以下簡稱本校）將如何處理本表單所蒐集到的個人資料。
當您勾選「我同意」並簽署本同意書時，表示您已閱讀、瞭解並同意接受本同意書之所有內容及其後修改變更規定。若您未滿二十歲，應於您的法定代理人閱讀、瞭解並同意本同意書之所有內容及其後修改變更規定後，方得使用本服務，但若您已接受本服務，視為您已取得法定代理人之同意，並遵守以下所有規範。

一、基本資料之蒐集、更新及保管

(一)本校蒐集您的個人資料在中華民國「個人資料保護法」與相關法令之規範下，依據本校「隱私權政策聲明」，蒐集、處理及利用您的個人資料。
(二)請於申請時提供您本人正確、最新及完整的個人資料。
(三)本校因執行業務所蒐集您的個人資料包括姓名、職稱、聯絡方式(E-Mail、電話及地址)等(視實際狀況，各表單自行調整)。
(四)若您的個人資料有任何異動，請主動向本校申請更正，使其保持正確、最新及完整。
(五)若您提供錯誤、不實、過時或不完整或具誤導性的資料，您將損失相關權益。
(六)您可依中華民國「個人資料保護法」，就您的個人資料行使以下權利：
1、請求查詢或閱覽。2、製給複製本。3、請求補充或更正。4、請求停止蒐集、處理及利用。5、請求刪除。

但因本校執行職務或業務所必須者，本校得拒絕之。若您欲執行上述權利時，請參考本校「隱私權政策聲明」之個人資料保護聯絡窗口聯絡方式與本校連繫。但因您行使上述權利，而導致權益受損時，本校將不負相關賠償責任。

二、蒐集個人資料之目的

(一)本校為執行gm2電子郵件帳號申請業務(視實際狀況，各表單自行調整)需蒐集您的個人資料。
(二)當您的個人資料使用方式與當初本校蒐集的目的不同時，我們會在使用前先徵求您的書面同意，您可以拒絕向本校提供個人資料，但您可能因此喪失您的權益。
(三)本校利用您的個人資料期間為即日起至您於本校畢業後3年內(視實際狀況，各表單自行調整)，利用地區為台灣地區。

三、基本資料之保密

本校如因天災、事變或其他不可抗力所致者，致您的個人資料被竊取、洩漏、竄改、遭其他侵害者，本校將於查明後以電話、信函、電子郵件或網站公告等方法，擇適當方式通知您。

四、同意書之效力

(一)當您勾選「我同意」並簽署本同意書時，即表示您已閱讀、瞭解並同意本同意書之所有內容，您如違反各該條款時，本校得隨時終止對您所提供之所有權益或服務。
(二)本校保留隨時修改本同意書規範之權利，本校將於修改規範時，於本校網頁(站)公告修改之事實，不另作個別通知。如果您不同意修改的內容，請勿繼續接受本服務。否則將視為您已同意並接受本同意書該等增訂或修改內容之拘束。
(三)您自本同意書取得的任何建議或資訊，無論是書面或口頭形式，除非本同意書條款有明確規定，均不構成本同意條款以外之任何保證。

