Password Policy

1.0 Overview
Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Oklahoma County Government's entire corporate network. As such, all Oklahoma County Government employees (including contractors and vendors with access to Oklahoma County Government systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.0 Purpose
The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

3.0 Scope
The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Oklahoma County Government facility, has access to the Oklahoma County Government network, or stores any non-public Oklahoma County Government information.

4.0 Policy
4.1 General

- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed whenever there is a change in system-level personnel.
- All production system-level passwords must be part of the MIS administered global password management database.
- All user-level passwords (e.g., email, web, desktop computer, etc.) will no longer be reset every 90 days. (Per the NIST guidelines)
- User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
- All user-level and system-level passwords must conform to the guidelines described below.
- Passwords stored in databases should go through salting and hashing to make sure they are harder to crack.
- All user-level passwords should be longer than twelve characters.
- All user-level passwords will have complexity enforced. (Upper characters and special characters)
- All system-level passwords should be at least sixteen characters.
- All system-level passwords will have complexity enforced. (Upper characters and special characters)

4.2 Guidelines
A. General Password Construction Guidelines
Passwords are used for various purposes at Oklahoma County Government. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than twelve characters
- 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 "Oklahoma County Government", "sanjose", "sanfran" 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)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least twelve alphanumeric characters long.
- Passwords for system level accounts should be at least sixteen characters long.
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. 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.

NOTE: Do not use either of these examples as passwords!

B. Password Protection Standards
Do not use the same password for Oklahoma County Government accounts as for other non-Oklahoma County Government access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various Oklahoma County Government access needs.

Do not share Oklahoma County Government passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential Oklahoma County Government information.

Here is a list of "dont's":

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't reveal a password to the boss
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation

If someone demands a password, refer them to this document or have them call someone in the MIS department.

Do not use the "Remember Password" feature of applications (e.g., Firefox, Chrome, and Internet Explorer).

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including mobile devices) without encryption.

Passwords won't be changed unless suspected of compromise. (except system-level passwords which must be changed when system-level personnel change).

If an account or password is suspected to have been compromised, report the incident to MIS and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by MIS or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

C. Application Development Standards
Application developers must ensure their programs contain the following security precautions. Applications:

- should support authentication of individual users, not groups.
- should not store passwords in clear text or in any easily reversible form.
- should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
- should support TACACS+ , RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

D. Use of Passwords and Passphrases for Remote Access Users
Access to the Oklahoma County Government Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

E. Passphrases
Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

All of the rules above that apply to passwords apply to passphrases.

F. Passwordless
The purpose of passwordless authentication is to provide a more secure and user-friendly alternative to traditional password-based authentication methods. By eliminating the need for users to create and remember passwords, passwordless authentication reduces the risk of password-related security breaches such as phishing, brute force attacks, and password reuse.

The standard for passwordless should be Fidokey2 for the authentication method.

5.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Definitions

Terms	Definitions
Application Administration Account	Any account that is for the administration of an application (e.g., Oracle database administrator, ISSU administrator).

7.0 Revision History

Jerad Dodson	9/12/18	Reviewed

Jerad Dodson	3/14/24	Added Passwordless section, revised password expiration, and revised password length requirement

County Request No. 263

REQUEST FOR LEGAL SERVICES

This form is used to provide legal opinions and contract approval by the District Attorney's Office. Only that advice that is related to a pending or potential claim against the County or its officers and employees is protected by the attorney-client priviledge. Opinions that are privileged should not be disclosed to anyone or the priviledge may be waived.

All legal opinions and approvals rendered are based only on the documentation and information stated below or attached to this form and, thus, it is important that all relevant facts and information be provided at the time of review. Please advise the District Attorney's Office of new or additional information, as it may cause the opinion to change. In all cases, the opinions of the District Attorney's Office are not binding on the County, its officers or employees and may be followed or disregarded in the discretion of the elected official.

Date of Request: 05/08/2024 Department: D3

State the nature of the legal request:

Does the Oklahoma County Password violate any federal or state laws?

RECEIVED
MAY 08 2024
CIVIL DIVISION
DISTRICT ATTORNEY

Colton Murphy
County Officer or Department Director

Reply of District Attorney's Office:

Reviewed - OC

Date of Reply: 5/8/24

Assistant District Attorney