OKLAHOMA CITY
COMMUNITY COLLEGE

NO. 9005 ACCOUNT MANAGEMENT AND CONTROL

1. POLICY STATEMENT. Access to Oklahoma City Community College (OCCC) information systems and data is controlled by the implementation of an appropriate access control policy to manage accounts and define the processes of authentication, authorization, administration, identification, and termination of access rights.

2. PURPOSE. The purpose of this policy is to establish a standard for the creation, administration, use and removal of accounts that facilitate access to information and technology resources at OCCC. An account, at minimum, consists of a user ID and a password and may include different levels of access to additional systems and databases based on job description and title upon prior written access authorization from the user’s Department Leader.

3. SCOPE. This policy is applicable to individuals that access information and technology resources at OCCC as well as those responsible for the management of accounts or access to shared information or network(s). This policy covers departmental accounts as well as those managed centrally.

4. PROCEDURES AND STANDARDS. Accounts that access electronic computing and information resources require prudent oversight. The following security standards are a part of OCCC's account management environment.

4.1. ACCOUNT ADMINISTRATION.

4.1.1. Issuing Accounts. Account setup and modification require the approval of the requestor's supervisor on access authorization forms.

4.1.2. Information Technology Systems (ITS) is responsible for the activation of accounts. Business owners assign "least required access" to perform their business function.

4.1.3. ITS is also responsible for the prompt deactivation of accounts when necessary. Accounts for terminated individuals shall be removed/disabled/revoked from any computing system at the end of the individual's employment or when continued access is no longer required. The accounts of transferred individuals may require removal/disabling to ensure changes in access privileges are appropriate to the change in job function or location.

4.1.4. The identity of users must be verified before providing them with account and password details.

4.1.5. Passwords for new accounts must be set to require a password change upon first logon.

4.1.6. All guest accounts (for those who are not official members of the OCCC community) with access to OCCC computing resources shall contain an expiration date of thirty days or the work completion date, whichever occurs first. All guest accounts must be sponsored by the appropriate authorized member of the administrative entity managing the resource.

4.1.7. Disabling/Revoking/Deleting Accounts. All accounts may be disabled, revoked, or deleted if account privileges are no longer commensurate with an individual's function at OCCC or their need-to-know due to changes in their status.

4.1.8. All accounts may be disabled, revoked, or deleted if it is determined the account has been compromised or misused.

4.1.9. Individual departments leaders are responsible to notify OCCC Human Resources (HR) of separated employees using the PAF process.

4.1.10. Colleague account access: Access is removed upon separation and account is locked.

4.1.11. Active Directory Accounts Faculty/Staff: All access and shared storage access is removed upon separation, and AD account is disabled.

4.1.12. AD Accounts Students: AD accounts (and email) will be deleted after 18 months of non-enrollment.

4.1.13. Email Accounts Faculty/Staff: Email account access is removed when PAF termination date is reached and PAF has been completed and applied. Any temporary extension of email access must be requested by the employee's department head and/or VP and approved by VP for ITS. In particular, cases, email accounts may need to remain in place for temporary use by the immediate supervisor or for legal or business continuity purposes.

4.1.14. AD/Email Retired Faculty/Staff: Retiree accounts (with the exception of emeritus email accounts) are treated the same as other Faculty/Staff removals.

4.1.15. Supervisors of full and part-time employees are required to provide sufficient and timely notice of account termination as follows:

4.1.15.1. Resignation/Retirement (Personnel Action Form provided with a minimum of two weeks before last day worked, unless such notice is not provided by the employee in which case the supervisor must start the PAF process on the day notice is received).

4.1.15.2. Immediate termination (as soon as practical by phone or email).

4.1.16. Supervisors of adjunct faculty must submit notice of account termination by the end of the first week of the term if the individual is not assigned a course a subsequent term.

4.1.17. ITS shall terminate access immediately or within 24 hours of the last day of work as specified by notification.

4.2. INDIVIDUAL ACCOUNT STANDARDS.

4.2.1. Account Lockout. Account lockouts for domain computers will be controlled by ITS. The following settings must be applied to any information device that is not directly managed by ITS.

4.2.1.1. Account lockout durations no less than 15 minutes.

4.2.1.2. Account lockout threshold no more than 10 invalid login attempts.

4.2.1.3. Reset account lockout counter after no less than 15 minutes.

For any devices that cannot meet these requirements an approved exception to policy will need to be created by the Office of the Vice President for Information Technology Services.

4.3. DEPARTMENTAL ACCOUNTS. For access to sensitive information managed by a department, account management should comply with the standards outlined above. In addition, naming conventions must not cause contention with centrally managed email addresses or usernames. Should the potential for contention arise, the applicable system(s) should not be connected to the campus network until a mutually satisfactory arrangement is reached.

4.4. SHARED ACCOUNTS. Use of shared accounts is not allowed.

4.5. ADMINISTRATION OF PASSWORD CHANGES

Procedures for password resets:

User identities must be authenticated before providing them with ID and password details. In addition, stricter levels of authentication (such as face-to-face) shall be used for any account with privileged access.

4.6. WIRELESS REGISTRATION For access to OCCC's wireless network each device must be registered. Under normal circumstances access and registration will persist under the following schedule:

4.6.1. Once registration is completed, all devices must re-register once every 365 days.

4.6.2. There is a default idle timeout of 21 days, and all devices that are not seen by the system in this time period will need to re-register once rejoining the wireless network.

4.6.3. OCCC owned wireless devices have an idle timeout of 365 days, and the registration must be completed every 999 days.

5. APPLICATION AND SYSTEMS. Applications developed at OCCC or purchased from a vendor should contain the following security precautions:

5.1. Where technically or administratively feasible, shared ID authentication may not be permitted.

5.2. Passwords must not be stored in clear text or in any easily reversible form.

5.3. Role-based access controls should be used whenever feasible, to support changes in staff or assigned duties.

5.4. Where technically or administratively feasible, systems should allow for lockouts after a set number of failed attempts.

6. ACCOUNT ACCESS REVIEW

6.1. All accounts for any system connected to the OCCC network shall be reviewed and documented at least annually to ensure that access and account privileges are commensurate with job function, need-to-know, and employment status Outside of the ongoing periodic review the following events will warrant additional account reviews:

6.1.1. Internal Department Position Change.

6.1.2. External Departmental Transfer.

6.1.3. Additional and or a change in elevated/privileged access requested.

6.1.4. Change in user employment/enrollment status.

6.2. Permitted Actions without Identification or Authentication. All OCCC owned systems and applications are required to request proper identification and authorization prior to allowing permitted actions. Any system that is identified with a business use case that does not follow this standard must have an approved Exception to Policy completed by the department/college with approval from Vice President for ITS.

7. COMPLIANCE. All users of OCCC Information Technology Accounts are required to comply with this policy. OCCC reserves the right to deny, to limit, to restrict or extend privileges and access.

8. VIOLATIONS. Violations of this policy will be addressed in accordance with relevant OCCC policies. The appropriate level of disciplinary action will be determined on an individual case basis by the appropriate executive or designee, with sanctions up to or including termination or expulsion depending upon the severity of the offense.

9. MISCELLANEOUS. OCCC, through an appropriate review and amendment, reserves the right to amend this policy at any time and without prior notice to provide better information and technology access to faculty, staff, students, contractors, or any other individual using these accounts at OCCC.

Effective: May 10, 2023