個人資料保護認知宣導
(個資檔案保護及外洩處理原則解析)

副總經理 彭至賢 (Sam Peng)

ISO27001/BS10012/ISO29100/ISO9001主導稽核員

PMP&APMP國際專案管理師

TTQS國家訓練品質計畫評核委員

Mobile: 0952-695460

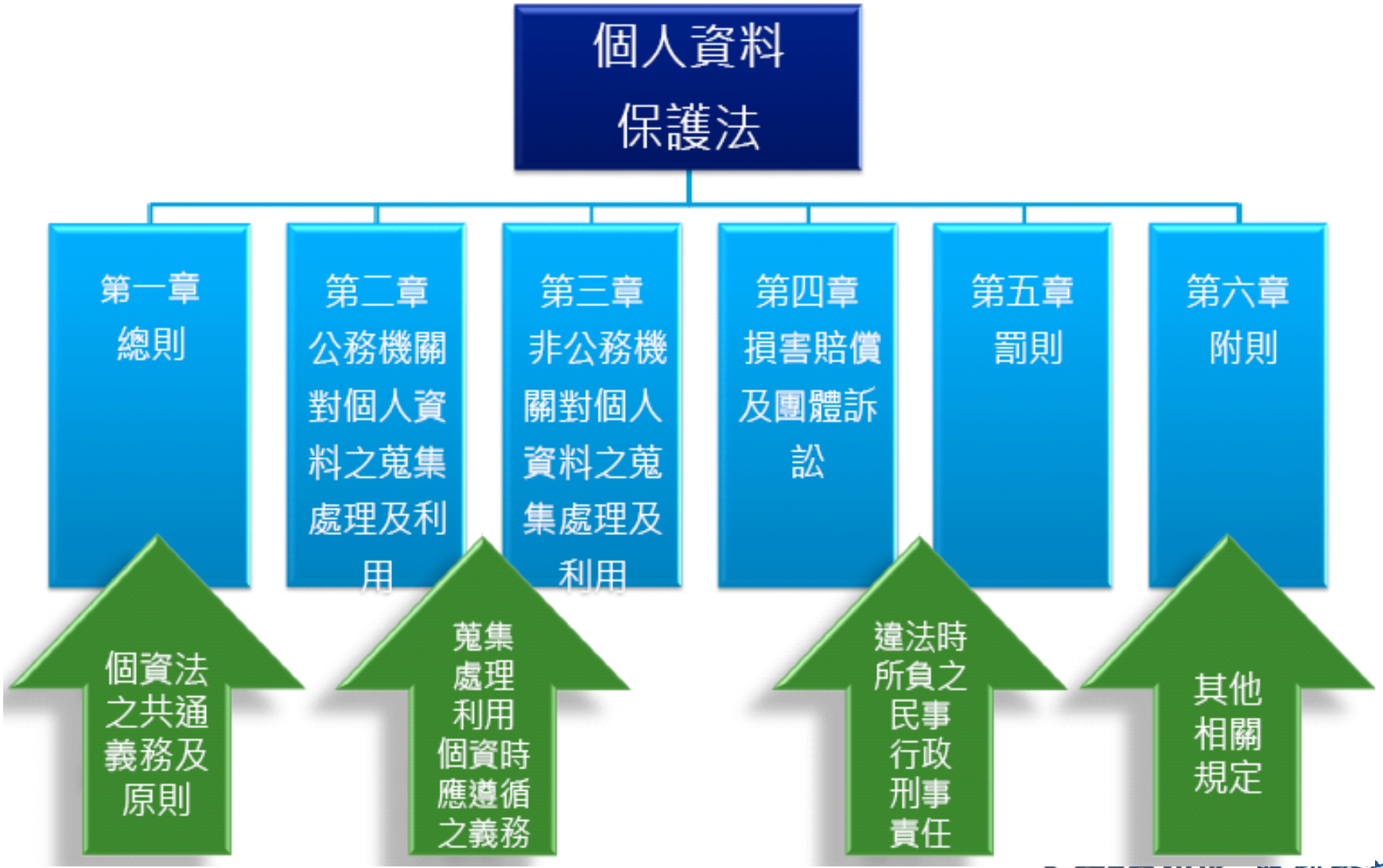
E-mail: sam@safelink.com.tw

SafeLink 博創資訊科技股份有限公司

簡報大綱

- **個人資料保護法重點摘要說明**
- 本校個資保護管理制度(PIMS)摘要說明
- 違反個資法之法律責任
- 個資外洩之通報、應變與處理方法
- 辦公室個資檔案加密保護觀念宣導與實作

