他校資安稽核之缺失要點

稽核結果綜合

1.備份資料應對資料加密控管，並定期進行回復測試，以確保備份資料意見的有效性。

2.宜落實追蹤過去缺失之改善情形（如：安全維護計畫）。

3.宜加強資訊機房環境安全控管，如：易燃性物品（如：紙箱）需移除、適切地使用安全性消防設施、設置監視器裝置。

4.應再加强資通安全維護計畫及資安政策的更新，並適時公告相關訊息。

5.應依資通安全維護計畫要求，加強盤點資通訊系統清冊的完整性，與落實風險評估表的風險評估作業。

6.應再加主機系統的資訊安全防護與控管，如：

（1）通行碼超過一年以上未更新：個人電腦（X.X.200.159）、會計請購系統、校務系統（前端）

（2）防毒軟體超過半年未更新病毒碼：個人電腦（X.X.200.42、X.X.200.159）

（3）未設定螢幕保護程式：個人電腦（X.X200.38、X.X.200.42）

（4）安裝非授權軟體WinRAR：個人電腦（X.X.1.99）

（5）應安裝授權的防毒軟體：校務系統（前端）

（6）Windows版本過舊：教師室個人電腦（Windows7）、會計請購系統（WindowServer2012R2）、校系統（前端）、校務系統（後端）

（7）7-zip版本過舊：個人電腦（X.X200.30、X.X.200.159）

（8）應禁止共同使用管理者帳號：會計請購系統

(9) 是否有安裝teamviewer這類軟體

7.委外約應納入資安相關條款，如：校務行政系統維護合約（欣河資訊有限公司），並與委外人員簽署保密切結。

8.應再加強系統帳號之權限審查，如：會計請購系統（kaway）、校務系統（前端）的廠商帳號

9.單位施作資安相關工作，應適時留存紀錄以利後續之追踪及控管。

10.給老師們借用的公用筆電要設密碼。

11.會查電腦的軟體如果有盜版或是過期的就會被記缺失。

12.110 年校園資通安全實地稽核訪視作業-學校不符合項目共通性問題

13.110 年校園資通安全維護計畫實施情形線上審查結果-學校不符合項目共通性問題

14.如果稽核委員到學校，他們自帶筆電到校，建議讓委員連 eduroam 或 TAnetRoaming 訊號，然後兩個無線訊號連線後直接出校外，不能存取內網，不然委員會去試用他的筆電連線校內行政系統或遠端桌面。（eduroam 或 TAnetRoaming 只是去漫遊認證中心認證，IP應該還是校內IP，除非在這2 SSID走其他線路或這別針對這兩SSID隔開內網。可以設 vlan 或是特定的虛擬 ip，然後從 core switch 或 防火牆設定）

15.行政用的電腦要上密碼並定期更換

16.舊的Flash 要刪掉 Line, Anydesk, TeamViewer 那些都要刪掉

17.本校LINE由校長裁示可安裝在公務電腦，有行政會議記錄。

18.更新防毒軟體

19.桌面要淨空

20.儲存媒體要上鎖