Operational Area:	Information and Technology
Responsible Executive:	Chief Information Officer
Responsible Office:	Information Technology Services
Effective:	April 1, 2022

User Account (NetID) Management

Information and Technology

Contents

I. Introduction

A. **Authority:** Colorado Revised Statutes (C.R.S.) § 23-54-102, *et seq.* (2022) authorizes the Trustees of Metropolitan State University of Denver ("MSU Denver" or "University") to establish rules and regulations to govern and to operate the University and its programs. The MSU Denver Trustees retain authority to approve, to administer, and to interpret policies pertaining to University governance. The MSU Denver Trustees authorize the MSU Denver President to approve, to administer, and to interpret policies pertaining to University operations.

B. **Purpose:** The purpose of this policy is to document acceptable use of user accounts and identities within University computer systems and software and to establish rights and responsibilities of account holders.

Operational Area:	Information and Technology
Responsible Executive:	Chief Information Officer
Responsible Office:	Information Technology Services
Effective:	April 1, 2022

User Account (NetID) Management

Information and Technology

C. **Scope:** This policy applies to all users of MSU Denver computer systems, including students, faculty, staff, contractors, consultants, and others granted access to University systems. Accounts covered through this policy include the MSU Denver NetID, as well as other accounts for systems purchased or maintained by and on behalf of the University.

II. Roles and Responsibilities

A. **Responsible Executive:** Chief Information Officer

B. **Responsible Administrator:** Chief Information Security Officer

C. **Responsible Office:** Information Technology Services Office

D. **Policy Contact:** Chief Information Security Officer

E. **Additional Roles and Responsibilities:** IT Services, www.msudenver.edu/technology, 303-352-7548

III. Policy Statement

A. **All Account Creation**

MSU Denver NetIDs and other user accounts are to be created and managed via Information Technology Services systems, following established systems processes. All manual user account creation or modification requests must be submitted through ITS Helpdesk tickets.

B. **Account Management**

Changes to MSU Denver NetIDs will be documented with Service Desk Requests to ensure that all changes are documented. These changes can include but are not limited to:

1. Adding or removing VPN access
2. Adding elevated administrative permissions
3. Modifying access to network file shares
4. Modifying user account privileges
5. Modification of NetID for name changes

C. **Modifications to User Roles**

It is the responsibility of supervisors to notify IT Services when a staff, student employee, or faculty member will be changing roles in relation to access to systems or data. This notification must be made through a Service Desk request and must outline what access will be added, removed, or modified. Examples could include a student employee who leaves a department. While the student employee's NetID may remain active, access to a departmental folder or specialized application may need to be revoked. If a fulltime employee ends their employment but retains a student role, a new NetID will be created and their former NetID will be deactivated.

D. **Vendor and Contractor User Accounts**

User accounts for vendors or contractors will be created upon request via Service Desk Requests. These accounts must be provisioned with access limited to the minimum amount of systems permissions required. Vendor and contractor user accounts must be provisioned with end-dates aligning with the duration of their assignment. Vendor, contractor, and other non-fulltime or temporary accounts must be reviewed at least each semester to ensure that account access is managed in a timely manner.

E. **Account Timeout and Locking Sessions**

Accounts within the MSU Denver Active Directory domain (WinAD) environment will be created with pre-defined inactivity timeouts. If an account session remains idle for longer than the pre-defined limit, the system will activate a screensaver, and the user will be required to re- enter their network credentials to return to their session. Depending on job duties and departmental policy, users may have the ability to extend or shorten the timeout for each workstation they use. If a user steps away from their workstation, they must lock the workstation to prevent access to their session(s) by another person.

F. **Privileged User Accounts.** User accounts with elevated administrative privileges will be granted when required for performance of assigned job duties. Completion of basic security awareness training and submission of a request

will be required before providing administrative privileges. Elevated administrative privileges must be revoked when no longer needed for performance of assigned duties. These privileges may be temporarily or permanently revoked if they are used in violation of University policy.

G. **Account Deactivation**

User accounts will be deactivated when access to systems is no longer authorized or required. It is the responsibility of supervisors to notify Human Resources and Information Technology Services when an employee or contractor will be separating from University employment or contract. Such notifications should be immediate, but no longer than two business days of employment separation. If notification is given prior to employee separation, Information Technology Services will deprovision the user account on the planned separation date. If notification is given after separation, Information Technology Services will deprovision the user account within three business days. Student accounts will be active while the student is actively enrolled and will remain active until the student has not completed a course for three consecutive semesters.

H. **Sanctions**

Adherence to MSU Denver information-security policies is mandatory and may be based on state or federal statute, contract language, or information-security standards. These policies are not intended to unreasonably interfere with system utilization. Individuals should contact the IT Service Desk to report security risks, violations of policy, or to make requests for exceptions or

amendments to the policies. The Chief Information Security Officer (CISO) and other IT Services staff will respond to all reported security issues and will work with the policy subcommittee to allow for development of appropriate updates to policies. Violations of these policies may result in fitting administrative action up to and including revocation of system privileges, employee termination, or student expulsion.

IV. Related Information

A. MSU Denver Acceptable Use of Computing Systems Policy, https://www.msudenver.edu/policy/acceptable-use-computing-systems/

B. MSU Denver Information Security Awareness Training Policy, https://www.msudenver.edu/policy/information-security-training/

C. MSU Denver Remote Access to Computing Systems Policy, https://www.msudenver.edu/policy/remote-access-to-computing-systems/

D. MSU Denver Office of IT Services webpage, https://www.msudenver.edu/technology/

V. Policy History

A. **Effective:** April 1, 2022

B. **Enacted:** July 1, 2017

C. **Revisions:** Clarifications on scope, account creation, deactivations, and related identity and account administration actions.

D. **Review:** This policy will be reviewed every three years or as deemed necessary by University leadership.

Operational Area:	Information and Technology
Responsible Executive:	Chief Information Officer
Responsible Office:	Information Technology Services
Effective:	April 1, 2022

User Account (NetID) Management

Information and Technology

VI. Policy Approval

Janine Davidson, Ph.D.
President, Metropolitan State University of Denver

N/A

Chair, Board of Trustees, Metropolitan State University of Denver