JMU COMPUTING STANDARDS
Password Management

Introduction

In keeping with University policy, Information Technology (IT) establishes password requirements for the multi-user systems it administers. IT also consults with system owners responsible for distributed systems to assure that the established minimum requirements are also enforced for these systems whenever possible. In general the requirements are consistent across systems, but due to specific technical requirements they may vary somewhat.

Responsibilities and General Requirements

Most of the responsibility for effective password management lies with those who use computer systems. Individuals using University computer systems shall assure effective password management and information security by being aware of and following the password management standards for each system (machine, service and/or software application) they access. Most notably, this means choosing strong passwords and safeguarding their integrity.

Computer passwords represent an individual's identity to the system and must <u>never</u> be disclosed to or used by others. Unauthorized use of an electronic ID is a violation of JMU policies [including, but not limited to, Information Security (JMU Policy 1204) and Appropriate Use of Computer Resources (JMU Policy 1207).] Violations of such policies are punishable under provisions of the Employee Standards of Conduct; faculty, employee and student handbooks, and the University honor and judicial systems. Violations of standards for password management and information security may result in sanctions including dismissal from the university and/or criminal/civil action.

Minimum Standards for Un-privileged Accounts

Un-privileged accounts are those created for a specific individual and purpose and that do not include the ability to create or modify additional accounts; modify system data or files or those belonging to other users; or perform application or database functions outside the control of the application system for which the account was issued.

Following are the **minimum** standards for passwords to un-privileged accounts on all multi-user systems. Multi-user systems are those where more than one user accesses/shares the resources. Examples include academic/general use systems (Canvas, etc.), the administrative systems (Student Administration, Finance, Human Resources, etc.) and shared fileservers (e.g. Microsoft fileservers, departmental/college servers) and in some cases individual workstations. These standards shall be used on all systems unless there is a technical reason why they cannot be used. In such cases, the reasons and impacts of deviating from the standard will be reviewed by IT before such a system is installed and/or connected to the campus network.

For unprivileged access to a system or application, the **minimum** password standards are:

- Minimum password length: 8 characters
- Specific Characteristics: must contain a combination of alpha (upper- and lowercase), numeric and punctuation characters (Note: some systems do not allow passwords that begin with a number or punctuation character, so this should be avoided)
- Cycle for password change: no more than 90 days
- History requirement: 13 previous retained for 1 year
- Maximum unsuccessful log-in attempts before lockout: 10 attempts
- Minimum lockout duration: 30 minutes

Minimum Standards for Privileged Accounts

Privileged accounts are those created with elevated capabilities and are generally used by system or application administrators. Privileged accounts may include the ability to create or modify additional accounts; modify system data or files or files belonging to other users; or perform application or database functions outside the control of the application system for which the account was issued. Because of the additional capabilities associated with privileged accounts, they carry additional responsibilities for their owners. Privileged accounts should be used only when their additional capabilities are truly necessary. Routine work should be done with unprivileged accounts whenever possible.

In light of the potential impact of a breach or misuse of a privileged account, the following, more rigorous, minimum requirements must be strictly observed:
- An approved request must be on file; elevated privileges must be appropriately documented, approved and acknowledged.
- An annual review of the status of privileged accounts must be performed to assure/validate that the additional privileges remain necessary and are being wisely used.
- Minimum password length: 14 characters
- Specific Characteristics: must contain a combination of alpha (upper- and lowercase), numeric and punctuation characters
- Cycle for password change: no more than 90 days (unless otherwise specified
- History requirement: 13 previous retained/checked
- Maximum unsuccessful log-in attempts: 10 attempts
- Minimum lockout duration: 60 minutes

Additional Requirements

As stated above, the minimum standards for password management apply on all multi-user machines owned by JMU or connected to the JMU network, whether administered by IT or by departments or individuals outside of IT.

Software application systems that require a login separate from the one used to access the machine must also meet the minimum password standards above. An application administrator must be assigned and password requirements must be met or otherwise justified.

Guidelines for Selecting Good Passwords

The responsibility for effective password management is shared by all users of the university's computing and communications resources and begins with selecting good passwords. To assist in this process, consider the following general guidelines:

- Good passwords are passwords that are difficult for either a human or a machine to guess. They have the following characteristics:
    - They are not a word found in any dictionary
    - They have no real world significance – i.e. pet names, license numbers, etc.
    - They contain both upper and lower case letters
    - They contain at least one numeral
    - They contain at least one punctuation mark

- They are of sufficient length (8 characters for unprivileged accounts/14 characters for privileged accounts).
  Use a phrase or sentence to assist you in remembering character strings. For example, add a number or symbol and "long strange trip it's been" can be Lst10iB as a password.

- **NEVER share your personal passwords!** Do not give out your passwords to IT or system personnel during help sessions. The password is your protection that only you have access to your data and to data owned by the university and used from your account.

- If you have several computer accounts, you may wish to have the same password on every machine and/or application. However, if you have the same password on many accounts and it is compromised, all of your accounts are compromised. Therefore, be sure to select passwords appropriately and **NEVER** use the same password for both privileged and non-privileged accounts.

- Notice prompts or system messages that report failed log-in attempts. If you are sure that you did not fail to input your password correctly or to become connected, report the situation to abuse@jmu.edu or to the appropriate system administrator. IT is always interested in investigating any and all password problems or security concerns**.**

Password Testing and Monitoring

Information Technology is responsible for monitoring the overall security of the university computing and communications environment. To discharge these duties, IT will perform on-going review and evaluation of system and network security. Activities may include conducting vulnerability scans, testing the strength of passwords or performing other activities aimed at evaluating overall risk. Individual system administrators and owners are expected to cooperate fully with such testing and monitoring activities.

Communication

Information Technology (IT) encourages individuals to understand the specific privileges and potential impacts associated with access to their account(s). In addition to basic security principles outlined in the RunSafe information, individuals should become aware of the data

stewardship responsibilities associated with their data/account access. IT has staff available to assist with specific questions or problems. General inquiries should be directed through the Help Desk by email or by calling 568-3555.

Password Problems

Computer users who are having difficulty logging-on due to invalid or expired passwords should contact the Help Desk at 568-3555 for help in correcting the problem. Be prepared to present positive proof of identification in order to have your account reset. Once the account is reset, a temporary password is used to log-on and the system will prompt for selection of a new password for continued use. Be sure to select a strong password in keeping with the minimum requirements and capabilities of the system.

Compromise of Passwords or Accounts

Computer users who suspect that their password or account has been compromised should immediately contact abuse@jmu.edu or call the appropriate system administrator. Individual system administrators are responsible for initiating response by reporting any potential security incidents immediately to the Information Security Officer (ISO@jmu.edu) and by taking steps to preserve evidence and prevent disclosure of the incident to those without the need to know until an organized response by IT can be mounted.

To help avoid such security incidents and assist forensic and recovery efforts should they occur, system administrators are responsible for maintaining an overall awareness of the operating posture of the machines and/or applications they administer, implementing regular updates, configuring the system(s) and implementing safeguards as appropriate for the resources being protected, enabling and monitoring auditing features, making the system, accounts, and data available to IT, and performing diagnostic or investigative work requested by IT in relation to security or misuse investigations. An incident response and reporting process will be established by the Information Security Officer and shall be followed in order to assure that all necessary information is collected and secured for use in possible follow-up.