MISSOULA COUNTY
PASSWORD PROTOCOLS

Purpose

A password is the primary form of authentication used to permit access to the information systems at Missoula County (the County). To maximize the security potential of a password, it must be carefully created and used. Without strict guidelines for creating a password, it may be easy to decipher, permit illicit access to the County's information systems, and compromise the security of those systems.

Scope

This Password Policy applies to all information systems and information system components of Missoula County. Specifically, it includes:

- Servers and other devices that provide centralized computing capabilities;
- Storage area network (SAN), area network (AN), network attached storage (NAS), and other devices that provide centralized storage capabilities;
- Desktops, laptops, tablets, and other devices that provide distributed computing capabilities;
- Routers, switches, and other devices that provide network capabilities;
- Firewalls, identity provider (IDP) sensors, and other devices that provide dedicated security capabilities; and
- Cloud services, including but not limited to, infrastructure as a service, platform as a service, and/or software as a service.

Policy

1. A password must be constructed according to set length and complexity requirements and conform to these complexity requirements when created or changed. A password must:
    a. Not contain the user's account name or any part of the user's full name exceeding two consecutive characters;
    b. Be at least eight (8) characters in length, more is preferred.
    c. Contain characters from three of the following four categories:
        i. English uppercase characters (A through Z);
        ii. English lowercase characters (a through z);
        iii. Base 10 digits (0 through 9);
        iv. Non-alphabetic "special" characters (!, @, #, $, %, &).
    d. Passwords should not be reused across multiple systems.
    e. Easily guessable personal information should not be utilized in passwords; i.e. family names, pet names, birthdays, etc.
    f. Passphrases in the form of a sentence with punctuation are best.

2. A password will have a maximum lifespan of 90 days.

3. A password may not be reused more frequently than every 24 password refreshes. Reuse includes the use of the identical password or the use of the same root password with appended or pre-pended sequential characters.
4. A password must be used and stored securely. It must not be written down or stored electronically unless it is encrypted.
5. County log-in protocols must provide for obscured passwords and encrypted transmission.
6. A password belongs to the individual user and must be kept confidential. It may not be shared under any circumstances with coworkers, Technology staff, family members, or friends.