METROPOLITAN STATE UNIVERSITY™ OF DENVER

ADMINISTRATIVE POLICY STATEMENT

Functional Area:
Information & IT

Responsible Executive:
Chief Information Officer

Responsible Office:
Information Technology Services

Effective: July 1, 2017

Information Security Policies

CONTENTS

INTRODUCTION 2

ROLES AND RESPONSIBILITIES 2

ENFORCEMENT AND REPORTING 2

POLICY STATEMENTS 3
- Data Classification 3
- Information Security Awareness Training 6
- Acceptable Use 6
- Email and Electronic Communications Security 9
- User Account (NetID) Management 10
- Device Security 12
- Remote Access 12

RELATED INFORMATION 14

POLICY HISTORY 15

REVIEW 15

APPROVAL 15

INTRODUCTION

Background: These policies were created by the IT Strategic Oversight Committee (ITSOC) Information and Instructional Technology Policies Subcommittee and reviewed by the University's Policy Advisory Committee. Review of these policies will be made on an annual basis, with any changes or additions being submitted through the University's policy review and approval process.

Purpose: MSU Denver's Information Security Policies are focused on protecting critical data and information systems of Metropolitan State University of Denver from loss, damage or inappropriate modification or disclosure. The policies contained in this document are designed to ensure that the University adheres to security standards commensurate with the data and systems referenced, while maintaining appropriate functional access for students, faculty, and staff.

Scope: These policies apply to all individuals, including students, faculty and staff, provided access to university data and information technology systems. Contractors and otherwise affiliated individuals must agree to abide by the Information Security Policies before accessing university systems and data. Role-based policies and procedures that apply to specific groups of users will be provided where applicable, in accordance with functional requirements and data classification.

ROLES AND RESPONSIBILITIES

- **Responsible Executive:** Chief Information Officer
- **Responsible Administrator:** Chief Information Security Officer
- **Responsible Office:** Information Technology Services
- **Policy Contact:** IT Services, msudenver.edu/technology, 303-352-7548

ENFORCEMENT AND REPORTING

Adherence to 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 Services Help 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.

Information about the Information and Instructional Technology Policy subcommittee is located at: http://www.msudenver.edu/technology/itgovernance/technologypolicysubcommittee/.

POLICY STATEMENTS

Data Classification

The purpose of this policy is to educate the University community about the importance of protecting data generated, accessed, transmitted, received, and stored by the University, to identify procedures that should be in place to protect the confidentiality, integrity, and availability of University data, and to comply with local and federal regulations regarding privacy and confidentiality of information.

Responsibility for Data Management

Data is a critical asset of the University. All members of the University community have a responsibility to protect the confidentiality, integrity, and availability of data generated, accessed, modified, transmitted, received, stored, or used by the University, irrespective of the medium on which the data resides and regardless of format, such as in electronic, paper or other physical form.

Individual departments are responsible for following appropriate managerial, operational, physical, and technical controls for access to, use of, verbal or electronic transmission of, and disposal of University data in compliance with this policy. Data owned, used, created, or maintained by the University and University personnel is classified into the following three categories:

- Public
- Official Use Only
- Confidential

Departments and administrative branches should carefully evaluate the appropriate data classification category for information handling within their environment. When provided in this policy, examples are illustrative only, and serve as identification of implementation practices rather than specific requirements. Nothing in this policy is intended to identify a restriction on the right of departments or administrative branches to require policies and/or procedures in addition to the ones identified in this document.

Data Classification

Public Data

Public data is information that may or must be open to the general public. It is defined as information with no existing local, national, or international legal restrictions on access or usage. Public data, while subject to University disclosure rules, is available to all members of the University community and to all individuals and entities external to the University community. By way of illustration only, some examples include:

- Publicly posted press releases
- Publicly posted schedules of classes
- Publicly posted interactive University maps, newsletters, newspapers, and magazines

Official Use Only Data

Official Use Only Data is information that must be guarded due to proprietary, ethical, or privacy considerations, and must be protected from unauthorized access, modification, transmission, storage, or other use. This classification applies even though there may not be a civil statute requiring this protection. Official Use Only Data is information that is restricted to members of the University community who have a legitimate purpose for accessing such data.

