資訊安全常見違失及處理（一）

資訊安全「系統存取控制」檢查常見違失：

1、 系統安全防護不足：Windows作業系統、應用軟體漏洞未更新、未安裝防毒或防木馬程式之軟體，防毒軟體未更新、掃毒功能無法執行、電腦防毒軟體更新設定錯誤、未開啟螢幕保護程式等。

2、 密碼設定及安全確保原則未周延：開機密碼與帳號相同、電腦主機作業系統登入密碼簡略、未定期更新密碼、螢幕通行碼保護時間設定過長、未設開機密碼等缺失。

3、 安裝未經授權之軟體：安裝未經核准之通訊軟體、不明或無版權之系統優化工具、使用單機版或個人免費版防毒軟體。

4、 公務信箱未設定預防社交工程之使用環境：未針對電子郵件社交工程防範進行安全設定，如電子信箱未關閉預覽功能。

5、 利用公務電腦從事非公務用途：上班時間利用電腦從事非公務用途、公務用Ｔ槽置放個人家屬之照片集錦檔案。

6、 網站管理未周延：值班台受理民眾報案系統電腦螢幕顯示畫面，於暫離座位時，未立即縮小畫面或登出系統。

7、 網路流量異常：不當連結非公務網站或下載檔案，致公務電腦網路流量異常。

8、 電腦系統遭植入惡意程式：作業系統疑遭植入間諜程式。

9、 其他：委外廠商使用網站線上掃毒，衍生資安疑慮。

資訊安全「系統存取控制」之建議事項：

1、 帳號密碼應自行記憶及定期更新，並提高密碼強度3，不 得隨手張貼於桌面、主機、螢幕等，避免第三人取得；另個人離開座位時應登出電腦或啟動螢幕保護密碼，避免機敏資料遭竊或因人為疏漏發生資安事件。

2、 數字及字母組成的 6 字元密碼在短短的 1.18 秒鐘就被破解(Intel評估密碼強度測試網頁)，網址：https://www-ssl.intel.com/content/www/us/en/forms/passwordwin.html。

3、 電腦作業系統及應用軟體應即時更新修補程式，並將防火牆保持在開啟狀態，必要時加裝入侵偵測防護系統4；另電子郵件收發軟體，應進行防範社交工程攻擊之安全設定，如應關閉電子郵件預覽功能，避免遭植入木馬程式或間諜軟體。

4、 嚴禁安裝非合法購置、無版權或來路不明之軟體；另電腦應加裝防毒軟體，並保持啟動及設定自動掃描功能，亦須即時更新病毒碼。

5、 公務電腦應避免從事非公務用途，且不瀏覽或下載非業務需要之網站及檔案，避免網路流量異常，影響正常公務使用之網路頻寬。

6、 資訊委外作業於契約中未明定廠商應付保密義務及違約應受處罰等條款；另定期辦理資安訓練，提升機關同仁對於正確資安觀念之認識。