

規定密碼設定原則如下

(含 windows account, 專區 account, sql account)

1. 使用者密碼需英數字混合
 2. 不得與帳號名稱相同
 3. 使用者密碼長度至少 8 碼
 4. 密碼不得與前次設定相同
 5. 每半年要換密碼 (sql account 不用)
-

個人電腦或主機的存取控制原則如下:

1. 含上述密碼設定原則
 2. 設定密碼保護或採取 Ctrl+Alt+Del 登出方式進行鎖定
 3. 自行啟動螢幕保護程式之時間設定應不超過 10 分鐘
 4. 不可使用記錄密碼之功能，導致開機時自動登入系統
 5. 系統應有設定連續密碼登入錯誤次數限制
-

電腦設定步驟：

密碼設定原則及個人電腦或主機控制原則

1. 首先按下 Windows Key + R (或者 [開始] > [執行])
2. 輸入 gpedit.msc
3. 點到 [電腦設定] > [Windows 設定] > [安全性設定] > [帳戶原則] > [密碼原則]
4. 點兩下 [密碼必須符合複雜性需求] 打開設定，點選已啟用，按確定儲存
5. 點兩下 [密碼最長使用期限] 打開設定，輸入 182 天，按確定儲存
6. 點兩下 [最小密碼長度] 打開設定，輸 8 個按確定儲存
7. 點到[電腦設定] > [Windows 設定] > [安全性設定] > [帳戶原則] > [帳戶鎖定原則]
8. 點兩下 [帳戶鎖定閾值] 打開設定，輸 3 次按確定儲存，他會先提示把下面兩個設定的時間改成 30 分鐘，按確定

9. 點兩下 [帳戶鎖定時間] 打開設定，輸 10 分鐘按確定儲存
10. 點兩下 [重設帳戶鎖定計數器的時間間隔] 打開設定，輸 10 分鐘按確定儲存
11. 在 [開始] 上按右鍵選擇 [電腦管理]
12. 點到[本機使用者和群組] > [使用者]
13. 找到你的帳戶(通常就是那個 CIC)，在上面按右鍵選內容
14. 取消勾選[密碼永久有效]，按確定儲存

螢幕保護程式設定(win10)

1. 在桌面上按右鍵選[個人化]
2. 點選左側 [鎖定畫面]
3. 點一下視窗下方的[螢幕保護程式設定]
4. 在下拉選單任選一個喜歡的螢幕保護程式，將分鐘數設定為 10 分鐘，勾選[繼續執行後，顯示登入畫面]，按確定儲存設定。

螢幕保護程式設定(win8)

1. [控制台] > [所有控制台項目] > [個人化] > [螢幕保護程式]。
2. 在下拉選單任選一個喜歡的螢幕保護程式，將分鐘數設定為 10 分鐘內，勾選 [繼續執行後，顯示登入畫面]，按確定儲存設定。

防毒軟體更新設定

1. 開啟 [防毒軟體] > [防護狀態]為開啟，[更新] > 病毒資料庫版本應為最新版本。
2. 在 [更新] 畫面上按 F5 跳出 [進階設定] > [工具] > [遠端管理] 勾選 [連接到遠端管理伺服器]
3. [主要伺服器] 頁籤中 伺服器位置：“140.137.1.84” 連接埠：“2222”

作業系統更新設定(win10)

1. 在 [開始] 上按右鍵選擇 [設定]
2. 點選左下方 [更新與安全性]
3. 點選左側 [Windows Update] 確認更新到最新版本

作業系統更新設定(win8)

[控制台] > [所有控制台項目] > [Windows Update] > [變更設定] > 在重要更新區塊選擇 [自動安裝更新]。

檢查特殊軟體程式(win10)

1. 在 [開始] 上按右鍵選擇 [設定]
2. 點選右側 [APP]
3. 點選左側 [應用程式與功能] 確認無特殊軟體程式
4. 或由 [控制台] > [程式集] > [程式和功能] 確認無特殊軟體程式

檢查特殊軟體程式(win8)

[控制台] > [所有控制台項目] > [程式和功能]，檢查並確保沒有安裝特殊軟體程式，例如 eMule、eDonkey、BT、Clubbox、Foxy 等，或其他雲端軟體。

