

資安研習評量 重點摘要

1. 資安是專業工作，若非專責人員的單位主管，對於資安的督導不力，也**會**受處分。
2. 無論哪一等級防護基準的資訊服務與作業環境的個人電腦，**都需要**鐘訊同步。
3. 不是把核心資訊系統放到上級機關指定的雲端，資安責任等級就可以維持為 D。
4. 不要利用鍵盤順序或電影名稱組合來設定密碼
5. 若老師自己開發系統在學校公務上使用，無論系統是否單純，都應盤點資訊資產，也需要依照安全軟體開發生命週期(SSDLC)的要求。
6. 公務使用的資訊系統，無論是委外廠商開發或老師職員開發 都須要求做安全檢測(如弱點掃描)。
7. 網路有很多免費的App 或工具軟體，不應隨便下載使用。
8. 資安責任等級D級的機關也需要盤點核心業務與資訊資產。
9. 學校的資安政策、資安事件應變程序、資安相關訊息都放在學校網站首頁的資安專區。
10. 收親友寄來或群組轉發的美圖、好文或好康訊息，應該要檢視或查證再分享。
11. 學校的資安通識訓練，無論正式編制的教職員、約聘僱人員或臨時人員一定要上滿3小時。
12. 在學校官網公告的訊息經過核可後，應設定公告期限，也需檢視是否有太久的資訊。
13. email 郵寄或傳送含有公務機敏或個資的檔案，不管個資數量多少，都要將檔案加密，密碼再另外傳送。
14. 要辦理活動收集報到、報名資料，最簡單可用 Google 表單來做。做好表單**一定要**再檢查設定，不可直接上線。
15. 學校老的系統不少，即使缺少經費去更新，也要去檢查個資蒐集的種類或數量是否太多，盡量減少個資之蒐集。
16. 上級機關來文要求協助公告或宣導，簽請主管核准後。要再檢查內容是否適合公告給校外人士，不可以直接整份公文貼到官網。
17. 本校人員於知悉資通安全事件後，如發現公務電腦被勒索病毒鎖住檔案了，應在**1**小時內通知要本校資安專責人員做處理。
18. 若發生第一、二級資通安全事件應於知悉事件後**72小時**完成處理，第三、四級事件要在**36小時**完成處理。
19. 不可把所有資訊系統都用同一組帳號密碼。
20. 無論 系統管理者或其他一般使用者帳號都不能共用。

