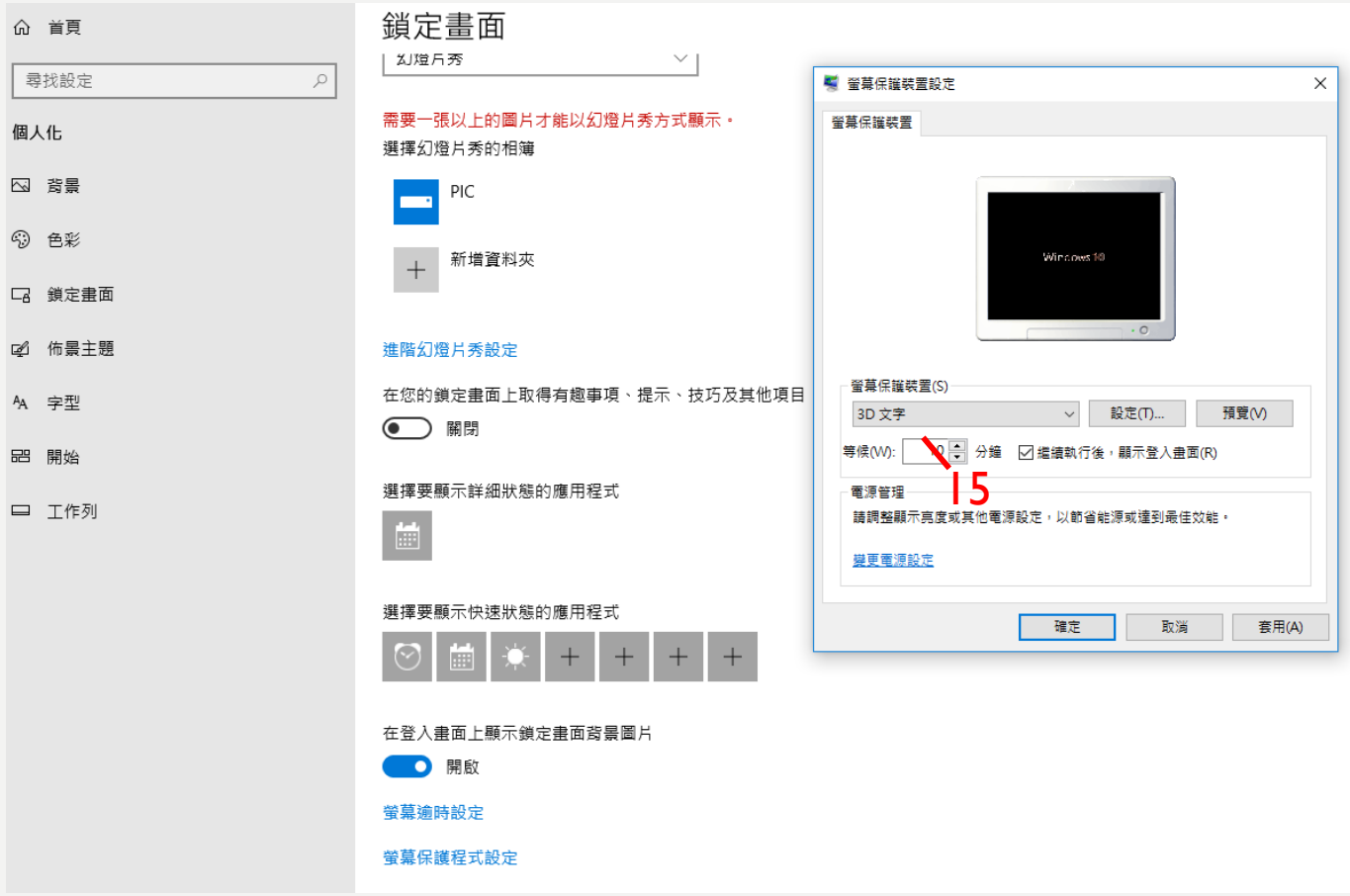
資安實地稽核前需對所有個人電腦進行設定

32	機關應依據規定要求執行個人電腦管理作業，查檢重點如下: 1). 設定螢幕保護機制。 2). 密碼符合密碼設定要求。 3). 嚴禁下載或使用非法軟體與檔案。 4). 安裝防毒軟體，病毒碼之更新，應設定為自動。 5). 作業系統應進行安全性更新。 6). 機敏性資料應有適當之保護措施。 7). 電子郵件關閉郵件預覽功能，使用文字模式瀏覽。 (所有機關)	抽查之個人電腦中，符合規定的小於 50%(含)。	0			☐ 符合 ☐ 建議 ☐ 觀察 ☐ 不符合 ☐ 不適用
		抽查之個人電腦中，符合規定的介於 50%(不含) - 75%(含)。	1			
		抽查之個人電腦中，符合規定的介於 75%(不含) - 100%(不含)。	3			
		抽查之個人電腦中，全部都符合規定。	5			

