國立基隆女中110年度資通安全教育訓練

目次

1. 前言
2. 教育雲電子郵件申請狀況
3. 公務機關資安宣導單
4. 辦公處室宣導
5. 資安實地稽核前需對電腦進行之各項設定

前言

- 短片欣賞：一場沒有中立國的戰爭

https://www.youtube.com/watch?v=RyQiz8AudQo&list=PL92E2EC876AC450BE&index=13&ab_channel=%E8%B6%A8%E5%8B%A2%E7%A7%91%E6%8A%80TrendMicro

- 機敏性之情資定義：

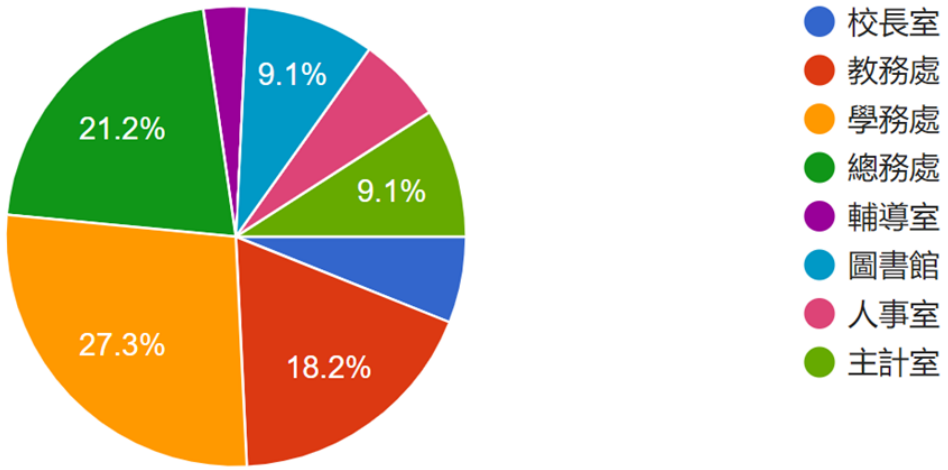
「資通安全情資之內容如包含姓名、出生年月日、國民身份證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病例、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接識別之個人資料，或涉及個人、法人或團體營業上秘密或經營事業有關之資訊，或情資之公開或提供有侵害公務機關、個人、法人或團體之權利或其他正當利益，或涉及一般公務機密、敏感資訊或國家機密等內容，屬機敏性之情資。」

教育雲電子郵件申請狀況

- 請行政同仁傳送機敏公務資料時，務必使用教育雲電子郵件傳送，保障資料資通安全。
- 申請狀況圓餅圖

- 尚未申請教育雲信箱：

教務處：6人
學務處：2人
總務處：2人
輔導室：1人



公務機關資安宣導單

1. 資安宣導：密碼換新、程式更新、下載要當心。
2. 辦公環境內必須使用機關提供之資訊設備、網路，及規定之軟體，不得使用個人私有設備及中國廠牌產品，公務設備亦不得連結個人私有手機上網。若有業務上的需求，必須經資安長(校長)同意後，列冊管理並定期檢討。
3. 上班期間不應連結非公務需要之網站，並避免連結惡意網站或釣魚網站，如發現異常連線，請通知資安窗口。
4. 不得使用公務電子信箱帳號登記做為非公務網站的帳號，如社群網站、電商服務等。
5. 公務資料傳遞及聯繫必須使用公務電子郵件帳號，不得使用非公務電子郵件傳送或討論公務訊息。
6. 即時通訊軟體使用應注意不得傳送公務敏感資料。

7. 傳送公務資訊應有適當保護，例如加密傳送。
8. 帳號密碼必須妥善保存，並遵守機關規定，如有外洩疑慮，除儘速更換密碼外，並應通知資安窗口。
9. 主動通報資安事件或可能資安風險者，依規定獎勵。
10. 未遵守機關資安規定，初次予以告誡，若持續發生或勸導不聽者，依規定懲處；若因而發生資安事件，加重處分。
11. 有資安疑慮或異常時，應即時通報資安窗口。
12. 應遵守個人資料保護法及資通安全管理法。

