明新科技大學
Minghsin University of Science and Technology

個人資料檔案盤點暨風險評鑑教育訓練

2023.05.02

2023.05.10

財團法人中華民國國家資訊基本建設產業發展協進會
National Information Infrastructure Enterprise Promotion Association

大綱

- 執行個人資料管理制度的目的
- 個人資料的定義
- 個資盤點實作說明
- 風險評鑑作業說明
- Q&A

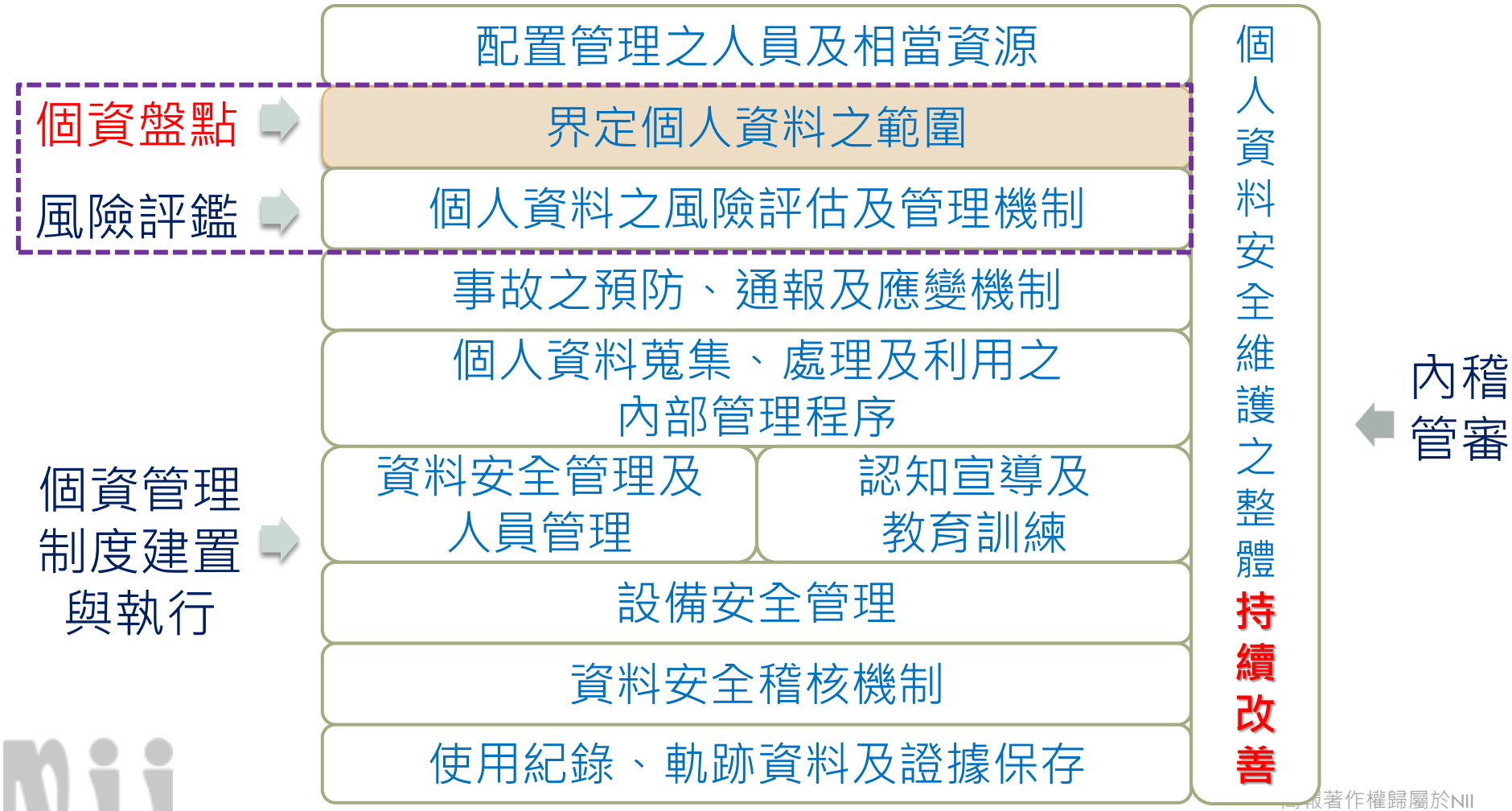
3

執行個人資料管理制度的目的

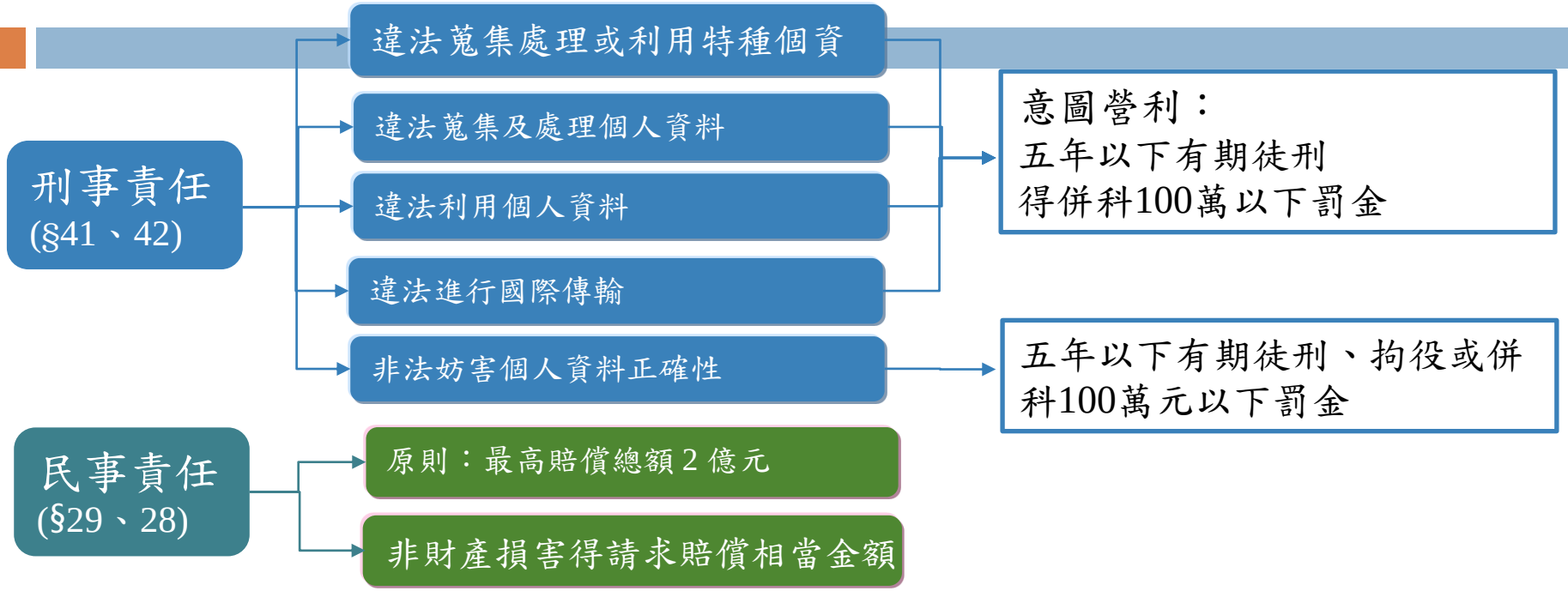
執行個人資料管理制度的目的

- 個資法第27條
  - 非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。
- 個資法施行細則第12條
  - 個資法...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。

適當安全防護措施 (個資法施行細則§12)



法律責任-非公務機關



非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但能證明其無故意或過失者，不在此限。(§29)

個資法罰則說明

個人資料保護法第28條

- 公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但損害因天災、事變或其他不可抗力所致者，不在此限。
- 被害人雖非財產上之損害，亦得請求賠償相當之金額；其名譽被侵害者，並得請求為回復名譽之適當處分。
- 依前二項情形，**如被害人不易或不能證明其實際損害額時，得請求法院依侵害情節，以每人每一事件新臺幣五百元以上二萬元以下計算**。
- 對於同一原因事實造成多數當事人權利受侵害之事件，經當事人請求損害賠償者，其合計最高總額以新臺幣二億元為限。但因該原因事實所涉利益超過新臺幣二億元者，以該所涉利益為限。
- 同一原因事實造成之損害總額逾前項金額時，被害人所受賠償金額，不受第三項所定每人每一事件最低賠償金額新臺幣五百元之限制。
- 第二項請求權，不得讓與或繼承。但以金額賠償之請求權已依契約承諾或已起訴者，不在此限。

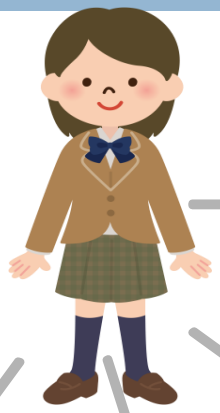
個人資料保護法第29條

- 非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但能證明其無故意或過失者，不在此限。
- 依前項規定請求賠償者，適用前條第二項至第六項規定。