個人資料保護法整體架構



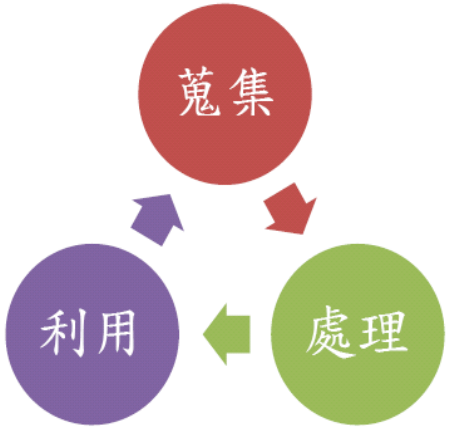
個人資料保護法架構

- 新版個資法：共56條條文
  - 修正日期：民國104年12月30日
  - 生效狀態：自中華民國105年03月15日施行。

個人資料保護法規範的行為(態樣)

- 個人資料檔案
  - 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。
    - 非經電腦處理的個人資料（如紙本）亦納入規範
- 蒐集
  - 以任何方式取得個人資料
    - 不限於為建立「個人資料檔案」取得
    - 包括直接向當事人蒐集、間接從第三人取得
- 處理
  - 為建立或利用「個人資料檔案」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。
    - 不限於電腦處理，可能是快遞寄送、影印機複製等行為。
- 利用
  - 將個人資料為處理以外之使用。
    - 直接對當事人使用其個人資料，例如對當事人從事行銷。
    - 將資料提供當事人以外之第三人亦屬於利用之行為

個人資料保護法規範的行為



- **蒐集(合法蒐集)**
  - 為建立個人資料檔案而取得個人資料
  - 取得方式不限，任何方式取得皆為蒐集
  - 包括「直接蒐集」與「間接蒐集」。
- **處理(安全地處理、儲存、傳輸及銷毀)**
  - 為建立或利用個人資料檔案所為之紀錄、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(特定目的內利用)**
  - 將蒐集之個人資料為「處理」外之使用。
- **國際傳輸**
  - 將個資作跨國(境)之處理或利用。

◎組織內部資料傳送 – 處理
◎將個資提供第三人 – 利用

公務機關個人資料之蒐集、處理及利用

- 第 15 條 (立法院於104年12月15日完成三讀修正)
  - 公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有**特定目的**，並符合下列情形之一者：
    - 一、執行法定職務必要範圍內。(§§10)
    - 二、經當事人同意。
    - 三、對當事人權益無侵害。

公務機關個人資料之蒐集、處理及利用

- 第 16 條 (立法院於104年12月15日完成三讀修正)
  - 公務機關對個人資料之**利用**，除第六條第一項所規定資料外，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：(§§10)
    - 一、法律明文規定。(§§9)
    - 二、為維護國家安全或增進公共利益所必要。
    - 三、為免除當事人之生命、身體、自由或財產上之危險。
    - 四、為防止他人權益之重大危害。
    - 五、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。(§§17)
    - 六、有利於當事人權益。
    - 七、經當事人同意。

資料違法外洩，一定要和當事人說嗎？

- 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**。(§12)

個資法規定的安全保護相關規定有哪些？

- 公務機關保有個人資料檔案者，**應指定專人辦理安全維護事項**，防止個人資料被竊取、竄改、毀損、滅失或洩漏。(§18)
- 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。(§27)
  - 中央目的事業主管機關得指定非公務機關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。
  - 前項計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關定之。(§27)

個資法施行細則所列之安全維護事項

- 保護標的：防止個人資料被竊取、竄改、毀損、滅失或洩漏。
  - 一、配置管理之人員及相當資源。
  - 二、界定個人資料之範圍。
  - 三、個人資料之風險評估及管理機制。
  - 四、事故之預防、通報及應變機制。
  - 五、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。
  - 七、認知宣導及教育訓練。
  - 八、設備安全管理。
  - 九、資料安全稽核機制。
  - 十、使用紀錄、軌跡資料及證據保存。
  - 十一、個人資料安全維護之整體持續改善。

必要措施以所須支出之費用與所欲達成之個人資料保護目的符合適當比例者為限。

此11項安全措施內容為參照英國BS10012:2009及日本JISQ15001:2006等個人資料管理系統之規範，以P-D-C-A 循環之概念予以建立。

簡報大綱

- 個人資料保護法重點摘要說明
- **本校個資保護管理制度(PIMS)摘要說明**
- 違反個資法之法律責任
- 個資外洩之通報、應變與處理方法
- 辦公室個資檔案加密保護觀念宣導與實作