- 作業系統目前win7已經不支援！請安裝win10版本！否則市府資安稽核直接就是缺失起跳！
- 也請注意win10的版本~~~
- https://support.microsoft.com/zh-tw/help/13853/windows-lifecycle-fact-sheet

1.螢幕保護程式時間

- 個人桌上型電腦、可攜式電腦應設定於一定時間不使用或離開後，應自動清除螢幕上的資訊並登出或鎖定系統，以避免被未授權之存取。
- Windows設定→個人化→鎖定螢幕→螢幕保護裝置設定→等候至少「15」分鐘(可以更短)



通行碼規範

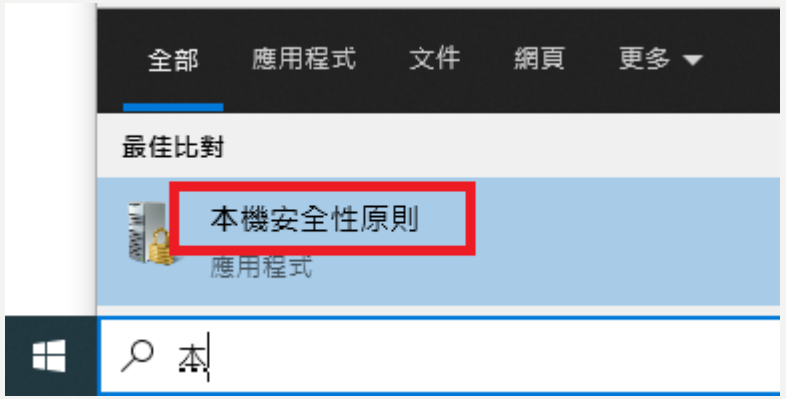
通行碼應符合政府組態基準（GCB）規範及資通安全責任等級分級辦法之政策，政策如下：

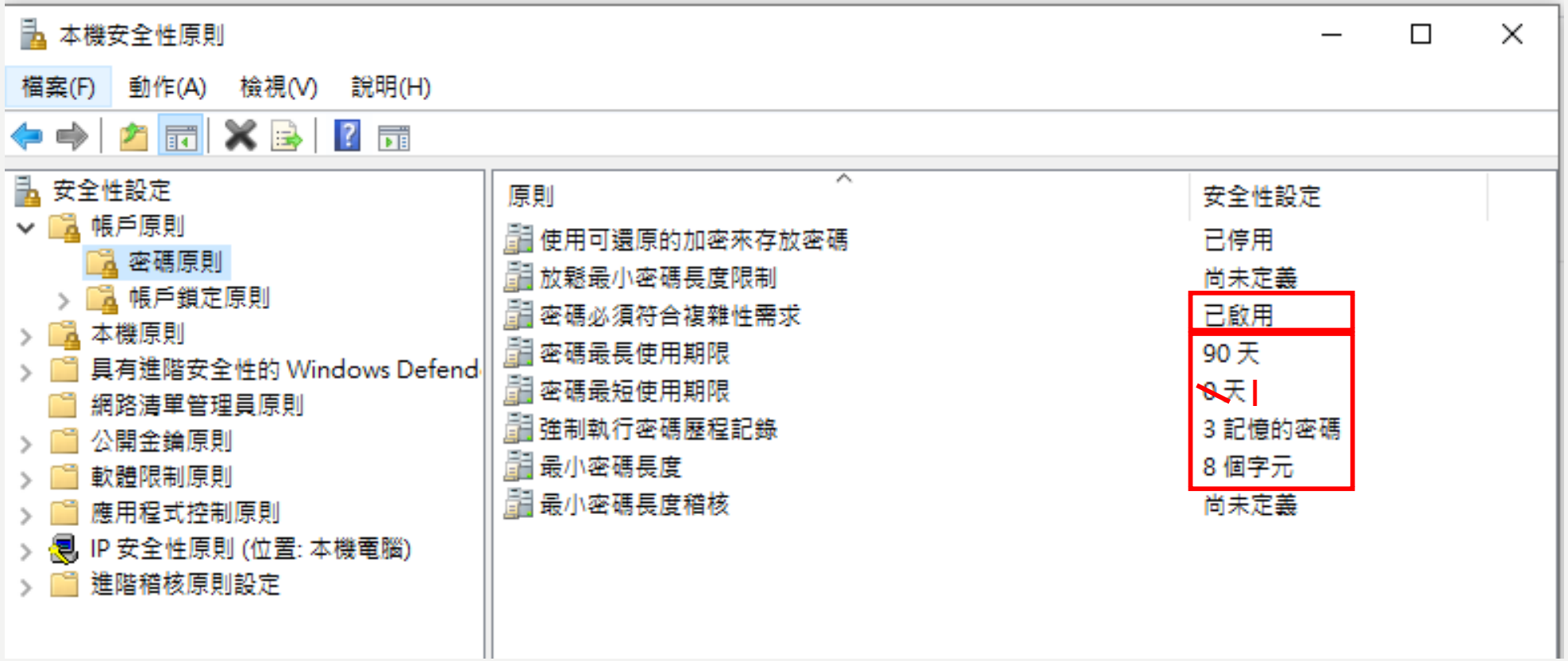
1. 通行碼長度8碼以上。
2. 通行碼複雜度應包含英文大寫、小寫、特殊符號或數字三種以上。
3. 使用者每90天應更換一次通行碼。
4. 使用者通行碼最短需使用1天，最長使用期限為90天，且通行碼需保留三次歷史紀錄不得相同。

