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

Acceptable Use of Computing Systems

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:** 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 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.

C. **Scope:** These policies apply to all individuals, including students, faculty, staff, and contractors 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 when applicable, in accordance with functional requirements and data classification.

II. Roles and Responsibilities

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

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

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

D. **Policy Contact:** IT Services, msudenver.edu/technology, 303-352-7548

III. Policy Statement

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.

A. **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 the Student Code of Conduct, Faculty Handbook, and Staff Handbook.

B. **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 credentials, and

users must not share or allow others to use their account credentials. Users should take reasonable precautions to protect their identity, passwords, and access to University computing systems.

C. **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.

D. **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)

E. **Privacy.** Computer users must respect the privacy of others by refraining from inspecting, disclosing, 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.

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

G. **Interference.**

1. 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.
2. 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.
3. 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.
4. Faculty and staff may be required to accept membership in an electronic mailing list for the purpose of official University communications.
5. 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.

H. **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, Staff Handbook, and the Classified Employee Handbook are provided below.

I. **Enforcement.** Computer and network activity are monitored by automated systems and by authorized individuals for purposes of maintaining system performance and security. Files, logs, and systems will be scanned in response to system security alerts for the purpose of identifying, evaluating and investigating risks from potential malware or compromise of systems and accounts. 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.

J. **Exceptions:** 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.

K. **Sanctions.**

1. Violation 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.

2. 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.
3. 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, notice will be given in advance of revocation.

IV. Enforcement and Reporting

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.

V. Related Information

A. Equal Opportunity Office Policies and Procedures
B. Faculty Handbook
C. Staff Handbook
D. Classified Employee Handbook https://dhr.colorado.gov/state-employees/employee-resources

E. See MSU Denver Email and Electronic Communications Policy, https://www.msudenver.edu/policy/email/

F. See MSU Denver User Account Policy, https://www.msudenver.edu/policy/user-accounts/

G. EDUCAUSE - Using Software: A Guide to the Legal and Ethical Use of Software for Members of the Academic Community," Educom/ITAA, https://www.educause.edu/ir/library/html/code.html

VI. History

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

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

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

VII. Approval

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

N/A

Chair, Board of Trustees, Metropolitan State University of Denver