不是只有 A 咖女星,才該擔心個資成公開秘密

辦公處室宣導

- **電腦不用要登出**

- 離開座位，電腦應設定螢幕保護程式或是其他控制措施保護，將螢幕鎖定
- 長時間離開辦公室，建議將電腦關機
  - » 杜絕來自網路破壞
  - » 防止帳號或密碼被盜用
  - » 防止重要資料遭竊

●機密資料要保護

◆使用者可能會把機密性資料文件、備忘紙(抄寫各系統密碼)、以及記載個人相關資訊等文件，隨意放置於桌上。或者將資料進行完善的分類，並且儲存在電腦桌面上，這些動作都很容易導致資料的外洩。

◆因處理業務保有敏感性、機密性電腦資料或檔案者，應加強安全保護措施，如下班時應該上鎖或以其他方法妥為收存。

- 連接網際網路(非公務網路)的個人電腦、筆記型電腦
  - 不得處理機敏公務
  - 不得放置機敏公務資料
  - 禁止連接儲存機敏公務資料之可攜式儲存媒體（光碟片、隨身碟、外接式硬碟等），以防止後門（木馬）程式竊取資料

- 避免USB儲存裝置讓電腦系統感染病毒

重要資料要備份

- 不論是紙本或電子檔的重要資料，皆應：
  - » 定期備份
  - » 存放在不同地方(異地備份)。
- 資料備份原則
  - » 資料價值較高時應優先備份。
  - » 備份的資料需定期做資料回復測試，以確認備份資料的可用性。

使用網路要注意

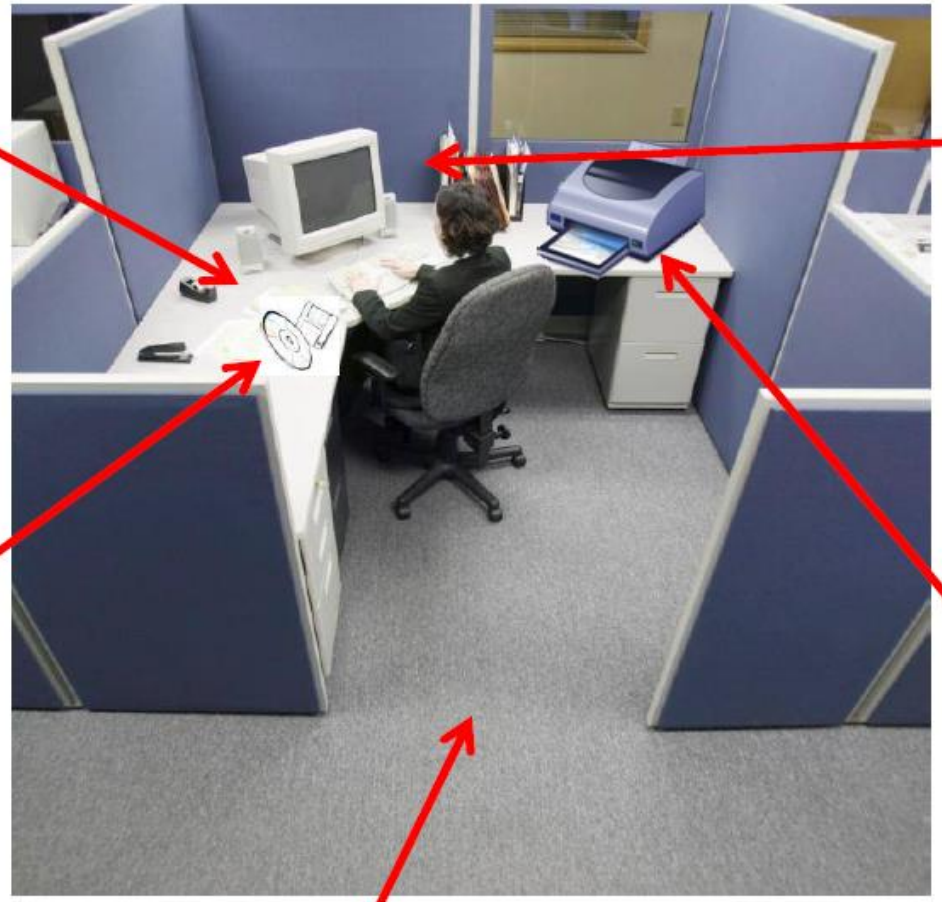
- 公務電腦原則上限公務使用，且必須加入網域。
- 不得將私人個人電腦、筆記型電腦連接公務網路(內外網)