個資.....在那裡？

電信/網路
服務提供業者

帳單地址
電子郵件信箱
帳戶資料



開立帳戶資料
保單資料
貸款徵信資料
會員資料
週年慶抽獎券

銀行/證券/保險公司
百貨公司/大賣場

信用卡資料
客戶資料
宅配地址
教育程度

線上購物/網拍
社群網站

身分證號碼
結婚登記
報稅資料、領據
駕照申請/換發

監理/戶政
財稅等政府單位

健檢報告
病歷資料
診斷書
醫療證明
身心障礙證明

醫院/診所
健康檢查中心

學籍資料
人事資料
註冊/報名料
家長會聯絡
社團聯絡資料

學校/補習班
社區活動中心

可能的個資外洩管道

- 問卷、報名表→未妥善保護，造成個資外洩。
- 社群網站、網購→網站設計不良，導致APT、駭客攻擊，造成個資外洩。
- 內部人員、委外廠商→誤點釣魚網站，造成個資外洩。
- **人員→無個資保護認知**

威秀影城50萬筆個資疑外洩 這些號碼1字不差！還要求提供帳戶

資料來源-壹蘋新聞網 2023/03/30

邱先生向《壹蘋新聞網》投訴，他是威秀影城的會員，今年2月25日上網訂購電影票，他昨天接到自稱威秀會計的女子來電， 表示系統有誤導致該筆消費重覆扣款20筆，公司會將重覆扣款的款項匯款給會員，並要求留下銀行存簿帳號，還說會補發500元補助金做為會員點數，下次消費可以折抵使用。

邱先生說，對方與他核對個人資料，包括**姓名、生日、電話、身分證字號、16碼信用卡卡號、有效年月等**，均1字不差，但他仍覺得有異，**未立即提供帳號給對方，事後向銀行查詢**，發現信用卡正常，並無重覆扣款的情形。

邱先生不滿表示，目前網路上已有多名威秀會員表示接獲詐騙電話，**威秀明知個資外洩，第一時間未以簡訊、電話主動通知會員，官網公告內容也不夠詳細。**

台中大魯閣新時代威秀影城。翻攝威秀影城官網

iRent用戶疑個資外洩 公路總局：若違個資法未改正「最重罰20萬」

資料來源-台視新聞網 2023/02/21

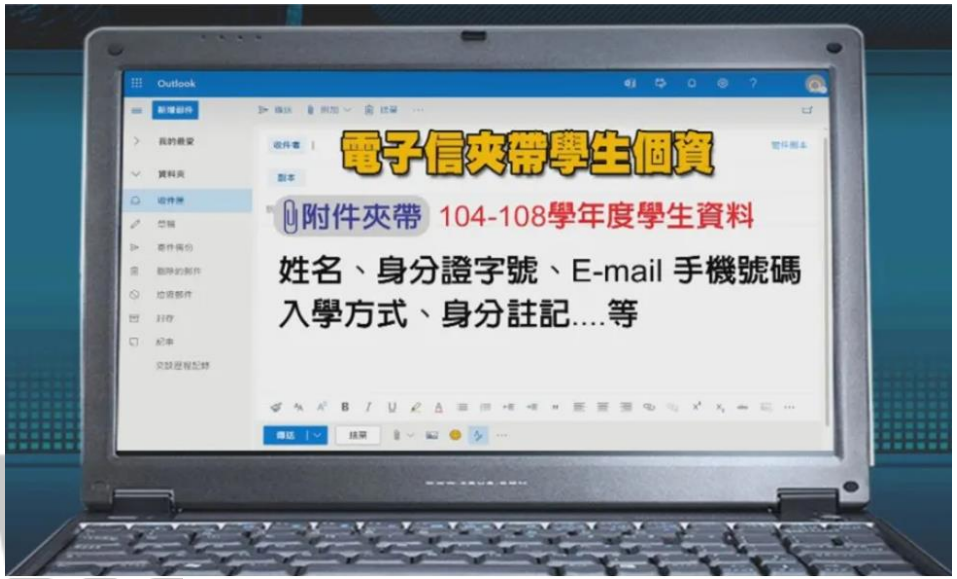
台灣和泰集團旗下的共享汽車服務iRent日前出現用戶個資外洩事件，一名安全研究人員在和泰所擁有的雲伺服器上發現沒有受加密保護的資料庫，其中包含**iRent用戶的姓名、手機號碼、電子郵件地址、居家住址、自拍照，以及部分信用卡資訊等**。

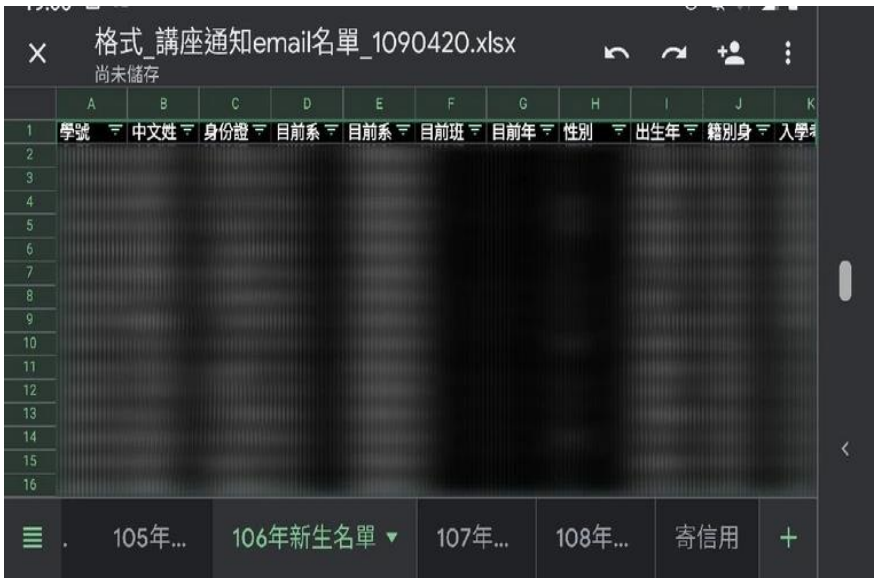
為掌握個資外洩情形，公路總局所轄台北市區監理所已於今天下午派員至和雲行動服務股份有限公司辦理行政檢查，若有違反個人資料保護法相關情事將要求限期改正，如屆期未改正，依個人資料保護法按次處新台幣2萬元以上20萬元以下罰鍰。另外，公路總局將依個人資料保護法及汽車運輸業個人資料檔案安全維護計畫及處理辦法，要求業者查明後強化個人資料檔案安全維護措施暨妥善個人資料處理及維護，保障消費者個資權益，並以適當方式通知當事人。

中正大學資安大出包！5年學生個資寄給200人

資料來源-民視新聞網，2020/10/14日、蘋果新聞網2020/10/13

有學生收到通識中心寄來的講座通知電子信，發現有附件好奇打開，赫然發現裡頭竟然是104~108學年度，所有入學學生的個人資料，就這樣隨信夾帶，寄送給200多位收件者，裡頭除了**身分證手機等基本資料，就連入學方式和身分註記都有**，學生個資全都露，主任秘書楊宇勛回應，「未來做好加密的動作，再來後端也要微控發送email或其他途徑，學校有沒有可能攔截的，有個資疑慮的，學校覺得很抱歉。」





政院提修法 企業個資外洩罰鍰最重1000萬、可按次開罰

資料來源-中央通訊社，2023/4/13

行政院會今天通過個資法相關修法草案，未來非公務機關、也就是民間業者若未遵行安全維護義務，造成民眾個資外洩情節重大，罰鍰將大幅提升，從目前的最重新台幣200萬元提高至1000萬元，且可按次處罰。

（行政院提供）

正確面對「個資法」

迴避個資法

過度恐慌

避免接觸個資

瞭解個資法

適當刪除與銷毀

安全處理與使用

維護個資正確

降低違法風險

個人資料的定義

何謂個人資料 (個資法§2、§6)

