OKLAHOMA
Office of Management
& Enterprise Services

Password Requirements Standard

Introduction

Passwords are an important part of computer security at the State of Oklahoma. They often serve as the first line of defense in preventing unauthorized access to state computers and data. Poor password complexity, including insufficient length or the inclusion of commonly used words, may allow an attacker to guess the password and gain unauthorized access to the state infrastructure. Generally, the more complex and cryptic the password, the more difficult it is for an attacker to guess. As such, the state requires account passwords to comply with state standards to help protect the integrity of state resources and data.

Purpose

This document outlines the complexity requirements and proper management practices of passwords for all computer systems and mobile devices at the State of Oklahoma.

Standard

The State of Oklahoma requires account passwords to comply with state standards to help protect the integrity of state resources and data. All current and new accounts are subject to the following password requirements.

- Passwords must be a minimum length of 8 characters.
- Passwords for elevated privileges to include access to highly regulated data sets (e.g., Federal tax information, criminal justice systems data, etc.) must be a minimum of 15 characters.
- Must contain at least one lower case letter, uppercase letter, numeral and special character.
- Passwords expire in a maximum of 90 days.
- Passwords for elevated privileges are required to change passwords at least every 60 days.
- Passwords are deactivated if not used for a period of 60 days.
- Password reuse is prohibited for 24 generations.

All passwords are treated as sensitive, confidential state information and therefore must be protected as such. Employees and contractors are responsible for keeping passwords secure and confidential. The following principles must be adhered to for creating and safeguarding passwords.

- Passwords cannot be stored or shared in plain text.
- Keep passwords confidential.
- Avoid keeping a paper record of passwords.
- Change passwords whenever there is any indication of possible system or password compromise.
- Select quality passwords with a minimum length of eight characters which are:
    - Easy to remember.
    - Not based on anything somebody else could easily guess or obtain using person related information (e.g., names, telephone numbers and dates of birth).
    - Free of consecutive identical characters or all-numeric or all-alphabetical groups.
- Change passwords at regular intervals.
- Avoid reusing old passwords.
- Change temporary passwords at the first log-on.

- Do not include passwords in any automated log-on process (e.g., stored in a macro or function key).
- Do not share individual user passwords.

Compliance

This standard shall take effect upon publication and is made pursuant to Title 62 O.S. §§ 34.11.1 and 34.12 and Title 62 O.S. § 35.8. OMES IS may amend and publish the amended standards policies and standards at any time. Compliance is expected with all published policies and standards, and any published amendments thereof. Employees found in violation of this standard may be subject to disciplinary action, up to and including termination.

Rationale

To coordinate and require central approval of state agency information technology purchases and projects to enable the chief information officer to assess the needs and capabilities of state agencies as well as streamline and consolidate systems to ensure that the state delivers essential public services to its citizens in the most efficient manner at the lowest possible cost to taxpayers.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 04/26/2022	**Review cycle:** Annual
Last revised: 10/18/2022	**Last reviewed:** 08/30/2023
Approved by: Joe McIntosh, Chief Information Officer	