徵集意見：密碼規範建議

起因

公家機關及政府系統都有設定 90 天密碼最長使用期限、密碼複雜度等規定，其脈絡為資安法定義 A 級機關須符合資安院定義 GCB 政府組態設定 [國家資通安全研究院- 政府組態基準(GCB)]
（例如其中[帳戶原則與精細密碼原則設定說明**(2022/12/26更新)**]附表）定義密碼最長使用期限，及諸多非現今合適的密碼原則設定。如：

```
Unset
msDS-MaximumPasswordAge 密碼最長使用期限 dd:hh:mm:ss
如:90:00:00:00
```

有些過時或不適用現今時代的規則常讓使用者感到頭痛，而開發者或廠商想改善系統卻又受限於國內政府規範。

一直以來，許多人敲碗，希望能有機會推動國內法規跟上國際標準，
目前有機會能夠修正、改善相關規範，希望能蒐集大家的想法。

（因此規範訂定後，不論等級之大大小小系統都須符合、採用，作為一個基礎基準，故此規範不宜制定得太過嚴峻。）

編修方法與注意事項

本文件僅供想法交流、意見討論。

此文件為公開文件，請大家直接以註解方式提供意見、於註解中討論。

預計開放數日，我（BlueT 練喆明 [練喆明 Matthew Lien (BlueT)]）將不定期將意見彙整入內文。
彙整入內文中之項目不代表一定會成為未來新版本定案之內容，畢竟還有層層關卡、各級機關之審核與調整。

注意事項：

- 請參考現行「GCB 政府組態基準」服用。[國家資通安全研究院- 政府組態基準(GCB)]
- GCB 規範內容主要為規範「至少、必須」的「最低基準」，而非「最好的狀況」。

    - 例：一個整包預算只有十萬的表單或活動報名系統，也須符合此規範，所以定得太嚴峻只會造成法規修訂失敗。
- 本文件範圍只討論「系統」要做哪些「關於密碼」的「限制」，而不討論使用者端之技術選擇（例：是否自行想採用 password manager 等），也不討論全面導入Passwordless 等（考量許多目前的環境限制、經費限制、全民普及度、應用場域適用性、過渡期等，密碼還是必須的存在）。
- 提出之規範實踐須考量是否造成經費成本太高（例：行動電話、Ubikey）、技術成本太高、過度依賴境外或單一提供商。
- 各項期許，須有國際標準或各國政府指導方針等 ref 作為有力支持論述之參考指標，不然會造成修訂闖關失敗。

相關但不在此範圍的討論，請於「其他建議」中討論。
超過本文件範圍之討論，會評估是否納入正在起草中之 Resilient Architecture Best Practices 文件。

建議調整項目

不建議《密碼 90 天過期》參考規範/文件

將導致使用者選擇使用具重複性、有規則性、易被破解的密碼。
只有在「有證據」顯示密碼遭「破解或外洩時」，得要求使用者更換密碼。

美國標準單位 National Institute of Standards and Technology（NIST）800-63 有對應規範

- https://pages.nist.gov/800-63-FAQ/#q-b05
- https://pages.nist.gov/800-63-3/sp800-63b.html#memsecretver
  Verifiers SHOULD NOT require memorized secrets to be changed arbitrarily (e.g., periodically). However, verifiers SHALL force a change if there is evidence of compromise of the authenticator.

1password 跟英國政府也有些參考資料

- https://blog.1password.com/should-you-change-passwords-every-90-days/
- https://www.ncsc.gov.uk/blog-post/problems-forcing-regular-password-expiry
- https://www.ncsc.gov.uk/collection/passwords/updating-your-approach

「有證據顯示密碼遭破解或外洩」的參考範例：

- 收到資安通報
- 於暗網中出現該組織資料庫外洩之消息

- 密碼被 Hardcode 在自動化系統中，而該自動化系統程式碼有可能洩漏
- 發生不明登入事件，使用者無法驗證該不明登入時間或是地點為使用者知曉之時間地點
- Twitter曾因bug意外於log中紀錄使用者密碼明碼，要求使用者更新密碼

不建議《密碼複雜度》參考規範/文件

將導致使用者選擇使用可預測、僅為了滿足規則而產生的密碼（例如固定在不安全的密碼後方加上！），或導致使用者因難以記憶，而使用不安全的方法紀錄密碼（例如寫在便條紙上並貼在螢幕上）。

- 密碼長度比複雜度更重要。
- 可輔以其他密碼檢核機制，如：不可使用已知遭破解之密碼（ex, have I been pwned）

美國標準單位 National Institute of Standards and Technology（NIST）800-63 有對應規範

- https://pages.nist.gov/800-63-FAQ/#q-b06
- https://pages.nist.gov/800-63-3/sp800-63b.html#memsecretver
  Verifiers SHOULD NOT impose other composition rules (e.g., requiring mixtures of different character types or prohibiting consecutively repeated characters) for memorized secrets. Verifiers SHOULD NOT require memorized secrets to be changed arbitrarily (e.g., periodically). However, verifiers SHALL force a change if there is evidence of compromise of the authenticator.

