密碼複雜度原則

一、 密碼最短使用期限 => 每次變更密碼後，24 小時內密碼不能再變更

二、 密碼最長使用期限 =>密碼每 90 天要變更一次

三、 最小密碼長度 =>最少要 8 個字元

四、 密碼必須符合複雜性需求 =>

1、 不得包含使用者的帳戶名稱

2、 長度至少為 8 個字元

3、 包含下列四種字元中的三種

(1) 英文大寫字元(A 到 Z)

(2) 英文小寫字元(a 到 z)

(3) 10 進位數字(0 到 9)

(4) 非英文字母字元(例如：!、$、#、%)

五、 強制執行密碼歷程記錄 => 不得重複前 3 次密碼

※參考資料:

1. 行政院國家資通安全會報技術服務中心之政府組態基準

2. 資通安全責任等級分級辦法

3. 105 年國家資通安全防護整合服務計畫電子郵件安全參考指引修訂

參考資料:

政府組態基準
Microsoft Windows 10
(V1.3)

行政院國家資通安全會報技術服務中心

中華民國109年11月

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
4	Windows 10 Account Settings	TWG CB-01-005-0004	帳戶原則\密碼原則	密碼必須符合複雜性需求	▪此項原則設定決定密碼是否必須符合複雜性需求 ▪如果啟用了此原則，則密碼必須符合下列最小需求： -不包含使用者的帳戶名稱全名中，超過兩個以上的連續字元 -長度至少為 6 個字元 -包含下列四種字元中的三種： (1)英文大寫字元(A 到 Z) (2)英文小寫字元(a 到 z) (3)10 進位數字(0 到 9) (4)非英文字母字元(例如：!、$、#、%) ▪建立或變更密碼時會強制執行複雜性需求	電腦設定\Windows 設定\安全性設定\帳戶原則\密碼原則\密碼必須符合複雜性需求	啟用	CCE-ID：CCE-42872-2

法規名稱：資通安全責任等級分級辦法 EN

第 11 條

1 各機關應依其資通安全責任等級，辦理附表一至附表八之事項。

2 各機關自行或委外開發之資通系統應依附表九所定資通系統防護需求分級原則完成資通系統分級，並依附表十所定資通系統防護基準執行控制措施；特定非公務機關之中央目的事業主管機關就特定類型資通系統之防護基準認有另為規定之必要者，得自行擬訂防護基準，報請主管機關核定後，依其規定辦理。

3 各機關辦理附表一至附表八所定事項或執行附表十所定控制措施，因技術限制、個別資通系統之設計、結構或性質等因素，就特定事項或控制措施之辦理或執行顯有困難者，得經第三條第二項至第四項所定其等級提交機關或同條第五項所定其等級核定機關同意，並報請主管機關備查後，免執行該事項或控制措施；其為主管機關者，經其同意後，免予執行。

4 公務機關之資通安全責任等級為A級或B級者，應依主管機關指定之方式，提報第一項及第二項事項之辦理情形。

5 中央目的事業主管機關得要求所管特定非公務機關，依其指定之方式提報第一項及第二項事項之辦理情形。

附表十　資通系統防護基準修正規定

系統防護需求分級 / 控制措施 構面	措施內容	高	中	普
識別與鑑別	內部使用者之識別與鑑別	一、對資通系統之存取採取多重認證技術。 二、等級「中」及「普」之所有控制措施。	資通系統應具備唯一識別及鑑別機關使用者(或代表機關使用者行為之程序)之功能，禁止使用共用帳號。	
	身分驗證管理	一、身分驗證機制應防範自動化程式之登入或密碼更換嘗試。 二、密碼重設機制對使用者重新身分確認後，發送一次性及具有時效性符記。 三、等級「普」之所有控制措施。		一、使用預設密碼登入系統時，應於登入後要求立即變更。 二、身分驗證相關資訊不以明文傳輸。 三、具備帳戶鎖定機制，帳號登入進行身分驗證失敗達五次後，至少十五分鐘內不允許該帳號繼續嘗試登入或使用機關自建之失敗驗證機制。 四、使用密碼進行驗證時，應強制最低密碼複雜度；強制密碼最短及最長之效期限制。 五、密碼變更時，至少不可以與前三次使用過之密碼相同。 六、第四點及第五點所定措施，對非內部使用者，可依機關自行規範辦理。

105年國家資通安全防護整合服務計畫

電子郵件安全參考指引修訂

(V3.0)

執行單位：財團法人資訊工業策進會

中華民國105年11月

2.1.3.4. 字典檔與暴力攻擊

有些惡意攻擊者會運用字典檔攻擊(Directory Harvest Attack, DHA)與暴力攻擊(Brute-Force attack)試圖入侵受害單位。字典檔攻擊的原理是發送大量有著不同拼字組合或是常見用的詞庫(例如常見姓名)，做為收件人帳號的Email至攻擊目標單位主機，以確認該郵件主機具有哪些真實存在的使用者帳號，待攻擊者取得真實帳號後，即有可能鎖定該帳號進行針對性攻擊，因此也稱為猜帳號攻擊。

而暴力攻擊則是假設使用者的帳號或密碼之長度，由於變化有限而易於猜測，例如若某機關的帳號是六碼數字或是某單位的密碼允許使用者只設定六碼。則六碼的長度內，舉例而言，僅有英文26種、大小寫、數字10個，則每一碼共62個變化，六碼的變化為62^6，以時下的個人電腦效能而言，這樣的六碼密碼只需約2小時就可由程式試完所有組合將之破解。暴力攻擊的原理即是將所有變化都測試過，即可測得正確的帳號密碼為何。由於網路服務，每次測試需要主機回應，一般暴力攻擊會配合字典攻擊、常見姓名或常見密碼等方式，減少測試的次數、並拉長每次攻擊間距，迴避主機端的偵測與阻擋。主要的防制方式還是需要每位使用者設定長度足夠的密碼。密碼長度或複雜度等相關規定請參考政府組態基準(GCB)。

由於尋找攻擊目標真實帳號可能是駭客攻擊的第一步，而取得密碼則幾乎等同取得使用者身分，建議政府機關導入郵件服務的同時，也應確認是否有防制字典檔(猜帳號)與防制暴力攻擊的機制，相關的防護方式將於本指引「2.4.1 閘道過濾與處置」當中說明。