**雲林科技大學**

個人電腦安全設定作業說明書

**Windows 11版**

**文件編號：YUNTECH-ISMS-C-003**

**版 次：**1.0

**發行日期：111.10.13**

目錄

[一、 個人電腦密碼設定 1](#_Toc121921816)

[二、 密碼安全性原則設定 4](#_Toc121921817)

[三、 螢幕保護程式設定 5](#_Toc121921818)

[四、 關閉資源分享設定 7](#_Toc121921819)

[五、 停止共用資源設定 10](#_Toc121921820)

[六、 檢查新增移除程式 11](#_Toc121921821)

[七、 防毒軟體安裝 13](#_Toc121921822)

[八、 服務埠檢查 15](#_Toc121921823)

[九、 Guest帳號關閉設定 16](#_Toc121921824)

[十、 開啟WINDOWS系統自動更新程式設定 18](#_Toc121921825)

[十一、 設定Office 2019巨集安全性 19](#_Toc121921826)

[十二、 關閉插入可攜式儲存媒體或光碟時之自動執行功能 (autorun) 22](#_Toc121921827)

[十三、 開啟Windows系統防火牆功能 25](#_Toc121921828)

# 個人電腦密碼設定

密碼設定原則：

1.電腦設備應設定帳號密碼並定期檢查，密碼建議每6個月更新一次。

2.密碼設定原則密碼建議長度至少8個字元，可採用包含大寫及小寫字母、數字、標點符號、特殊字元之組合以增加複雜度。

3.密碼之設定不得與帳號相同。

4.妥善保管帳號及密碼，不隨意透漏或提供給他人使用；勿將密碼記載在他人垂手可得之地方，如：貼在螢幕上。

5.懷疑密碼外洩，立即變更密碼。

|  |  |
| --- | --- |
| 【**個人電腦密碼設定說明**】  1.點選【1】：點選『本機』  2.點選【2】：右鍵點選『管理』，開啟『電腦管理』視窗  3.點開【3】：點開『本機使用者和群組』  4.點選【4】：點選『使用者』  5.按下【5】：點選欲設定密碼的『使用者名稱』，按滑鼠右鍵，點選『設定密碼』  6.按下【6】：按下『繼續』  7.輸入【7】：鍵入欲設定之密碼  8.按下【8】：按下『確定』按鈕，再以設定之密碼登入電腦即可。 | |
|  |  |
| **3** | |
| **5**  **5**  **4** | |
| **6** | |
| **7**  **8** | |

# 密碼安全性原則設定

密碼安全性原則設定原則：

個人電腦除設定登入密碼外，也應設定系統密碼安全性原則，避免使用低安全度的密碼，使電腦安全性存在風險。

|  |  |
| --- | --- |
| 【**密碼安全性原則設定說明**】  1.開啟【1】：點選『開始』，輸入『secpol.msc』，開啟secpol.msc  2.點選【2】：點開『帳號原則』底下的『密碼原則』  3.設定【3】：將『密碼必須符合複雜性要求』設定為『已啟用』  4.設定【4】：將『密碼最長使用期限』設定為『180天』、『密碼最短使用期限』設定為『1天』  5.設定【5】：將『最小密碼長度』設定為『8個字元』 | |
|  |  |

# 螢幕保護程式設定

螢幕保護程式設定原則：

1.電腦應採用螢幕保護程式，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。

2.個人電腦不使用時，需採用密碼保護、鎖定或登出離線等安全措施。

|  |  |
| --- | --- |
| 【**螢幕保護程式設定說明**】  1.點選【1】：在桌面上按滑鼠右鍵，點選開啟『個人化』  2.點選【2】：點選個人化分頁中的『鎖定畫面』  3點選【3】：向下捲動並點選開啟『螢幕保護裝置』  4.設定【4】：設定等候時間為10分鐘，並勾選『繼續執行後，顯示登入畫面』  5.按下【5】：按下『確定』，設定完成 | |
| **1** | **2** |
| **3** | |
| **5**  **4** | |