By way of illustration only, some examples of Official Use Data include:

- Employment data
- University partner or sponsor information where no more restrictive confidentiality agreement exists
- Internal telephone books and directories

Official Use Only Data:

- Must be protected to prevent loss, theft, unauthorized access, and/or unauthorized disclosure.
- Physical copies must be stored in a closed container (i.e. file cabinet, closed office, or department where physical controls are in place to prevent disclosure) when not in use.
- Electronic files must not be stored in unsecure locations, on PCs or other hardware, nor posted on any publicly accessible website.
- Must be destroyed when no longer needed subject to University and/or departmental Records Retention Schedules. Destruction may be accomplished by:
    - "Hard Copy" materials must be destroyed by shredding or another process that destroys the data beyond either recognition or reconstruction. After destruction, materials may be disposed of with normal waste.
    - Electronic storage media shall be sanitized appropriately by overwriting or physical destruction prior to disposal. Disposal of electronic equipment must be performed in accordance with IT Service's surplus equipment process.

Confidential Data

Confidential Data is information protected by statutes, regulations, University policies, or contractual language. Managers may also designate data as confidential. Confidential Data may be disclosed to individuals on a need-to-know basis only. Disclosure to parties outside the University should be authorized by executive management. By way of illustration only, some examples of Confidential Data include:

- Medical records
- Student records and other non-public student data
- Social Security Numbers
- Personnel and/or payroll or records
- Bank account numbers and other personal financial information
- Any data identified by government regulation to be treated as confidential, or sealed by order of a court of competent jurisdiction

Confidential data:

- When stored in an electronic format, must be protected with strong passwords and stored on servers that have protection and encryption measures provided by MSU Denver IT Services in order to protect against loss, theft, unauthorized access, and unauthorized disclosure.
- Must not be disclosed to parties without explicit management authorization or appropriate contracts.
- Must be stored only in a locked drawer or room or an area where access is controlled by a guard, cipher lock, and/or card reader, or that otherwise has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without a need-to-know.
- When sent via fax must be sent only to a previously established and used address or one that has been verified as using a secured location.
- Must not be posted on any public website.
- Must be destroyed when no longer needed subject to the University Records Retention Schedule. Destruction may be accomplished by:
    - "Hard Copy" materials must be destroyed by shredding or another process that destroys the data beyond either recognition or reconstruction. After destruction, materials may be disposed of with normal waste.
    - Electronic storage media shall be sanitized appropriately by overwriting or physical destruction prior to disposal. Disposal of electronic equipment must be performed in accordance with IT Service's Surplus Equipment Process.
- References to intellectual property exclude faculty and do not preclude standing policies.

The Chief Information Security Officer must be notified in a timely manner if data classified as confidential is lost, disclosed to unauthorized parties, or is suspected of being lost or disclosed to unauthorized parties, or if any unauthorized use of the University's information systems has taken place or is suspected of taking place. The Chief Information Security Officer must notify the University President of said loss or disclosure, with notifications to other parties as required.

Data Classification Roles and Responsibilities

The IT Strategic Oversight Committee (ITSOC) Information and Instructional Technology Policies subcommittee is the primary entity charged with recommending and developing policy and procedures subordinate to and in support of this policy.

The Chief Information Security Officer is charged with the promotion of security awareness within the University community, as well as responsibility for the creation, maintenance, enforcement, and design of training on relevant security standards in support of this policy. The Chief Information Officer will receive and maintain reports of incidents, threats, and malfunctions that may have a security impact on the University's information systems, and will receive and maintain records of actions taken or policies and procedures developed in response to such reports. The Chief Information Officer will assist with internal audits, as appropriate, to determine compliance with this policy.

MSU Denver IT Services will facilitate distribution of this policy, will assist in the investigation of policy breaches, and will respond promptly to reports of suspected misconduct or violations of law or University policies.

The Office of General Counsel will review procedures issued under authority of this policy for compliance with applicable regulations. The Office of General Counsel will also respond to court-ordered releases of information.

Information Security Awareness Training

The purpose of this policy is to ensure that University faculty and staff are provided adequate and relevant information about information security risks and best practices associated with accessing and using University computing systems.

General Information Security Awareness Training

All users of University computing systems will be required to participate in information security awareness training on at least an annual basis. MSU Denver IT Services will ensure that this training is made available to all users, and will ensure that all users employed by the University are provided training materials and that all employees pass a basic test of information security awareness skills. MSU Denver IT Services is responsible for reviewing the content of this training on an annual basis, and for notifying users and their supervisors of minimum awareness training requirements.
Access to sensitive systems and permissions is dependent on completion of appropriate security awareness training. VPN access, ad-hoc access to Banner, and extended password aging require completion of the basic annual security awareness training.

Area-Specific Information Security Awareness Training

Users of sensitive systems, such as those containing confidential or regulated data, may require training specific to the system or the type of data that is contained in the system.

Acceptable Use

This policy is not designed to impose restrictions that prevent users from performing their duties. The purpose of this policy is to ensure that all users of MSU Denver computing systems utilize these resources in a manner that supports the mission of the University and in a manner that protects these resources and their associated data from inappropriate access, usage, or other harm. All faculty, staff, students, contractors, and other users of University owned and maintained computer equipment and network resources must follow acceptable use policies.

Acceptable Use Standards

Users of MSU Denver computing systems must apply standards of normal academic and professional ethics while utilizing computing systems resources. These standards are found in:

- Student Code of Conduct
- Faculty Handbook
- Staff Handbook

Identification and Authentication

Users of MSU Denver computing systems must utilize user IDs or other unique user identification when accessing computer and/or network resources. Individuals must not knowingly access systems using another person's account, and users must not share or allow others to use their accounts. Users should take reasonable precautions to protect their identity, passwords, and access to University computing systems.

Personal Use

MSU Denver computer systems may be accessed for incidental personal use, provided that such use does not result in noticeable impacts to system performance, incremental costs, or negatively impact performance of employee duties. Any personal use must not violate University policies, and must not violate applicable laws and regulations. Unauthorized use of University computing systems for personal profit is prohibited.

Intellectual Property and Copyright

Users of MSU Denver computing systems may only use legally licensed and obtained software in compliance with University policies and applicable copyright and intellectual property laws. MSU Denver is a member of EDUCAUSE, and users are expected to adhere to the Code of Software and Intellectual Rights which states:

> *Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to works of all authors and publishers in all media. It encompasses respect for the right to acknowledgement, right to privacy, and right to determine the form, manner, and terms of publication and distribution. Because electronic information is easily reproduced, respect for the work and personal expression of others is especially critical in computer environments. Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access, and trade secret and copyright violations, may be grounds for sanctions against members of the academic community.*
>
> *(See: "Using Software: A Guide to the Legal and Ethical Use of Software for Members of the Academic Community," Educom/ITAA)*

Privacy

Computer users must respect the privacy of others by refraining from inspecting, broadcasting, or modifying data without the consent of the individual or individuals involved, except as permitted as part of their employment, and then only to the extent necessary for employment. University employees and others may not seek out, examine, use, modify, or disclose, without authorization, personal or confidential information which they need not access as part of their job function.

Employees must take necessary precautions to protect the confidentiality of personal or confidential information encountered in the performance of their duties or otherwise.

False Identity

University users of e-mail or other electronic communications shall not employ a false identity, nor may e-mail be sent anonymously with the intent to deceive.

Interference

University computing services shall not be used for purposes that cause, or could reasonably be expected to cause, directly or indirectly, excessive strain on any computing facilities or unwarranted/unsolicited interference with others' use of Computing Systems and Services. This provision explicitly prohibits the posting of unsolicited electronic mail to lists of individuals, and the inclusion on electronic mail lists of individuals who have not requested membership on the lists.

Students may be required to accept membership in an electronic mailing list for a class in which they are registered or for the purpose of official communications between authorized University personnel and an identified group of students.

Faculty and staff may be required to accept membership in an electronic mailing list for the purpose of official University communications.

The University may take action to protect computer users from interference. Information Technology Services (ITS) or someone designated by the Chief Information Officer (CIO) or the Chief Information Security Officer (CISO) may authorize the termination of connections with internal or external systems or services whose users interfere with the operation of University computing facilities.

Obscenity and Harassment

University Computing Systems and Services may not be used in a manner that would violate University policies on sexual harassment and equal opportunity. Links to the Student Code of Conduct, Faculty Handbook, Handbook for Professional Personnel, and the Classified Employee Handbook are provided below.

Enforcement

Computer activity may be monitored by authorized individuals for purposes of maintaining system performance and security. In instances when individuals are suspected of abuse of computer usage, the contents of user files may also be inspected upon the approval of the Office of General Counsel, in addition to one or more of the following offices: Human Resources, Equal Opportunity, or the Dean of Students. Any such monitoring or inspection must be formally requested and approved through IT Services HelpDesk tickets to ensure that the request and any related activities are appropriately documented.

Violations of University policies governing the use of University computing services may result in restriction or termination of access to University information technology resources. In addition, disciplinary action may be applicable under other University policies, guidelines, procedures, or collective bargaining agreements, up to and including dismissal.

