VIRGINIA UNIVERSITY OF LYNCHBURG PASSWORD POLICY

Password Security

Password Security is an integral aspect of information security. As passwords are the first layer of protection for user accounts, a poorly chosen (weak) password may result in compromise of personal user information and possibly confidential Virginia University of Lynchburg information. As such, all Virginia University of Lynchburg faculty, staff, and students (including visitors, contractors, and vendors with access to Virginia University of Lynchburg systems) are responsible for taking appropriate measures, as outlined below, to select and secure passwords.

Application

The purpose of this policy is to establish a standard for creation of strong passwords and protection of those passwords. This policy applies to all persons who have or are responsible for an account (or any form of access that supports or requires a password) on any system managed by Virginia University of Lynchburg, has access to the Virginia University of Lynchburg network, or stores any non-public Virginia University of Lynchburg information.

Password Privacy Statement

Notwithstanding utilization of a secret password, users of the University's computer system assets maintain no personal privacy rights with respect to content created, stored, received or sent from the University's information systems. In accordance with the Virginia University of Lynchburg Acceptable Use Policy, Virginia University of Lynchburg, or its delegates, reserves the right to intercept, monitor, or record all information stored on its information systems and inspect activity to diagnose problems or identify security threats and/or violations.

Password Selection Guidelines

Passwords are used for various purposes within Virginia University of Lynchburg. For this reason, all users of Virginia University of Lynchburg managed assets should understand how to select strong passwords.
A strong password has the following characteristics:

- Contains no less than eight characters
- Contains at least one upper case alpha character (A-Z)
- Contains at least one lower case alpha character (a-z)
- Contains at least one numeric character (0-9)
- Contains at least one non-alphanumeric character (!@#$%^&*()-_+=;:'"}{[]|\`~)
- Is not a word in any language, slang, dialect, jargon, etc.
- Is not based on personal information, names of family, etc.

A poor, weak password has the following characteristics:

- Contains less than eight characters
- Is a word found in a dictionary (English or foreign)
- 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 "VirginiaUniversityofLynchburg", "lynchburg", "vul" 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)

Password Secrecy Guidelines

The following suggestions provide a guideline for protecting password secrecy.

- Never share passwords with anyone, including instructors, assistants, technology service staff, or
- supervisors, either verbally, via email, fax, photocopy, or any other means of communication
- Do not use similar passwords utilized on external accounts (AOL, Yahoo, MSN, etc.)
- Do not write down passwords on paper and store them in insecure places
- Do not store passwords on electronic media (hard drives, Palm Pilots, etc.) without the use of
- strong encryption capability
- Change passwords immediately if compromise is suspected

Password Aging and Expiration

In accordance with this policy, all users must change any Virginia University of Lynchburg managed password in their control, at a minimum, every 180 days. Passwords exceeding this limitation are subject to enforcement as defined in the 'Password Policy Enforcement' paragraph of this policy.

Password Policy Enforcement

Virginia University of Lynchburg, or its representatives, reserves the right to utilize password auditing tools on any University managed asset. Users found to employ weak or aging passwords will be notified and required to change their password to one in compliance with this policy. Users may report any violation of this policy to the Virginia University of Lynchburg IT Help Desk at (434) 528-5276 or abuse@vul.edu Violating any portion of this policy may result in suspension of Virginia University of Lynchburg computer access or other action as directed by University policy or, where applicable, by law.