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

2025.11.05

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、Win11)**

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、Win11)

20250204「學校使用資通系統或服務蒐集及使用個人資料注意事項」

學校為特定目的使用資通系統或雲端資通服務（如Google 表單、Microsoft Forms 等問卷調查服務，YouTube等影音平台等）涉及蒐集、處理及利用個人資料者，應注意下列事項：

（一）資料蒐集最小化：僅蒐集**適當、相關且限於處理目的所必要**之個人資料。

（二）資料處理及利用：**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）存取控制：應注意檔案存取權限設定，應**採最小權限原則**，僅允許使用者依目的，指派任務所需之最小授權存取。

（四）使用雲端資通服務者，應詳閱設定內容，不宜使用者共同編輯個人資料檔案清冊，並應注意**避免設定允許顯示其他使用者作答內容（如Google 表單不應勾選「顯示摘要圖表和其他作答內容」），避免使用者能瀏覽其他使用者資料**，造成個人資料外洩。公佈前應確實做好相關設定檢查，並實際操作測試，確認無誤後再行發布。

20250204「學校使用資通系統或服務蒐集及使用個人資料注意事項」

（五）傳輸之機密性：網路傳輸應採用網站安全傳輸通訊協定（HTTPS）**加密傳輸**，並使用TLS 1.2 以上版本傳輸。

（六）資料儲存安全：如涉及蒐集個人資料保護法第六條之個人資料或其他敏感個人資料，**應以加密方式儲存**。其餘個

十八條及第二十七條資料儲存安全措施之

（七）應**訂定個人資料保存期限，並於**

予以刪除或銷毀，避免個人資料外洩。

服務電話：+886-3-5593142#2531、2543、2532
地址：30401新竹縣新豐鄉新興路1號資訊大樓1樓
Email： pims@must.edu.tw

（八）應設置**個人資料保護申訴或諮詢窗口**，以確保個資當事人具明確行使其權利之管道，且該管道應明確並便利當事人使用。

（九）學校在蒐集個人資料前，除符合個人資料保護法第八條第項各款情形外，應**明確告知當事人同法第八條第一項各款應告知事項及適當之申訴管道**，俾利當事人充分了解所蒐集之目的及相關權利。

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、Win11)

何謂個人資料 (個資法§2、§6)

個資法§2

一般資料

- 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
- 得以直接或間接方式識別該個人之資料

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)

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。
  - 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) 漏盤點。 (去年外部稽核發現)**
- 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**。
- 保有依據不適切。(**法律>執行法定職務或履行法定義務>當事人同意**) 。

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**)。
- 因未定義保存期限，所以目前資料都永久保存(**應參考法令法規或內部規定，訂定適切之保存期限**)。

「個人資料檔案清冊」請務必取得單位主管核可之紀錄。

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
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(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(1/2)

- 本年度可接受風險值建議為12，風險值為12以上之個人資料檔案，須進行風險處理作業。
- 114年度本校共計鑑別出18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	15	16	總計
教務處-註冊組	4	0	4
教務處-進修教務組	2	0	2
學生事務處-衛生保健組	0	3	3
學生事務處-課外活動指導組	3	0	3
學生事務處-諮商輔導暨職涯發展中心	1	0	1
人力資源處	0	3	3
總務處-文書組	2	0	2

本年度風險評鑑結果(2/2)

單位 / 風險值	15	16	總計
財務處	3	0	3
圖書資訊處-系統維運組	1	1	2
圖書資訊處-人工智慧與網路維安組	1	0	1
圖書資訊處-圖書資源服務組	1	0	1
國際事務處-外籍暨僑生輔導中心	4	0	4
國際事務處-新南向暨新住民中心	3	0	3
半導體學院-半導體與光電科技系	2	0	2
半導體學院-電機工程系	3	0	3
半導體學院-應用材料科技系	3	0	3
民生學院-幼兒保育系	1	0	1
民生學院-休閒事業管理系	1	0	1
總計	35	7	42