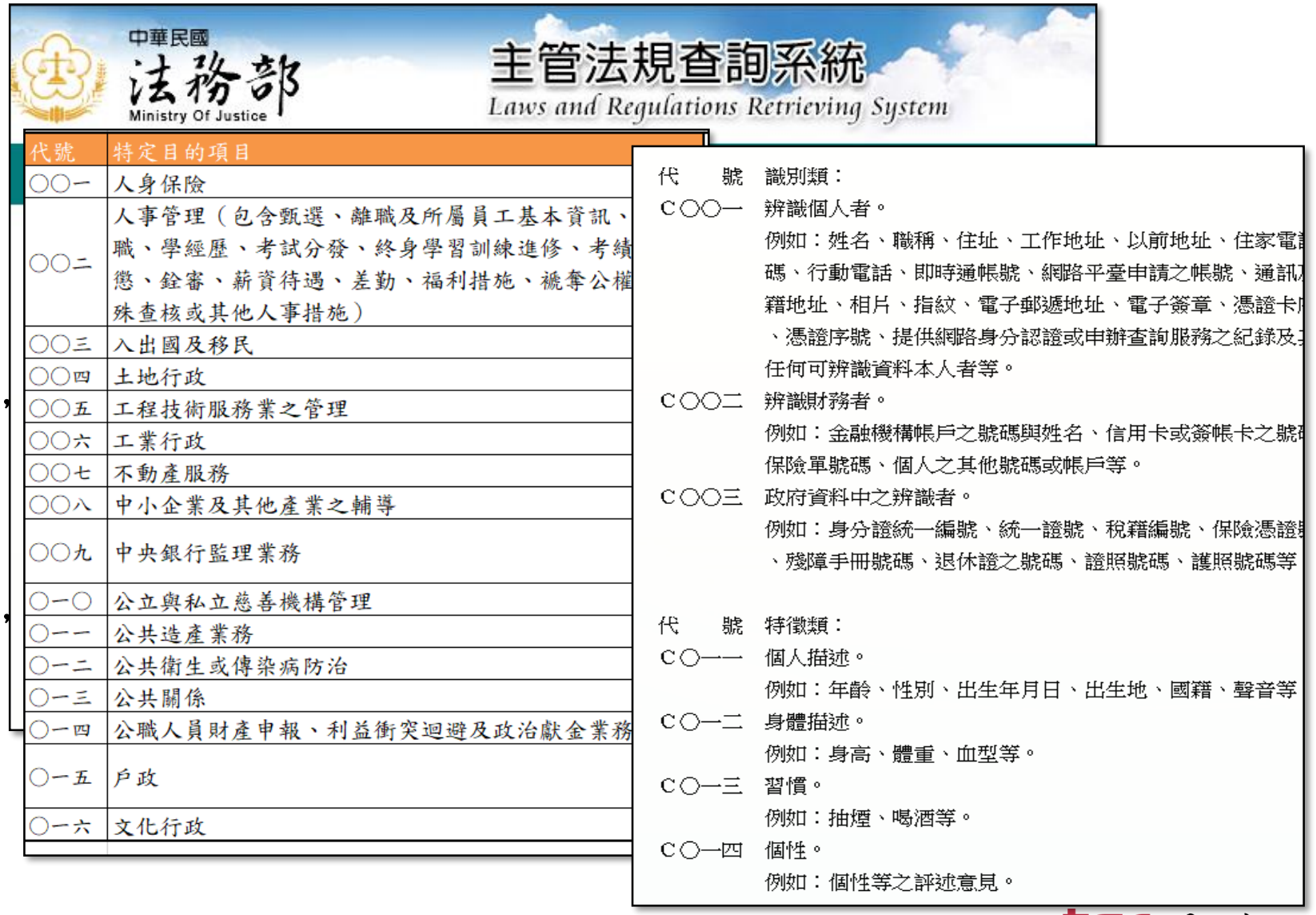
五、準據法與管轄法院

本同意書之解釋與適用，以及本同意書有關之爭議，均應依照中華民國法律予以處理，並以臺灣臺南地方法院為管轄法院。

□我已閱讀並接受上述同意書內容　當事人簽名：_____中華民國__年__月__日

蒐集目的與個人資料類別(補充說明)

- 法務部於民國101年正式對外公告個資法的特定目的及個人資料類別，特定目的有182 項，而個資類別有10 大類共134 項，這些是為了提供公務和非公務機關在個資蒐集、處理和利用時，衡量「符合特定目的內的利用」時的重要參考依據。



中華民國 法務部 Ministry Of Justice

主管法規查詢系統 Laws and Regulations Retrieving System

代號	特定目的項目
○○一	人身保險
○○二	人事管理（包含甄選、離職及所屬員工基本資訊、職、學經歷、考試分發、終身學習訓練進修、考績懲、銓審、薪資待遇、差勤、福利措施、褫奪公權殊查核或其他人事措施）
○○三	入出國及移民
○○四	土地行政
○○五	工程技術服務業之管理
○○六	工業行政
○○七	不動產服務
○○八	中小企業及其他產業之輔導
○○九	中央銀行監理業務
○一○	公立與私立慈善機構管理
○一一	公共造產業務
○一二	公共衛生或傳染病防治
○一三	公共關係
○一四	公職人員財產申報、利益衝突迴避及政治獻金業務
○一五	戶政
○一六	文化行政