2.密碼原則

【Win10】：

- 搜尋「本機安全性原則」(可參照右圖方法)
- 本機安全性原則→安全性設定→帳戶原則→密碼原則



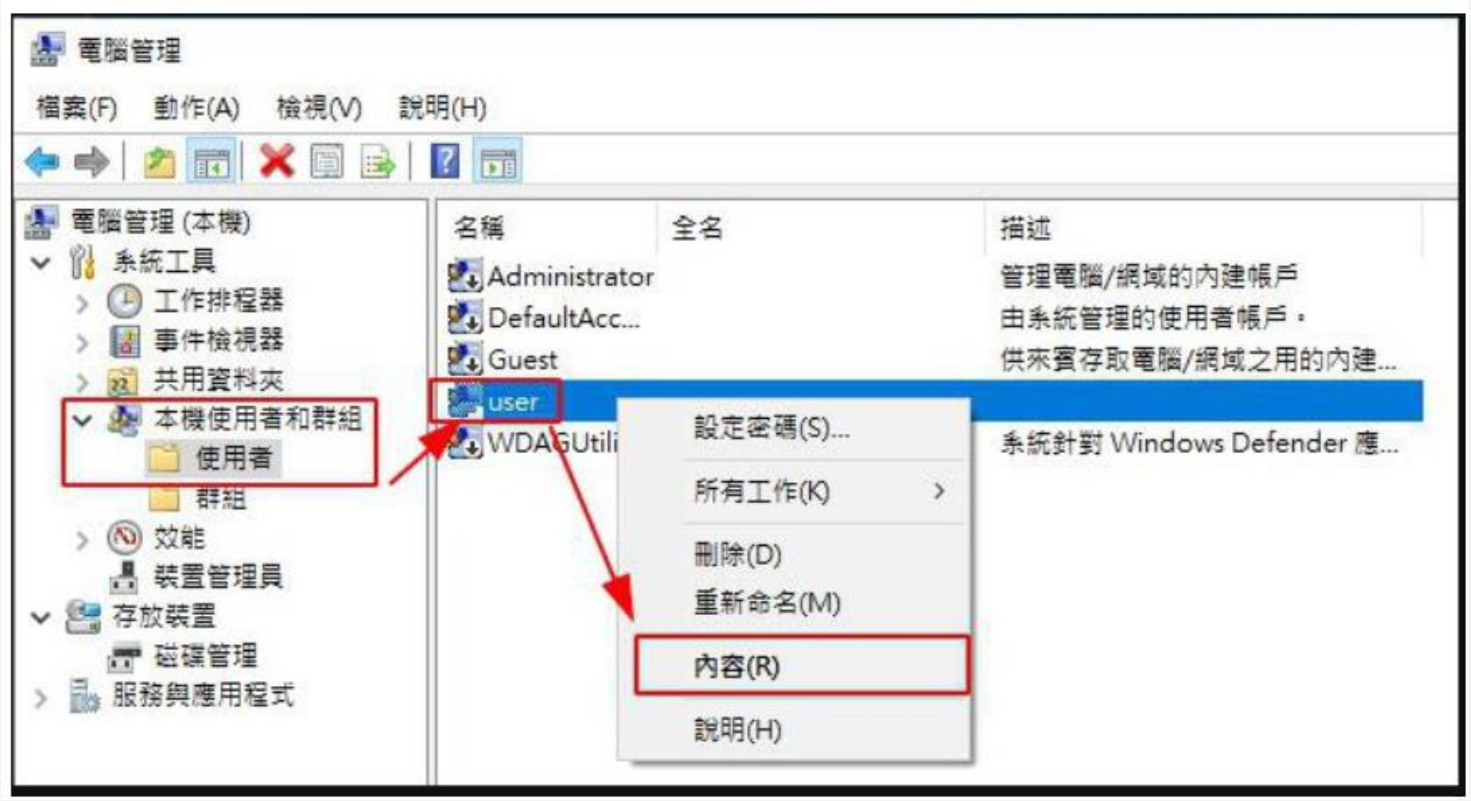


2.密碼原則

【Win10】：

- 點右鍵→電腦管理
- 本機使用者和群組→使用者→找到您的帳號→內容