At the discretion of the manager of the computer system or service in question, or designee, in collaboration with the appropriate authority, computer use privileges may be temporarily or permanently revoked pending the outcome of an investigation of misuse, or finding of violation of this policy. When practical and appropriate, 24-hour notice will be given in advance of revocation.

All data, programs, and files placed on or contained in the university computer systems are subject to the University's copyright, patent, and privacy policies. Additional rules may be in effect at specific computer facilities at the discretion of the directors of those facilities.

Email and Electronic Communications Security

The purpose of this policy is to govern usage of MSU Denver's email and other electronic communications services. As email is the official means of communications at MSU Denver, it is critical that appropriate use of these services be defined and enforced.

Electronic Mail (email) Access

All users of University computing systems will be provided an email address and email functionality based on their role on campus. Official email communications should be addressed to the University-issued email address.

Users have the option of accessing their email accounts from University-issued devices using University-licensed software, but may opt to utilize personal devices and personally licensed software to access their mailbox. MSU Denver IT Services is responsible for maintaining University-issued devices and software and will exercise best efforts to support personal devices. Users may choose to forward their email from their University mailbox to an external personal mailbox, but MSU Denver IT Services is only responsible for guaranteeing delivery to MSU Denver mailboxes.

Systems maintained by MSU Denver IT Services which are used to generate email must abide by the Email and Electronic Communications Security Policy. These systems include but are not limited to:

- Lyris
- Blackboard Learn

Use of Email for Transmission of Confidential Data

Inappropriate Usage

Use of MSU Denver email services should follow standards of normal academic and professional ethics, and is governed by University policies and applicable law. Inappropriate

use may result in revocation of access to University computing systems, and could result in disciplinary action pursuant to the Student Handbook, Faculty Handbook, and Staff Handbook.

Inappropriate use examples include, but are not limited to:

- Unauthorized attempts to access or use another person's email account
- Sharing MSU Denver account NetID and password with other individuals
- Using email in a harassing, obscene, or violent manner
- Using email in a manner that is illegal, violates University policy, or which could adversely impact the University's computing systems resources

Incidental personal use is permitted as long as this use does not adversely affect the functionality of University computing systems, incur additional costs, interfere with the performance of job duties, or violate applicable laws or University policies.

Email Privacy

MSU Denver email services are subject to disclosure per the Colorado Open Records Act and other e-discovery requests. Computer activity may be monitored by authorized individuals for purposes of maintaining system performance and security. In instances when individuals are suspected of abuse of computer usage, the contents of user files may also be inspected upon the approval of the Office of General Counsel, in addition to one or more of the following offices: Human Resources, Equal Opportunity, or the Dean of Students. Any such monitoring or inspection must be formally requested and approved through IT Services HelpDesk tickets to ensure that the request and any related activities are appropriately documented.
Mass Communications Tools

Use of mass communications tools such as Listserves, global distribution lists, or mass marketing services are governed by the Global Email Policy found at: https://www.msudenver.edu/brandcentral/webemail/globalemailpolicy/.

User Account (NetID) Management

The purpose of this policy is to identify acceptable use of user accounts and identities within University computer systems and software, and to establish rights and responsibilities of account holders. 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.

Account Creation

MSU Denver NetIDs are to be managed within Banner, and must be created in accordance with IT Services account creation procedures. All NetID account creation requests must be submitted through ITS Helpdesk tickets.

Account Management

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

- Adding or removing VPN access
- Adding PC administrative permissions
- Modifying access to network file share
- Modifying user privileges
- Modification of NetID for name changes

Vendor and Contractor User Accounts

User accounts for vendors or contractors will be created upon request via help ticket. These user accounts must be provisioned with access limited to the minimum amount of systems permissions required. Vendor and contractor user account status must be reviewed each semester to ensure that accounts no longer in use are deactivated in a timely manner.

Account Timeout and Locking Sessions

MSU NetID accounts within the MSU Denver Active Directory domain (WinAD) will be created with pre-defined timeouts with screensavers. 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.

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.

Account Deactivation

User accounts will be deactivated when access to systems is no longer authorized. It is the responsibility of supervisors to notify Human Resources when a staff or faculty member will be separating from the University. Human Resources will then notify IT via help ticket to ensure that account deactivation occurs in a timely manner.

Student accounts will be active while the student is actively enrolled and will remain active until the student has not been enrolled for three consecutive semesters.

Modifications to User Roles

It is the responsibility of supervisors to notify IT Services when a staff or faculty member will be changing roles in relation to access to systems or data. This notification must be made through help ticket, and should outline what access will be added, removed, or modified. Examples could include a student employee who leaves a department. While their accounts will remain active, access to a departmental folder or specialized application may need to be revoked.