代號	識別類：
C○○一	辨識個人者。 例如：姓名、職稱、住址、工作地址、以前地址、住家電話碼、行動電話、即時通帳號、網路平臺申請之帳號、通訊籍地址、相片、指紋、電子郵遞地址、電子簽章、憑證卡、憑證序號、提供網路身分認證或申辦查詢服務之紀錄及任何可辨識資料本人者等。
C○○二	辨識財務者。 例如：金融機構帳戶之號碼與姓名、信用卡或簽帳卡之號保險單號碼、個人之其他號碼或帳戶等。
C○○三	政府資料中之辨識者。 例如：身分證統一編號、統一證號、稅籍編號、保險憑證、殘障手冊號碼、退休證之號碼、證照號碼、護照號碼等

代號	特徵類：
C○一一	個人描述。 例如：年齡、性別、出生年月日、出生地、國籍、聲音等
C○一二	身體描述。 例如：身高、體重、血型等。
C○一三	習慣。 例如：抽煙、喝酒等。
C○一四	個性。 例如：個性等之評述意見。

個人資料儲存及銷毀管控重點

- 儲存應注意保存年限，不必要的複本盡量降低產生之數量與份數。
- 紙本資料儲存應注意環境與安全問題，例如：溫濕度、消防設備、門禁管制等；電子資料儲存應注意設備安全與存取控制問題，例如：設備資安漏洞更新、資料存取權限、加密儲存、上櫃上鎖、進出紀錄等。
- 超過保存年限或業務不需要再使用之個人資料應規劃銷毀或刪除作業。
- 紙本資料可造冊確認銷毀之數量及範圍，並留存相關銷毀紀錄，例如：拍照、錄影、銷毀人員及監銷人員確認；電子資料應留存儲存媒體銷毀紀錄、電子檔案刪除過程與結果截圖。

個人資料紀錄銷毀申請單

文件編號：NUTN-PIMS-D019	版次：1.0	機密等級：限閱
紀錄編號：	申請日期：　年　月　日	

本表單蒐集之個人資料，僅限於特定目的使用，非經當事人同意，絕不轉做其他用途，亦不會公佈任何資訊，並遵循本校資料保存與安全控管辦理。

申請單位	
申請人員	
個資檔案清冊名稱	
銷毀資訊	□起迄流水號＿＿＿＿＿＿＿＿~＿＿＿＿＿＿＿＿ □起迄日期＿＿＿年＿＿＿月＿＿＿日~＿＿＿年＿＿＿月＿＿＿日 □數量＿＿＿＿＿＿＿＿＿＿
銷毀方式	□自行銷毀　□委外銷毀
委外銷毀陪同人員	（委外銷毀始需填寫此欄位）
委外銷毀廠商	（委外銷毀始需填寫此欄位）
銷毀日期	＿＿＿年＿＿＿月＿＿＿日

承辦人	委外銷毀陪同人員	單位主管	文管人員
	（委外銷毀始需填寫此欄位）		

註 1：若委外執行銷毀，應確認相關陪同紀錄已附於此表單，始得存檔。

註 2：本表單之保存期限為至少保留三年。

111年演練信件類型及主旨清單

類型	演練郵件主旨
保健類	濕熱體質易好發汗皰疹 烤、炸、辣、酒不要碰
科技類	越來越多人不相信食評網評價 Google地圖將會一統天下
個人訊息類1	人壽保險費委託轉帳/信用卡通知書(請輸入身分證號碼開啟附件)
個人訊息類2	PChorne 線 土 購 物 - 構 買 清 單 (訂 單 編 號 : 20230611901611)
個人訊息類3	土地銀行【非約定轉帳結果通知】

演練觸發結果

對象為擁有電子郵件帳號之同仁。
演練結果為：
開啓信件36人
點擊連結64人
開啓附件65人
(計算方式為(觸發人數/測試人數)*100%)。

檢測項目	演練人數	總信件數	觸發人數	比率
開啓信件人數(比率)	504	2,520	36	7%
點擊連結人數(比率)			64	13%
開啓附件人數(比率)			65	13%