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、Win11)

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(1/4)

- **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，114年度為**12，超過12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(2/4)

- 個資告知聲明

(去年外部稽核發現 :未告知或告知不完整)

- 個資蒐集最小化、特定目的合宜性
- 個資保存期限設定、銷毀紀錄填寫完整性

(去年外部稽核發現 :未銷毀、未填寫「FO-PIMS-3-03-01 個人資料銷毀紀錄表」、銷毀紀錄資訊不完整)

- 當事人權利行使紀錄
- 委外管理(合約、保密切結、監督責任等)

稽核重點說明(3/4)

- 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、系統帳號清查、密碼管理、實體保護等)

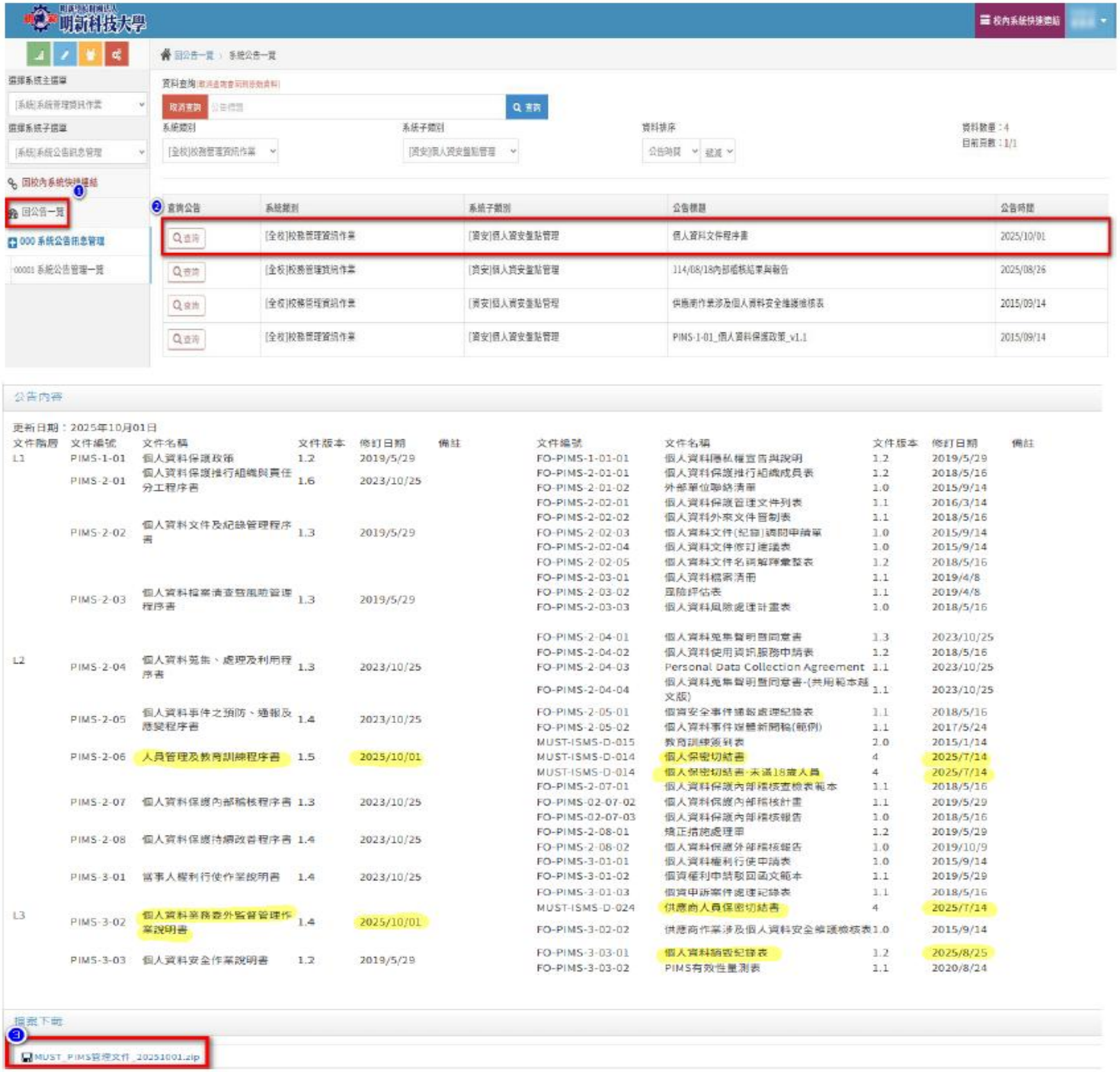
去年外部稽核發現：

- 密碼長度或變更頻率不符合規定
- 安裝無正式授權軟體
- 個資實體保護不足(跨單位共用資料櫃)

稽

- 本
- 登
- 人
- MU

個



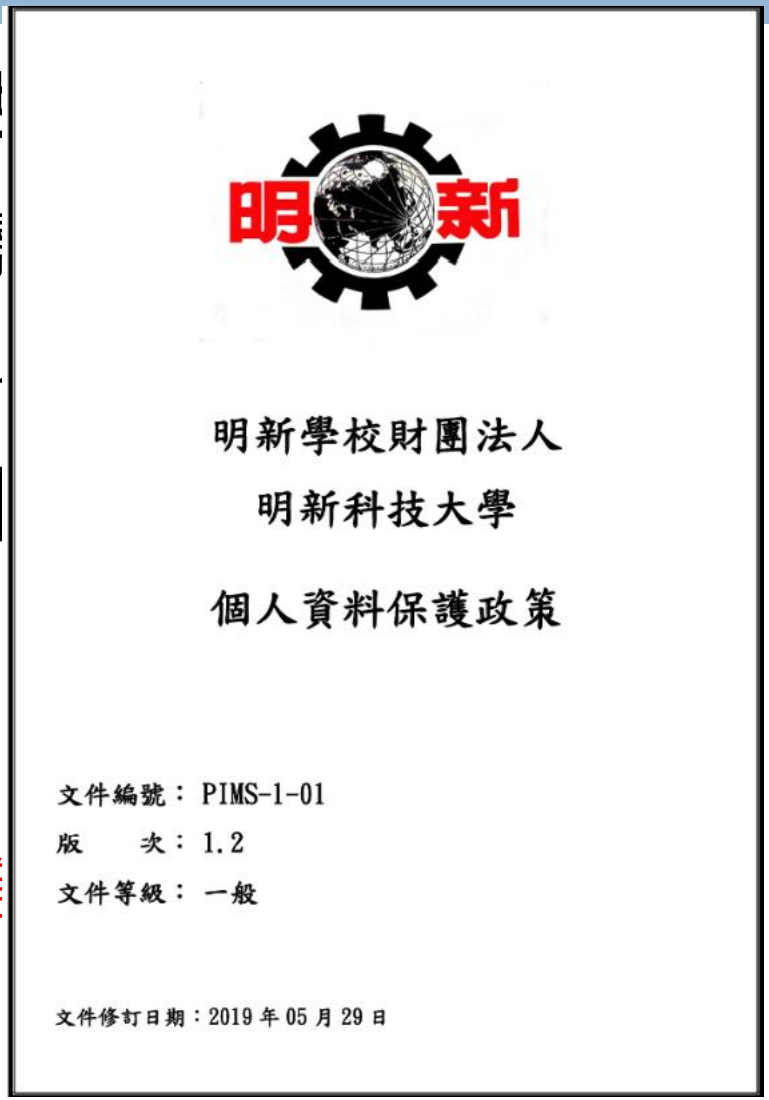
稽核前自我檢核事項(1/3)

- **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、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

- 簡報完畢，謝謝聆聽