資訊傳輸要注意

- 機密性資料及文件，不得以非教育雲電子郵件方式傳送
- 機密性資料以外之機敏性資料及文件需適當加密
- 應確認對方的郵件地址，不要隨意轉寄未確認來源之信件

資訊安全宣導 - 辦公室設備使用注意事項

- 離開座位時，機密文件不應置於辦公桌
- 下班前需清理工作場所



- 電腦閒置時，應設定螢幕保護程式或鎖定螢幕
- 不應將使用者之帳號密碼紀錄於紙本
- 定期檢視防毒軟體及Windows Update是否確實更新

- 儲存媒體(如USB隨身碟)應妥善保管
- 使用、移動及存取多媒體應遵循管制程序
- 報廢的儲存媒體需確實銷毀

- 印表機、影印機應有專人負責
- 紙本文件回收前應確認是否含有機密資訊
- 文件銷毀需確實
- 會議後須將會議室桌面及白板淨空

- 限制區域應有門禁管制非經允許與陪同，外部人員不得進入
- 辦公區域檔案櫃、抽屜、辦公室應上鎖

- 短片欣賞：
- 駭客如何利用員工的社群網站入侵公司?

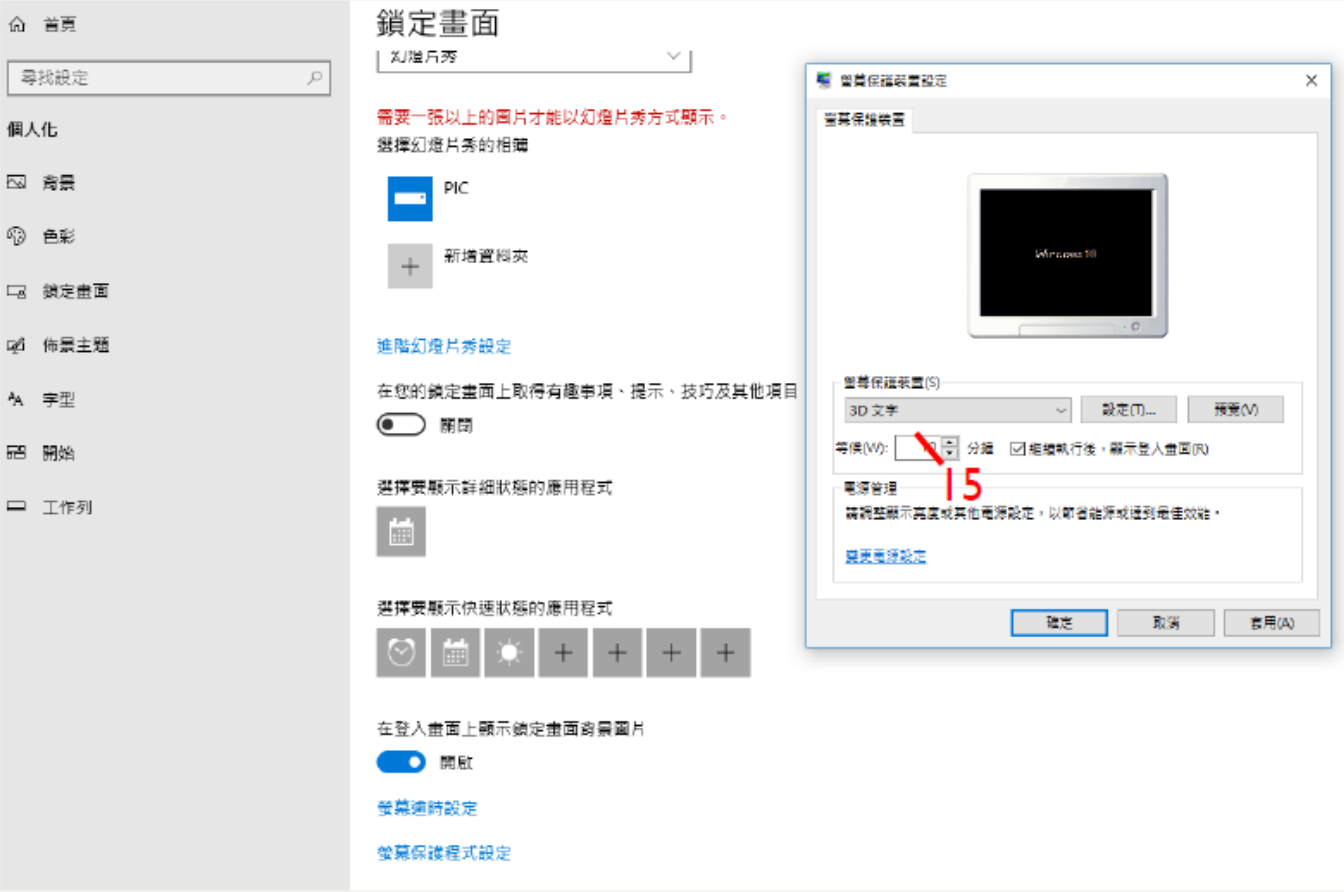
資安實地稽核前需對電腦進行之各項設定

- 作業系統目前win7已經不支援！
  請確認版本是否為win10！

（否則資安稽核直接就是缺失起跳）

1.螢幕保護程式時間

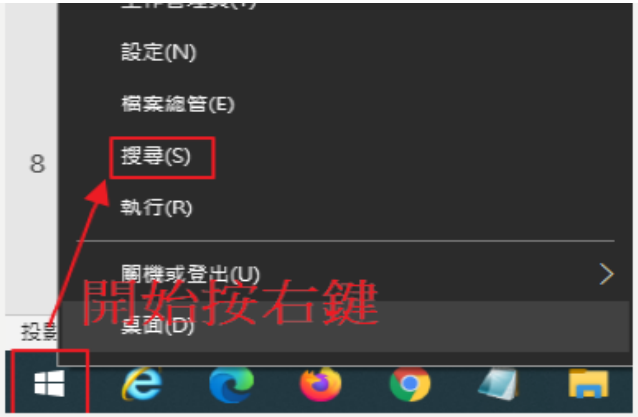
- 個人桌上型電腦、可攜式電腦應設定於一定時間不使用或離開後，應自動清除螢幕上的資訊並登出或鎖定系統，以避免被未授權之存取。
- Windows設定→個人化→鎖定螢幕→螢幕保護裝置設定→等候「15」分鐘