演練信件觸發數量

項次	類型	演練郵件主旨	觸發動作	觸發動作數量
1	保健類	濕熱體質易好發汗皰疹 烤、炸、辣、酒不要碰	開啓信件	4
			點擊連結	3
			開啓附件	1
2	科技類	越來越多人不相信食評網評價 Google地圖將會一統天下？	開啓信件	6
			點擊連結	1
			開啓附件	1
3	個人訊息類1	人壽保險費委託轉帳/信用卡通知書(請輸入身分證號碼開啟附件)	開啓信件	24
			點擊連結	23
			開啓附件	27
4	個人訊息類2	PChorne線上購物-構買清單(訂單編號：202306119016111)	開啓信件	12
			點擊連結	13
			開啓附件	15
5	個人訊息類3	土地銀行【非約定轉帳結果通知】	開啓信件	18
			點擊連結	31
			開啓附件	33

防範社交工程

開啓信件、點擊連結及開啓附件源自使用者於第一時間無立即察覺，此行為可能對資安環境帶來外部威脅，同仁們切勿開啓任何未受信任來源的郵件，並注意所收到的信件是否真的為貴校宣導政令、同仁間寄送訊息之用的受信任Domain Name寄件者來源。

https://www.nutn.edu.tw/cc/emailse/index.htm

防範社交工程

演練期間所發送的偽造信件均屬網路訊息，並非公務往來信件，同仁所使用的公務信箱不應該作為外部社群網站、私人服務(金融、電商)及會員註冊之用，應持續宣導如有填寫資料(如：網路平台申請的會員資料)時，不該使用公務信箱，應使用私人信箱接收「外部訊息」及「個人訊息」。

防範社交工程

使用電子郵件信箱時，開啟來路不明郵件，可能造成電腦或行動裝置中毒；或輕信郵件的真實性，而讓惡意攻擊者有機可乘，發動社交工程攻擊

1. 接收電子郵件時保持警覺
2. 切勿於網頁隨意提供機密資訊，如：公務用電子郵件帳號、密碼、信用卡號碼
3. 使用者電腦/手機需安裝防毒軟體，確實更新病毒碼至最新版本
4. 關閉信箱中自動下載圖片，並取消郵件預覽功能
5. 設定信箱的過濾垃圾郵件機制