依個資保護生命週期建置 PIMS

個資保護管理制度(PIMS)內涵說明

- 本校個資保護管理制度(PIMS)清單
  - **PIMS-2-001-02管制文件一覽表(紀錄)**

個資檔案防護實務

- 個人保管的紙本個資(包括名片)建議存放於上鎖的櫃子裡
- 個人電腦設備裡的個資檔案最好進行加密，可使用免費加密軟體如TrueCrypt、AxCrypt等
- 個人電腦設備裡已不再使用的個資檔案，應採用徹底刪除的軟體予以刪除，如 Eraser
- 透過網路(E-mail、即時通訊等)傳輸個資之前，應先進行加密，並以其他管道傳送加密的密碼
- 隨身碟因易遺失或遭偷竊盜用，應確保內含個資資料經過加密保護
- 社群網站上，不要隨意透漏個資，包括電話、地址、家人資訊、個人習慣、旅遊計畫等，且除非必要，儘量不要同意網站使用個人資料在其他用途及分享，另使用各種社交網站需進行相關「隱私設定」
- 收到各種訊息(簡訊、即時通訊、電子郵件)，若其中含有附檔或網址，應特別留意是否詐騙，點選前最好確認
- 個人的電腦設備和手機，應安裝防毒軟體，並注意軟體更新至最新版本
- 勿使用P2P軟體，不安裝非公務使用及非法不明之軟體

個人資料保護措施提醒

各單位辦公環境下班無人時，門、窗須上鎖或設定門禁。

處理完之個人資料檔案(紙本、電子)，若無需保留應立即絞碎或刪除(電子檔案應確實清除「資源回收筒」)，含有個人資料之報廢紙張不得回收及再利用。

針對存有個人資料之紙本文件及可攜式儲存媒體，不使用或下班時，應遵守桌面淨空政策，放置於抽屜或儲櫃並上鎖，以避免外洩。

伺服器、個人電腦及筆記型電腦應設定螢幕保護程式，並設定密碼或採取登出鎖定方式保護；自行啟動螢幕保護程式的時間設定應不超過10分鐘。

個人電腦(含筆記型電腦)應設密碼保護，密碼須英數字混合(密碼複雜度)且不得與帳號名稱相同，長度至少6碼，並不得與前次設定相同；原則上密碼至少3個月變更一次，最長不得超過6個月變更。

個人資料保護措施提醒(續)

- 個人保管的紙本個資(包括名片)建議存放於上鎖的櫃子裡
- 個人電腦設備裡的個資檔案最好進行加密，可使用免費加密軟體如TrueCrypt、AxCrypt等
- 個人電腦設備裡已不再使用的個資檔案，應採用徹底刪除的軟體予以刪除，如 Eraser
- 透過網路(E-mail、即時通訊等)傳輸個資之前，應先進行加密，並以其他管道傳送加密的密碼
- 隨身碟因易遺失或遭偷竊盜用，應確保內含個資資料經過加密保護
- 社群網站上，不要隨意透漏個資，包括電話、地址、家人資訊、個人習慣、旅遊計畫等，且除非必要，儘量不要同意網站使用個人資料在其他用途及分享，另使用各種社交網站需進行相關「隱私設定」
- 收到各種訊息(簡訊、即時通訊、電子郵件)，若其中含有附檔或網址，應特別留意是否詐騙，點選前最好確認
- 個人的電腦設備和手機，應安裝防毒軟體，並注意軟體更新至最新版本
- 勿使用P2P軟體，不安裝非公務使用及非法不明之軟體

注意委外廠商之監督與管理

- 蘋果日報 2013年04月04日
- 明志科大一名學生投訴，3月22日登入個人臉書帳號時，發現有同學發文表示，使用入口網站搜尋學校的電子郵件信箱網域mail2.mcut.edu.tw，搜尋結果會有多筆同學在學校網站線上填寫的個人履歷，包括姓名、電話、地址、電子郵件、生日、大頭照等對此，明志科技大學圖書資訊處系統開發組組長劉錫斌說，在3月初至3月中請廠商測試校內媒合工作的系統功能，約200筆個人資料，不慎遭搜尋引擎取得資料連結路徑，廠商作業有疏失，自行發現後處理未完全，經學生反映，已完全刪除完畢，會要求廠商負責相關責任