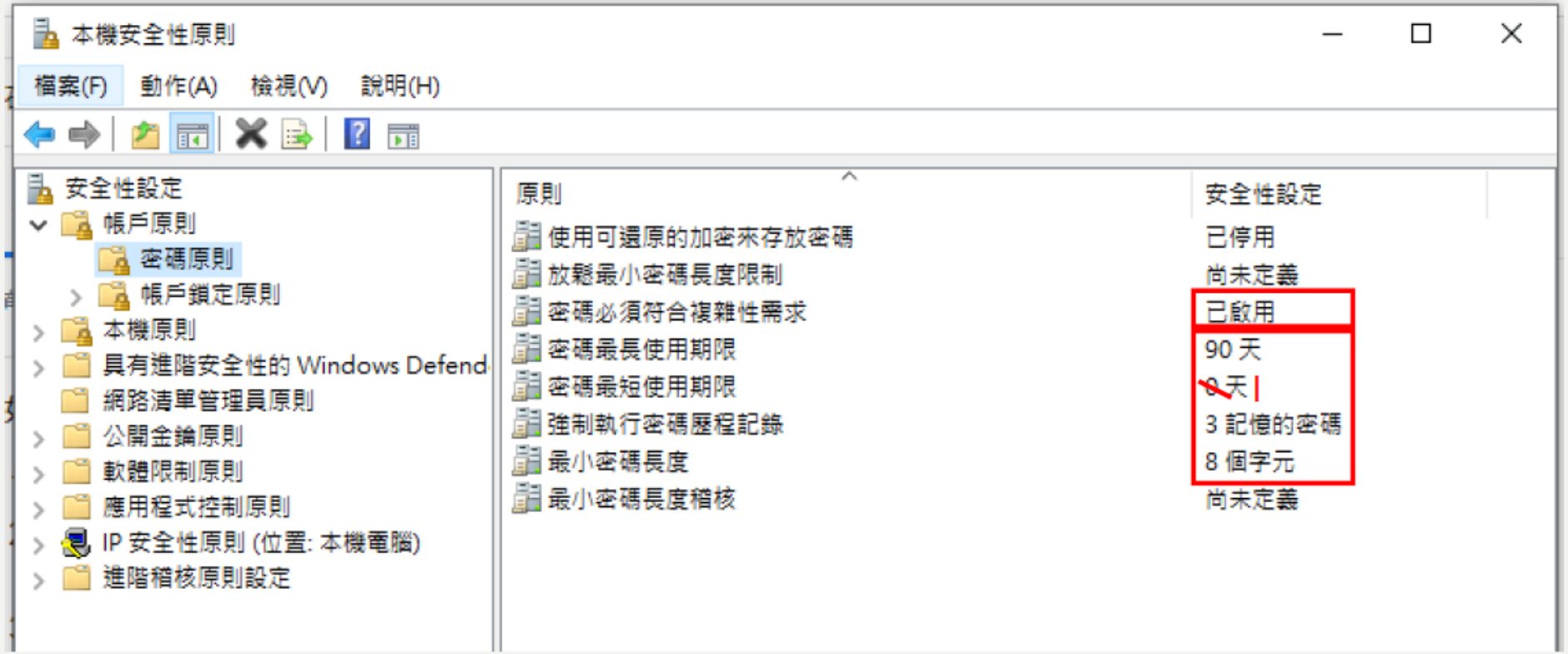


2.密碼原則

【Win10】：

- 開始按右鍵->搜尋->鍵入「本機安全性原則」
- 本機安全性原則→安全性設定→帳戶原則→密碼原則





通行碼規範

通行碼應符合政府組態基準（GCB）規範及資通安全責任等級分級辦法之政策，政策如下：

1. 通行碼長度8碼以上。
2. 通行碼複雜度應包含英文大寫、小寫、特殊符號或數字三種以上。
3. 使用者每90天應更換一次通行碼。
4. 使用者通行碼最短需使用1天，最長使用期限為90天，且通行碼需保留三次歷史紀錄不得相同。

