112年基隆市中和國小

資安三小時研習

2003.09.20

請記得簽到

資安法

附表七　資通安全責任等級D級之各機關應辦事項

制度面向	辦理項目	辦理項目細項	辦理內容
技術面	資通安全防護	防毒軟體	初次受核定或等級變更後之一年內，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。
		網路防火牆	
認知與訓練	資通安全教育訓練	一般使用者及主管	每人每年接受三小時以上之資通安全通識教育訓練。

備註：特定非公務機關之中央目的事業主管機關得視實際需求，於符合本辦法規定之範圍內，另行訂定其所管特定非公務機關之資通安全應辦事項。

近期資安威脅

- 網路犯罪集團導入企業經營手法
- 存取權限對駭客至關重要
- 受攻擊面正在擴大且修補更新屢屢失效
- 發掘藏匿在雲端的弱點
- 網路攻擊對業務的衝擊
- 應對戰術日益靈活的駭客的防範策略

2023資安威脅預測

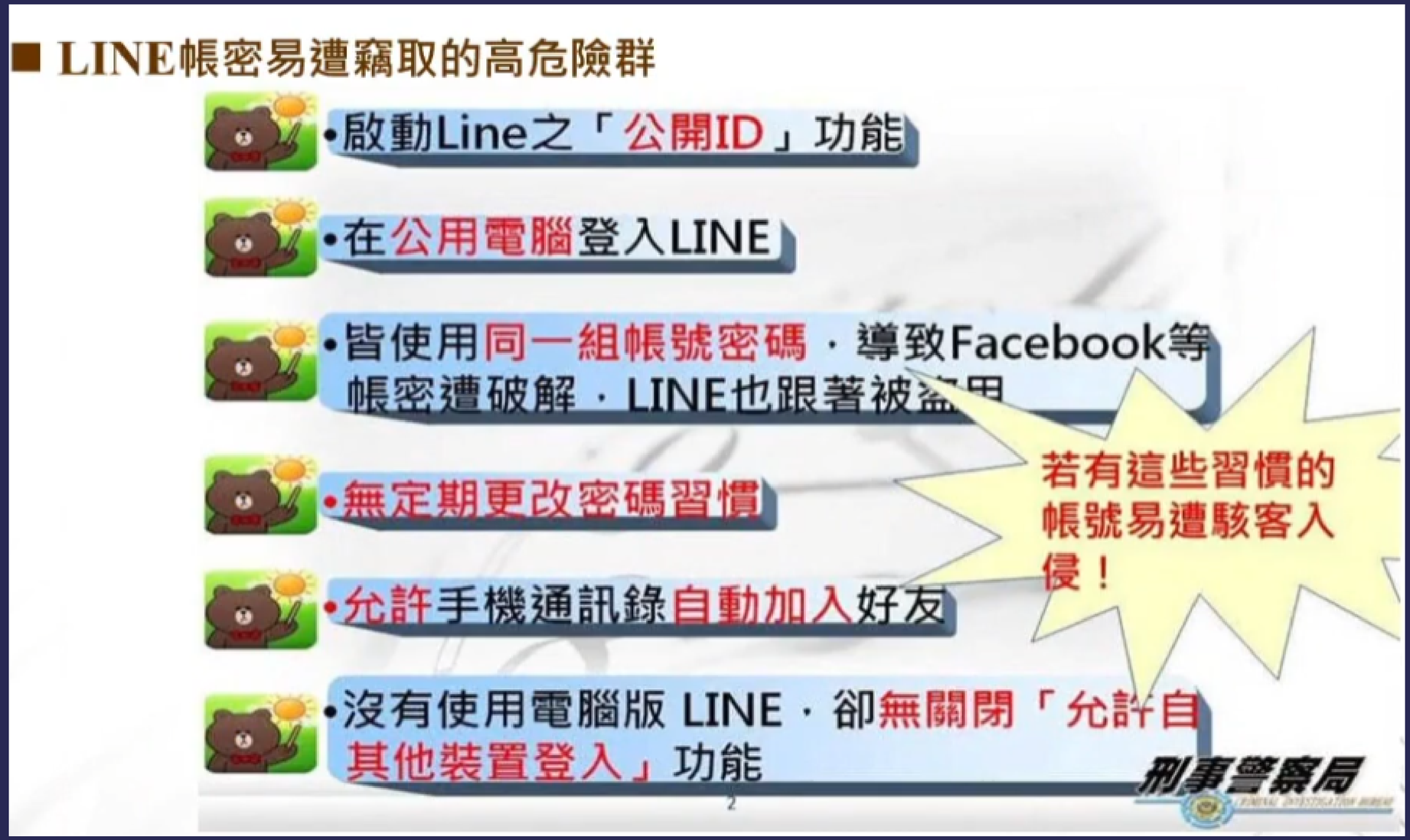
LINE訊息查證

- 先加入「LINE 訊息查證」官方帳號以添加好友、啟動相關功能。
- 必須透過轉貼的方式，將文章連結分享「LINE 訊息查證」以進行辨識。
- 轉傳成功後，「LINE 訊息查證」會跳出訊息告訴用戶，該則新聞是否已經有相關的查核。若系統內，沒有該則文章的查核資料，處於「待查證」的狀態，「LINE 訊息查證」會詢問用戶，是否要回報給查核單位進行，若已經有查核資料，則會跳出結果。
- 「LINE 訊息查證」平台，提供「最新查核消息」、「即時議題看板」，可查看當前最多爭議的連結

如何辨識假訊息

- 對標題保持懷疑態度：假新聞/假消息通常會使用聳動的標題，如果標題內容令人難以置信，很有可能就是不實報導。
- 調查消息來源：如果報導來自不熟悉的機構或組織，請調查它們的詳細資料，了解更多背景資料再對訊息的真實性進行判斷。
