



NO. 9001 PASSWORD GUIDELINES

- 1.0 POLICY STATEMENT. Passwords are an important aspect of Information Technology security at Oklahoma City Community College (OCCC). They are the front line of protection for user accounts.
- 2.0 SCOPE. The Scope of this policy includes all employees, students, and all others who have or are responsible for an account or access to an OCCC network or system.
- 3.0 PASSWORD REQUIREMENTS. ITS shall manage password guidelines, including the following requirements:
- 3.1. All user-level and system-level passwords must conform to these Guidelines.
 - 3.2. Users must use a separate, unique passphrase for each of their work-related accounts. Users may not use any work-related passwords or passphrases for their own, personal accounts. Users may not use any work-related passwords or passphrases for any other purpose or for access to any other accounts.
 - 3.3. User accounts that have administrator or system-level privileges must have a unique password from all other accounts held by that user to access system-level privileges.
 - 3.4. Strong passwords are long, and the more characters, the stronger the password.
 - 3.5. OCCC recommends the use of passphrases, passwords made up of multiple words and includes numbers or symbols.
 - 3.6. Passwords must not be shared with anyone, including supervisors, coworkers or family. All passwords are to be treated as sensitive, confidential OCCC information.
 - 3.7. Passwords must not be inserted into email messages.
 - 3.8. Members of the OCCC should not use the "Remember Password" feature of applications for your OCCC password (for example, web browsers)
 - 3.9. Passwords should be changed when there is reason to believe a password has been compromised or when prompted to do so by OCCC.
 - 3.10. Any user suspecting that their password may have been compromised must report the incident to OCCC.
- 4.0 MULTIFACTOR AUTHENTICATION. Multi-factor authentication (MFA) is required and must be used whenever available.
- 5.0 COMPLIANCE. All OCCC users are required to comply with these Guidelines. OCCC reserves the right to deny, to limit, to restrict or extend access and/or privileges to OCCC accounts, networks and systems as a result of violations of these Guidelines.

Effective: August 5, 2002
Revised: December 20, 2004
Revised: May 17, 2010
Revised: October 26, 2021
Revised: May 10, 2023