Texas Veterans Commission
Password Standard

I. Purpose

Poor password construction or management imposes risks to information resource systems of the Texas Veterans Commission (TVC). Standards for construction and management of passwords greatly reduce these risks. This document describes the acceptable standards for password construction and management.

II. Scope

The requirements in this standard apply to passwords for any information resource account of the TVC, to the users of any such accounts, and to system administrators and developers who manage or design systems that require passwords for authentication. The Information Security Officer (ISO) is responsible for enforcing this standard.

III. Standard

A. Password Construction

- **a.** Passwords must be a minimum of eight randomly selected characters.
- **b.** Words and phrases may supplement the eight randomly selected characters.
- **c.** For help with generating random characters either:
  - **i.** Visit https://www.random.org/passwords/
    - **1.** Click the “Get Passwords” button.
    - **2.** Pick the password that appeal to you or click the “Again!” button.
    - **3.** Note: you may have to add certain characters to satisfy complexity requirements of some systems (e.g. ! # = @ | ? ~, etc.).
  - **ii.** Or, obtain a card of random character sequences from the ISO to form the basis for constructing a password.

B. Password Management

- **a. Storage**
  - **i.** Passwords are most secure when memorized. Please try to commit passwords to memory to achieve the highest security benefit. The card of random character sequences from the ISO maybe useful memory aid.
  - **ii.** Passwords may be written down on paper documents provided the following guidelines are strictly adhered:
    - **1.** Do not include the associated user name.
    - **2.** Do not include the associated site, application or system.
    - **3.** Keep the paper document with your personal valuables always, such your credit cards or cash, and nowhere else.
  - **iii.** Approved password managers may be used.
    - **1.** Contact the ISO for approval of your chosen password manager.
    - **2.** Use of dis-approved password managers must be discontinued immediately and all passwords it contained must be changed.

3. Do not use any other electronic means for storing passwords to include Excel, Word or text files.

iv. Never allow applications such as browsers running on non-TVC devices to remember TVC passwords.

b. **Password Aging**

i. Systems may not require arbitrary password changes (e.g. periodically).

ii. Users and System Administrator must change passwords when inappropriate disclosure is suspected or at the direction of the Information Security Officer.

c. **Password Reuse**

i. Passwords for TVC information resources may not be used on any other non-TVC devices, site, application or systems. For example, do not reuse TVC passwords in your social media accounts.

ii. Users must use a different account and password for roles with escalated system privileges.

d. **Password Sharing and Transfer**

i. Passwords shall not be transferred or shared with others unless the account user obtains appropriate authorization to do so from the ISO.

ii. Passwords shall not be transferred electronically over public networks using insecure methods. Security protocols including IMAPS, FTPS, HTTPS, etc. shall always be used.

iii. Temporary passwords must expire after twenty-four hours.

iv. When it is necessary to disseminate passwords in writing, reasonable measures shall be taken to protect the password from inappropriate disclosure.

v. When communicating a password to an authorized individual orally, measures to ensure that the password is not overheard by unauthorized individuals must be taken.

C. **Requirements for System Administrators**

a. Require Passwords for Login – TVC information resource systems shall be protected with password login. Exceptions shall be granted for common access devices (e.g. check out and conference laptops) when these devices are configured with public user accounts that have extremely restricted permissions (e.g. web only) that are separate from user or administrative accounts**.**

b. Protect Against Password Hacking - System administrators shall harden TVC information resource systems to deter password cracking by using reasonable methods to mitigate "brute force" password attacks. For example, enabling account lock out mechanism, or detect where the attack is coming from and block further attempts from that location.

c. Logging - Practicable measures shall be put in place to log successful and failed login attempts**.** Such logs must be reviewed weekly to detect misuse and abuse.

d. Changing Password after Compromise or Disclosure - System administrators shall, in a timely manner, reset passwords for user accounts or require users to reset their own passwords in situations where continued use of a password creates risk of unauthorized access to TVC information resources. Such changes must be logged.

- **e.** Default Passwords - System administrators shall not use default passwords for any account. Furthermore, system administrator accounts must be distinct from their individual accounts and with different passwords.

D. Requirements of Application Developers

- **a.** Require Secure Transmission - Application developers shall develop applications that require secure protocols for authentication approved by the Information Security Officer.
- **b.** Storing Passwords - Application developers shall not store passwords in applications or in associated files. If password storage cannot be avoided, the alternative solution must be approved by the Information Security Officer.
- **c.** Unique User Accounts and Passwords - Applications shall support unique user accounts and passwords distinct from individual user accounts are not required to share a password to use the application.
- **d.** Use Federated Identity Whenever Possible - Applications shall, whenever capable, use TVC's Azure Active Directory for authenticating TVC users instead of requiring another set of credentials. For external users, consider integrating with existing accounts, such as social media where appropriate.

IV. Compliance

Everyone is responsible for complying with the TVC Password Standard. Non-compliance will result in actions consistent with policies of the Information Security Program to include loss of access to agency information resources. Exceptions may be granted in cases where security risks are mitigated by alternative methods, or in cases where security risks are at a low, acceptable level and compliance with minimum security requirements would interfere with legitimate business needs. To request a security exception, contact the Information Security Officer.

V. Version History

1.0 March 1, 2018 – Adoption

VI. References

- NIST Special Publication 800-63B Digital Identity Guidelines
- NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations