



President's
Policy Statement
University Policy Library

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

Information Security Awareness Training

Information and Technology

Contents

- I. **Introduction**
- II. **Roles and Responsibilities**
- III. **Policy Statement**
- IV. **Related Information**
- V. **History**
- VI. **Approval**

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 ensure that users of MSU Denver technology resources are provided adequate and relevant information about information security risks and best practices associated with accessing and using University systems.



President's
Policy Statement
University Policy Library

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

Information Security Awareness Training

Information and Technology

- 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 Office
- D. **Policy Contact:** Chief Information Security Officer, msudenver.edu/technology

III. Policy Statement

All users of University computing systems will be required to participate in information security awareness training on at least an annual basis. All users employed by the University will be provided formal, security-awareness training, and all employees must pass an annual test of basic 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 privileged, user-account permissions is dependent on completion of relevant security awareness training. VPN access, *ad hoc* access to



President's
Policy Statement
University Policy Library

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

Information Security Awareness Training

Information and Technology

Banner, and administrative computing accounts require completion of the basic annual security awareness training.

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 Remote Access to Computing Systems Policy
<https://www.msudenver.edu/policy/remote-access-to-computing-systems/>
- B. MSU Denver User Account (NetID) Management Policy
<https://www.msudenver.edu/policy/user-accounts>
- C. Link to Banner mandatory training page https://admin.fifoundry.net/met-state-denver/sign_in#/
- D. 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



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

Information Security Awareness Training

Information and Technology

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.

v. Policy History

- A. **Effective:** April 1, 2022
- B. **Enacted:** July 1, 2017
- C. **Revisions:** Update to Scope and responsible parties. Added link to Remote Access policy.
- D. **Review:** 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