President's
Policy Statement
University Policy Library

Operational Area	Information and Technology
Responsible Executive	Chief Information Security Officer
Responsible Office	Information Technology Services
Effective	February 1, 2025

Accessing Electronic Communications and Data of Others

Information and Technology

Contents:

I. INTRODUCTION

A. **Authority:** Colorado Revised Statutes (C.R.S.) § 23-54-102, *et seq.* (2021) 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 Board of Trustees retain authority to approve, to administer, and to interpret policies pertaining to university governance. The MSU Denver Board of 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 ensure that access to the electronic communications and data another individual has stored in their university accounts is provided in a manner consistent with university policy and relevant privacy standards. Common requests that would be guided by this policy include family members requesting access to a deceased individual's personal files and electronic communications stored in university accounts, or supervisors requesting access to a former employee's work files and electronic communications for the purpose of business continuity.

C. **Scope:** This policy applies to all individuals, including students, faculty, and staff, and contractors provided access to university data and information technology systems. These 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.

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:** Chief Information Security Officer

E. **Additional Roles and Responsibilities:** General Counsel, AVP of HR, Dean of Students, and Registrar

III. POLICY STATEMENT AND SANCTIONS

A. **Policy Statement:** When it is necessary to grant access to the electronic communication and data that a former university employee or student has stored in their university accounts, requests for that access under this policy must be submitted through an IT Services service request. IT Services will document the request, and the acquisition of the associated approvals as set forth in this policy, thereby indicating the proof of legal authorization or legitimate business need has been met.

Individuals not employed by the university requesting access must be a legally authorized individual, (e.g., executor, person with power of attorney) with documentation describing their authorization. These external requests must outline the specific data or documents which are needed and cannot include 'access to all email', 'access to the account holder's password', or other widespread requests, but can include all personal data. Access to former university employee electronic communications and data requires approval by both the General Counsel and the Vice President of Human Resources or their designees. Access to former student electronic communication and data requires approval by both the Dean of Students and the Registrar or their designees.

Individuals employed by the university requesting access to another employee's or a student's electronic communication and data must demonstrate a legitimate business need. Access to former university employee electronic communication and data requires approval of both the General Counsel and the Vice President of Human Resources or their designees. Access to former student electronic communication and data requires approval of both the Dean of Students and the Registrar or their designees.

Nothing contained herein shall be construed to limit the university's obligations under the Colorado Open Records Act.

B. **Sanctions:** 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.

IV. RELATED INFORMATION

A. MSU Denver Email Security Policy

B. MSU Denver Account Management Policy

C. Family Educational Rights and Privacy Act (FERPA)

D. Summary of the HIPAA Privacy Rule | HHS.gov

E. Health Information of Deceased Individuals | HHS.gov

F. MSU Denver Public Records Access (CORA) Policy

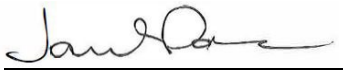
V. POLICY HISTORY

A. **Effective:** February 1, 2025

B. **Revised:** N/A

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

VI. POLICY APPROVAL



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

N/A
Chair, Board of Trustees, Metropolitan State University of Denver