自然人的
- 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

個資法§2

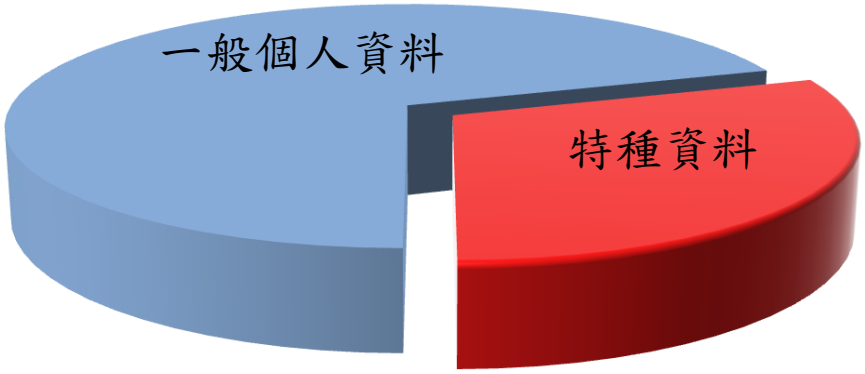
一般資料

特種資料
- 病歷
- 醫療
- 基因
- 性生活
- 健康檢查
- 犯罪前科

其他資料
- 得以直接或間接方式識別該個人之資料

特種資料

- 確定蒐集客體



特種資料
病歷
醫療
基因
性生活
健康檢查
犯罪前科

原則不得蒐集處理或利用

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。（§6）

特種個資(個資法第6條/個資法

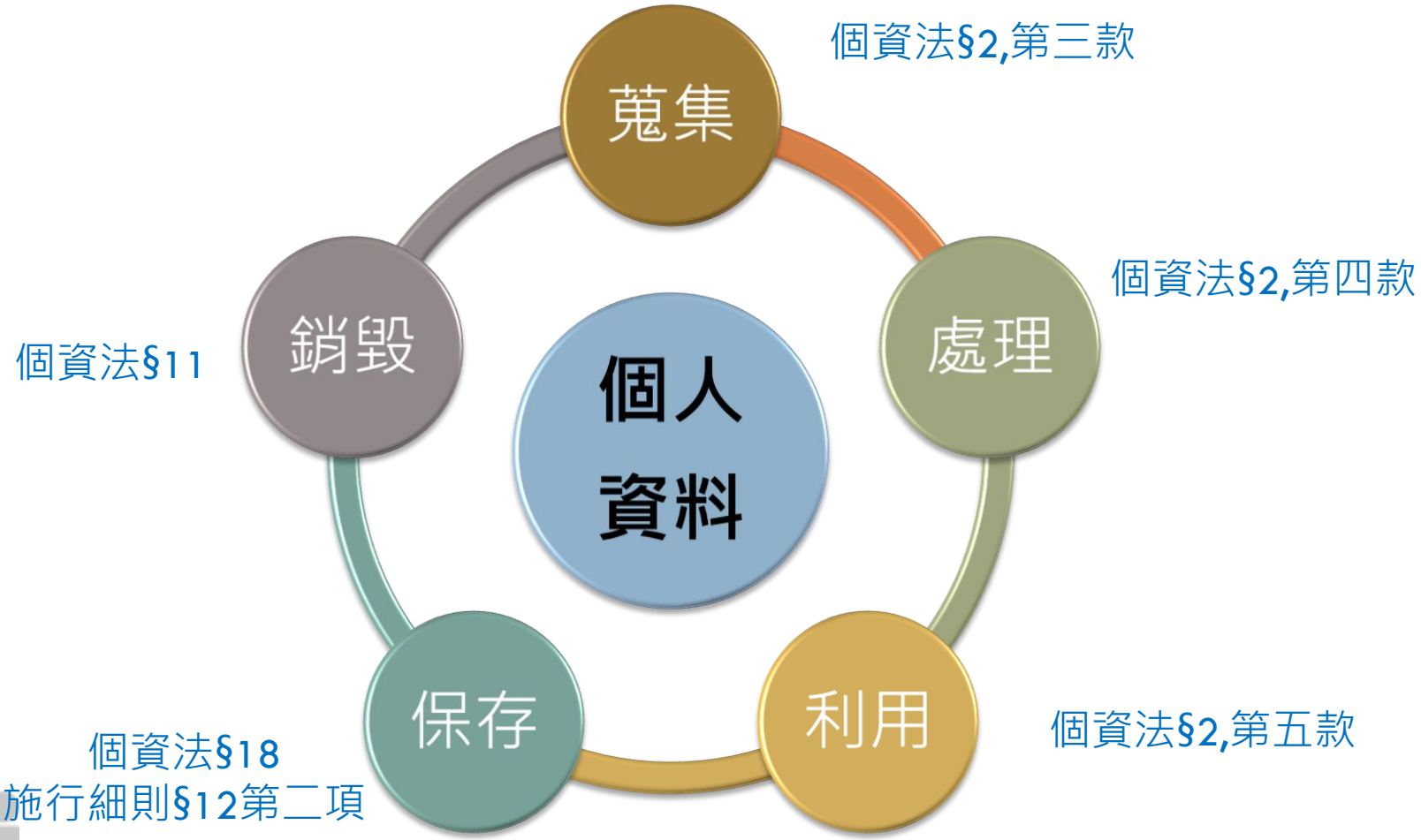
類別	特種個資之意涵(糾
病歷	醫療法第67條2項 病歷，應包括下列各款之資料： 一、醫師依醫師法執行業務所製作之病歷 二、各項檢查、檢驗報告資料。 三、其他各類醫事人員執行業務所製作之紀錄
醫療	指病歷及其他由醫師或其他之**醫事人員**，以治療、矯正、預防人體疾病、傷害、殘缺為目的，或其他醫學上之正當理由，所為之**診察及治療**；或**基於以上之診察結果，所為處方、 用藥、施術或處置所產生之個人資料**。
基因	由人體一段去氧核醣核酸構成，為人體控制特定功能之遺傳單位訊息。
性生活	指性取向或性慣行之個人資料 。
健康檢查	指非針對特定疾病進行診斷或治療之目的，而以醫療行為施以檢查所產生之資料 。
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 。

醫療法第10條所稱醫事人員，係指領有中央主管機關核發之**醫師**、**藥師**、**護理師**、物理治療師、職能治療師、醫事檢驗師、醫事放射師、營養師、助產師、**臨床心理師**、**諮商心理師**、呼吸治療師、語言治療師、聽力師、牙體技術師、驗光師、藥劑生、護士、助產士、物理治療生、職能治療生、醫事檢驗生、醫事放射士、牙體技術生、驗光生及其他醫事專門職業證書之人員。

特種資料得蒐集、利用或處理之例外情況

- 法律明文規定。
- 公務機關執行法定職務或非公務機關執行法定義務所必要，且有適當安全維護措施。
- 當事人自行公開或其他已合法公開。
- 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，且經一定程序所為蒐集、處理或利用。

