i Security

管理者的密碼維護手冊

NII產業發展協進會

密碼設定與管理是維護資訊系統安全使用、確保資訊系統，讓具有正當授權身份者使用的第一道防線。為避免資訊系統遭受入侵與防範不正當使用，企業內部資訊系統管理者可搭配企業的資訊安全政策，建立一套電腦密碼設定規範，並定期進行密碼的稽核與檢驗；此外，也應對全體員工進行密碼設定的基礎訓練與正確觀念的傳達。

隨科技技術的進步，駭客入侵、竊取、竄改與破解密碼的案例層出不窮，駭客們能在短時間內透過技術配合快速的破解密碼；因此為防範密碼設定遭受到破壞，瞭解如何選擇、設定、更新使用者與相關行政人員的密碼，已成為企業內部資訊系統管理者的重大課題。

何謂密碼管理？

密碼多半是由一組字彙（中、英文皆可）、數字、符號所組成的字串，提供使用者進入特定系統之初步過濾功能，以確保資訊系統只由已授權者所存取。避免密碼外洩與設定安全密碼為管理資訊系統安全的基礎工作，為維護密碼使用的安全，以下列出為管理者須知的密碼管理要點：

1. 定期更新密碼與密碼稽核

為確保密碼的機密性，使用者應定期更新密碼，減少密碼外流的機率。

- 可利用電腦系統設定密碼更新日期，以倒數記日的方式，提醒使用者應於何時進行密碼更新。

- 當公司內部若有人員異動，應立即進行相關密碼與使用代號更新。
- 至少每三個月、更新一次密碼。
- 將密碼存放於高安全性的地方。
- 刪除無效的使用者帳號。
- 密碼更新後可以利用下表進行密碼更新稽核，確保系統受到安全保護：

需要密碼管理的伺服器	是否知道密碼？	密碼更新週期
1. 開機啟動		
2. 電子抹除式唯讀記憶體		
3. 資料庫管理員帳號		
4. 伺服器管理帳號		
5. 瀏覽器		
6. 用戶端		
7. 不斷電系統監視軟體		
8. 路由器管理		
9. 防火牆管理		
10. 任何附掛於自己系統上的其他主機應用程式或伺服器		
11. 伺服器上的所有應用軟體		
12. 遠端登入/遠端檔案傳輸(Telnet/Ftp)的系統		

2. 設定優質密碼

設定優質的密碼（不容易被猜中的密碼）保護各個電腦系統是非常重要的。為減少密碼遭受駭客破解所造成損失，電腦管理者也需要一套程序來確保密碼的正常運作。設定優質密碼的秘訣如下：

- **設定至少 8 個字元的密碼**

  密碼設定建議字元至少需為 8 個字元的字串。駭客可藉高效能密碼對比器在 2 天破解含有 6 個字元的密碼字串；7 個數字的密碼字串能在 4 個月內被破解。為提高密碼使用的安全性，設定 8 個以上字元的密碼字串，並且定期更新密碼，可提高密碼的安全性。

- **避免使用重複的字母或數字，如 aaa1122, 555iii99。**
- **使用數字、字母、符號混合穿插的密碼字串**

  為增加密碼受破解的難度，應避免使用簡單且他人容易取得的資料為個人密碼（姓名、電話、生日、電子信箱網址等）。建議以大小寫字母、數字、及符號（＃％＄@...）混合方式設定密碼。

- **不使用過於複雜而無法記憶的密碼**

  過於複雜的密碼導致使用者必需寫下密碼便於記憶，卻提高了密碼外洩的風險。

- **利用特殊符號記憶密碼**

  若要使得密碼簡單易記，使用者可以選擇喜愛的名字但務必穿插數字或符號以增加密碼破解的難度，並將特定的字母用類似的符號或數字取代，例如將 happiness 修改為 h@pp1n3ss ，可同時使得密碼簡單易記，又能增加密碼使用的安全性。

- **避免重複使用已使用過的密碼**

  建立密碼歷史資料庫，以管理使用過的密碼，避免密碼重複使用。

- **避免使用簡單且字典查得到的單字或企業名稱縮寫**
- **利用電腦符號轉換技術輸入密碼**

  利用電腦符號轉換技術，以小於 255 的數字當作密碼；在輸入數字時同時按住 Alt 鍵，則電腦會將數字轉換成符號；當數字為 2 位數時，數字前加上數字 0。如此可降低密碼被破解之機率。

- **利用事件描述法記憶與設定密碼**

  使用者有時想要利用熟悉的事件為密碼，可擷取單字字首並將某些字母改為數字，即可組合成他人無法理解的密碼，如將「On April 16, I ate a Chucky Cheese pizza」，擷取單字的第一個字母，組合成「oA16I8aCCp」。

3. 對員工進行密碼保密的教育訓練

系統管理者需清楚知道企業內部密碼儲存管理的方式為何，並針對其管理特性，設定密碼管理機制以確保密碼管理機制的正常運作。此外，不僅管理者應負其密碼管理的重任，也應要強力要求一般員工也需就其密碼進行保密；管理者應傳達下列要點至公司內部所有員工。

- 不告訴別人密碼，包括男女朋友、職務代理人、上司等。
- 不寫下密碼。
- 一旦懷疑有人可能知道你的密碼時，即刻更改。
- 不使用失效的帳號與訪客帳號。
- 不設定過於複雜難記的密碼。
- 定期更換密碼。