



個人資料管理制度稽核宣導 教育訓練

2024.11.14

大綱

2

- 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、Win11)



大綱

3

- 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、Win11)



20241107各級學校使用資通系統或服務蒐集及使用個人資料之注意事項

4

- 一、鑒於學校使用媒體網路影音平臺（如Youtube等）上傳作業時，可能因權限管理不當導致學生權利受到侵害，請各校使用媒體網路影音平臺請學生上傳作業者，應注意旨揭事項，做好帳號及權限之管理，降低風險，並請各校主管機關加強宣導所轄學校。
- 二、綜上，為了維護學生的基本權益，各校應加強宣導學生使用數位平臺之相關知能及素養，例如須注意隱私、分享等相關設定，降低資料非經當事人同意之使用行為風險；此外，教師使用數位平臺進行教學活動時，若課程所蒐集之學生作業或報告內含個資或隱私資訊者（如學生影音資料等），教師應妥為保管，並注意使用權限，於課程結束後，應做適當處置。

20241107各級學校使用資通系統或服務蒐集及使用個人資料之注意事項

5

- (一)依個人資料保護法第11條第3項「個人資料蒐集之特定目的消失或期限屆滿時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。」，當事人之影片應於作業批改完成後立即刪除並下架，並確保離線備份皆已刪除。
- (二)依個人資料保護法第16條「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。」，僅蒐集適當、相關且限於處理目的所必要之個人資料，處理及利用時，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。
- (三)依個人資料保護法第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。」，應注意當事人影片或其他個人資料是否正當使用及留存，以避免違反個人資料保護法之規定。

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。

					
<u>1. 「個人資料蒐集聲明」的處理方式</u>	<u>2. 落實「資料最少蒐集原則」</u>	<u>3. 避免不小心公開作答內容</u>	<u>4. 不應執行「發布到網路」功能</u>	<u>5. 不應開放給不相關人員存取權限</u>	<u>6. 雲端檔案切勿放置在共用資料夾</u>

大綱

7

- 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、Win11)



何謂個人資料 (個資法§2、§6)

8

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)

9

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。

個資盤點清冊作業常見問題(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(前年外部稽核發現)。
 - 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)。

簡報內容僅供參考，並非任何法律意見，請斟酌使用簡報。

個資盤點清冊作業常見問題(2/2)

- 「個人資料檔案名稱」填寫校外系統(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(前年外部稽核發現、今年度盤點結果)。

風險評鑑工具

12

□ 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： <input type="checkbox"/> 機密 <input checked="" type="checkbox"/> 限閱 <input type="checkbox"/> 內部 <input type="checkbox"/> 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							0	
9								
10								
11								
12								

個資檔案風險值計算

13

□ 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： <input type="checkbox"/> 機密 <input checked="" type="checkbox"/> 限閱 <input type="checkbox"/> 內部 <input type="checkbox"/> 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							0	
9								
10								
11								
12								

風險值
取
最大值

風險評估分析構面表-1-1

14

評估值	衝擊影響
4	<p>嚴重傷害：</p> <ol style="list-style-type: none">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. <u>對組織形象造成嚴重的影響</u>，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	<p>重大傷害：</p> <ol style="list-style-type: none">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

15

評估值	衝擊影響
2	<p>中度傷害：</p> <ol style="list-style-type: none">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	<p>低度傷害：</p> <ol style="list-style-type: none">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

16

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(1/2)

- 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



風險評估作業注意事項(2/2)

- 風險評估表構面一未依據程序書要求之數量級距進行評分。
- 風險值計算公式錯誤，應該為風險值 = 個資範圍評估值X（衝擊影響 + 可能性）。



本年度風險評鑑結果

19

- 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。
- 113年度本校共計鑑別出3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	總計
學生事務處-衛生保健組	3	3
人力資源處	3	3
圖書資訊處-系統維運組	1	1
總計	7	7

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： <input type="checkbox"/> 機密 <input checked="" type="checkbox"/> 限閱 <input type="checkbox"/> 內部 <input type="checkbox"/> 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
										<input type="checkbox"/> 接受風險 <input type="checkbox"/> 降低風險 <input type="checkbox"/> 轉移風險 <input type="checkbox"/> 避免風險										
										<input type="checkbox"/> 接受風險 <input type="checkbox"/> 降低風險 <input type="checkbox"/> 轉移風險 <input type="checkbox"/> 避免風險										
										<input type="checkbox"/> 接受風險 <input type="checkbox"/> 降低風險 <input type="checkbox"/> 轉移風險 <input type="checkbox"/> 避免風險										

