

國立臺南女中電腦安全自我檢查表

請同仁依序檢查個人電腦及筆記型電腦，並於檢查結果欄位勾選是否完成、簽名，經單位主管核章後，送交資訊組彙整。

檢查日期：____年____月____日

編號	檢查項目	檢查結果	檢查說明
1	已完成電腦系統帳號密碼設定	☐ 是 ☐ 否	個人電腦設備應設定登入帳號密碼，密碼至少每 6 個月更換一次密碼長度應至少 8 碼及穿插數字、大小寫英文字元以符合複雜度。
2	已完成螢幕保護密碼設定	☐ 是 ☐ 否	電腦應使用螢幕保護程式，設定螢幕保護密碼，並將螢幕保護啟動時間設定為 10 分鐘以內。保護電腦在業務人員離開座位時能自動上鎖。
3	已將網路位置設定為公用，並關閉資源分享	☐ 是 ☐ 否	電腦連線至網路時，網路位置應設定為公用網路。請勿開啟網路芳鄰分享目錄與檔案。
4	已關閉 Guest 帳號	☐ 是 ☐ 否	停用 Guest 帳號，避免未經授權的使用。
5	無來路不明、未授權或危害軟體	☐ 是 ☐ 否	嚴禁下載、安裝或使用來路不明、有違法疑慮(如侵害版權、智慧財產權等)、未經授權、與公務無關或影響電腦網路環境安全之軟體。如有發現來路不明或未授權檔案，立即移除。
6	已安裝防毒軟體	☐ 是 ☐ 否	進行下載、複製、使用不明來源檔案前，請確認檔案安全無虞，應先完成掃毒，嚴禁任意移除或關閉防毒軟體。
7	已完成瀏覽器安全設定	☐ 是 ☐ 否	IE、Firefox 等相關瀏覽器安全等級應設定為中級或更高，並關閉快顯功能、ActiveX 等主動執行功能及封鎖彈跳視窗。如果執行特殊程式須降低安全性或需加裝外掛功能，請先進行安全檢查及管理。
8	郵件軟體已關閉信件預覽	☐ 是 ☐ 否	電子郵件軟體應關閉收信預覽功能，請勿任意開啟不明來源的電子郵件，為避免惡意連結及圖片危害請使用文字模式閱讀信件。
9	已完成 MS-Office 軟體巨集安全設定	☐ 是 ☐ 否	使用文書處理軟體(包括 Word、Excel、Powerpoint 等)應將巨集安全性設定為高級或更高。如果執行特殊程式須降低安全性，請先進行安全檢查及管理。
10	已開啟 Windows 系統自動更新程式	☐ 是 ☐ 否	配合進行軟體更新，修補漏洞，保持更新至最新狀態，勿自行關閉系統自動更新程式。
11	無閱覽不當之網站	☐ 是 ☐ 否	禁止於上班時間閱覽不當之網路(如暴力、色情、賭博、駭客、惡意網站、釣魚詐欺、傀儡網路等)及瀏覽非公務用途網站，以避免內部頻寬壅塞。 於上班時間使用即時訊息軟體(如 LINE、Messenger 等)，應作公務用途。
12	無使用外部 Webmail 辦理公務	☐ 是 ☐ 否	禁止使用外部網頁式電子郵件(Webmail)辦理公務，以避免資訊外洩風險。辦理公務應使用公務信箱。
13	無啟用 Web、FTP、Mail 等網路設站服務	☐ 是 ☐ 否	電腦設備不可任意架站或做私人、營利用途。
14	已知悉本校資通安全管理要點及相關資料公告位置	☐ 是 ☐ 否	學校首頁右側專案網頁有資通安全專區，宣導資安相關資訊。
15	已知悉每年須完成 3 小時資通安全教育訓練並完成評量	☐ 是 ☐ 否	參加學校辦理的資安研習或線上課程(例如 e 等公務園+學習平臺、教師 e 學院)並完成評量。
16	已知悉不得任意使用遠端桌面軟體	☐ 是 ☐ 否	不得任意使用 AnyDesk、TeamViewer、VNC 等遠端桌面高風險軟體，從校外連線校內電腦。遠端存取採「原則禁止、例外允許」方式，須經核准後始得使用。

編號	檢查項目	檢查結果	檢查說明
17	重要業務文件已備份	☐ 是 ☐ 否	1. 應定期備份個人電腦設備內重要文件及資訊，至少每個月1次。使用個人電腦設備處理機密資料或公文時，應作加密處理且勿存放於個人電腦中，應存放於實體隔離媒體並完成加密。
18	機密資訊加密儲存於實體隔離媒體	☐ 是 ☐ 否	2. 應避免使用非本校防護範圍內之網路及電腦設施辦理公務，若確有必要使用外部(如住家、公共場所)資訊環境，務請確認資訊使用環境是否具備下列防護措施： (1) 儲存於攜帶式儲存媒體(如行動碟)之公務相關電子檔案應予加密。 (2) 使用之連網電腦設備應安裝防毒軟體(含最新版之病毒碼更新)及防火牆，並應保持啟動運作狀態。 (3) 處理公務之電腦設備以不連上網路為原則，於處理完畢後應將公務相關電子檔案移除，不得存放於主機。 (4) 電子檔案如須於網路上傳輸或複製時，必須使用加密措施予以加密處理，以防資訊外洩。

單位：_____ 職稱：_____ 姓名：_____ 單位主管：_____