

# 彰化縣政府資訊安全作業注意事項

## 一、通行密碼設定原則

1. 通行密碼長度至少 12 個字元。
2. 通行密碼至少每 60 天更新一次。
3. 通行密碼必須符合複雜性需求：大小寫英文字母+數字或特殊符號。
4. 通行密碼應避免設定具有意涵之內容，如姓名、出生日期、身分證號碼、車牌號碼等，或密碼與帳號相同。
5. 應避免重複或循環使用舊的通行碼。
6. 不得將通行碼張貼在個人電腦或其他容易洩漏秘密之場所。

## 二、電腦環境安全：

1. 應遵守軟體授權規定，使用具合法版權軟體，不得安裝來路不明、非經合法授權使用之軟體。
2. 不可擅自更改系統環境設定，若需更改環境設定需填寫『政府組態基準設定 (GCB) 例外原則申請單』。
3. 單位若有新購置電腦須請電腦廠商依『政府組態基準設定 (GCB) 例外原則申請單』之規則基準值進行系統環境設定。
4. 電腦設備不可任意架站或做私人、營利用途。
5. 下班時，應先行關機始得離去，電腦關機應依正常程序操作。
6. 應配合進行軟體更新，修補漏洞，保持更新至最新狀態，勿自行關閉系統自動更新程式。
7. 啟用螢幕保護程式，設定螢幕保護密碼，並將螢幕保護啟動時間設定為 15 分鐘。
8. 禁止使用點對點互連 (P2P) 軟體及 tunnel 相關工具下載或提供分享檔案。
9. 使用外來檔案，應先掃毒，請勿任意移除或關閉防毒軟體。

## 三、隨時注意個人電腦防毒軟體之病毒碼是否為最新版本

1. 病毒碼更新日期最長不得超過一週，如有問題立即連絡計畫處資訊科  
操作方法：

將滑鼠移至右下角圖示，按右鍵「元件版本」，檢視上次更新時間

2. 本府每週四中午自動執行一次防毒軟體掃毒，所需時間約需 1~2 小時，若該時段電腦未開機者請自行進行手動掃毒。

操作方法：

將滑鼠移至右下角圖示，按右鍵「掃描」，『我的電腦』打勾，按「掃描」

## 四、電子信箱應關閉郵件預覽的功能，不認識寄件者的來信，請勿隨意開啟並點選超連結或附件檔，若無法確認信件來源請將郵件刪除。

## 五、資料保護：

1. 定期備份個人重要檔案。
2. 機密檔案不得在網路上傳送。
3. 因處理業務保有敏感性、機密性電腦資料或檔案者，應加強安全保護措施，如檔案加密、下班時應該上鎖或以其他方法妥為收存。
4. 各單位報廢之設備應執行儲存媒體重新格式化，移除相關作業軟體、資料及具有版權之系統軟體；報廢之磁帶、磁碟或光碟片等媒體進行實體銷毀；含有機密性資料之書面文件，使用碎紙機予以銷毀。
5. 請儘量避免使用電子郵件傳送個人機敏資料檔案。若欲使用電子郵件傳輸個人機敏資料前，請先加密處理。

## 六、資訊安全事件之通報：

資訊作業如因資訊安全事件（包括病毒無法立即清除、系統有安全漏洞、遭受非法入侵及破壞、遭遇阻斷服務攻擊及功能不正常事件等），致電腦系統無法運作或影響執行效率時，應迅速通報計畫處資訊科人員。