資通訊產品帳號權限與密碼管理原則

一、依資通安全管理法暨資通安全責任等級分級辦法附表 10、資通系統防護基準辦理。

二、因近日教育體系資安威脅情資頻傳，請強化貴校教職員之資安防護知能，並於辦理資訊業務時，參考以下帳號權限與密碼管理原則，落實管理資通系統，以避免資安事件發生：

(一) 最高管理者權限帳號數量，原則不得超過 3 個。

(二) 使用者於第一次登錄系統時，應立即更改預設密碼，並妥善保管帳號與維持密碼之機密性。

(三) 使用者禁止共用自己或他人的帳號及密碼。

(四) 使用者每次存取系統時應輸入密碼登入系統，避免使用記錄密碼功能，導致開機時自動登入系統。

(五) 密碼長度設定至少 8 碼，且應符合帳號及密碼內容設置原則。

(六) 密碼內容之設定，應參雜數字、英文字母大小寫及特殊符號，至少符合下列 4 項要求中之 3 項。

1、內含至少 1 個大寫英文字母。

2、內含至少 1 個小寫英文字母。

3、內含至少 1 個阿拉伯數字。

4、內含至少 1 個特殊符號。

(七) 密碼內容之設定，應儘量避免使用易猜測或公開資訊，如下說明：

1、個人姓名、出生年月日、身分證字號。

2、機關、單位名稱或是其他相關事項。

3、使用者 ID、其他系統 ID。

4、電腦主機名稱、作業系統名稱。

5、電話號碼、空白、字典字彙(具有意義的英文單字，例如：password 等)。

6、禁止使用鍵盤順序鍵(如：qwer)。

7、密碼不得與帳號相同。

(八) 密碼最短使用期限為 1 天，並應定期更換，90 天(含)以內必須更換密碼一次，逾期未變更者，應暫停其系統登入之權限，以避免盜用情形；密碼變更時不得使用與前 3 次相同的密碼。

(九) 管理者及使用者帳號應避免共用，並負帳號及密碼保管之責，不得對任何人透露或以任何形式公開自己帳號及密碼，亦避免將帳號、密碼記錄在書面上，或張貼在個人電腦、螢幕或其他未保護且容易洩漏秘密之處所，以避免密碼外洩。

(十) 懷疑密碼被他人知悉或發現密碼可能遭破解時，應立即更改密碼。

(十一) 帳號登入進行身分驗證失敗達 5 次後，系統將自動鎖定帳號時間至少 15 分鐘不允許該帳號繼續嘗試登入。

(十二) 使用者職務異動或離職時，部門主管應即時通知相關單位調整或終止使用者之存取權限。

(十三) 系統之帳戶，若超過 6 個月未曾登錄，則視需要清除閒置帳號。