附件 5

臺南市政府因應傳染病防疫
居家辦公使用公務電腦自我查檢表

一、 公務電腦攜出前

項次	查檢內容	查檢結果
1	檢查是否已申請個人防疫 VPN 帳號，並安裝完成防疫期間 VPN 遠端連線軟體(FortiClient VPN)。 (1) 防疫期間 VPN 遠端連線軟體安裝步驟請於本府公務入口網\公務檔案區\資通安全專區中下載。 (2) 個人電腦攜出前請依各機關財產管理規定登錄設備借出作業。 (3) 攜出公務電腦為公務用途，禁止將該設備作為非公務用途，並避免非本府公務人員使用或操作該電腦。	□符合，已安裝 VPN 程式。 □不符合
2	公務電腦是否完成帳號、密碼強度及螢幕保護程式設定。 (1) 檢查電腦登入帳號並登入一次，登入(AD)帳號為 _____。 (2) 檢查電腦登入帳號之密碼強度是否符合本府資通安全相關規定(如密碼長度 8 碼以上且英文大小寫和數字與特殊符號交錯、勿使用個人敏感資訊為密碼等) (3) 電腦是否已完成螢幕保護程式設定。	□符合 □不符合
3	檢查個人電腦是否已安裝防毒軟體(趨勢 OfficeScan)並更新至最新版。	□符合 □不符合
4	檢查個人電腦是否已完成公文管理系統基礎環境設定及安裝筆硯文書編輯軟體。	□符合 □不符合
5	檢查個人電腦現有網路設定(如 IP 位址)並記錄。 (1) 點選個人電腦視窗左下角「開始」圖示  (2) 點選「設定」→「網路和網際網路」→「變更介面卡設定」→選擇「乙太網路」→按右鍵點選「內容」→在「允許 APP 改變您的電腦中」選「是」→「乙太網路內容」中選擇「網際網路通訊協定第 4 版(TCP/IPv4)」→點選「內容」→抄下「IP 位址」後的數字。 (3) 原有個人電腦的 IP 位址是：_____._____._____._____ (4) 如使用家裡的有線線路，請將「使用下列位址」改為「自動取得 IP 位址」，DNS 設定改為「自動取得 DNS 伺服器位址」；使用 Wi-Fi 網路作業時，請勿連結公用 Wi-Fi 熱點，並以專用 Wi-Fi 熱點或個人手機熱點為連入端口。	□符合 □不符合

執行日期		公務電腦攜出人簽名	

※如無法完成 1~5 項作業，請各機關資訊人員協助完成；府內機關可至本府公務入口網登錄電腦線上報修，由電腦維護駐點工程師協助完成自評。

※本自評表完成後，正本請交付各機關政風人員處備查，影本附於各機關設備攜出或借用申請表單後。

二、居家辦公之公務電腦攜回前

項次	查檢內容	查檢結果
1	居家辦公期間利用 VPN 遠端連線作業所處理之重要公文書或資料應依行政院資訊安全及個人資料等相關規範，妥為保護相關數位資訊並防止數位檔案外流。	□符合 □不符合
2	個人電腦是否已依機關要求於集中地點，針對個人電腦完成必要之消毒措施。未完成消毒措施前，電腦設備禁止攜回機關辦公處所。	□符合 □不符合
3	個人電腦在未連線狀態下以趨勢 T-CLEAN 軟體針對攜回電腦進行全機詳細掃描，並確認無感染惡意軟體。 (1) 掃描無惡意軟體時，方可放行攜回機關辦公處所。 (2) 趨勢 T-CLEAN 軟體可於本府公務入口網\公務檔案區\資通安全專區中下載。	□符合 □不符合
4	檢查個人電腦 IP 設定是否已回復原 IP。	□符合 □不符合

執行日期		公務電腦攜出人簽名	

※本自評表完成後，正本請交付各機關政風人員處備查，影本附於各機關設備攜出或借用申請表單後。

臺南市政府因應傳染病防疫
居家辦公使用自備電腦自我查檢表

一、 開始使用自備電腦前

項次	查檢內容	查檢結果
1	檢查是否已申請個人防疫VPN帳號，並安裝完成防疫期間VPN遠端連線軟體(FortiClient VPN)。 (1) 防疫期間VPN遠端連線軟體安裝步驟請於本府公務入口網\公務檔案區\資通安全專區中下載。 (2) 本VPN帳號使用者應依相關安裝文件安裝及建構網路資訊傳輸安全機制(如VPN加密連線)，遠端連線作業期間所處理之重要公文書或資料應依行政院資訊安全及個人資料等相關規範，妥為保護相關數位資訊並防止數位檔案外流。	□符合，已安裝VPN程式 □不符合
2	檢查個人電腦是否已安裝防毒軟體並更新至最新版。	□符合 □不符合
3	郵件軟體是否已關閉信件預覽功能。	□符合 □不符合
4	檢查個人電腦是否已完成公文管理系統基礎環境設定及安裝筆硯文書編輯軟體。	□符合 □不符合
5	居家辦公期間應遵守本府資通安全級個人資料保護等相關規範。 (1) 用來存取本府VPN遠端連線作業的電腦，應為本人專用並避免非本府人士使用或操作該電腦。 (2) 離開電腦時，應立刻鎖定螢幕，並注意外人偷窺螢幕或碰觸該電腦，以防敏感資訊外洩。 (3) 該電腦禁止插入來路不明的隨身碟或裝置，需上傳數位相關檔案時，應先以防毒軟體掃瞄上傳檔案，確認檔案無相關惡意程式後始得上傳，以防網路惡意程式入侵及確保相關資訊核心系統安全。 (4) 該電腦禁止閱覽不當之網路（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，以避免電腦遭惡意程式攻擊。	□符合 □不符合
6	檢查並保持該電腦網路於正常連線狀態。 (1) 請保持電腦現有網路於正常連線狀態，如使用Wi-Fi網路進行VPN遠端作業時，請勿連結公用Wi-Fi熱點，並以專用Wi-Fi熱點或個人手機熱點為連入端口。	□符合 □不符合

執行日期		使用人員簽名	

※本自評表完成後，正本請交付各機關政風人員處備查。

二、停止使用自備電腦後

項次	查檢內容	查檢結果
1	居家辦公期間利用 VPN 遠端連線作業所處理之重要公文書或資料應依行政院資訊安全及個人資料等相關規範，妥為保護相關數位資訊並防止數位檔案外流。	□符合 □不符合
2	居家辦公期間因公務產出之重要公文書或資料，於停止使用後，需將數位資料繳回機關，繳回資料需先以趨勢 T-CLEAN 軟體進行詳細掃描，於確認無感染惡意軟體後回存資料。 (1) 掃描無惡意軟體時，方可放行攜回機關辦公處所使用。 (2) 趨勢 T-CLEAN 軟體可於本府公務入口網\公務檔案區\資通安全專區中下載。	□符合 □不符合

執行日期		使用人員簽名	

※本自評表完成後，正本請交付各機關政風人員處備查。