- **宇軒國際法律事務所律師廖芳萱表示，校方委外廠商疏失致學生個資洩露，可歸責於校方，依法如不易或不能證明損害者，可請求500元以上、2萬元以下賠償**

簡報大綱

- 個人資料保護法重點摘要說明
- 本校個資保護管理制度(PIMS)摘要說明
- **違反個資法之法律責任**
- 個資外洩之通報、應變與處理方法
- 辦公室個資檔案加密保護觀念宣導與實作

法律責任之範圍

行政責任

法定義務

法定職務

民事責任

刑事責任

行政責任

- §§47~50行政責任 (僅限非公務機關)
  - §47違反特定目的外之利用
    - §6 I 特種個人資料蒐集、處理、利用~~(暫緩施行)~~
    - §19 非公務機關蒐集、處理應有特定目的
    - §20 I 非公務機關特定目的外之利用
    - §21 國際傳輸之限制
    - 處新臺幣五萬元以上五十萬元以下罰鍰，並令限期改正，屆期未改正者，按次處罰之
  - §48 違反告知及基本權利履行未訂定個資檔案安全維護計畫
    - §8 直接蒐集之告知
    - §9 間接蒐集之告知
    - §10 答覆查詢、閱覽或製給複製本
    - §11 請求更正或補充
    - §12 適當方式通知當事人
    - §13 受理准駁之決定
    - §20 II,III 當事人拒絕行銷之決定
    - §27 I,II 個人資料檔案安全維護計畫
    - 限期改正，屆期未改正者，按次處新臺幣二萬元以上二十萬元以下罰鍰
  - §49 規避、妨礙或拒絕行政檢查
  - §50 連帶處罰

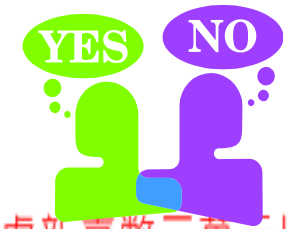
違反者立即處分

限期改正！誰會被罰？

規避行政檢查、連帶處罰

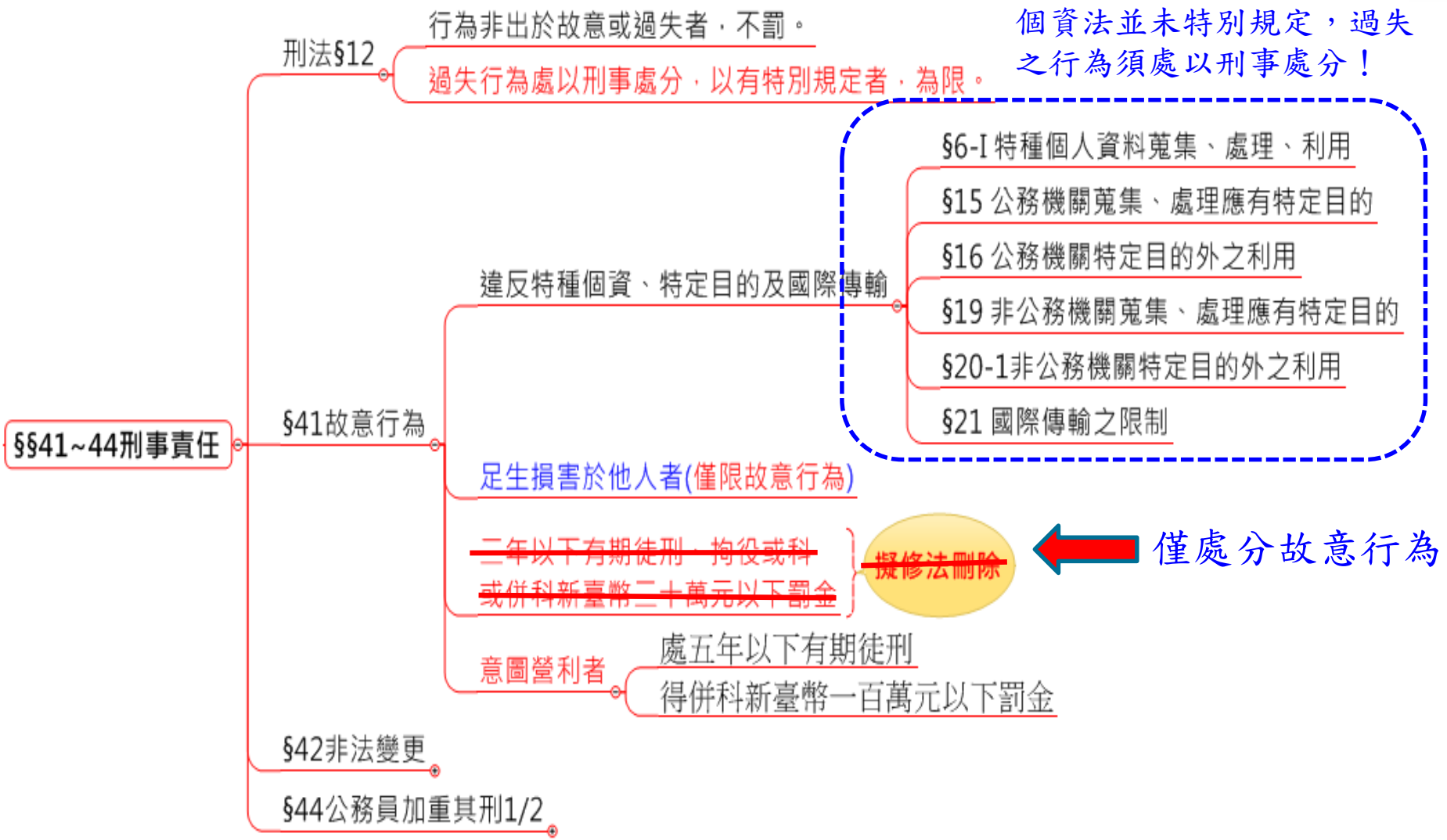
§§47~50行政責任
(僅限非公務機關)

