# 防疫不忘資安，居家辦公注意事項~

居家遠距辦公除了機關提供的線路、架構、機制之外，使用者本身的資安意識、規範、安全性設定也一樣重要。

**一、設備操作**

1、 **設備登入密碼**：裝置登入時必須設定密碼，避免外人直接操作。

2、 **個人帳號密碼**應避免自動記憶於家中電腦設備，造成其他人亦可使用或操作機關網路系統。

3、 **使用密碼管理工具並設定「強密碼」**：可以考慮使用密碼管理工具並將密碼設為全隨機產生包含英文、數字、符號的密碼串。

4、 **不同系統帳號使用不同密碼**：建議每個系統皆使用不同密碼，防止撞庫攻擊。

5、 **避免使用公用 Wi-Fi 連接公司網路**：公眾公用網路是相當危險的，恐被側錄或竄改。若必要時可使用手機熱點或透過 VPN 連接網際網路。

6、 **禁止使用公共電腦登入機關系統**：外面的公共電腦難確保沒有後門、Keylogger 之類的惡意程式，一定要禁止使用公共電腦來登入任何系統。

7、 **確認連線裝置是否可取得內網 IP 位址**：確認內網 IP 位址是否無誤，是否能夠正常存取機關內部系統。

8、 **安裝個人電腦防火牆或防毒軟體**：個人防火牆可以基本監控有無可疑程式想對外連線。

9、 **工作時建議關閉不必要的連線**（如藍牙等）：部分資安專家表示，建議在工作時將電腦的非必要連線管道全數關閉，如藍牙等，在外部公眾環境或許有心人士可以透過藍牙攻擊個人裝置。

**二、 資料管理**

1、 **只留存在機關設備**：機關的機敏資料、文件等，必須只留存在機關設備中，避免資料外洩以及管理問題。

2、 **稽核記錄**：記錄機敏資料的存放、修改、擁有人等資訊。

3、 **重要文件加密**：重要的文件必須加密，且密碼不得存放在同一目錄。

4、 **備份資料**：機敏資料一定要備份，可以遵循「3-2-1 Backup Strategy」：三份備份、兩種媒體、一個放置異地。

三、 **實體安全**

1、 **離開電腦時立刻鎖定螢幕**：離開電腦的習慣是馬上進入螢幕保護程式並且鎖定，不少朋友是放著讓他等他自己進入鎖定，但這個時間差有心人士已經可以完成攻擊。

2、 **禁止插入來路不明的隨身碟或裝置**：社交工程的手法之一，就是讓同仁插入惡意的 USB，甚至有可能摧毀電腦（Bad USB, USB Killer）。

3、 **注意外人偷窺螢幕或碰觸設備**：若常在外工作處於公共空間，可以考慮採購螢幕防窺片。

4、 **不放置電腦設備在車上**：雖然台灣治安不錯，但也是不少筆電在車上遭竊，重要資產記得隨身攜帶，或者放置在隱密處。

- 網路的攻防就是一場戰爭，如果不從攻擊者的面向去思考防禦策略，不但無法有效的減緩攻擊，更可能在全世界疫情逐漸失控的當下，讓惡意人士透過這樣的時機癱瘓或攻擊遠距工作的機關，提醒所有遠距辦公者，提升資安注意能力。

以上資訊摘錄自「遠距工作的資安注意事項」https://devco.re/blog/2020/03/04/telework-security/