明新科技大學
Minghsin University of Science and Technology

個人資料管理制度稽核宣導教育訓練

2023.11.20

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

- 重要個資政策宣導
- 個資清冊、風險評估表 重點說明
- 稽核宣導
  - 稽核過程注意事項
  - 稽核重點說明
  - 稽核前自我檢核事項
- 電腦安全性設定提醒(Win 10)

大綱

- 重要個資政策宣導
- 個資清冊、風險評估表 重點說明
- 稽核宣導
  - 稽核過程注意事項
  - 稽核重點說明
  - 稽核前自我檢核事項
- 電腦安全性設定提醒(Win 10)

20210908學校使用資通系統或服務蒐集及使用個人資料注意事項

一、鑒於學校使用雲端資通服務(如Google表單等)蒐集個人資料時，可能因設定不當而增加個資外洩及資安風險，請各校使用資通系統或雲端資通服務蒐集教職員、學生及家長個人資料者，應注意旨揭事項，以「最小化」為原則，降低風險，並請各校主管機關加強宣導並督導所轄學校。

二、另提醒教職員工在處理個人資料時，應注意以下法規：

(一)個人資料保護法第28條第1項「公務機關違反個人資料保護法規定，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。」

(二)個人資料保護法第41條第1項「違反個人資料保護法有關特種資料的蒐集、處理或利用規定，足生損害於他人者，處二年以下有期徒刑、拘役或科或併科新臺幣二十萬元以下罰金。」

Google表單蒐集個人資料使用原則

- 以「Google表單蒐集個人資料」為例，特別說明以下六點應特別注意的操作細節，以免處理不當導致嚴重個資外洩事件。

資料來源：教育機構資安驗證中心
https://sites.google.com/email.nchu.edu.tw/g-form/%E9%A6%96%E9%A0%81?authuser=1#h.y1xo3nv42k4r

大綱

- 重要個資政策宣導
- **個資清冊、風險評估表 重點說明**
- 稽核宣導
  - 稽核過程注意事項
  - 稽核重點說明
  - 稽核前自我檢核事項
- 電腦安全性設定提醒(Win 10)

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

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。(個資法§6)

其他資料
- 得以直接或間接方式識別該個人之資料

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。

個資盤點清冊諮詢常見問題(1/2)

- 盤點表內容與同仁實際作業流程不符，如：
  - **個資檔案名稱不明確(去年外部稽核發現)。**
  - 蒐集個資範圍、保存期限、處理或利用行為不一致。
- 不清楚個資流程角色定義(控制者/處理者/共同控制者)。
- 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)
- **個資範圍評估值誤植(去年外部稽核發現)**。

風險評鑑工具

- 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								

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。

風險評估作業注意事項

- 風險值評分漏列，例如有利用行為(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

本年度風險評鑑結果

- 本年度可接受風險值建議為15，風險值為15以上之個人資料檔案，須進行風險處理作業。
- 112年度本校共計鑑別出5個單位應進行風險處理作業，高風險個人資料檔案統計如下表所示。

單位 / 風險值	16	18	24	總計
學生事務處-衛生保健組	3	0	0	3
學生事務處-進修學務組	1	0	0	1
總務處-文書組	0	2	0	2
國際暨兩岸事務處-境外招生中心	1	0	0	1
人力資源處	0	0	2	2
總計	5	2	2	9

風險處理工具

- 個人資料風險處理計畫表→確認是否已完成改善及風險再評鑑作業

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										

大綱

- 重要個資政策宣導
- 個資清冊、風險評估表 重點說明
- **稽核宣導**
  - 稽核過程注意事項
  - 稽核重點說明
  - 稽核前自我檢核事項
- 電腦安全性設定提醒(Win 10)

稽核過程注意事項(1/3)

- 先聽完問題再回答
- 問題不了解，可以請稽核員再說明
- 如果明確了解，請直接回答
- 如果不記得，請先查找程序書再回答
- 視情況請其他同事支援，**不要硬答**

稽核過程注意事項(2/3)

- **要做 或 可以做**
  - 說明應依據公告管理制度文件為主
  - **提供執行證據**
  - 客氣回答與請教語氣
  - 適時導向其他負責人說明
  - **被發現有問題也要展現在你的控制之中（不要擴大解釋）**

稽核過程注意事項(3/3)

- **不要做**
  - 激辯、強烈反駁
  - 說謊、圓謊
  - **否定稽核員的發現**
  - 抱怨
  - 私下的作法
  - 反駁其他同事的回答
  - **回答「不知道」**
  - **遲遲不提供證據**

稽核重點說明(1/2)

- **前次內外稽矯正確認**
  - 矯正預防處理單，確認實際處理情況，並完成追蹤簽核
  - 未矯正完成，容易變成缺失
- **風險評鑑作業**
  - 風險評估表、風險評鑑彙整表、風險處理計畫
    - 風險值=個資範圍評估值×（衝擊影響+可能性）
    - 可接受風險值，112年度為**15，超過15以上須進行風險處理**
    - 風險再評鑑(前一年度高風險追蹤)

稽核重點說明(2/2)

- 個資告知聲明
- 個資蒐集最小化、特定目的合宜性
- 個資保存期限設定、銷毀紀錄
- 當事人權利行使紀錄
- 委外管理(合約、保密切結、監督責任等)
- 使用Google表單活動結束後是否確實關閉
- 個資安控紀錄(防毒、更新、備份、帳號清查等)