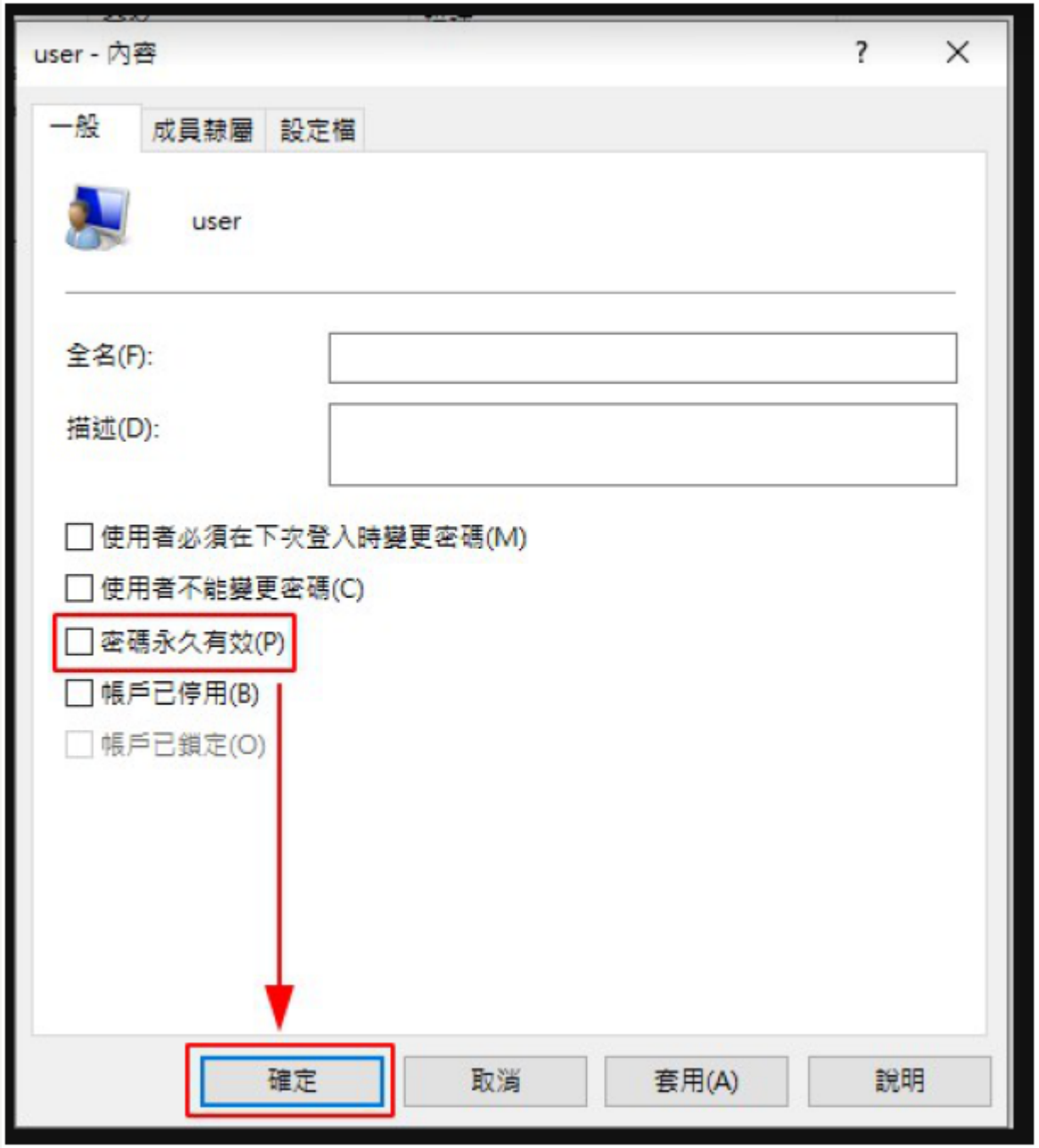
建議使用者帳號
不要使用user/administrator等已知帳號



2.密碼原則

【Win10】：

- 把「密碼永久有效」的勾勾取消



2.密碼原則(檢查是否已設定成功)

- 搜尋「cmd(命令提示字元)」(可參照右圖方法)
- 以系統管理員身分執行

2.密碼原則(檢查是否已設定成功)

輸入

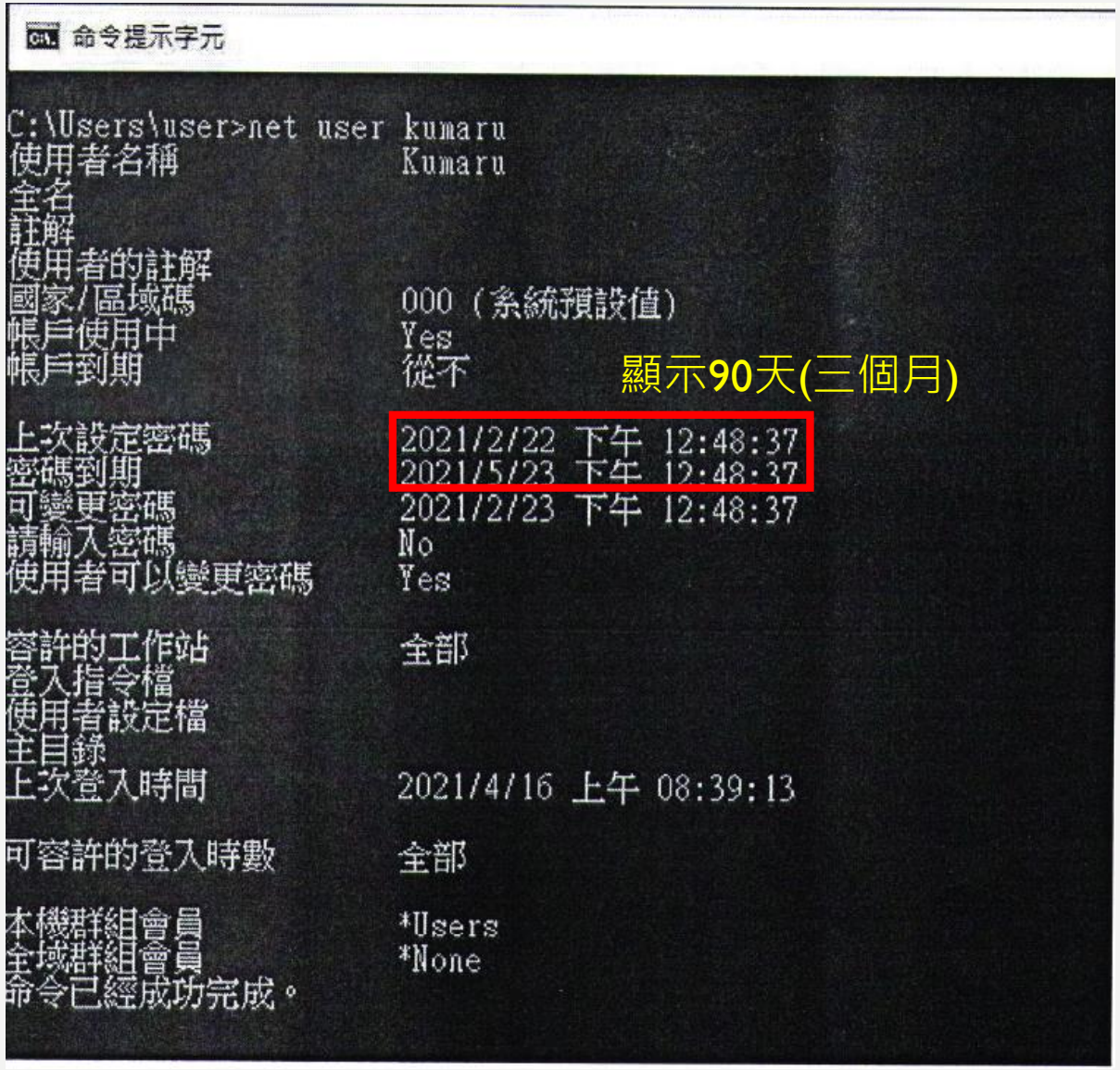
net user 您的使用者名稱

再按鍵盤的enter鍵

(例如：您的電腦使用者名稱為kumaru

請輸入

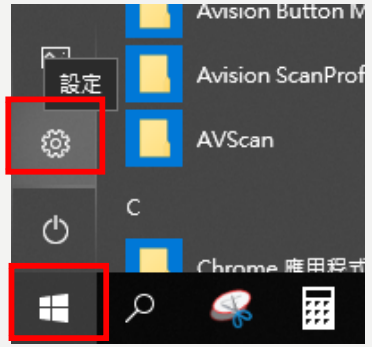
net user kumaru



3.嚴禁下載或使用非法軟體與檔案

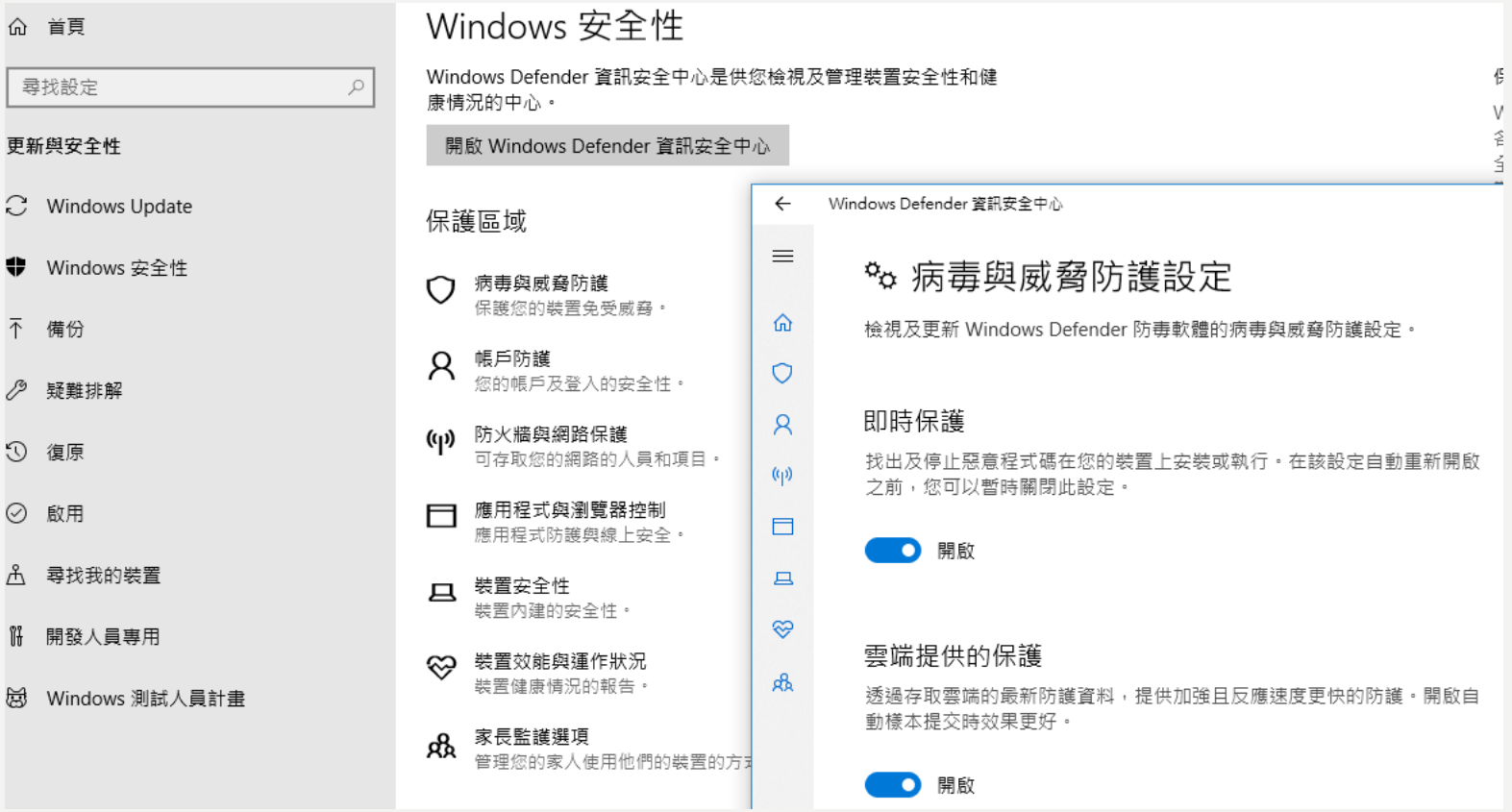
1. 禁止於個人電腦安裝線上遊戲、點對點傳輸（ Peer to Peer ）軟體（如BitComet 、迅雷、 KKBOX 、愛奇藝等等）、挖礦程式，以及跳牆程式、 VPN等 tunnel 相關工具下載或提供分享檔案。
2. 禁止下載或安裝來路不明、有違反法令疑慮如版權、智慧財產權等或與業務無關的電腦軟體。
3. 禁止於上班時間瀏覽不當之網路如暴力、色情、賭博、駭客、惡意網站、釣魚詐欺、傀儡網站等及非公務用途網站， 各單位主管應加強監督同仁使用網路情形。
4. 本府及所屬機關之個人電腦等資通設備，非經授權只能經由單一網卡連接機關內部網路連線上網。
5. 本府及所屬機關如須自行申裝專線或無線網路連線上網者，應經機關權責單位同意始得申裝；既有之線路應檢視與確認其必要性，非必要者應立即退租；如確有需要者，單位主管應要求連線之設備必須與機關內部網路實體隔離。
6. 教育部已公布禁用ZOOM！請記得解除安裝！

