University of Oklahoma
Information Technology Policies
Subject: Passwords

I. Purpose
The purpose of this policy is to establish a standard for password creation and protection at the University of Oklahoma.

II. Scope
This policy applies to the password of any individual who connects to the University of Oklahoma's network and systems.

III. Policy
Users are responsible for assisting in the protection of the systems they use. The integrity and secrecy of an individual's password is a key element of that responsibility. Each individual has the responsibility for creating and securing an acceptable password.

Length
Passwords must have a minimum of twelve (12) and a maximum of thirty-two (32) characters.

Complexity
Passwords must contain 3 of the 4 following character elements:
- 1) At least one upper case letter (A-Z)
- 2) At least one lower case letter (a-z)
- 3) At least one digit (0-9) that is not the initial or final character
- 4) At least one special character that is not the initial or final character. The following special characters are not allowed: Spaces @ ' ? + :

Secrecy
The confidentiality of passwords must be protected.
- Passwords must not be shared with anyone.
- If a password is written down, it must be stored in a secure location.
- If you have either evidence or suspicion that your password has been appropriated by another person and/or your account accessed, the password should be changed immediately and the suspected violation reported.

Password Change Frequency
Passwords must be changed to a new password within a maximum password age appropriate for the account. For Standard Privileged accounts, passwords should be changed at least once every 180 days. Passwords can be changed by visiting https://password.ou.edu.

Password Reuse/History
- Previous passwords must not be reused and simplistic variations thereof must not be used.
- Temporary passwords must be changed at first log-on.

Credential Transmission
Passwords must never be transmitted by e-mail or other insecure method unprotected (i.e., unencrypted)

Automated Password Processes
Passwords must never be included in any automated log-on process, such as in a script, macro, or stored in a function key.
**Duplication**
The same or similar passwords must not be used for university and non-university systems and accounts.

**Originality**
System default passwords must not be used.