國立成功大學資訊安全守則

102 年 11 月 25 日國立成功大學資訊安全管理委員會會議通過

1. 目的

為落實本校資訊通訊安全，維護資訊及處理設備與個人資料之機密性、完整性、可用性及適法性，特訂定此守則。

2. 範圍

本守則適用於本校教職員生及相關作業之委外人員。

3. 作業守則

3.1 電腦應設定登入之帳號、密碼。如閒置 20 分鐘以上，應設定螢幕保護程式與密碼。
3.2 電腦作業系統及應用軟體之漏洞應即時更新、修補。電腦應安裝防毒軟體，並定期更新病毒碼，視需要設置防火牆或防間諜軟體。
3.3 電腦之資料應定期備份，並依其重要性設定備份頻率及備份版本。
3.4 避免開啟不明之網頁與來路不明之電子郵件及其附件，以防止電腦中毒或遭植入惡意程式。
3.5 當收到系統管理員告知郵件系統之帳號、空間問題而需提供帳號及密碼或點選連結時，此類郵件應為詐騙信，切勿直接依其指示處理，必要時請洽詢計算機與網路中心確認。
3.6 當有跡象顯示電腦系統可能遭入侵時，應儘速進行系統安全檢查，必要時請洽計算機與網路中心協助。
3.7 禁止未經授權破解他人電腦密碼、進行網路監聽、惡意干擾他人系統或網路服務。
3.8 機密或敏感資料與個人資料皆應妥善保存。若為電子檔案應考慮設定保護密碼。不再使用或超過保存年限之文件或檔案應予銷毀。
3.9 丟棄任何電子儲存媒介前，應將電子儲存媒介中的資訊刪除，並銷毀至無法解讀與還原之程度。
3.10 資訊設備送修時，應考量設備內所存有之機敏資料，必要時應移出含機敏資料的儲存媒體後再送修。
3.11 應遵守「個人資料保護法」規定，保護個人資料使用之合法性及機密性。

4. 密碼使用原則

4.1 一般資訊系統之使用者應至少每 6 個月更換通行密碼一次,並勿重複使用相同的密碼。
4.2 應避免將密碼記錄在書面上、張貼於個人電腦主機、螢幕或其他容易洩漏秘密之位置。
4.3 密碼長度應至少 8 位以上，且最好同時包括文字與數字。
以下為容易被猜測或破解之密碼，應避免使用：
4.3.1 連續的數字或字母，如：123456，abc123 等。
4.3.2 與使用者帳號相同。
4.3.3 英文名字、出生年月日、身分證字號、電話號碼。
4.3.4 常見的英文單字或專有名詞。
4.3.5 機關或單位的識別代碼或英文簡稱。

5. 伺服器管理

5.1 架設伺服器（www、mail、ftp 等）之單位，應指派專人管理，定期檢視系統狀態。

5.2 不必要之服務應給予關閉，以免留下資訊安全漏洞遭入侵。

5.3 設置網站應注意不可洩露機密或敏感資料與應受保護之個人資料。即使不在網頁連結架構內之檔案，若未設定適當權限，亦可能透過搜尋引擎搜尋造成資料外洩。

6.尊重智慧財產權

6.1 禁止濫用網路資源下載或上傳違反智慧財產權之檔案。

6.2 電腦安裝之軟體應有合法版權，不得安裝非法軟體。

7.公告與實施

本守則由本校資訊安全管理委員會通過後公告實施，修訂時亦同。