- 查詢相關報導：如果有多個具公信力的來源都報導了相同的內容，則新聞內容較可能屬實。
- 只分享可信的消息：還沒確認新聞/消息的真實性之前，不要在網路上分享。
- 善用各種假訊息查證管道(例如LINE官方提供之「LINE訊息查證」帳號、趨勢科技「防詐達人」等)，彙整各方提供的資訊後再對新聞/消息的真實性進行判斷。

安全使用LINE


LINE帳密易遭竊取的高危險群
•啟動Line之「公開ID」功能
•在公用電腦登入LINE
•皆使用同一組帳號密碼，導致Facebook等
帳密遭破解，LINE也跟著被盜用
•無定期更改密碼習慣
•允許手機通訊錄自動加入好友
•沒有使用電腦版 LINE，卻無關閉「允許自
其他裝置登入」功能
若有這些習慣的
帳號易遭駭客入
侵！
刑事警察局

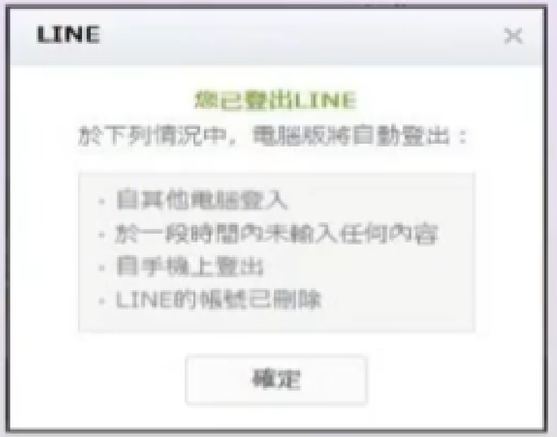
■ 避免LINE發生盜用詐騙之2不1要原則

不設定與其他社群網站相同帳密

- 建議民眾應設定一定複雜程度的密碼(如大/小寫英文、數字及特殊符號)及各自設定完全不同的密碼。

不隨意點選不明的網址連結

- 不隨意替別人代發驗證碼簡訊。
- 不點選不明網址及不轉傳他人，以保護自己及他人被害。

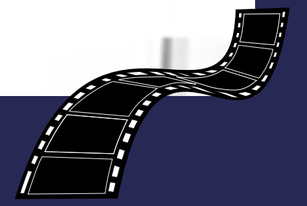


要速向LINE申請被盜用帳號之停權

- 帳號被盜用時要儘快向LINE網站(https://contact.line.me/zh-hant/)申請停權，避免發生詐騙。

雲端服務使用不當 - 事件案例

- 事件說明
  - OO高級中學OO室以Google表單蒐集學生資料，因表單管理設定失當，致使填報人可查看其他已填人員之填寫資訊(包含個人資料)，可能造成個資外洩。
- 發生原因
  - 承辦人於設計Google表單時，因對於其管理設定功能不熟悉，錯誤勾選允許檢視其他回應選項。