- §47違反特定目的外之利用
- §48
- §49 規避、妨礙或拒絕行政檢查
  - 處新臺幣二萬元以上二十萬元以下罰鍰
- §50 連帶處罰
  - 受前三條之罰鍰處罰
    - 代表人、管理人或其他有代表權人，除能證明已盡防止義務者外，應並受同一額度罰鍰之處罰

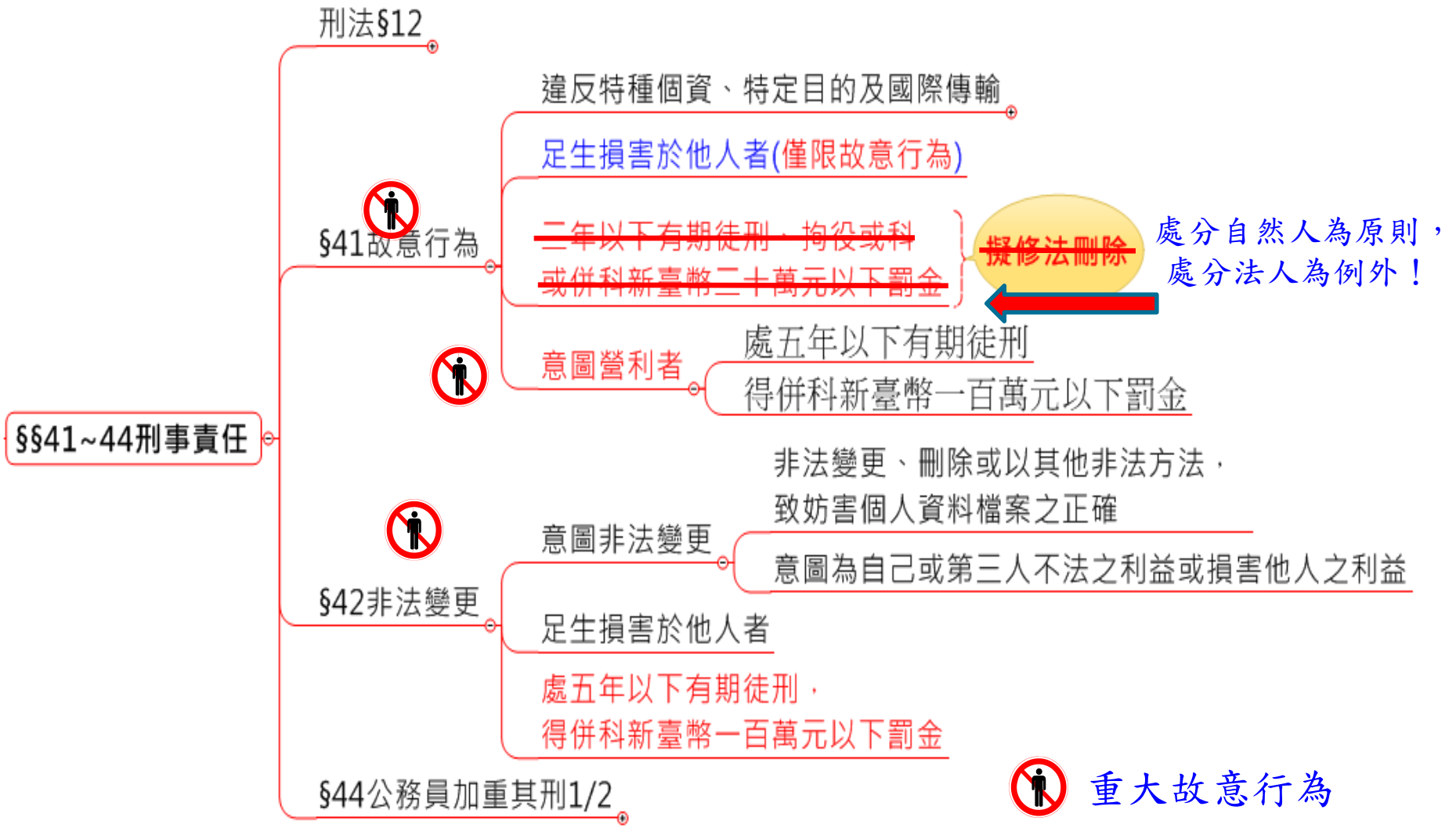


第五十條　非公務機關之代表人、管理人或其他有代表權人，因該非公務機關依前三條規定受罰鍰處罰時，除能證明已盡防止義務者外，應並受同一額度罰鍰之處罰。

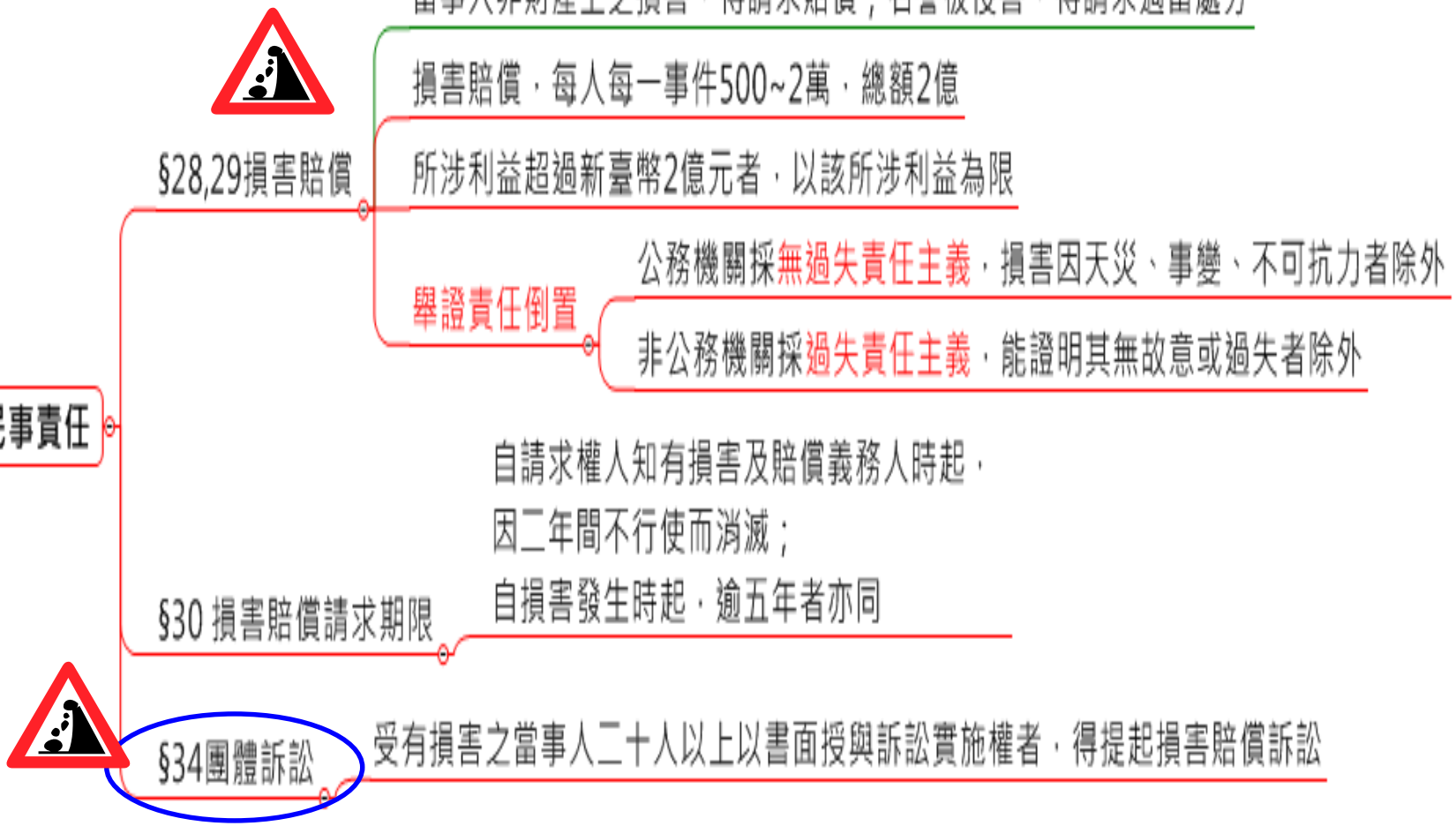
刑事責任


§§41~44刑事責任
刑法§12
行為非出於故意或過失者，不罰。
過失行為處以刑事處分，以有特別規定者，為限。
§41故意行為
違反特種個資、特定目的及國際傳輸
§6-I 特種個人資料蒐集、處理、利用
§15 公務機關蒐集、處理應有特定目的
§16 公務機關特定目的外之利用
§19 非公務機關蒐集、處理應有特定目的
§20-1非公務機關特定目的外之利用
§21 國際傳輸之限制
足生損害於他人者(僅限故意行為)
二年以下有期徒刑、拘役或科
或併科新臺幣二十萬元以下罰金
擬修法刪除
意圖營利者
處五年以下有期徒刑
得併科新臺幣一百萬元以下罰金
§42非法變更
§44公務員加重其刑1/2
個資法並未特別規定，過失之行為須處以刑事處分！
僅處分故意行為

意圖營利、非法變更



民事責任


§§28~34民事責任
§28,29損害賠償
當事人非財產上之損害，得請求賠償；名譽被侵害，得請求適當處分
損害賠償，每人每一事件500~2萬，總額2億
所涉利益超過新臺幣2億元者，以該所涉利益為限
舉證責任倒置
公務機關採無過失責任主義，損害因天災、事變、不可抗力者除外
非公務機關採過失責任主義，能證明其無故意或過失者除外
§30 損害賠償請求期限
自請求權人知有損害及賠償義務人時起，因二年間不行使而消滅；
自損害發生時起，逾五年者亦同
§34團體訴訟
受有損害之當事人二十人以上以書面授與訴訟實施權者，得提起損害賠償訴訟