個資管理常見問題與案例分享

個資管理常見問題-為何需要建立管理制度？

- 法律遵循
- 管理能力
- 組織形象
- 專業能力
- 社會責任
- 風險控管

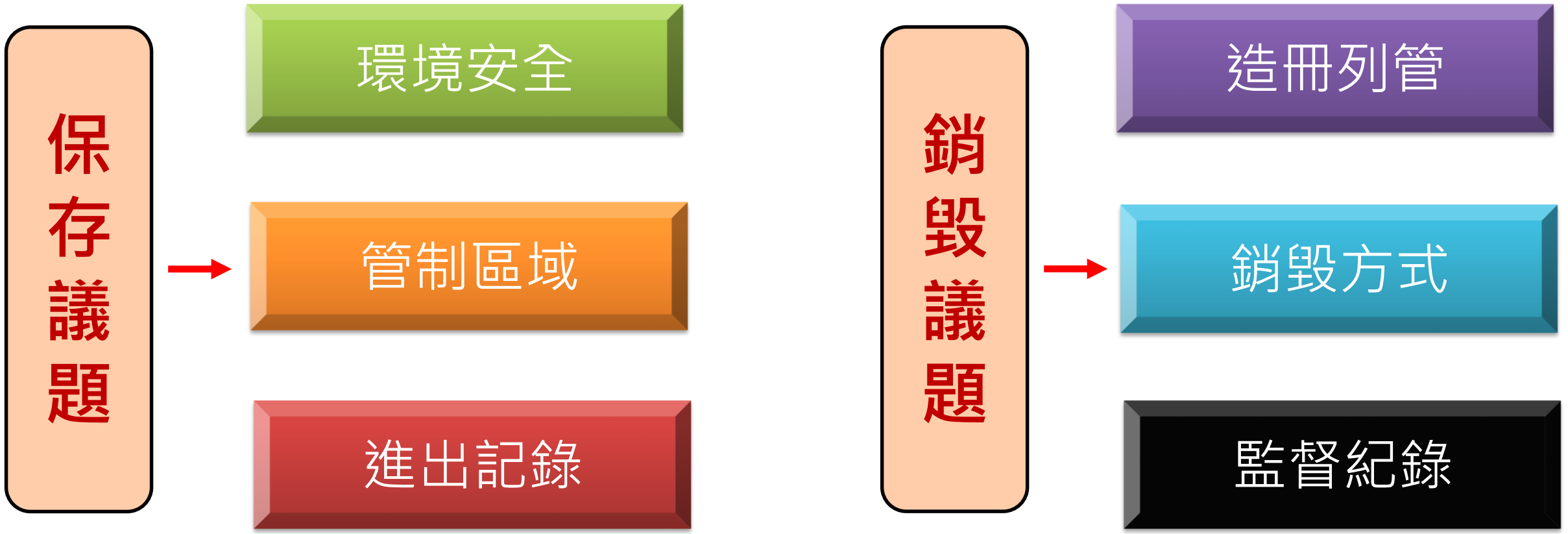
個資管理常見問題-如何降低個資風險？

合理使用

最小化原則

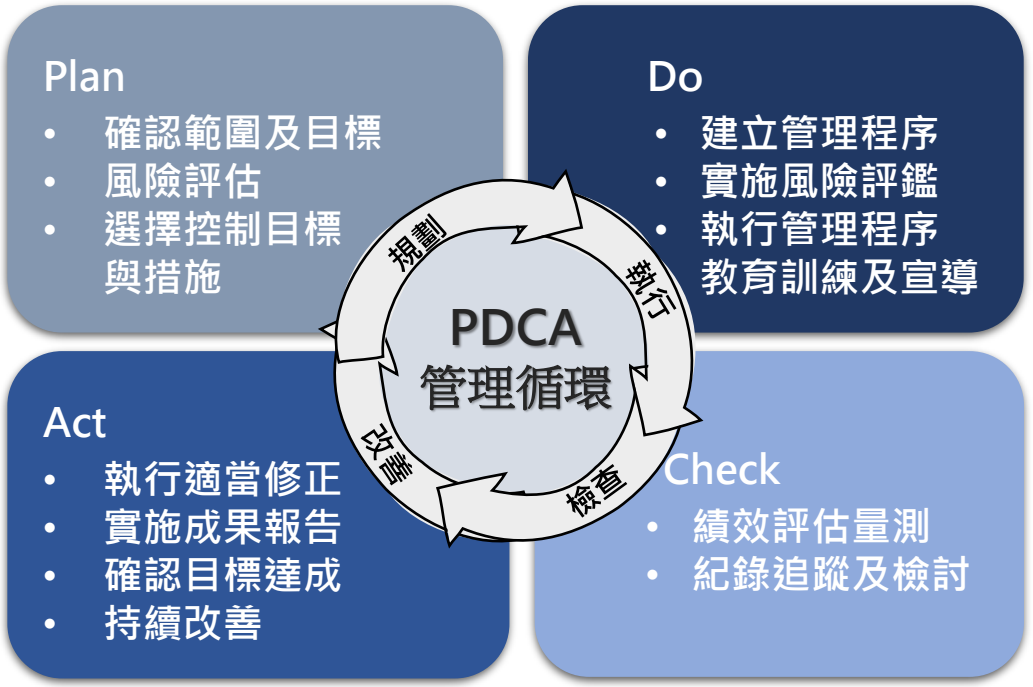
#風險管理（Risk Management）
是一個管理過程，包括對風險的定義、測量、評估和應對風險的策略。

個資管理常見問題-如何規劃個資保存與銷毀？



個資管理常見問題-如何成功導入PIMS？

- 反映組織營運目標之個資保護政策
- 建立與組織文化一致之個資管理方法
- 高階管理階層之支持與承諾
- 持續傳達個資管理觀念給組織人員
- 定期辦理適當之訓練與教育
- 量測個資保護政策目標之達成