個人資料生命週期

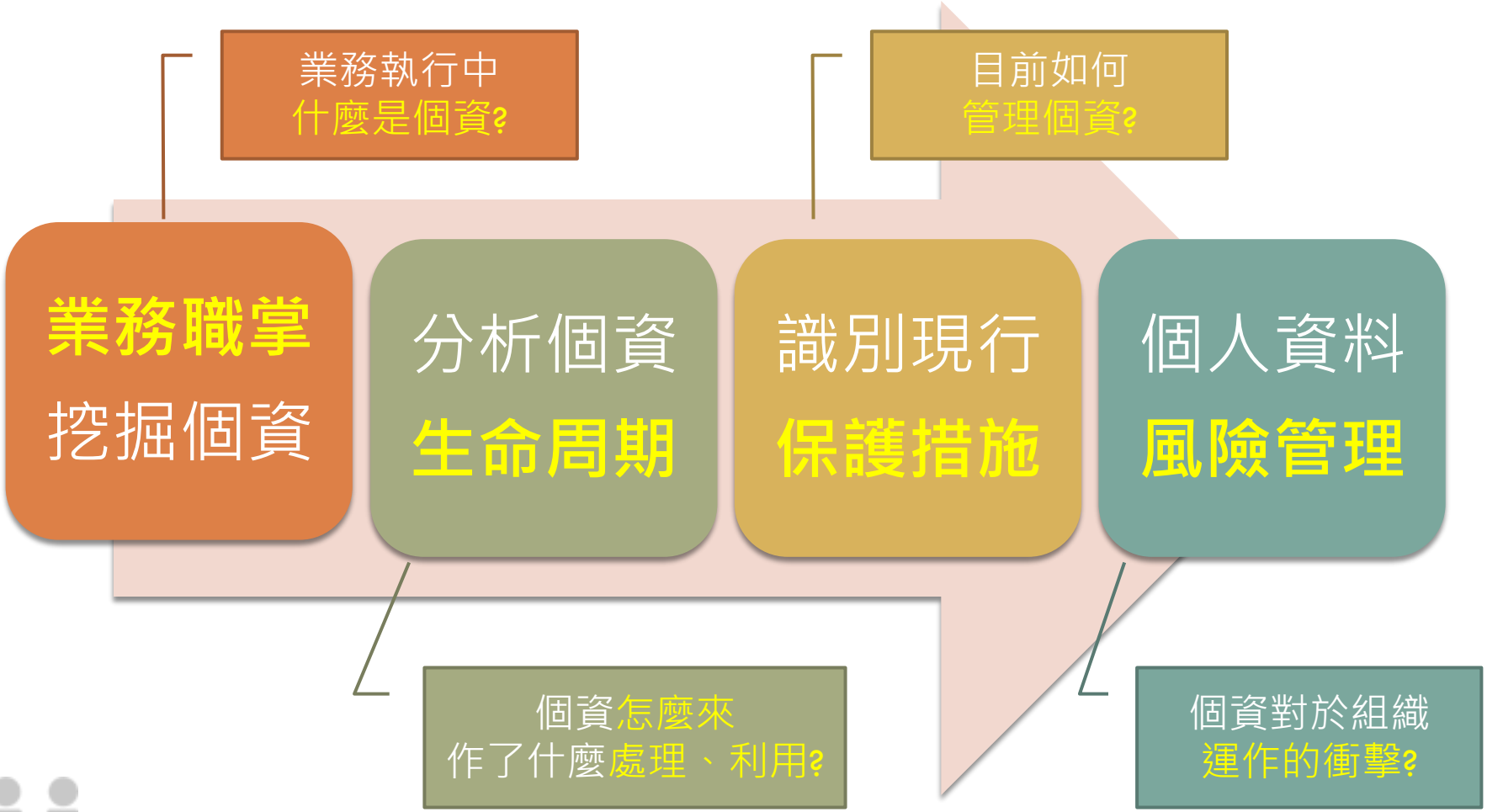


個資盤點實作說明

個資盤點注意事項

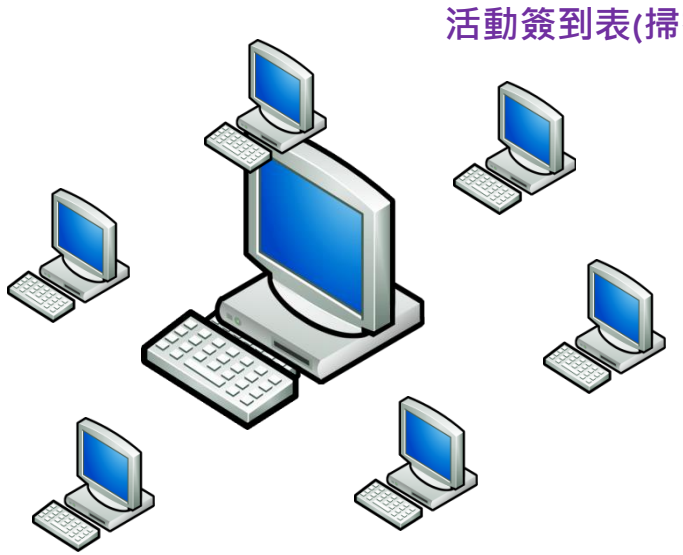
- **每年應至少執行一次個資檔案鑑別作業**
- **得因應變動情況，調整個資清冊**
  - 組織異動或作業流程改變
    - 處理方式或使用表單調整，適當調整清冊欄位
    - 業務增加會簽單位，於處理單位欄位註記
  - 個資資產異動
    - 依個資檔案屬性變動，刪除或增加個資資產
    - 一次性業務之銷毀
  - 因應法規之修改
    - 法律/保存依據若有修訂、調整
    - 保存期限改變

個資檔案盤點程序

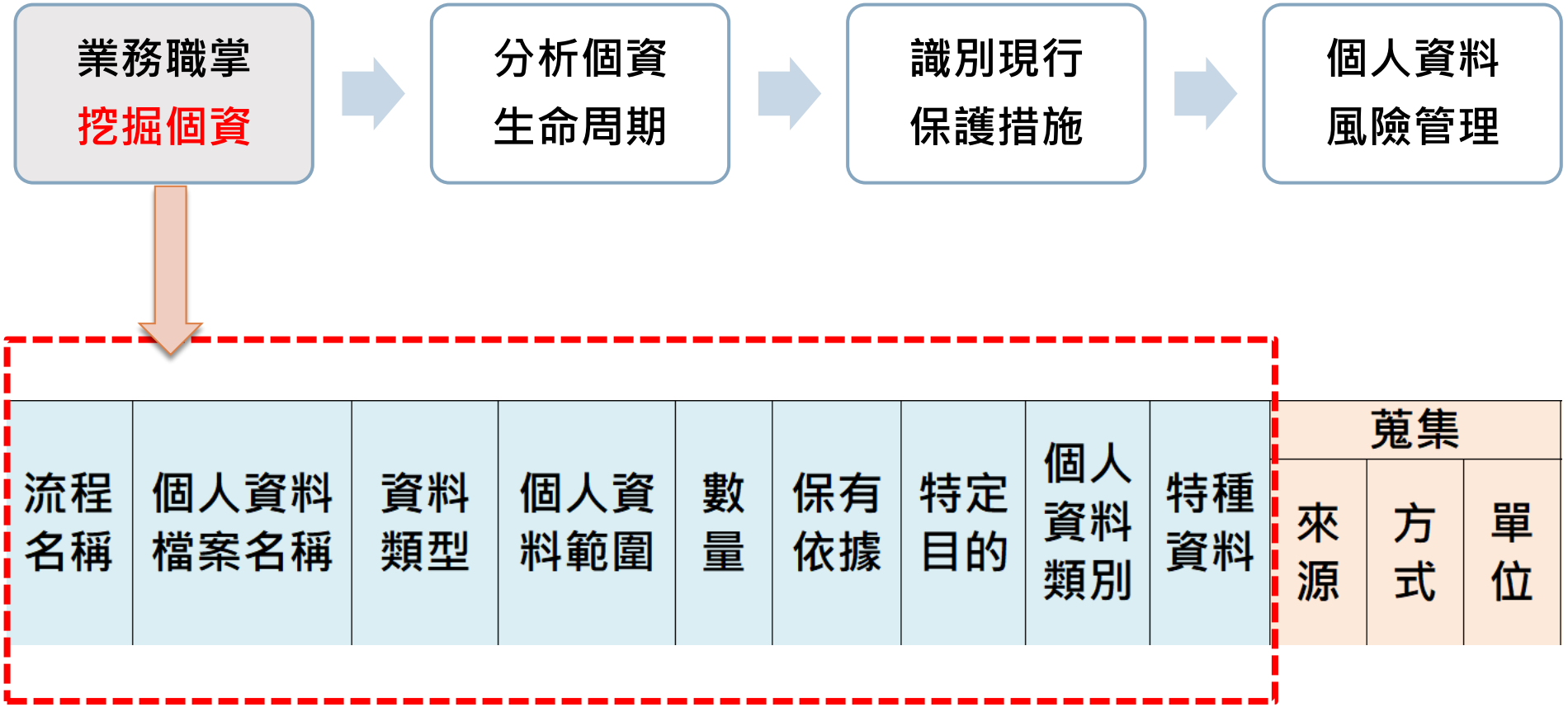


個資盤點群組化觀念

- 相同屬性之紙本文件、電子檔案，且其生命週期(蒐集、處理、利用、儲存、銷毀...)活動均相同者，可將之群組化，列為同一筆個資資產



個人資料檔案清冊說明



個資業務流程 (識別來源/個人資料流分析)

- 識別出業務流程主要的元件
  - 工作執掌一覽表、業務分層明細表
  - 紙本：表單/作業紀錄等
  - 電子：系統/個人電腦 等相關自動化儲存設備
- 個人資料流分析
  - 個人資料如何透過業務流程被蒐集、處理、利用、保存、銷毀等行為
  - 非例行業務之個資流(會簽業務，資料留存時)

個人資料檔案資料類型

紙本文件
(Document)

- 以紙本形式存在之文書資料，包含公文、報表、表單、計畫書、合約、外來文件等

電子檔案
(Data)

- 儲存於系統、硬碟、光碟等儲存媒介之數位資訊，包含公文、報表、表單、計畫書、合約、外來文件及資料庫資料等電子檔

同一個資檔案，同時存在紙本/電子形式，應分開明例

個人資料範圍_蒐集欄位

個人資料範圍(§2)	內容
姓名	中文姓名、英文姓名
出生年月日	民國/西元 出生年月日
國民身分證統一編號	身分證字號
員工編號 / 學號	員編、員工編號、工號、學號
護照號碼	護照號碼 或 居留證號碼
特徵	身高、體重、性別、年齡、血型、照片、生物辨識系統資料（虹膜、掌紋、臉部）、捺印指紋、指紋資料庫、指紋辨識門禁系統
婚姻	婚姻狀況（已婚、未婚、單身）
家庭	家庭背景、家庭成員關係
教育	學經歷、專長、證照、專業訓練、語文能力、班級、科系
職業	服務單位、職稱、公務人員職等、評分表分數、差勤紀錄、工作績效
聯絡方式	手機、公務電話、住家電話、E-mail、戶籍住址、住家住址、公司住址
財務情況	金融帳號、薪資
社會活動	會員證號

個資數量

- **每年**
  - 年度蒐集約略數量
- **總量**
  - 單位保存總數量

- **計算方式**
  - 以紀錄/檔案裡的個資量為計數基礎
    - 例如：一份通訊錄紙本/電子檔裡有10筆通訊資料
      每年：約10筆；總量：約10筆

保有依據

法律明文規定

EX.大學法、學生輔導法、全民健康保險法、會計法...