舉證責任倒置

- 公司舉證責任：（第29條）
  - 公司必須負責「舉證責任」，證明自己符合法規要求且已善盡保管責任，無故意或過失責任才能免責

  - 各種告知義務、取得當事人同意或回應個人請求等行為，都必須留下記錄以作為未來舉證之用

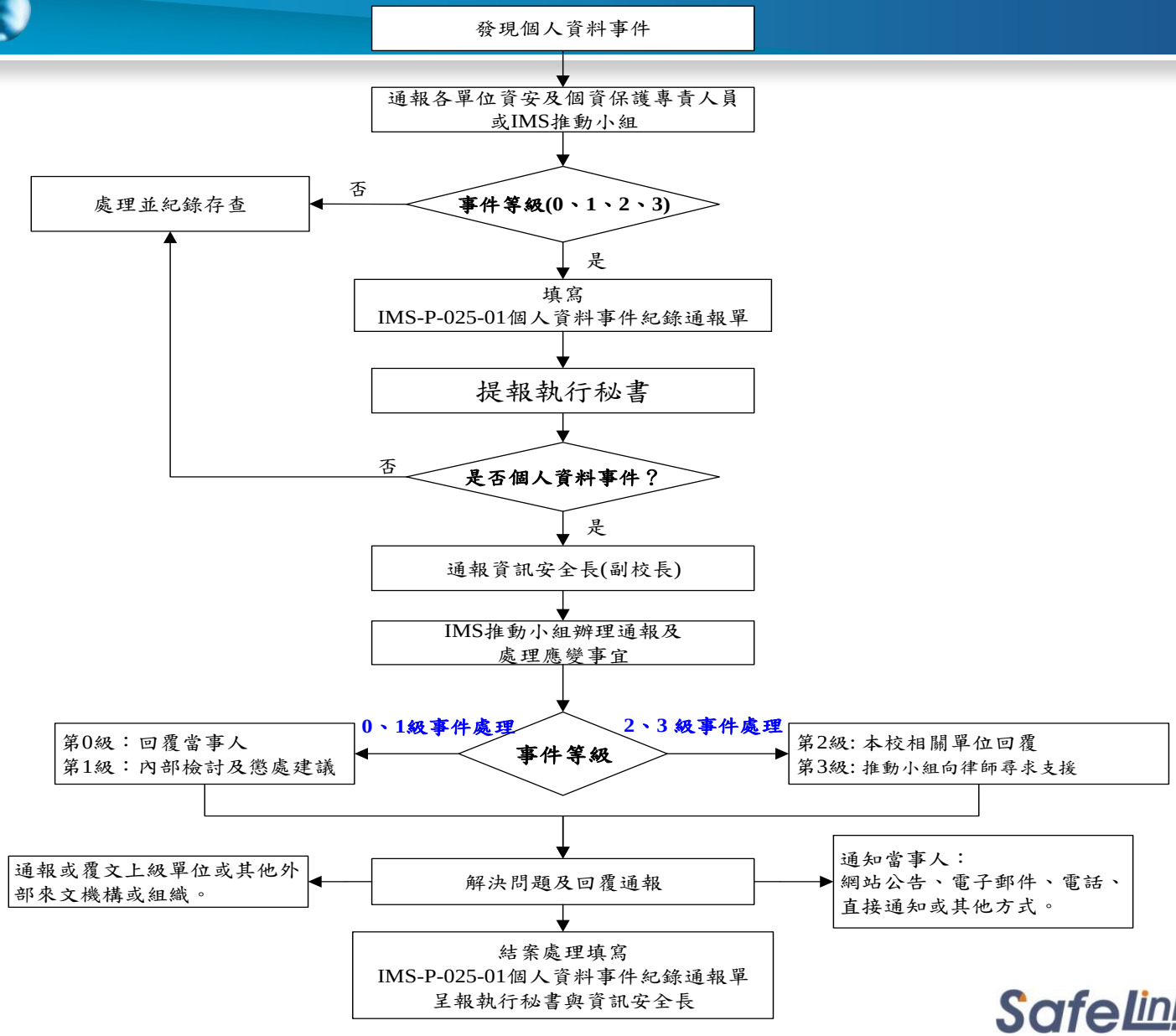
簡報大綱

- 個人資料保護法重點摘要說明
- 本校個資保護管理制度(PIMS)摘要說明
- 違反個資法之法律責任
- **個資外洩之通報、應變與處理方法**
- 辦公室個資檔案加密保護觀念宣導與實作

個資外洩之通報、應變與處理方法

- 本校已建立違反個資法之個資事件通報與處理之作業程序(SOP)
  - **PIMS-2-012個人資料事件管理程序**
  - **PIMS-2-012-01個人資料事件紀錄通報單**
- 某學校個資外洩案例之處置與分享
  - 案例描述：**人事室同仁於107年X月X日15時34分以電子郵件轉寄全校教職員工有關終身學習時數完成名單，因一時失察將名單以附件方式寄出，導致該名單揭露給校內所有同仁。本事件共計揭露個人資料60筆，內容包含：機關名稱、部門、身分證號、姓名、職稱、人員區別、官職等一般個資。**
  - **處置方式詳如矯正及預防措施處理單及個人資料事件紀錄通報單。**

個資事件之通報及處理流程圖



簡報大綱

- 個人資料保護法重點摘要說明
- 本校個資保護管理制度(PIMS)摘要說明
- 違反個資法之法律責任
- 個資外洩之通報、應變與處理方法
- **辦公室個資檔案加密保護觀念宣導與實作**

辦公室個資檔案加密保護觀念宣導與實作

- 檔案加密實作演練
  - **Word**檔案類型加密碼實作演練
  - **Excel**檔案類型加密碼實作演練
  - **Powerpoint**檔案類型加密碼實作演練

- 使用**WinZip**軟體檔案加密實作演練

Q&A 問題與討論

～如有任何問題，歡迎隨時來電詢問～

SafeLink

博創資訊科技股份有限公司

臺中市西屯區國安一路208巷6號

TEL：(04)2525-0535

FAX：(04)2461-5268

http://www.safelink.com.tw/

E-mail: sam@safelink.com.tw