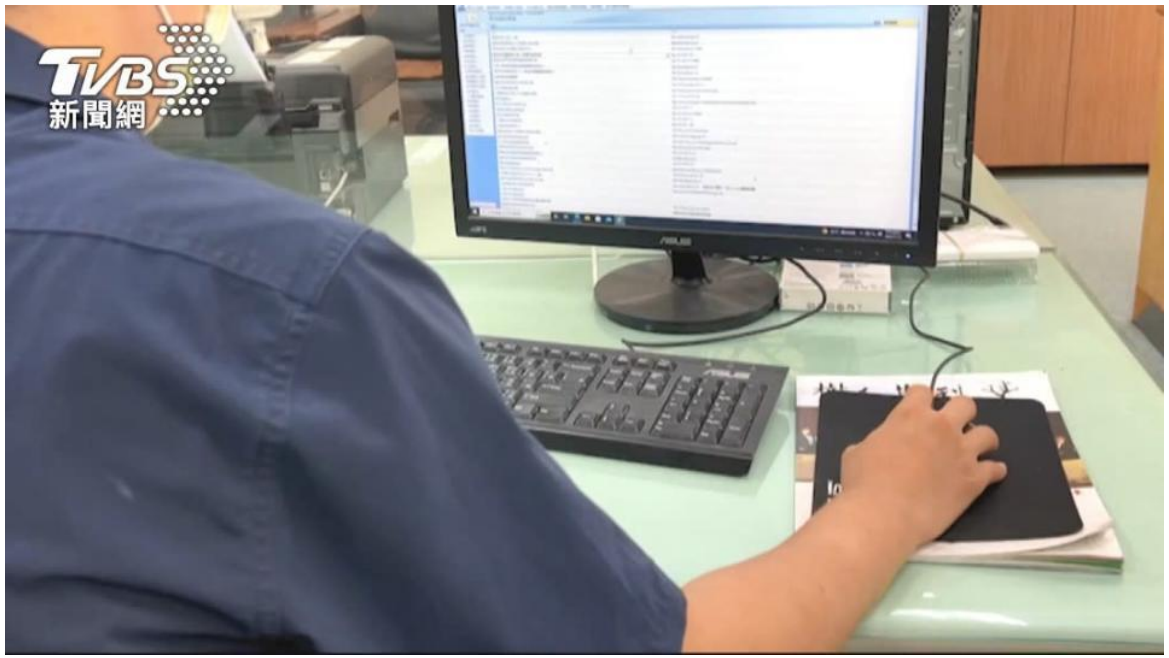
案例1.上班用公務電腦查啦啦隊個資 員警下場GG所長連帶處分

台南市一名員警，利用警政電腦系統，偷偷查詢職棒啦啦隊成員的資料，由於內部有人看不下去，在臉書社群爆料，質疑有人包庇，分局立刻發表聲明，強調依法處理，該名員警火速被記過、停權，連所長都遭到連帶處分。

南市第四警分局督察組長郭榮木：「調查後是基於該員個人好奇心，未涉及洩密，已針對該員加重核宜，記過兩次處分，並暫停該員查詢權限。」

被點名的是台南市警局，四分局華平所的一名劉姓員警，他涉嫌在六月份，利用上班時間，偷查啦啦隊成員資料，雖然消息曝光，分局強調連所長都被連帶處分，但看在律師眼裡，恐怕涉及的還有法律層面。

原來根據法規，警務人員要查詢當事人個資，除了要有法律的明文規定，還有當時正在執行法定職務，或是有公益目的，否則就要當事人願意公開以及有學術目的，但顯然這名員警，利用上班時間查詢，只為了滿足個人私利而且還連帶讓其他員警，使用個資查詢系統的威信受到質疑。



#使用目的　#軌跡資料　#證據保存

資料來源：https://tw.news.yahoo.com/上班用公務電腦查啦啦隊個資-員警下場gg所長連帶處分-153053435.html

案例2.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

課程結論

課程結論

資訊安全是持續精進的風險管理，資訊安全亦包含個人資料安全管理。

資訊安全與個人資料安全管理，人人有責。

當面對資安惡意攻擊時，您自己就是最佳的資安防禦，善用常識，保持警覺。

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/DFHAf1DxgREzNmAJ8

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