雲端服務使用不當 - 改善事項

■建議改善事項：

- 依各級學校使用資通系統或服務蒐集及使用個人資料注意事項：
  - ■應加強並留意表單設計所開啟的功能，是否會造成機敏資料或個人資料外洩情事發生。
  - ■以Google表單為例，於製作完成發送前，應確實做好相關設定檢查，並實際操作檢驗，確認無風險疑慮再行送出。
- 針對雲端服務之使用，加強人員教育訓練與安全宣導。

個人資料保護法

1995 年 8 月 11 日公布	電腦處理個人資料保護法	只規範經電腦處理的個人資料 只有 8 類行業、13 個特定事業必須遵守
	修法	
2010 年 5 月 26 日公布	個人資料保護法	電腦處理或紙本個人資料皆受保護 任何人、任何機關團體都必須遵守 依循國際個資保護原則，與國際接軌
2012 年 9 月 26 日公布	個人資料保護法施行細則	
2012 年 10 月 1 日	個人資料保護法上路	

資料來源：iThome

個人資料保護法

第一章 總則(第1條至第14條)

第二章
公務機關對個人資料之蒐集、處理及利用
(第15條至第18條)

第三章
非公務機關對個人資料之蒐集、處理及利用
(第19條至第27條)

第四章
損害賠償及團體訴訟
(第28條至第40條)

第五章
罰則
(第41條至第50條)

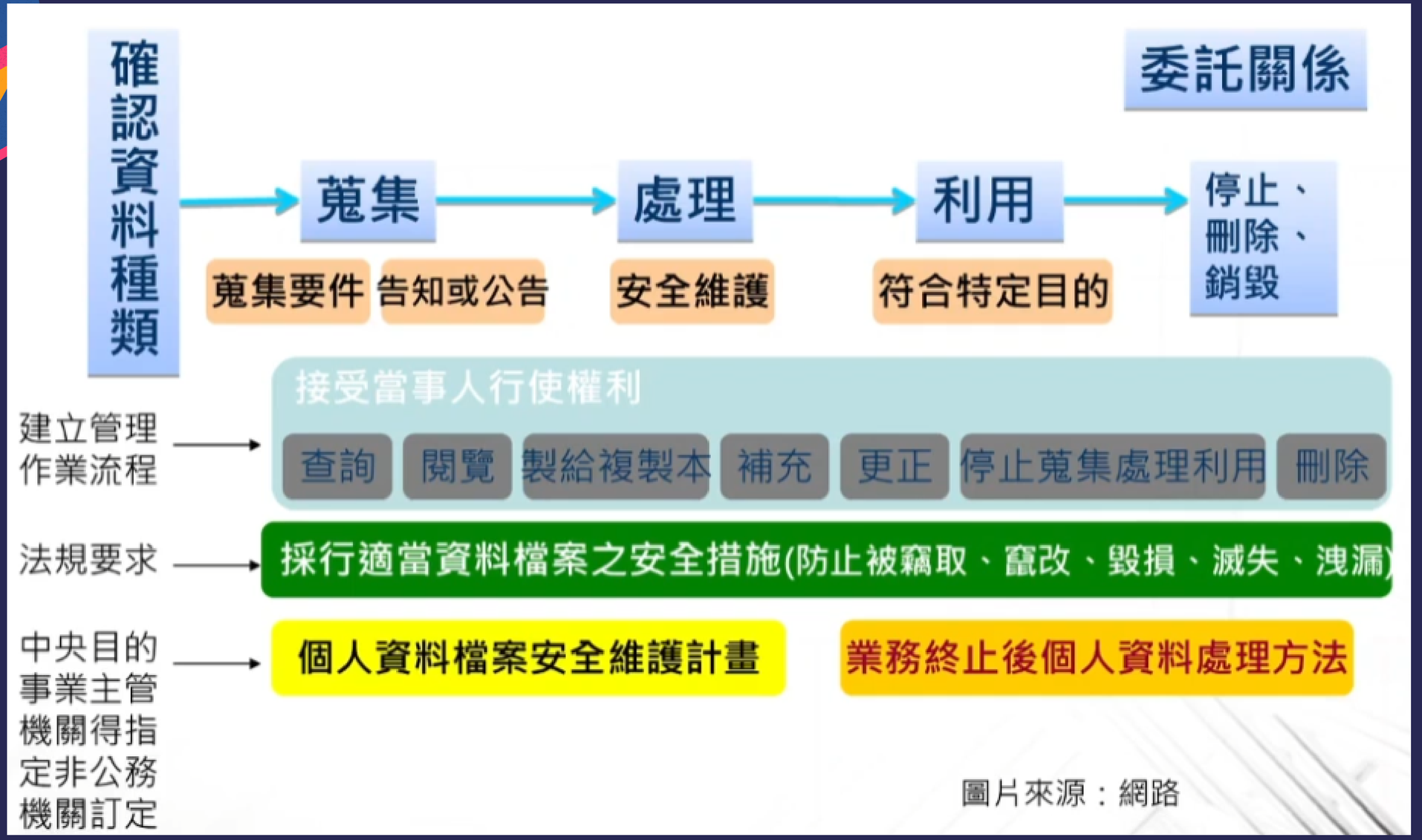
第六章
附則
(第51條至第56條)