執行業務所需

因應提供之業務/服務，內部制定之辦法或要點。

EX.明新學校財團法人明新科技大學組織規程、 學生選課辦法、校內工讀助學金實施要點 ... ...

當事人同意

當事人自願提供個人資料

EX. 同意書

特定目的及個人資料類別

- 法務部於104/12/30修正公布
  - 182項特定目的；134項個人資料類別

參考來源： https://mojlaw.moj.gov.tw/LawContent.aspx?LSID=FL010631

列舉-個人資料保護法之特定目的

特定目的 – **共182項**

代號	修正特定目的項目
〇〇一	人身保險
〇〇二	人事管理（包含甄選、離職及所屬員工基本資訊、現職、學經歷、考試分發、終身學習訓練進修、考績獎懲、銓審、薪資待遇、差勤、福利措施、褫奪公權、特殊查核或其他人事措施）
〇〇三	入出國及移民
〇〇四	土地行政
〇〇五	工程技術服務業之管理
〇三一	全民健康保險、勞工保險、農民保險、國民年金保險或其他社會保險
〇四二	兵役、替代役行政
〇四三	志工管理
〇六九	契約、類似契約或其他法律關係事務
〇七三	政府資訊公開、檔案管理及應用
一〇九	教育或訓練行政
一一〇	產學合作
一一八	智慧財產權、光碟管理及其他相關行政
一五八	學生（員）(含畢、結業生)資料管理
一五九	學術研究
一三五	資（通）訊服務
一三六	資（通）訊與資料庫管理
一三七	資通安全與管理

個人資料類別-節錄學校相關

- C001 辨識個人者
  - 姓名、職稱、住址、工作地址、以前地址、住家電話號碼、行動電話、即時通帳號、網路平臺申請之帳號、通訊及戶籍地址、相片、指紋、電子郵遞地址、電子簽章、憑證卡序號、憑證序號、提供網路身分認證或申辦查詢服務之紀錄及其他任何可辨識資料本人者等
- C002 辨識財務者
  - 金融機構帳戶之號碼與姓名、信用卡或簽帳卡之號碼、保險單號碼、個人之其他號碼或帳戶等
- C003 政府資料中之辨識者
  - 身分證統一編號、統一證號、稅籍編號、保險憑證號碼、退休證之號碼、證照號碼、護照號碼等
- C011 個人描述
  - 年齡、性別、出生年月日、出生地、國籍、聲音等

個人資料類別-節錄學校相關

- C052 資格或技術
  - 學歷資格、專業技術、特別執照（如飛機駕駛執照等）、政府職訓機構學習過程、國家考試、考試成績或其他訓練紀錄等
- C061 現行之受僱情形
  - 僱主、工作職稱、工作描述、等級、受僱日期、工時、工作地點、產業特性、受僱之條件及期間、與現行僱主有關之以前責任與經驗等
- C081 收入、所得、資產與投資
  - 總收入、總所得、賺得之收入、賺得之所得、資產、儲蓄、開始日期與到期日、投資收入、投資所得、資產費用等
- C111 健康紀錄 (§6)
  - **醫療報告**、**治療與診斷紀錄**、檢驗結果、**身心障礙種類**、**等級**、有效期限、**身心障礙手冊證號**及聯絡人等

個人資料檔案清冊說明

業務職掌 挖掘個資 → 分析個資 生命周期 → 識別現行 保護措施 → 個人資料 風險管理

蒐集			處理						利用						
來源	方式	單位	處理方式	處理單位	保存單位	保存期限	銷毀形式	銷毀頻率	期間	地區	單位	方式	揭露對象	揭露方式	揭露個資範圍

蒐集、處理或利用之定義

蒐集

- 指以任何方式取得個人資料。

處理

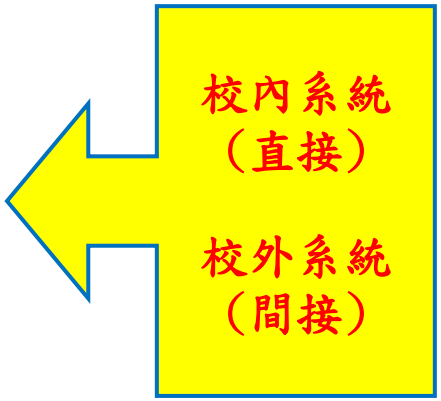
- 指為建立或利用個人資料檔案（指依系統建立而得以自動化機器或其他非自動化方式 檢索、整理之個人資料之集合。 ）所為資料之記錄、輸入、儲存、 編輯、更正、複製、檢索、刪除、輸出、連結或**內部傳送**。

利用

- 指將蒐集之個人資料為處理以外之使用。

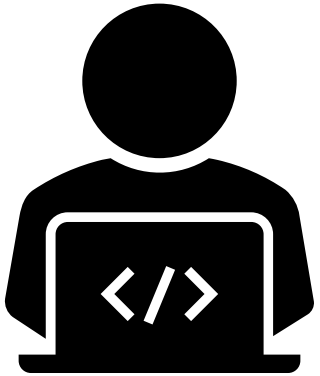
蒐集

- 蒐集來源
  - 當事人
  - 某系統提供
  - 別單位、網站、問卷
- 蒐集方式
  - 直接蒐集(§8)：直接從當事人取得個人資料
  - 間接蒐集(§9)：透過第三方(明新科大以外的組織)取得個人資料
- 蒐集單位：對當事人蒐集之源頭單位



處理

- 處理方式(描述資料蒐集後之處理流程)
  - 1.報名者至活動報名系統報名 (Input)
  - 2.彙整統計建置電子表單（或輸入至XX系統）
  - 3.查詢、列印使用
  - 4.內部傳送至A、B、C部門會簽
  - 5.儲存至個人電腦/內部伺服器主機
- 處理單位
  - 1.自己單位
  - 2.其他協助處理單位(下一關)



保存

- 保存單位：最終保存紙本或電子檔案或資料庫等資產之單位
- 保存期限：法律>辦法>內規
  - 保存10年
  - 離職後保存2年
  - 單位不留存
  - 業務持續期間

保存期限訂定參考方向：

一、法律明文規定

二、大專校院類檔案保存年限基準表

銷毀

- 形式：銷毀的方式
  - 碎紙機銷毀
  - 檔案刪除
  - 集中統一銷毀 / 委外銷毀
  - 提出系統需求單由資訊單位刪除
- 頻率：多久銷毀一次
  - 每年檢視
  - 每年一次
  - 檔案持續更新/覆蓋

利用

- 期間：利用個資期間
  - 業務期間
- 地區：利用地區
  - 境內、國外
- 單位：利用單位
  - 自己單位
- 方式：利用或揭露個資之方式
  - 聯絡當事人(如使用通訊錄打電話或E-mail)
  - 揭露

揭露

- 對象：揭露之機關、單位
  - 提供主管機關備查、提供勞健保給勞健保機構、提供報稅資料給國稅局、稅捐單位
- 方式目的：提供之方式
  - 透過系統上傳、E-mail方式、公文方式、彌封寄送、存放光碟片寄送
- 揭露個資範圍：揭露給第三方哪些個資欄位

個人資料檔案清冊說明

業務職掌挖掘個資 → 分析個資生命周期 → 識別現行保護措施 → 個人資料風險管理

處理						利用							現有控制措施
處理方式	處理單位	保存單位	保存期限	銷毀形式	銷毀頻率	期間	地區	單位	方式	揭露對象	揭露方式	揭露個資範圍	

現有控制措施

紙本文件
(Document)

- 上鎖倉庫、資料櫃、抽屜、防潮箱.....

電子檔案
(Data)

- 個人電腦帳密管理
- 儲放於**XX系統**帳密管理
- 共享資料夾權限管理
- 備份硬碟上鎖管理.....