大綱

21

- 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、Win11)



稽核過程注意事項(1/3)

22

- 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)

23

□ 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)

24

□ 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(1/3)

25

□ 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
 - $\text{風險值} = \text{個資範圍評估值} \times (\text{衝擊影響} + \text{可能性})$
 - 可接受風險值，113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(2/3)

26

- 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)
- (去年外部稽核發現 :委外廠商持有資料庫系統最高權限、共用帳號)

稽核重點說明(3/3)

27

- 本校個人資料文件程序書及表單：教職員校務行政資訊系統(單一簽入)→回公告一覽→個人資料文件程序書→MUST_PIMS管理文件_20231025.7z

明新科技大學

校內系統快速連結

回公告一覽 > 系統公告一覽

選擇系統主選單
[全校]校務管理資訊作業

選擇系統子選單
[登入]單一簽入管理作業

回校內系統快速連結
回公告一覽

BO 表單代登管理

資料查詢(取消查詢會回到原始資料)

取消查詢 公告標題

系統類別 系統子類別 資料掛序

[全校]校務管理資訊作業 [資安]個人資安盤點管理 公告時間 遞減

資料數量: 5
目前頁數: 1/1

查詢公告	系統類別	系統子類別	公告標題	公告時間
查詢	[全校]校務管理資訊作業	[資安]個人資安盤點管理	112/08/09內部稽核結果與報告	2023/08/23
查詢	[全校]校務管理資訊作業	[資安]個人資安盤點管理	個資清冊與風險評估表填寫注意事項	2020/05/12
查詢	[全校]校務管理資訊作業	[資安]個人資安盤點管理	個人資料文件程序書	2016/02/22
查詢	[全校]校務管理資訊作業	[資安]個人資安盤點管理	供應廠商涉及個人資料安全盤點稽核表	2015/09/14
查詢	[全校]校務管理資訊作業	[資安]個人資安盤點管理	PIMS-1-01_個人資料保護政策_v1.1	2015/03/14

更新日期：2023年10月26日

文件階層	文件編號	文件名稱	文件版本	修訂日期	備註	文件編號	文件名稱	文件版本	修訂日期	備註
L1	PIMS-1-01	個人資料保護政策	1.2	2019/5/29		FO-PIMS-1-01-01	個人資料隱私權宣告與說明	1.2	2019/5/29	
	PIMS-2-01	個人資料保護推行組織與責任分工程序書	1.6	2023/10/25		FO-PIMS-2-01-01	個人資料保護推行組織成員表	1.2	2018/5/16	
						FO-PIMS-2-01-02	外部單位聯絡清單	1.0	2015/9/14	
						FO-PIMS-2-02-01	個人資料保護管理文件列表	1.1	2016/3/14	
						FO-PIMS-2-02-02	個人資料外來文件管制表	1.1	2018/5/16	
PIMS-2-02		個人資料文件及紀錄管理程序書	1.3	2019/5/29		FO-PIMS-2-02-03	個人資料文件(紀錄)調閱申請單	1.0	2015/9/14	
						FO-PIMS-2-02-04	個人資料文件修訂建議表	1.0	2015/9/14	
						FO-PIMS-2-02-05	個人資料文件名詞解釋彙整表	1.2	2018/5/16	
						FO-PIMS-2-03-01	個人資料檔案清冊	1.1	2019/4/8	
PIMS-2-03		個人資料檔案清查暨風險管理程序書	1.3	2019/5/29		FO-PIMS-2-03-02	風險評估表	1.1	2019/4/8	
						FO-PIMS-2-03-03	個人資料風險處理計畫表	1.0	2018/5/16	

稽核前自我檢核事項(1/3)

28

□ 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(去年外部稽核發現)
- ▣ 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)

29

- 請確認下述事項，單位估
 - ▣ 無人看管之環境/設備(如影個人桌面，確認未涉及個
- 請確認單位同仁應知悉事
 - ▣ 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)

30

□ 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

31

- 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、Win11)



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

36

□ 簡報完畢，謝謝聆聽

