Title: Password Management Policy Policy: 6315

Purpose

The purpose of the Password Management policy is to identify the steps required for password use to protect University information systems. Further, the policy exists to ensure that all information system users are aware of their responsibilities in effective password management in light of the Virginia Information Technology Agency ("VITA") standards.

Authority, Responsibility, and Duties

The IT Security Program roles and responsibilities are assigned to individuals, and may differ from the actual role title or working title of the individual's position. Individuals may be assigned multiple roles, as long as the multiple role assignments provide adequate separation of duties, provide adequate protection against the possibility of fraud, and do not lead to a conflict of interests. Refer to Information Security Policy 6110 for roles and responsibilities.

Definitions

The IT security definitions and terms can be found in the Commonwealth of Virginia (COV) Information Technology Resource Management (ITRM) Glossary. It is referenced on the ITRM Policies, Standards, and Guidelines web page on www.vita.virginia.gov/library.

Policy Statements

It is the policy of VSU that all information systems users and applications be configured and utilized in such ways to meet the following criteria:

1. Users of IT systems must maintain exclusive control and use of their passwords, and protect them from inadve11ent disclosure to others (In other words, no sharing of passwords or other authentication information or data). Posting, "writing down" or displaying of passwords is prohibited.
2. If passwords, tokens or other credentials are thought to be compromised, users must immediately change their passwords and associated credentials then notify the VSU Information Security Officer (ISO) as soon as practicable.
3. User's passwords must have no personal significance (e.g., names of spouses, friends, favorite sports, pets, hobbies, children, etc.) and must not be a single dictionary word. The passwords must not be easily guessable.
4. Minimum IT System Configuration and setting requirements for System Administrators performing password administration and management:
   a. Non-shared unique passwords are required on all accounts on systems, including local, remote access, temporary accounts and application accounts.

b. The initial password assigned to a new user must be unique to that user so that the same initial password is not used repeatedly for all new users assigned system access.

c. The initial/temporary password must be delivered to the IT system user in a secure and confidential manner, if the system is sensitive (e.g., in person, secure email, etc.).

d. Technical or procedural controls must be implemented to require that the IT system user change the initial/temporary password upon his/her first successful login.

e. Forgotten initial passwords must be replaced, not reissued. In other words, passwords may not be reused.

5. Password creation or selection must meet the following, except for Commonwealth owned mobile devices:

   a. The minimum length of a password must be 9 characters. For internet facing web applications, the minimum password length must be 9 characters.

   b. Password complexity checking must be enabled, enforcing the use of at least three of the following four character types:

      1. Special characters.
      2. Alphabetical characters.
      3. Numerical characters.
      4. Combination of upper case and lower case letters.

   c. Users are encouraged to use Pass Phrase to assist in meeting the character minimum.

   d. Passwords must not be stored in clear text or displayed on the screen when entered.

6. General password related control requirements:

   a. Passwords (other than initial, temporary password) must be chosen by users, not assigned by system administrators or help desk staff.

   b. Passwords must not be included in any type of batch login file, clear text file, script or procedure, unless provided for by exception. See Appendix A.

   c. The use of an "auto-login" feature to automatically log a PC onto the network is strictly prohibited, unless the IT system is functioning as a kiosk.

   d. Passwords must be suppressed or masked from being viewed on-screen when the user is entering the password (e.g. ********).

   e. The transmission of identification and authentication data is prohibited without the use of acceptable industry encryption standards.

   f. Hardware passwords must be documented and stored securely.

   g. Default passwords must be changed immediately after installation.

   h. Passwords must be set on device management user interfaces for all network connected devices.

1. Access to files containing passwords or password hashes must be limited to the IT system and its administrators.

j. Users who have logon hour restrictions must be forcibly logged off when their hour(s) expire.

k. Passwords are required on Commonwealth owned mobile devices (i.e., PDAs and smart phones). For mobile phones, use a pin with a minimum of 4 alphanumeric characters. The account lockout parameters must be applied as practical.

l. Password Age: The maximum password age must not exceed 90 days for all IT systems unless an exception has been filed under the 365 day exception with VITA. The granting of this exception is very limited in scope and narrowly applied by VITA. Appendix A attached hereto must be completed and submitted to the VSU ISO for further processing. True service accounts that have no interactive login ability do not have to have password expirations. Passwords for sensitive systems shall only be changed once in a 24-hour period by the user. Further, passwords must meet the following expiration criteria based upon the classification of the user account:

   1. All Commonwealth of Virginia ("COV") asset domain account passwords must be changed every thirty (30) days.
   11. All regulatory accounts must have password expiration after forty-two days ("42").

m. Password History: For sensitive systems, a history of the last 24 passwords, at a minimum, must be retained by the IT system, which is to be configured to do so by the system administrator, and their reuse prevented.

n. Account Lockout Parameters: The following account parameters are:

   1. The account lockout is enabled, the threshold is 3 invalid attempts, and the duration is at least 30 minutes.
   2. Accounts that are unused for 90 consecutive days must be disabled.

o. P a s s w o r d protected screen saver lock periods must be implemented, documented and enforced after a period of no more than 30 minutes of inactivity.

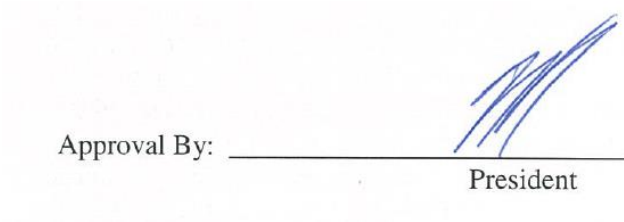
p. VSU devices with access to sensitive systems or those devices in less physically secure environments must have a lower time out interval documented and enforced.

References

Virginia Department of Human Resources Management:

Policy 1.60 Standards of Conduct (4116/08, 6/l/11)
Policy 1.75 Uses of Electronic Communication and Social Media (8/01101, 3117111)

Virginia Information Technology Agency (VITA): Information Security Standard (SEC 501-09.1, 12/8/2016)



Approval By: _____ Date: 06/20/2018

President