4.WINDOWS DEFENDER

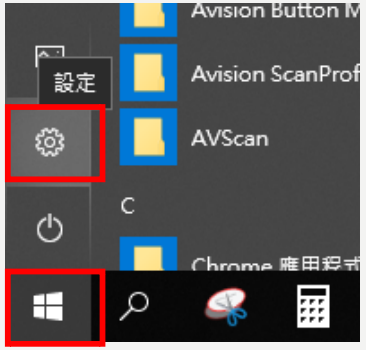


【Win10】：

- 找到「windows設定」(可參照右圖方法)
- windows設定→更新與安全性→Windows安全性→病毒與威脅防護→病毒與威脅防護設定→將「即時保護」、「雲端提供的保護」都開啟



5.WINDOWS UPDATE



【Win10】：

- 找到「windows設定」(可參照右圖方法)
- windows設定→更新與安全性→Windows Update→檢查更新

- **作業系統目前win7已經不支援！請安裝win10版本！否則市府資安稽核直接就是缺失起跳！**
- **也請注意win10的版本~~~**
- https://support.microsoft.com/zh-tw/help/13853/windows-lifecycle-fact-sheet

6.機敏性資料應有適當之保護措施

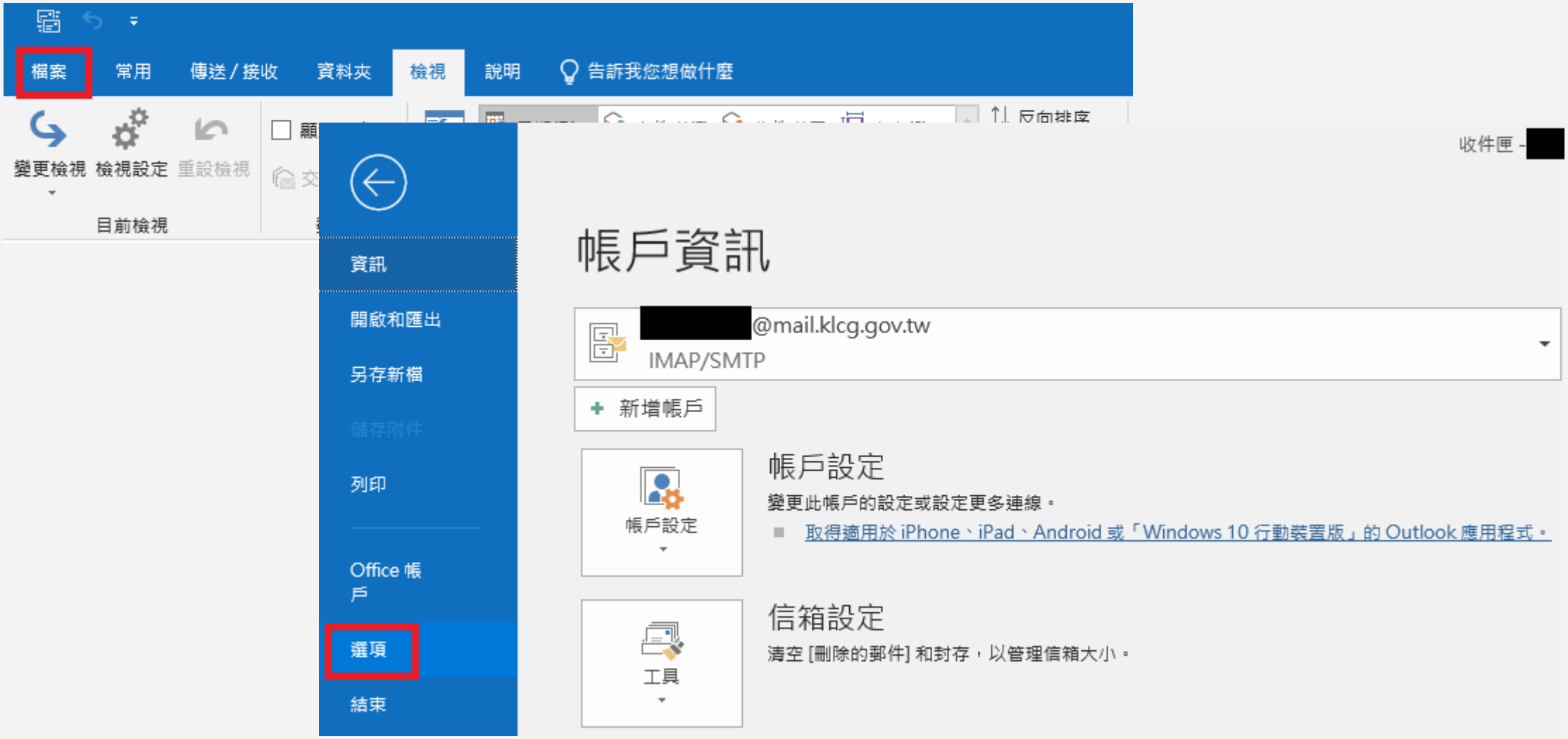
- 電腦設備內機敏性檔案，須由檔案擁有者以加密措施保護，如以壓縮軟體 7 zip 等方式執行壓縮加密碼，並限制不得於公務外電腦使用。
- 以word為例：點選「檔案」→保護文件→以密碼加密
- 以excel為例：點選「檔案」→保護活頁簿→以密碼加密
- 以PPT為例：點選「檔案」→保護簡報→以密碼加密

7.啟動電子郵件安全設定

- 以**市府信箱**為例：點選左下角「個人化設定」→右側「閱讀郵件設定」請勾選前三個，再按上方儲存

7.啟動電子郵件安全設定

- 以Outlook 2019為例：點選左上角「檔案」→「選項」



7.啟動電子郵件安全設定

- 以Outlook 2019為例：再點選左下角「信任中心」→「信任中心設定」→全勾選

7.啟動電子郵件安全設定

- 以G-mail為例：點選右上角齒輪→一般設定→勾選「顯示不明外部圖片時，必須先詢問我。」

校時

- 控制台→時鐘和區域→日期和時間→網際網路時間→變更設定→伺服器：ntp.kl.edu.tw