個資法範圍

第2條：個人資料：指自然人之姓名、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、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

第5條：個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，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。

個資處理程序


確認資料種類
委託關係
蒐集
處理
利用
停止、刪除、銷毀
蒐集要件
告知或公告
安全維護
符合特定目的
接受當事人行使權利
建立管理作業流程
查詢
閱覽
製給複製本
補充
更正
停止蒐集處理利用
刪除
法規要求
採行適當資料檔案之安全措施(防止被竊取、竄改、毀損、滅失、洩漏)
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
業務終止後個人資料處理方法
圖片來源：網路

個資注意事項

- 別以為你不會洩密

  只要經手個資的都可能受罰。

- 別隨手亂丟個資

  只要有記載個資的東西都必須做好保護，就連一張紙都要收好，別當作回收紙。

- 別貪快跳級搶資料

  千萬不要因為貪快，而開方便之門。必須嚴格遵守不同層級的資料存取權限制度，

  不要因趕著要資料，而跳過應有的管制流程。

- 別輕易人肉搜索

  別在網路上揭露他人的聯絡方式。

- 別隨便發布文章和照片

  在網路發表文章與照片，內容涉及到他人，必須要事先告知並取得當事人的同意。

個人資訊安全防護

弱密碼宣導

各式詐騙訊息:以line為例

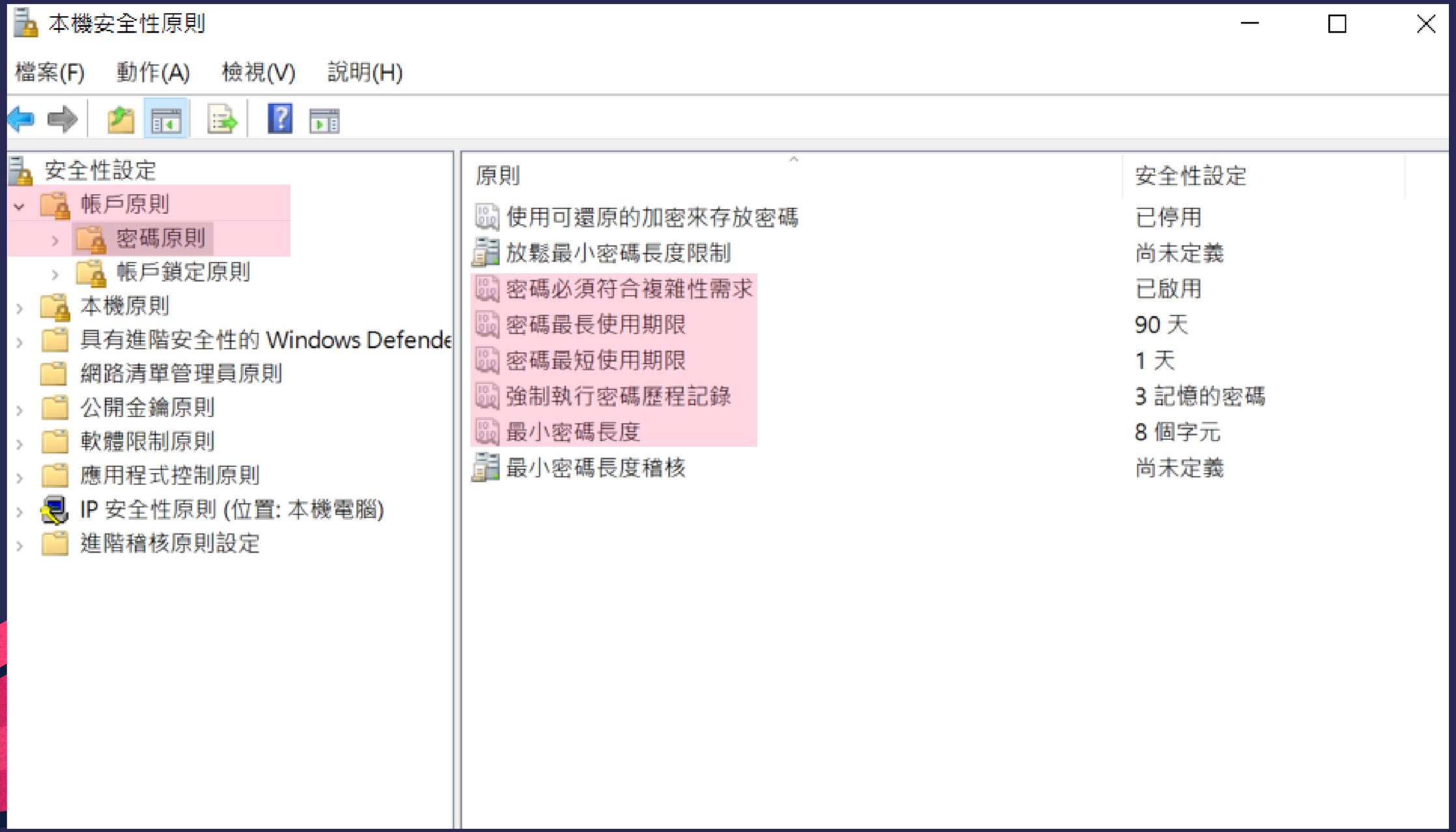
雲端使用不當

110資通安全演練，攻擊報告43%為弱密碼。

行政院資通安全處105年11月30日 院臺護字第1050185463號函：各政府機關資訊系統不應使用身分證字號做為帳號名稱，亦不可使用弱密碼做為使用者預設密碼。

政府組態基準 (GCB) 密碼原則：

- 通行碼長度，建議為8~12碼以上
- 通行碼複雜度，應包含英文大寫、小寫、特殊符號或數字3種以上


本機安全性原則
檔案(F)
動作(A)
檢視(V)
說明(H)
安全性設定
帳戶原則
密碼原則
帳戶鎖定原則
本機原則
具有進階安全性的 Windows Defende
網路清單管理員原則
公開金鑰原則
軟體限制原則
應用程式控制原則
IP 安全性原則 (位置: 本機電腦)
進階稽核原則設定
原則
安全性設定
使用可還原的加密來存放密碼
已停用
放鬆最小密碼長度限制
尚未定義
密碼必須符合複雜性需求
已啟用
密碼最長使用期限
90 天
密碼最短使用期限
1 天
強制執行密碼歷程記錄
3 記憶的密碼
最小密碼長度
8 個字元
最小密碼長度稽核
尚未定義

本校資通安全政策

放置中和國小網頁，並於公開會議宣導

- 本校之教職員工、專案工作人員、計畫人員、工讀生、委外服務廠商及訪客等皆應遵守本政策