# 關閉資源分享設定

非必要請盡量關閉資源分享功能，以防止網路病毒或不詳人士的惡意入侵，造成電腦被攻擊。

|  |  |  |
| --- | --- | --- |
| **【關閉資源分享設定說明】**  1.點選【1】：點選畫面右下角的管理區域，並點選其右下角齒輪圖案的『所有設定』  2.點選【2】：捲動網路和網際網路分頁至最下方，點選『進階網路設定』  3.點選【3】：點選開啟『更多網路介面卡選項』  4.點選【4】：點選開啟『乙太網路』 | | |
|  |  | |
| **3** | | |
|  | | |
| 5.點選【5】：開啟『乙太網路 內容』  6.點選【6】：將『File and Printer shering for Microsoft Networks』對話方框取消  7.選取【7】：選取『網際網路通訊協定第4版Internet Prptocol (TCP/IPv4)』  8.點選【8】：點選『內容』，開啟『Internet Protocol (TCP/IPv4) 內容』  9.點選【9】：點選『進階』，開啟『進階 TCP/IP 設定值』  10.點選【10】：點選『WINS』  11.點選【11】：點選停用『NetBIOS over TCP/IP』  12.按下【12】：按下『確定』，設定完成 | | |
|  | | |
|  | |  |

# 停止共用資源設定

非必要時，請勿開啟網路芳鄰分享目錄與檔案，並停用Guest帳號，避免遭受侵入攻擊。

|  |  |
| --- | --- |
| **【停止共用資源設定說明1】**  1.點選【1】：點選『本機』  2.點選【2】：右鍵點選『管理』，開啟『電腦管理』視窗  3.點開【3】：點開『共用資料夾』  4.點選【4】：點選『共用』  5.選取【5】：選取欲停止的共用資源，按滑鼠右鍵  6.點選【6】：點選『停止共用』  7.選取【7】：按下『是』，設定完成 | |
|  |  |
|  |  |

# 檢查新增移除程式

軟體使用安全原則：

1.請勿下載、安裝或使用來路不明、未經授權或影響電腦網路環境安全之電腦軟體。

2.進行下載、複製、使用軟體或不明來源檔案前，應先完成掃描檢查是否具有惡意軟體，確認檔案安全無虞，嚴禁任意移除或關閉防毒軟體。

3.移除電腦設備中非法或未經受授權軟體、音樂、影片檔等。

4.公務用電腦設備安裝軟體時，注意下列事項：

(1)安裝全校授權軟體時，請先參閱資訊中心授權軟體清單（<http://tcx.yuntech.edu.tw/index.php?option=com_content&task=view&id=822>），並確認其授權版本，避免使用無授權及非法軟體，以落實使用合法軟體。

(2)安裝自購軟體，請注意其授權數量、範圍、使用期限，與取得合法授權證明或相關佐 證(授權序號或授權資料網頁)，以確認所使用軟體之合法性。

|  |
| --- |
| **【檢查新增移除程式說明1】**  1.點選【1】：點選畫面右下角的管理區域，並點選其右下角齒輪圖案的『所有設定』  2.點選【2】：點選『應用程式』分頁中的『應用程式與功能』  3.點選【3】：選取非經授權之軟體請以滑鼠點選，點選右側之『…』並選擇『解除安裝程式』  **註：**請勿下載、安裝或使用來路不明、未經授權或影響電腦網路環境安全之電腦軟體 |
|  |
|  |
|  |

# 防毒軟體安裝

安裝防毒軟體可隨時監控電腦程式的舉動、及掃瞄系統是否含有病毒等惡意程式。

|  |  |
| --- | --- |
| **【防毒軟體安裝說明】**  開啟Microsoft Edge，連結至資訊中心首頁(http:// http://tcx.yuntech.edu.tw/) | |
|  | |
| 1.點選【1】：向下捲動網頁，並點選畫面中的『防毒軟體』 | |
|  | |
|  | |
| 2.點選【2】：點選『ESET 9版中文64Bit (支援Windows 10以上)』  3.點選【3】：點選OneDrive檔案下載頁面中的『Download』  4.安裝【4】：下載完成後，請開啟防毒軟體儲存位置，選點二下後即可自動進行安裝  註:如未能安裝成功，請先確認是否已安裝過，或已安裝其他防毒軟體 | |
|  |  |

|  |  |
| --- | --- |
| 服務埠檢查 通訊埠是電腦和網路之間的資訊門戶。每個通訊埠都有一個編號，而且專用於特定功能。例如，大部分網頁流量都會通過通訊埠編號 80。電子郵件則會通過通訊埠 25。心懷不軌的人可以掃描您的通訊埠，查看您哪個通訊埠是開放的，而如果有機可趁，他們即可利用這些通訊埠來攻擊您的電腦。 | |
| **【服務埠檢查說明】**  1.點選【1】：在桌面上按滑鼠右鍵，點選『在終端中開啟』  2.鍵入【2】：鍵入『netstat -an』  5.檢查【5】：檢查Local Address是否有80、21、25等服務埠，如發現以上資料，請作相關處理 | |
|  | 主要檢查是否有對外開啟的80, 21等服務埠 |
|  | |