Device Security

The purpose of this policy is to ensure that all devices used to process, transmit, or store data associated with Metropolitan State University of Denver computing systems are appropriately secured.

Institutionally Issued Devices

Devices issued by MSU Denver will be configured with certain security configurations and security applications. These devices may include disk encryption, virus protection, built-in firewalls, and other features. These security applications and settings must not be altered by end users without authorization from IT Services.

Mobile Devices

Mobile devices, including but not limited to, smart phones, personal digital assistants, mobile readers, laptops, and portable storage devices may be used to connect to MSU Denver computing systems. These devices must be appropriately secured and must never be used to store confidential information such as Social Security Numbers (SSN) or credit card numbers.

Personally owned devices

Personally owned devices may be used to connect to MSU Denver computing systems. These devices must be appropriately secured and must never be used to store University confidential information, such as Social Security Numbers (SSN) or credit card numbers.

Network Devices

MSU Denver networking systems are to be installed and maintained by MSU Denver IT Services Networking administrators. Unauthorized installation or use of networking devices such as wireless access points, network switches or routers, or other devices can interfere with MSU Denver Networking systems, and is therefore prohibited. Unauthorized devices found to be connected to MSU Denver networks may be disabled, disconnected, and/or confiscated if they are found to be inappropriately installed.

Remote Access

The purpose of this policy is to ensure that remote connections to Metropolitan State University of Denver computing systems are appropriately secured.

VPN Access

Access to MSU Denver administrative computing Virtual Private Networking services may be requested for any faculty or staff member of the University. Vendors, contractors, students, and other non-staff users requiring VPN access must contact IT Services to establish justification and appropriate access controls.

Users must complete Security Awareness Training before being granted VPN access, and must complete refresher training on an annual basis. Sharing of VPN access credentials is strictly prohibited.

Devices

Regardless of the ownership of devices used for VPN access, these devices must be appropriately secured and must never be used to store, confidential information.

RELATED INFORMATION

Data Classification Roles and Responsibilities

- Family Educational Rights and Privacy Act of 1974 (FERPA)
  - http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html
- Health Insurance Information Portability and Accountability Act (HIPAA)
  - http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html
- PCI Security Standards
  - https://www.pcisecuritystandards.org/security_standards/index.php
  - https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf
- Website Privacy Policy Statement
  - http://www.msudenver.edu/privacy/

Information Security Awareness Training Policy

- CRS 24-37.5-404.5. Institutions of higher education - information security plans.
  - Information security awareness training for employees of the institution of higher education to inform the employees, administrators, and users at the institution of higher education about the information security risks and the responsibility of employees, administrators, and users to comply with the institution's information security program and the policies, standards and procedures designed to reduce the security risks;
  - Link to training: http://www.msudenver.edu/snap/securityservices-computing/sans/

Acceptable Use Policy

- Equal Opportunity Office: http://www.msudenver.edu/eoo/policiesandprocedures/
- Handbook for Professional Personnel: https://msudenver.edu/hr/policies/handbooksmanualsrules/
- Classified Employee Handbook https://www.colorado.gov/pacific/sites/default/files/State%20of%20Colorado%20EE%20Handbook_0.pdf
- See User Account Policy
- EDUCAUSE - Using Software: A Guide to the Legal and Ethical Use of Software for Members of the Academic Community," Educom/ITAA https://net.educause.edu/ir/library/html/code.html

Email and Electronic Communications Security Policy

- See Acceptable Use Policy

User Account Policy

- See Acceptable Use Policy

Device Security Policy

- Global Email Policy
  http://www.msudenver.edu/brandcentral/webemail/globalemailpolicy/
- See Acceptable Use Policy
- ACTC Wireless Network Standard
  https://www.msudenver.edu/actc/wirelessnetworkstandard/

Remote Access Policy

- See Information Security Policy
- See Acceptable Use Policy
- VPN Request Form
- See Intellectual Property Policy, MSU Denver Trustees Manual (2007), https://msudenver.edu/trustees/policies/.

POLICY HISTORY

Effective: July 1, 2017

REVIEW

Policy Advisory Committee Review Date: February 20, 2017

University Community Review Date: February 27 - March 24, 2017

President's Cabinet Review Date: June 12, 2017

APPROVAL

Acting

President, Metropolitan State University of Denver — Date: 7-12-17

N/A, *operational policy*

Chair, Board of Trustees, if applicable — Date