瞭解本校檔案交換平台及郵件加密傳送

⇒採用本校授權使用之檔案交換平台（業務文件典藏）。如採電子郵件寄送，則確認使用者是否遵循規定，將含個資之附件予以加密後寄送。

檢查外部空間無儲存任何公務資料

⇒檢查個人電腦外部網路硬碟空間是否儲存個人資料或組織內部資訊。

依本校「資訊安全管理系統-通信與作業安全管理程序書 1.3 版」中要求行動裝置管理 應符合下列規範：

1. 本中心禁止使用行動裝置進行非經授權之機敏資訊之存取，若因業務或特殊使用之需求，應進行申請及授權方可進行使用存取。
 2. 行動裝置應妥善設定通行碼，以避免未經授權之存取。
 3. 行動裝置閒置時應設定螢幕保護鎖定功能，最長不得超過 10 分鐘。
 4. 行動裝置上所執行的作業系統、軟體及 APP，必須安裝具合法使用版權之軟體，且應保持在該設備或軟體所提供之最新版本。
 5. APP 安裝前應考量其要求開放之讀取權限是否合理，如：讀取設備通訊錄、讀取 GPS 訊息等相關權限與資訊，再評估是否進行安裝。
 6. 使用者應依設備特性，進行適當之防護設定。
 7. 禁止行動裝置儲存敏感等級以上資料，以避免檔案或資料遭洩露。
 8. 使用行動裝置時，應做好安全管理工作，避免裝置遺失或資料遭竊取等情事發生。
 9. 行動裝置內之重要資料應定期備份，確保重要機敏資料之完整性。若需於第三方提供之雲端空間進行資料備份，應謹評估其備份項目、資料屬性是否適宜放置於雲端空間，避免機敏資料暴露在公用網路，亦應透過加密軟體進行加密保護。
 10. 為避免行動裝置遺失或失竊造成資料外洩之風險，可於行動裝置安裝遠端資料抹除軟體，以達到資料安全防護。
 11. 應避免使用公開之無線 Wi-Fi 網路進行資料存取與傳遞。
 12. 若無傳輸連線之需求，裝置應關閉短距連線傳輸功能，如：Bluetooth、NFC 等。
 13. 若無定位之需求，建議裝置應關閉 GPS 定位功能。
 14. 如遭嚴重惡意程式感染且影響其他資訊設備安全，應立即與網路離線，直到確認惡意程式消除後，才可重新連線。
 15. 私人的行動裝置應做好安全管理工作，並依上述規範進行安全防護。
-

依本校「個人資料安全管理措施實施作業程序書」中第五項作業說明第十項技術管理措施，要求各單位資訊作業安全應符合下列要求：

1. 針對處理個人資料之電腦、相關設備或系統上應有設定認證機制，認證機制得採用帳號密碼之方式進行，且密碼應具備必要之安全複雜性。
 2. 針對保有個人資料檔案之個人電腦，應有啟用螢幕保護機制，要求於一定時間內無動作時應登出使用者帳號並鎖定畫面。若屬於處理機敏性個資之個人電腦，並得視情況安裝螢幕防窺片，以防資料處理過程中遭到非業務相關人員之窺視。
 3. 個人電腦均應安裝防毒軟體並定期更新病毒碼，且嚴格禁止卸載本校所安裝之防毒軟體。
 4. 個人電腦應啟用作業系統自動更新機制，以對作業系統之漏洞執行修補。
 5. 個人電腦非經授權，不得安裝檔案分享軟體。
 6. 如需傳遞含有個人資料之電子檔案，應優先採用本校所提供之系統。若以電子郵件方式進行傳遞，應將含有個人資料之檔案以附件方式設定密碼加密後使得進行寄送，且密碼應採另一途徑(如電話告知或簡訊等)遞交予郵件收件人。
 7. 對於個人資料存取權限其數量與範圍，應於作業必要之限度內設定之，且原則上不得共用存取權限。
 8. 單位所使用之資訊系統若有蒐集、處理或利用個人資料者，應定期清查單位內人員之帳號權限使用情況，以確保相關權限配置經適當授權且與實際執行業務人員相符。
-