Password Management Standard

August 2026

Purpose:

This standard establishes the minimum requirements for creating strong passwords and applies to all accounts used to access University Information Technology Resources.

Definitions:

Standard Account: A Standard Account provides routine system access for performing non-privileged tasks and functions. Standard Account access does not include the ability to create or modify other user accounts or make system-level changes.

Privileged Account: A Privileged Account provides elevated system access permissions and is typically used by system or application administrators. Privileged Accounts may include the ability to create or modify user permissions, system or data files, or files belonging to other users. Privileged accounts should be assigned to users only when the elevated permissions are required for a user's role. Routine work should be done using standard accounts whenever possible.

Service/Utility Account: Service/Utility accounts are non-human accounts used for executing specific system tasks or processes. MFA is not required for service/utility accounts.

University Information Technology Resources: These include, but are not limited to, equipment, software, systems, networks, data, and communication devices (stationary and mobile) owned, leased, or otherwise provided by James Madison University (JMU).

Standard:

1. Password Creation and Management

A good password is easy to remember, difficult for others to guess, and unique to the system. The longer the password, the stronger it is. IT recommends the use of passphrases to meet password length requirements. Passphrases are a series of random words put together or a unique sentence.

JMU password requirements are as follows:

<u>Standard Account:</u>

- Minimum of 16 characters
- Contain each of the following:
  - Uppercase Letter
  - Lowercase Letter
  - Number
  - Special Character
- Cannot contain username, first name, or last name
- Cannot be one of the last 24 passwords used

- Password change required annually
- Maximum number of unsuccessful log-in attempts before lockout: 10
- Minimum lockout duration: 30 minutes
- Minimum password age: 1 hour

*Care should be taken to protect applications administered with standard accounts (eID's) such as limiting access to appropriate IP ranges, using phish resistant MFA methods.

Privileged Accounts

- Minimum of 25 characters
- Contain each of the following:
    - Uppercase Letter
    - Lowercase Letter
    - Number
    - Special Character
- Cannot contain username, first name, or last name
- Cannot be one of the last 24 passwords used
- Password changes are required annually at a minimum
- Maximum number of unsuccessful log-in attempts before lockout: 10
- Minimum lockout duration: 60 minutes
- Minimum password age: 1 hour

*Domain accounts with workstation administration privileges have a 90-day password change interval.

Service/Utility Accounts

- Minimum of 25 characters
- Contain each of the following:
    - Uppercase Letter
    - Lowercase Letter
    - Number
    - Special Character
- Cannot contain username, first name, or last name
- Cannot be one of the last 24 passwords used
- No password change requirement
- Maximum number of unsuccessful log-in attempts before lockout: 10
- Minimum lockout duration: 60 minutes
- Minimum password age: 1 hour

2. Password Protection

The following best practices must be used for password protection on all accounts:

- Passwords must only be used by the authorized user and never shared with others.
- Keep passwords that have been written down in a safe location.
- Consider using a reputable password manager.
- Avoid reusing passwords. Unique passwords should be created for all accounts.
- Never enter your password on a computer, website, or wireless network you do not trust.
- Change default credentials before using systems or applications.