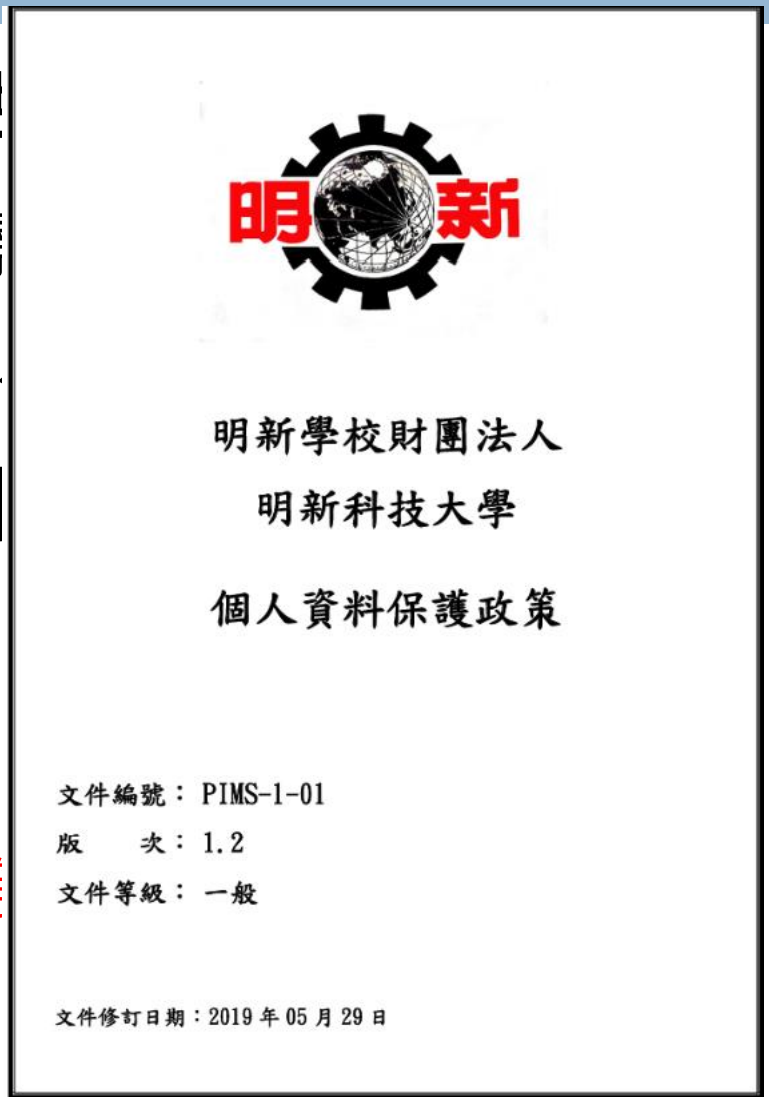
稽核前自我檢核事項(1/3)

- **請於稽核當天準備相關文件**
  - 前次內外稽矯正處理紀錄
  - 個資清冊、風險評估表、風險處理計畫
  - 個資銷毀紀錄
  - 個資告知事項與同意證明
  - 個資委外合約、保密切結書

請注意資料之正確性及表單記錄填寫之完整性

稽核前自我檢核事項(2/3)

- **請確認下述事項，單位**
  - 無人看管之環境/設備(如
    個人桌面，確認未涉及個
- **請確認單位同仁應知悉**
  - 本校「個人資料保護政策」
    同步通知委外廠商)
  - 個資範圍評估值、風險值等



明新學校財團法人

明新科技大學

個人資料保護政策

文件編號： PIMS-1-01

版　　次： 1.2

文件等級： 一般

文件修訂日期：2019 年 05 月 29 日

稽核前自我檢核事項(3/3)

- **請確認下述事項，單位做到了嗎？**
  - 個人電腦
    - 密碼長度至少8碼，至少180天更新1次
    - 作業系統安全性更新、病毒碼，應維持最新版本
    - 勿安裝非正版授權之軟體
    - 螢幕保護程式設定，不超過10分鐘
    - 請確認「資源回收筒」，未含機敏(個資)資料檔案之電子檔
  - 電子郵件信箱
    - 請確保「寄件備份」未含機敏(個資)資料檔案檔案之信件內容
    - 含有個資檔案於傳輸時應進行加密

大綱

- 重要個資政策宣導
- 個資清冊、風險評估表 重點說明
- 稽核宣導
  - 稽核過程注意事項
  - 稽核重點說明
  - 稽核前自我檢核事項
- **電腦安全性設定提醒(Win 10)**

大綱

- 重要個資政策宣導
- 個資清冊、風險評估表 重點說明
- 稽核宣導
  - 稽核過程注意事項
  - 稽核重點說明
  - 稽核前自我檢核事項
- **電腦安全性設定提醒(Win 10)**

帳戶/系統/軟體設定：

- 電腦登入密碼**最少8碼**
- 密碼複雜度[英文大小寫、數字、符號]
- 稽核系統事件紀錄
- 稽核特殊權限使用紀錄
- 稽核登入事件紀錄
- 【Guest】【Administrator】帳戶停用
- 螢幕保護程式**(不應超過10分鐘)**
- 檢查防毒軟體、P2P軟體

今年度個人資料落實情形自我查檢表，已請個資窗口進行設定，請同仁於外部稽核前再次自行確認。

Q & A

- 簡報完畢，謝謝聆聽