明確描述系統名稱

個人資料檔案清冊說明

業務職掌
挖掘個資

分析個資
生命周期

識別現行
保護措施

個人資料
風險管理

利用							現有控制措施	個資範圍評估值	個資檔案管理角色
期間	地區	單位	方式	揭露對象	揭露方式	揭露個資範圍			

隱私衝擊分析 (個資範圍評估值)

衝擊影響程度	個資範圍評估值	個資範圍
極高	4	符合下列一項： ●含自然人之姓名及特種個資。 ●含國民身分證統一編號 (或護照號碼) 及特種個資。
高度	3	符合下列一項： ●含國民身分證統一編號(或護照號碼)及其他個資。 ●含自然人之姓名及財務情況（如：帳號）。
中度	2	含自然人之姓名或學號及其他個資，但不包含國民身分證統一編號、財務情況或特種資料。
一般	1	符合下列一項： ●屬於保管單位，但不接觸個資。 ●兩項其他個資(含)以上，但不包含姓名、學號、國民身分證統一編號、財務情況等無法直接識別當事人之項目組合。

個資檔案管理角色

資料控制者
(Data Controller)

決定個人資料處理之目的與方法之主體。

主導該作業流程/業務

資料處理者
(Data Processor)

實際執行個人資料處理之主體，依**資料控制者**指示行事之主體。

協助或經手該作業流程/業務

共同資料控制者
(Joint Data Controller)

二個或二個以上資料控制者共同決定個人資料處理之目的及方法之主體。

有兩方(含)以上主導該作業流程/業務

不須盤入個人資料檔案之個人資料

- **剔除下列不受個資法保護的資料 (§ 51)**
  - **自然人為單純個人（例如：社交活動等）或家庭活動（例如：建立親友通訊錄等）而蒐集、處理或利用的個人資料。**
    - 上述資料屬私生活目的所為，與職業或業務職掌無關。
  - **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。**
    - 在網際網路上張貼影音個人資料，屬表現自由之一部分。

個資盤點清冊諮詢常見問題(1/2)

- 公開資訊不需列入盤點，例如學校官網查詢到之同仁姓名、單位、分機等資訊。
- 不清楚個資流程角色定義。
- 不同資料類型(電子/紙本)未分開盤點。(**面臨之風險不同**)
- 蒐集過多個人資料範圍(**欄位之合理性與最小化**)
- 個資數量未區分**每年數量**與**保有之總數量**。
- 保存期限的合理性(**法律>內部辦法或要點>當事人同意**)。

個資盤點清冊諮詢常見問題(2/2)

- 將校外系統列為「個人資料檔案名稱」(**校外系統本校無資料之控制權**)。
- 未依規定留存個資，如核銷單據正本已送財務處，但同仁自行留存影本(**特定目的已完成，不應繼續留存其個資**)。
- 清冊欄位定義不清楚，如：
  - 特定目的
  - 個資類別
  - 蒐集方式(直接蒐集/間接蒐集)
- 未識別「揭露」，如資料會提供給校外單位。

個人資料盤點自我檢查步驟

Step1
- 確認業務範圍，清點所有個人資料

Step2
- 清查蒐集個人資料之途徑與方式

Step3
- 確認是否須履行告知義務並建立告知機制 (個資法§8)

Step4
- 確認蒐集、處理、利用之特定目的與保有依據

Step5
- 檢視保存與利用之範圍與方式

Step6
- 確認個人資料的保存期限與銷毀方式

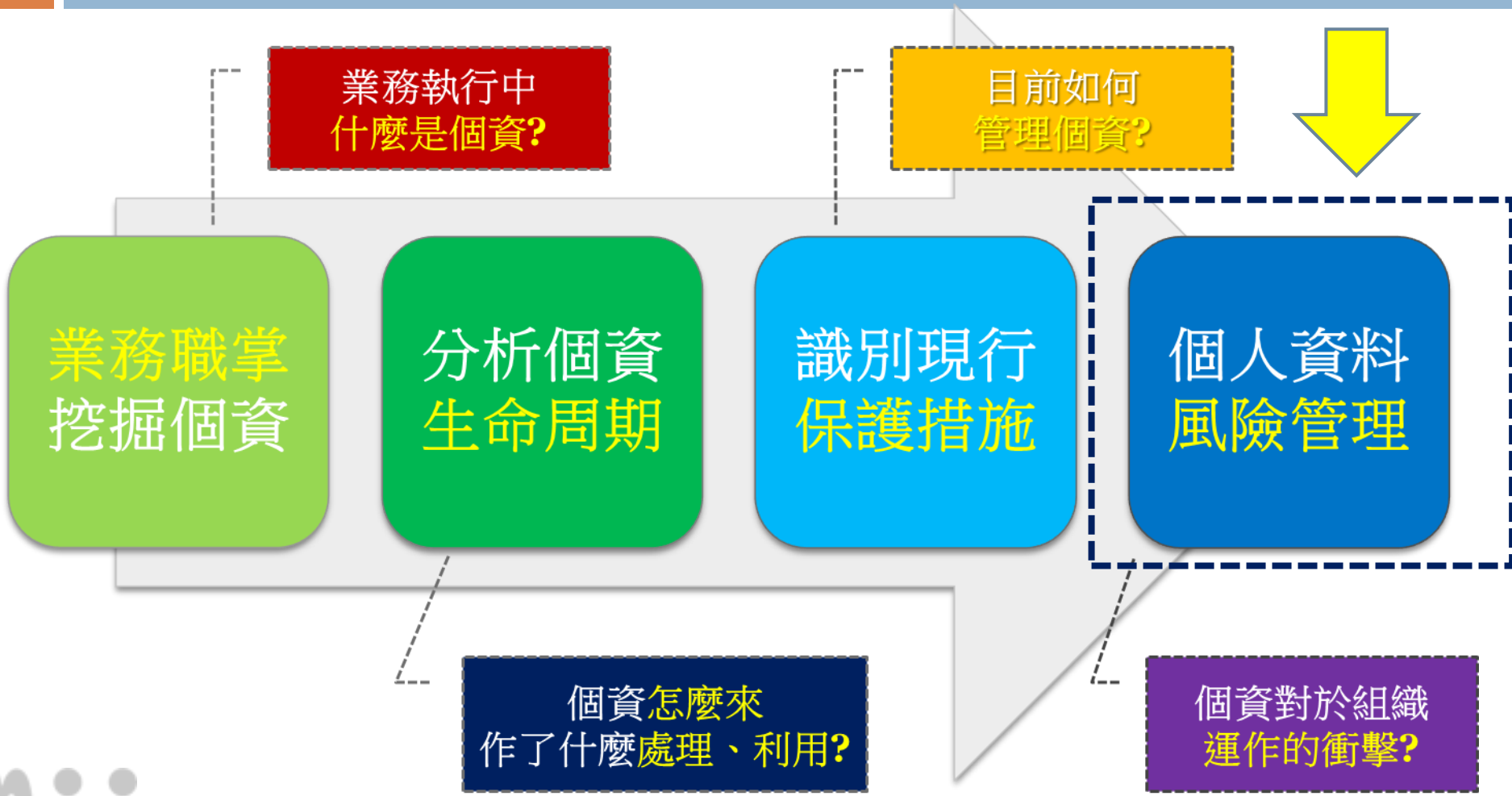
風險評鑑作業說明

風險管理所帶來的效益

- 識別個人資料檔案→我需要保護什麼
- 識別風險來源、事件→我需要採取何種對策
- 計算風險→我需要多少時間、人力、或成本來保護個人資料檔案

個資盤點及風險管理關聯(1/2)

本次課程重點



個資盤點及風險管理關聯(2/2)

業務職掌 挖掘個資 → 分析個資 生命周期 → 識別現行 保護措施 → **個人資料 風險管理**

本次課程重點

流程名稱	個人資料檔案名稱	資料類型	個人資料範圍	數量	保有依據	特定目的	個人資料類別	特種資料	蒐集			處理						利用							現有控制措施	個資範圍評估值	個資檔案管理角色
									來源	方式	單位	處理方式	處理單位	保存單位	保存期限	銷毀形式	銷毀頻率	期間	地區	單位	方式	揭露對象	揭露方式	揭露個資範圍			

隱私衝擊分析(個資範圍評估值)

衝擊影響程度	個資範圍評估值	個資範圍
極高	4	符合下列一項： ●含自然人之姓名及特種個資。 ●含國民身分證統一編號 (或護照號碼) 及特種個資。
高度	3	符合下列一項： ●含國民身分證統一編號(或護照號碼)及其他個資。 ●含自然人之姓名及財務情況（如：帳號）。
中度	2	含自然人之姓名或學號及其他個資，但不包含國民身分證統一編號、財務情況或特種資料。
一般	1	符合下列一項： ●屬於保管單位，但不接觸個資。 ●兩項其他個資(含)以上，但不包含姓名、學號、國民身分證統一編號、財務情況等無法直接識別當事人之項目組合。

風險評鑑與風險處理管理流程

風險評鑑程序

- 鑑別個資資產
- 評價個資衝擊
- 風險緣由與事件
- 評定風險等級
- 風險評鑑彙整

風險處理程序

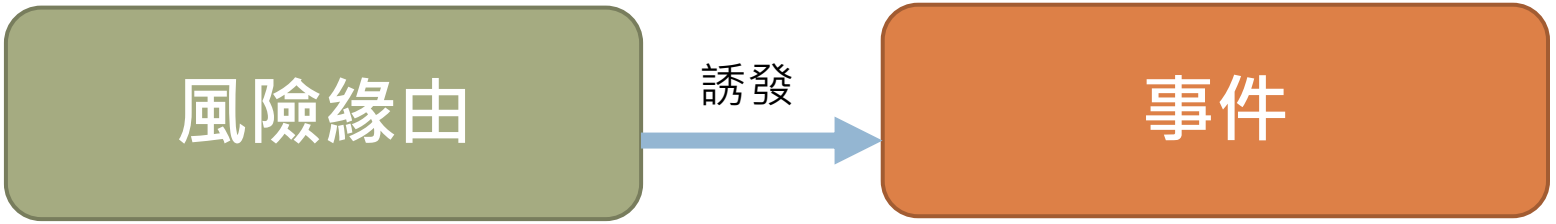
- 決定可接受風險
- 規劃與執行風險改善計畫
- 評估風險改善執行成效

風險評鑑工具

- FO-PIMS-2-03-02風險評估表

	A	B	C	D	E	F	G	H
1		風險評估表(紙本)			機密等級：☐機密 ■限閱 ☐內部 ☐公開			
2		文件編號：			填表日期：_____年_____月_____日			
3		個資資產編號：			蒐集單位：			
4		流程名稱：			保有單位：			
5		個人資料檔案名稱：			個資範圍評估值：			
6		個人資料範圍：						
7	資料週期	風險緣由	事件	衝擊影響	可能性	不適用	風險值	0
8								
9							0	
10								
11								
12								