其他參考單位：

- Microsoft - Microsoft Security Baseline / Password Guidance
- UK National Cyber Security Centre (NCSC) - NCSC Password Guidance / Password administration for system owners
- Australian Cyber Security Centre (ACSC) - ACSC Password Policy Guidelines
- New Zealand Government (CERT NZ) - CERT NZ Password Policy
- 德國聯邦信息安全辦公室 (BSI) - IT-Grundschutz-Kompendium
- 加拿大通信安全機構 (CSE) / 加拿大網路安全中心 (CCCS) - Password Guidance for the Government of Canada
-

建議《系統支援密碼長度》參考規範/文件

因密碼長度比複雜度更具備防破解特性，系統須支援至少 64 字元長度以上（包含）之密碼。
系統不可以截斷長密碼以偽裝為支援長密碼。

美國標準單位 National Institute of Standards and Technology（NIST）800-63 有對應規範

- https://pages.nist.gov/800-63-3/sp800-63b.html#memsecretver

Verifiers SHOULD permit subscriber-chosen memorized secrets at least 64 characters in length.
Truncation of the secret SHALL NOT be performed. For purposes of the above length requirements, each Unicode code point SHALL be counted as a single character.

其他參考單位：

- 64 chars
  - 開放網絡應用安全項目 (OWASP) - Authentication Cheat Sheet
  - 加拿大網路安全中心 (CCCS)
  - 加拿大通信安全機構 (CSE) - User Authentication Guidance for Information Technology Systems
  - 澳大利亞網絡安全中心 (ACSC) - Guidelines for System Hardening
- 128 chars
  - 歐洲網絡與信息安全局 (ENISA) - Password Recommendations
- More or unlimited
  - 英國國家網路安全中心 (NCSC)

建議《系統支援密碼字元種類》參考規範/文件

限制可輸入字元將導致使用者被迫選擇設定難以記憶之密碼，導致選擇使用可預測、僅為了滿足規則而產生的密碼（例如固定在不安全的密碼後方加上！），或導致使用者因難以記憶，而使用不安全的方法紀錄密碼（例如寫在便條紙上並貼在螢幕上）。
系統應支援所有可顯示之 ACSII 字元（包含空格）與 Unicode 字元（包含 0-9,a-z,A-Z, 可顯示之特殊符號），不應排除任何以上範圍內之字元輸入作為密碼之組成成份。（以 Salted Hash 處理後，並不會因此導致 SQLi 等安全問題）

美國標準單位 National Institute of Standards and Technology（NIST）800-63 有對應規範

- https://pages.nist.gov/800-63-3/sp800-63b.html#memsecretver
  Verifiers SHOULD permit subscriber-chosen memorized secrets at least 64 characters in length. All printing ASCII [RFC 20] characters as well as the space character SHOULD be acceptable in memorized secrets. Unicode [ISO/ISC 10646] characters SHOULD be accepted as well.

其他參考單位：

- UK National Cyber Security Centre (NCSC) - NCSC Password Guidance
- OWASP (Open Web Application Security Project) - OWASP Password Storage Cheat Sheet / Authentication Cheat Sheet
- European Union Agency for Cybersecurity (ENISA) - ENISA Password Security Guidelines / Password Recommendations
- 澳大利亞網絡安全中心 (ACSC) - Guidelines for System Hardening

- 加拿大通信安全機構 (CSE) - User Authentication Guidance for Information Technology Systems
- 微軟 (Microsoft) - Password Guidance

其他建議

- 定期複驗系統中已儲存密碼之安全性（ex, 字典檔、have I been pwned）
- 直接取消複雜性和長度要求很危險，應連同NIST-800-63B 5.1.1.2 以下兩點要求一起看：
    - Verifiers SHOULD offer guidance to the subscriber, such as a password-strength meter [Meters], to assist the user in choosing a strong memorized secret.
    - When processing requests to establish and change memorized secrets, verifiers SHALL compare the prospective secrets against a list that contains values known to be commonly-used, expected, or compromised.
    - 其中一種實作：https://github.com/dropbox/zxcvbn
        - 它還包了個簡單字典檔
- NIST-800-63-3 “6 Selecting Assurance Levels” 規定了很多使用場景都需要Assurance Level 2或以上 (註冊賬號認証IAL2, 驗証認証AAL2等)，而AAL2/3所需要的認証手段在NIST-800-63B Section 4中有列明。
    - 按**NIST-800-63**的規定，單單使用密碼，即使完全遵照**NIST-800-63B**的要求去實現，也不能達致**AAL2**。
    - 密碼+簡訊驗証碼即Memorized Secret + Out-of-band能達致AAL2
    - 上AAL3就要Webauthn + PIN之類了
- 在標準中的 SHOULD SHALL 意思和台灣的法律用語的「應」是不同意思，通常標準中的用語會區分為 MUST SHOULD MAY “SHOULD NOT” “MUST NOT” 這些等級 (RFC2119)，但是在台灣法律用語的「應」指的是強制的意思，是 MUST 的意思，如果要表示 SHOULD 的意思的話應該要使用「得」，另外要注意「不得」並不是「SHOULD NOT」的意思。更精確的翻譯我會建議不使用「得」，而是改使用較為白話的「應該」「不應該」或是「建議」「不建議」，而原本使用「應」「不應」的部分則是改成使用「必須」「必須不」或是「不得」。