Password Management Policy

Vishwakarma University

Ver. No	Release Date	Owner	Approved By	Change details
1.0	19-07-2020	CISO	Vice Chancellor	Initial

Table of Contents

1. Purpose

The purpose of this policy is to establish a standard for implementation of strong passwords.

2. Scope

This policy applies to all system having access to the VU's network.

3. Objective

The objective of this policy is to protect and manage the passwords.

4. Policy

- All administrator-level passwords (e.g., root, application administration accounts, etc.) shall be changed quarterly.
- All End user-level passwords (e.g., email, web, desktop computer, etc.) shall be changed every 180 days.
- User who has administrator-level access must keep a different password for all the other accounts held by that user.
- All user-level and administrator-level passwords must conform to the guidelines described below.

5. Guidelines

A. General Password Construction Guidelines

All users at VU's should be aware of how to select strong passwords.

B. Strong Passwords Have the following Characteristics

- Contain at least three of the five following character classes:
- Lower-case characters
- Upper-case characters
- Numbers
- Punctuation
- “Special” characters (e.g. @#$ %^&*()_+|~-=\`{}[]:";'<> / etc.)
- The Administrator-level password shall have ten alphanumeric characters, and a user-level password shall have at least eight alphanumeric characters.

C. Weak Passwords have the following Characteristics

- The password contains less characters than above mentioned guidelines
  - The password is a word found in a dictionary (English or foreign)
  - The password is a common usage word such as: Names of family, pets, friends, co-workers, fantasy characters, etc.
  - Computer terms and names, commands, sites, companies, hardware, software.
  - The words "Vishwakarma University’s", "vupune", "vishwakarma" or any derivation.
  - Birthdays and other personal information such as addresses and phone numbers.
  - Word or number patterns like aaabbb, QWERTY, zyxwvuts, 123321, etc.
  - Any of the above spelled backwards.

- Any of the above preceded or followed by a digit (e.g., secret1, 1secret)
- Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way to Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

D. Password Protection Standards

- Always use different passwords for VU’s accounts from other accounts access (e.g., personal ISP account, option trading, benefits, etc.).
- Always use different passwords for various access needs whenever possible. For example, select one password for systems that use directory services (i.e. LDAP, Active Directory, etc.) For authentication and another for locally authenticated access.
- VU’s passwords should strictly be not shared with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential VU’s information.
- Passwords should never be written down or stored on-line without encryption.
- Do not reveal a password in email, chat, or other electronic communication.
- Do not speak about a password in front of strangers.
- Do not give hints at the format of a password (e.g., "my family name")
- Do not reveal a password on questionnaires or security forms.

- If someone demands a password, refer them to this document and direct them to the Information Security Department.
- Always decline the use of the "Remember Password" feature of applications (e.g., Eudora, Outlook, and Netscape Messenger).
- If an account or password compromise is suspected, report the incident to the Information Security Department.
- Password files shall be stored separately from application data files.

6. Enforcement

Any staff found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Password cracking or guessing may be performed on a periodic or random basis by the Information Security Department or its delegates. If a password is guessed or cracked during these exercises, the user/owner will be required to change it.

7. Reference Documents

- Acceptable use of information assets policy
- Incident management policy
- HR IT policy
- Non-Disclosure Agreement
- Change Management policy

8. Distribution List

The following users have access to this policy:

- All staff of Vishwakarma University

9. Acronyms and Definitions

- VU: Here it refers to Vishwakarma University
- Staff: Here it refers to Teaching Staff/ Non-Teaching Staff/ Office Staff/ Peons
- Password: A password is a word or string of characters used for user authentication to prove identity or access approval to gain access to a resource, which should be kept secret from those not allowed access.
- User-level: here it refers to the normal users.
- System-level: it means System administrator, System head, CISO.
- Application Administration Account: Any account that is for the administration of an application.