風險緣由與事件



定義：可能導致風險的要項

- 未告知個資法要求應告知事項
- 教育訓練不足
- 資料銷毀處理程序不當或不足(如：儲存媒體內之資料沒有適當刪除就丟棄或重覆使用)

定義：所發生的變動或特定情況

- 未遵循法令法規
- 不熟悉法令法規及內部規範。
- 個人資料被竊取、竄改、毀損、滅失或洩漏。

風險評估分析構面表-1-1

評估值	衝擊影響
4	**嚴重傷害**： 1. 個資保管數量50,001筆以上，若全數外洩，對組織造成財務影響(損失超過1000萬元以上)。 2. 對組織形象造成嚴重的影響，該風險對組織造成嚴重的衝擊(電視及平面媒體或海外媒體大肆負面報導)。 3. 該風險產生會造成嚴重違反法令之情形，該風險會造成同仁與其直屬主管遭受法律上的求償及刑事訴訟，高階主管可能需下台負責。
3	**重大傷害**： 1. 個資保管數量5,001-50,000筆以內，若全數外洩，對組織造成財務影響(損失低於1000萬元以內)。 2. 對組織形象造成嚴重的影響，該風險對組織造成重大的衝擊(平面媒體的負面報導)。 3. 該風險會造成同仁與其直屬主管遭受法律上的求償。

風險評估分析構面表-1-2

評估值	衝擊影響
2	**中度傷害**： 1. 個資保管數量501-5000筆以內，若全數外洩，對組織造成財務影響(損失低於100萬元以內)。 2. 對組織形象造成輕微的影響，該風險造成的衝擊可接受。 3. 該風險會造成同仁與其直屬主管遭受內部的懲處。
1	**低度傷害**： 1. 個資保管數量500筆以內，若全數外洩，對組織造成財務影響(損失低於100萬元以內)。 2. 該風險造成任何關於法令法規的影響有限。

風險評估分析構面表-2

評估值	可能性	
4	該風險常導致此事件發生	1. 年度內曾發生類似的事件2次以上。 2. 組織未採用任何的控制或管理措施。（如：無制定保存年限且資料皆無銷毀、未識別法律依據且未對個資當事人進行告知）
3	該風險曾導致此事件發生	1. 年度內曾發生類似的事件。 2. 個人資料保護之程序機制已建立，惟未落實執行或程序機制不完整。（如：已制定保存年限但未銷毀、未進行安全管控機制）
2	該風險可能導致此事件發生	1. 3年內曾發生類似的事件。 2. 個人資料保護之程序機制未建立，但仍採有部分之控制措施。（如：尚未建立個資保護機制但進行文件上鎖、機敏檔案已進行加密控管）
1	該風險導致此事件發生的機會極低	1. 3年以上未曾發生類似的事件。 2. 個人資料保護之程序機制已建立並落實執行。

個資檔案風險值計算

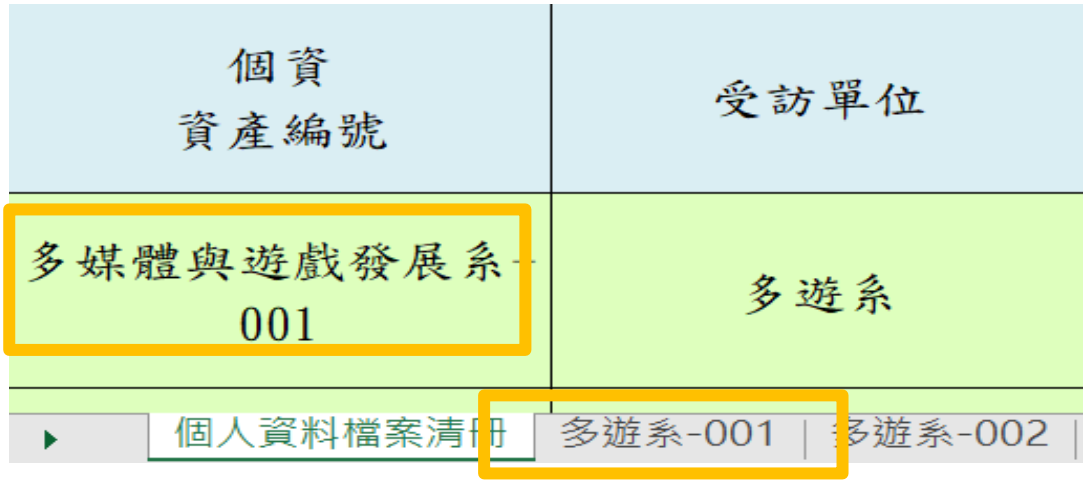
- 風險值 = 個資範圍評估值 X (衝擊影響 + 可能性)

	A	B	C	D	E	F	G	H
1	風險評估表(紙本)				機密等級：□機密 ■限閱 □內部 □公開			
2		文件編號：			填表日期：_____年_____月_____日			
3		個資資產編號：			蒐集單位：			
4		流程名稱：			保有單位：			
5		個人資料檔案名稱：			個資範圍評估值：			
6		個人資料範圍：						
7	資料週期	風險緣由	事件	衝擊影響	可能性	不適用	風險值	0
9							0	
10								
11								
12								

風險值取最大值

風險評估作業注意事項(1/2)

- 個資清冊欄位「個資資產編號」與「工作表名稱」不一致：



- 風險值計算未套用公式：風險值 = 個資範圍評估值 X（衝擊影響 + 可能性）

風險評估作業注意事項(2/2)

- 風險值評分漏列，有利用行為(如聯絡當事人)，未評分或評分為不適用：

資料週期	風險緣由	事件	衝擊影響	可能性	不適用	風險值
利用	未經授權下利用資料	個人資料被竊取、竄改、毀損、滅失或洩漏			0	0
利用	存取權限授與不當	個人資料被竊取、竄改、毀損、滅失或洩漏			0	0
利用	缺乏回收控管機制	個人資料被竊取、竄改、毀損、滅失或洩漏				0
利用	傳輸過程未有適當之加密或保護	個人資料被竊取、竄改、毀損、滅失或洩漏				0
利用	不了解個資法國際傳輸之要求	個人資料被竊取、竄改、毀損、滅失或洩漏				0

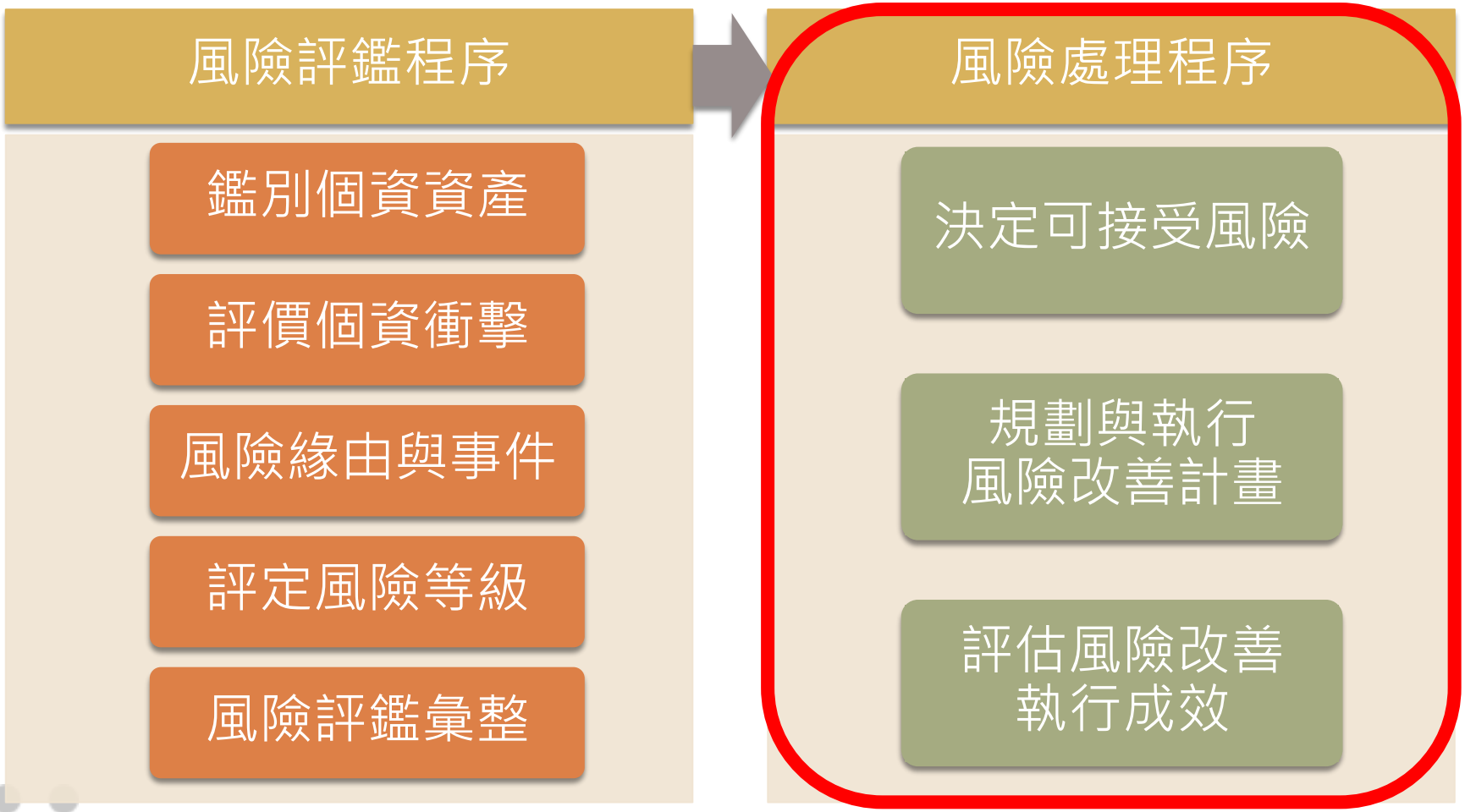
風險評估範例

學生保險清冊
- 個資範圍評估值=3

風險值
- 取最大值 = 18

資料週期	風險緣由	事件	衝擊影響	可能性	不適用	風險值
全階段	教育訓練不足	不熟悉法令法規及內部規範	3	1		12
蒐集	未告知個資法要求應告知事項	未遵循法令法規	1	3		12
處理	未訂定保存期限	個人資料被竊取、竄改、毀損、滅失或洩漏	3	3		18
利用	傳輸過程未有適當之加密或保護	個人資料被竊取、竄改、毀損、滅失或洩漏	1	1		6

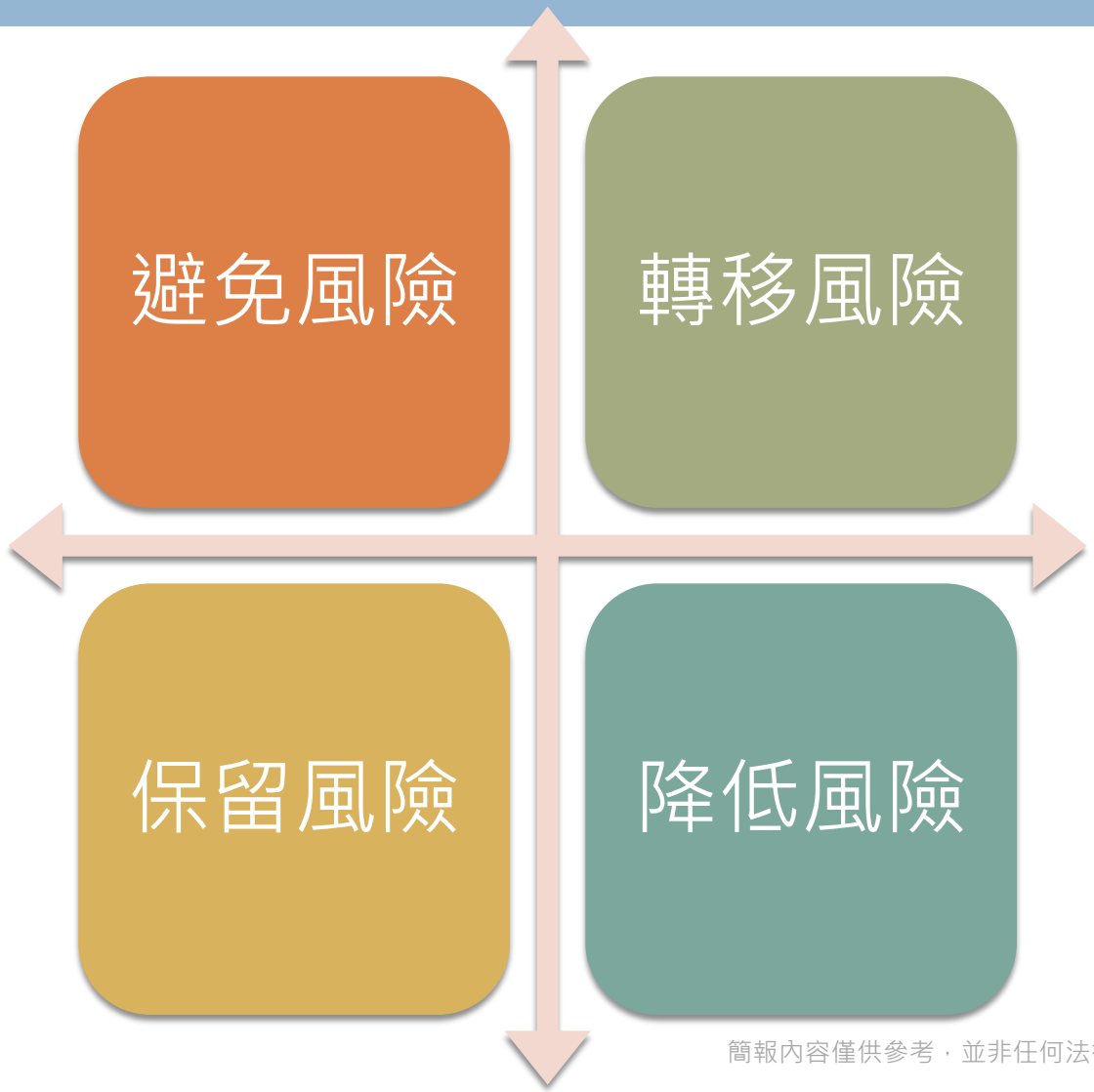
風險評鑑與風險處理管理流程



風險控管原則

- 決定組織可接受之風險值
- **高於可接受風險值者，優先控管或處理**
- 確認、控制及降低安全風險至可接受程度所採取的程序

風險控制策略



風險控制策略

- 避免風險
  - 修改作業方式或採用技術以避開風險
  - 經由政策或作業程序以禁止從事高風險交易或活動
- 轉移風險
  - 轉移相關之營運風險至他者，例如：承保商、供應商
- 保留風險
  - 知悉且客觀地接受風險
- 降低風險
  - 選擇適當之控制措施以降低風險
  - 藉由加強各項作業之內控以降低風險發生之機會

風險控制措施之選擇考量

- 時效性
  - 控制執行時間及有效期限為何
- 人力
  - 每年需要多少工時來監控和維護
  - 負責執行、監控及維護的人員需要接受多少訓練
  - 必須容易執行，了解對使用者造成多少程度不便
- 成本
  - 控制成本 < 資產價值, 威脅損失
- 法規或合約要求

風險處理階段

- 依據風險評鑑的結果，對於超出可接受程度之風險，進行處理
  - 降低風險發生機率
  - 降低風險造成之損害
- 風險處理計畫
  - 改善活動/控制措施
  - 風險進度追蹤
  - 風險再評鑑

風險處理工具

- 個人資料檔案風險處理計畫

個人資料檔案風險處理計畫

機密等級：□機密 ■限閱 □內部 □公開

文件編號：

版　　次：1.0

填表日期：　年　月　日

資產識別暨風險說明										風險處理措施		風險進度追蹤					風險再評鑑			
項次	單位	個資資產編號	資料類型	流程名稱	個人資料檔案名稱	個資評估值	風險緣由	事件	原風險值	風險處理型式	改善活動/控制措施	承辦人	預定完成日期	實際完成日期	覆核人員	風險處理進度	衝擊影響	可能性	風險值	覆核人員
										□接受風險 □降低風險 □轉移風險 □避免風險										
										□接受風險 □降低風險 □轉移風險 □避免風險										
										□接受風險 □降低風險 □轉移風險 □避免風險										

風險處理後

- **追蹤處理現況**
  - **建立評量指標(例如：KPI指標)**，協助控制目標達成
  - **執行內部稽核**，確保控制措施的有效性

- **除每年執行一次外，當有下列情況時，應執行風險評鑑作業**
  - 營運組織變更
  - 作業流程改變
  - 個人資料檔案新增或變更
  - 發生個資安全事件

專案時程提醒：

- 「個人資料檔案清冊(含風險評估表)」上傳校務行政資訊系統：**5/19(五)前**
- 內部稽核：8/9(三)、8/10(四)
- 外部稽核：11/23(四)、11/24(五)

Q & A

- 簡報完畢，謝謝聆聽