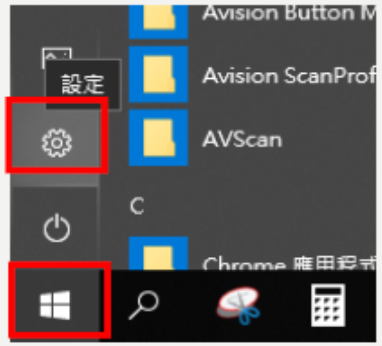
3.嚴禁 下載或使用非法軟體與檔案

- 禁止於個人電腦安裝線上遊戲、禁止下載或安裝來路不明、有違反法令疑慮如版權、智慧財產權等或與業務無關的電腦軟體。

- 禁止於上班時間瀏覽不當之網路如暴力、色情、賭博、駭客、惡意網站、釣魚、詐欺等非公務用途網站。

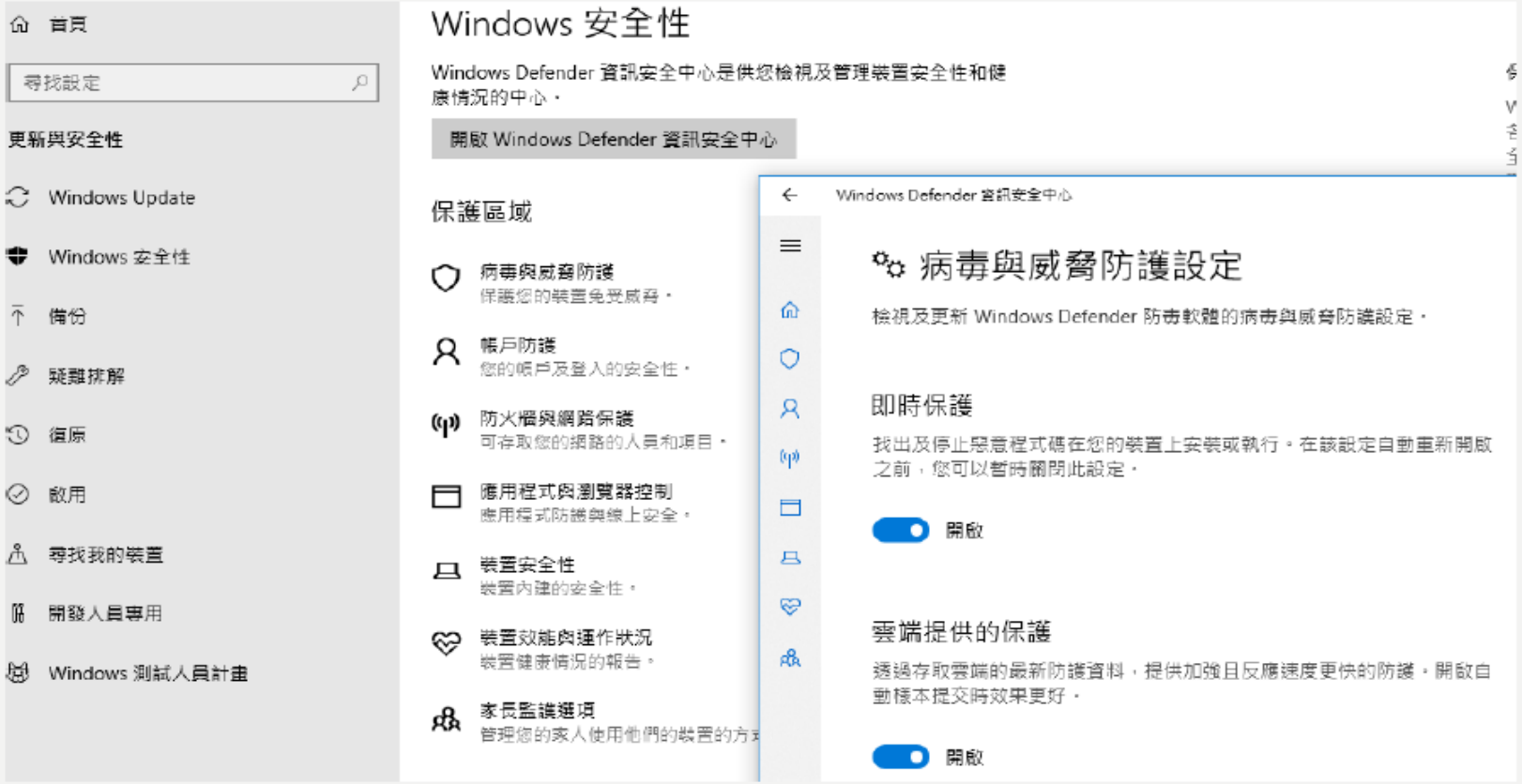
- ZOOM 視訊軟體，請記得解除安裝！

4.WINDOWS DEFENDER



【Win10】：

- 找到「windows設定」(可參照右圖方法)
- windows設定→更新與安全性→Windows安全性→病毒與威脅防護→病毒與威脅防護設定→將「即時保護」、「雲端提供的保護」都開啟



- windows設定→更新與安全性→Windows Update→檢查更新

5.電腦防毒要更新

- 防毒軟體的偵測與防範功能只有在該軟體有在運作、且有時常更新病毒碼情形下，才會產生效用。

◆防範訣竅：

» 隨時注意防毒軟體的病毒碼是在最新的狀態。

» 不關閉、不刪除防毒軟體。

» 定期執行掃毒。

» 不要隨意複製或下載不明檔案。

» 不要隨意開啟檔案。

6.機敏性資料應有適當之保護措施

- 電腦設備內機敏性檔案，須由檔案擁有者以加密措施保護，如以壓縮軟體 7 zip 等方式執行壓縮加密碼，並限制不得於公務外電腦使用。
- 以word為例：點選「檔案」→保護文件→以密碼加密
- 以excel為例：點選「檔案」→保護活頁簿→以密碼加密
- 以PPT為例：點選「檔案」→保護簡報→以密碼加密

7.電子郵件關閉郵件預覽功能，使用文字模式瀏覽

- 以G-mail為例：點選右上角齒輪→一般設定→勾選「顯示不明外部圖片時，必須先詢問我。」

沒有百分之百的資訊安全，

得靠每個人從小地方一起努力！

圖片轉自法務部調查局