# Guest帳號關閉設定

系統內建的帳戶，不需要使用的應停用，而需要使用的帳號可以更名與設定密碼來強化安全，Guest 這個來賓帳戶應關閉。

|  |  |
| --- | --- |
| **【Guest帳號關閉設定說明】**  1.點選【1】：點選『本機』，右鍵點選『管理』，開啟『電腦管理』視窗  2.點選【2】：點選『本機使用者和群組』  3.點選【3】：點開右邊視窗的『使用者』 | |
|  | |
|  | |
| 5選取【5】：選取『Guest』，按滑鼠右鍵  6.點選【6】：點選『內容』，開啟『Guest內容』  7.勾選【7】：將『帳戶已停用』選項打勾  8.按下【8】：按下『確定』，設定完成 | |
|  |  |

# 開啟WINDOWS系統自動更新程式設定

Windows系統自動更新程式可以自動定期檢查有沒有安全更新，如有即自動將安全更新傳送至您的電腦，只要一連上網際網路，就會透過未使用的頻寬進行下載更新。

|  |  |
| --- | --- |
| **【開啟WINDOWS系統自動更新程式設定說明】**  1.點選【1】：點選畫面右下角的管理區域，並點選其右下角齒輪圖案的『所有設定』  2.點選【2】：點選『Windows Update』分頁，開啟『進階選項』視窗  3.確認【3】：選擇更新安裝方式為「自動」， 開啟Windows自動更新功能 | |
|  |  |
| **5** | |

# 設定Office 2019巨集安全性

Visual Basic for Applications (VBA) 這種程式語言允許您建立功能強大的巨集讓重複性的工作變得更容易。但許多病毒的設計也旨在利用 VBA 巨集的能力，對您的系統及資料檔案造成傷害。對此問題的最佳防衛是將巨集安全性設定到『高』以上的等級，降低可能的威脅。

|  |
| --- |
| **【設定Office巨集安全性說明】**  由於每個Office軟體(Word,Excel,PowerPoint)的設定位置都相同，所以Word做畫面範例。  1.點選【1】：打開Word，先開啟空白文件，再點選上方工具列的『檔案』  2.點選【2】：選取『選項』  3.點選【3】：點選『信任中心』  4.點開【4】：點選右下角『信任中心設定』  5.按下【5】：選擇左方「巨集設定」，選擇「停用所有巨集」，按下『確定』，設定完成 |
|  |
|  |

# 關閉插入可攜式儲存媒體或光碟時之自動執行功能 (autorun)

自動執行（autorun） 程式是一個簡單的串接程式，會自動執行setup等執行檔，病毒可能藏autorun中指向病毒執行檔的位置，**如果沒有事先預防，即容易**導致中毒狀況發生。

|  |  |
| --- | --- |
| **【關閉插入可攜式儲存媒體或光碟時之自動執行功能 (autorun) 說明】**  1.開啟【1】：點選『開始』，輸入『gpedit.msc』，開啟gpedit.msc  2.點選【2】：點開『電腦設定』  3.點開【3】：點開『系統管理範本』  4.點選【4】：點選『Windows元件』  5.點選【5】：點選『自動播放原則』 | |
| **開始→搜尋→輸入”gpedit.msc** |  |

|  |
| --- |
| 6.點選【6】：點選『關閉自動播放』，開啟『關閉自動播放』視窗  7.點選【7】：點選『已啟用』  8.選取【8】：選取『停用自動撥放在：所有磁碟機』  9.選取【9】：按下『確定』，設定完成 |
|  |
|  |

|  |
| --- |
| 10.點選【10】：點選『開始』，輸入『自動播放設定』，開啟自動播放設定  11.點選【11】：為所有媒體與裝置使用自動撥放功能點選『關閉』 |
|  |
|  |

# 開啟Windows系統防火牆功能

電腦連線至網路時，應確保系統內建之防火墻有正確開啟，可避免未經許可的連線連入電腦。

|  |  |  |
| --- | --- | --- |
| **【開啟Windows系統防火牆說明】**  1.開啟【1】：點選『開始』，點選『搜尋』，輸入『 Windows 安全性』，開啟 Windows安全性視窗 | | |
|  |  | |
|  | | |
| 2.點選【2】：點開『防火牆與網路保護』  3.點選【3】：個別點選『網域網路』、『私人網路』、『公用網路』  4.點選【4】：確認各網路之防火牆都已啟用 | | |
|  | |  |